Indeed-Id
Enterprise Server

Руководство для администраторов предприятий

Установка и эксплуатация

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

Версия 6.3.0

Оглавление

Введение

Приветствуем вас и благодарим за приобретение программного комплекса Indeed Enterprise Authentication. Руководство поможет вам правильно подготовить и выполнить установку продукта Indeed-Id Enterprise Server и осуществить необходимые начальные настройки.

Условные обозначения

В Руководстве используются следующие условные обозначения:

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

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

О 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.

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 Indeed-Id Enterprise Server определяется в соответствии с индивидуальными требованиями к масштабируемости и отказоустойчивости.

Установка и настройка модуля Indeed-Id Enterprise Server

Количество устанавливаемых продуктов Indeed-Id Enterprise Server определяется в соответствии с индивидуальными требованиями к масштабируемости и отказоустойчивости. В качестве типового средства хранения данных и настроек решения используется Active Directory без расширения схемы.

Предварительные условия для установки Indeed-Id Enterprise Server

Аппаратные требования

- Не менее 4 ГБ оперативной памяти
- Не менее 50 ГБ свободного дискового пространства
- Аппаратные требования совпадают с требованиями, предъявляемыми к операционным системам, на которых функционирует ПО

Поддерживаемые операционные системы

- 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 установки и функционирования продукта Indeed-Id Enterprise Server необходимо следующее окружение:

- **Контроллер домена**:
    - Уровень функциональности леса и домена не ниже Windows Server 2003

Во избежание проблем при автоматическом запуске Indeed-Id Enterprise Server не рекомендуется выполнять установку модуля Indeed-Id Enterprise Server на Контроллере домена. Запуск Indeed-Id Enterprise Server выполняется успешно только при наличии доступной инфраструктуры Active Directory. В случае перезагрузки Контроллера Домена некоторые сетевые компоненты могут быть недоступны в момент запуска Сервера, что приведет к ошибке запуска сервера Indeed.

- Настроенная **служба Глобального каталога** на каждом Контроллере домена.
- **Настроенный DNS сервер** (необходимо добавление Reverse lookup zones). **Параметры DNS сервера** необходимо указать **в настройках сетевого подключения** на каждой рабочей станции.
- Для установки Indeed-Id Enterprise Server требуются права **Локального Администратора (Adminstrator)**. Для выполнения настройки Indeed-Id Enterprise Server необходимы права **Indeed-Id Server Admins**.

Настройки межсетевого экрана

Текущие параметры межсетевого экрана на Indeed-Id Enterprise Server и на рабочих станциях пользователей могут препятствовать нормальной работе модулей Indeed Enterprise Authentication. Проверьте и при необходимости измените следующие параметры:

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 Indeed-Id Enterprise Server.

3. Если при установке Indeed-Id Enterprise 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 Enterprise 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 Enterprise 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 Enterprise Server).

См. также: **Параметры совместимости с VIPnet Office Firewall v. 3.1**

Параметры совместимости с VIPnet Office Firewall v. 3.1

В случае, если модуль Indeed-Id Enterprise Server устанавливается в комбинации с модулями Indeed-Id Enterprise SSO и Indeed-IS ENTERPRISE SSO TMS Connector, необходимо обратить внимание на следующие параметры:

Режим VIPnet Office Firewall	Модуль	Результат
1 (Блокировать IP-пакеты всех соединений) – блокирует на сетевом интерфейсе все IP-пакеты.	Indeed-Id Enterprise Server	Блокируется
	TMS Server	Блокируется
	Консоль администратора Indeed Enterprise Management Console	Блокируется
	Агент Indeed-Id Enterprise SSO	Блокируется
2 (Блокировать все соединения кроме разрешенных) – действует только на локальный и широковещательный трафик, блокирует создание любых соединений, правила обработки которых, не заданы в локальных и широковещательных фильтрах.	Indeed-Id Enterprise Server	Блокируется
	TMS Server	Блокируется
	Консоль администратора Indeed Enterprise Management Console	Блокируется
	Агент Indeed-Id Enterprise SSO	Блокируется
3 (Пропускать все исходящие соединения кроме запрещенных) – действует только на локальный и широковещательный трафик, пропускает исходящие и блокирует входящие соединения.	Indeed-Id Enterprise Server	Блокируется
	TMS Server	Блокируется
	Консоль администратора Indeed Enterprise Management Console	Блокируется
	Агент Indeed-Id Enterprise SSO	Работает нормально

4 (Пропускать все соединения)* – является тестовым и разрешает создание любых локальных соединений.	Indeed-Id Enterprise Server	Работает нормально
	TMS Server	Работает нормально
	Консоль администратора Indeed Enterprise Management Console	Работает нормально
	Агент Indeed-Id Enterprise SSO	Работает нормально
5 (Пропускать IP-пакеты на всех интерфейсах без обработки)* – на всех интерфейсах прекращает обработку трафика модулем ViPNet.	Indeed-Id Enterprise Server	Работает нормально
	TMS Server	Работает нормально
	Консоль администратора Indeed Enterprise Management Console	Работает нормально
	Агент Indeed-Id Enterprise SSO	Работает нормально

Таким образом, для работы модулей без блокировки необходимо установить режим 3, 4, 5 для модуля Агент Indeed-Id Enterprise SSO и режим 4, 5 для остальных модулей.

Параметры приведены без учета дополнительных настроек VIPnet Office Firewall.
В режиме 4* компьютер открыт для несанкционированного доступа, поэтому данный режим может использоваться только для кратковременного включения.

В режиме 5* прекращаются любая фильтрация трафика, трансляция IP-адресов. В данном режиме информация в канале, компьютер и защищаемые сети открыты для несанкционированного доступа, поэтому режим 5 также может использоваться для кратковременного включения.

Включение Глобального каталога

Включение Глобального каталога необходимо для успешного поиска Indeed-Id Enterprise Server клиентом Indeed-Id (Indeed-Id Windows® Logon). Для включения Глобального каталога выполните следующие действия:

1. Откройте оснастку **Active Directory Сайты и Службы** (Active Directory Sites and Services) **Пуск > Панель управления > Администрирование > Active Directory - сайты и службы**.
2. В дереве консоли щелкните контроллер домена, в котором необходимо включить или отключить глобальный каталог (**Active Directory — сайты и службы > Сайты > *сайт, содержащий контроллер домена, который необходимо включить*** **> Серверы >Контроллер домена**).
3. На области сведений щелкните правой кнопкой мыши элемент **Параметры NTDS** (NTDS Settings) и выберите команду **Свойства** (Properties).
4. Установите флажок **Глобальный каталог** (Global Catalog), чтобы включить глобальный каталог.

Для выполнения этой процедуры необходимо быть членом группы "Администраторы домена" (Domain Admins) в домене выбранного контроллера домена или "Администраторы предприятия" (Enterprise Admins) в Active Directory, либо получить соответствующие полномочия путем делегирования.

Под встроенной учетной записью администратора можно входить в домен, даже когда глобальный каталог недоступен.

Включение Глобального каталога может вызвать дополнительный трафик репликации.

Контроллер домена, на котором включается Глобальный каталог, не объявляет о себе в службе DNS как о глобальном каталоге, пока не будут получены все отдельные разделы каталога домена.

Создание экземпляра системы Indeed-Id в Active Directory

В общем случае для создания экземпляра системы Indeed-Id в Active Directory в корне домена необходимы права Администратора домена (Domain Admins) – т.к. при создании экземпляра системы будут созданы новые объекты в Active Directory.

Возможно создание экземпляра системы от имени учетной записи с ограниченными правами (такая учетная запись, должна обладать правами Полный контроль (Full Control) в целевом подразделении.

Для выполнения действия от имени учетной записи с ограниченными правами требуются дополнительные настройки (см. **Установка от имени учетной записи с ограниченными правами**).

Создание экземпляра системы Indeed-Id с помощью утилиты IndeedID.instance.exe

Установка от имени привилегированной учетной записи

Для создания экземпляра системы Indeed-Id от имени привилегированной учетной записи в корне домена запустите утилиту IndeedID.instance.exe, находящуюся в каталоге \Misc дистрибутива Indeed-Id Enterprise Server, с параметром /i:<путь к экземпляру системы>, где <путь к экземпляру системы > - Distinguished Name (DN) для домена или подразделения домена, в котором необходимо создать экземпляр системы. Например, для домена demo.local уникальное имя (Distinguished Name) будет выглядеть следующим образом: "dc=demo,dc=local".

Пример:

После запуска команды **IndeedID.instance.exe /i:"dc=demo,dc=local"**[1] экземпляр системы Indeed-Id будет создан в корне домена demo.local.

В случае установки Indeed Enterprise Authentication относительно конкретного подразделения (Organizational Unit) домена в качестве параметра для утилиты IndeedID.instance.exe требуется указать полный путь к этому подразделению в виде Distinguished Name (DN).

Пример:

Команда **IndeedID.instance.exe /i:"ou=Indeed-MSK,dc=demo,dc=local"** создает экземпляр Indeed-Id в подразделении Indeed-MSK, которое в свою очередь расположено в корне домена demo.local:

[1] Здесь и далее в документе *demo.local* – пример имени домена. При копировании команд из данного документа необходимо указывать реальное имя домена. Путь также может быть задан в альтернативном формате: IndeedID.instance.exe /i:demo.local/.

После выполнения команды в указанном домене или подразделении создается контейнер системы со всеми необходимыми дочерними контейнерами и группами безопасности. Имена контейнера и подконтейнера по умолчанию соответствуют названию компании-разработчика и продукта.

В версии Indeed-Id Enterprise Server 5.0.0.0 и выше поддерживаются уникальные имена контейнера и подконтейнера (в том числе с использованием кириллических символов). Для создания экземпляра системы с уникальными именами запустите утилиту IndeedID.instance.exe с параметрами **/company** и **/product**:

Пример: **IndeedID.instance.exe /i:"dc=demo,dc=local" /company:"Access Control" /product:"Indeed Enterprise Authentication"**

По умолчанию при создании экземпляра системы Indeed-Id создаются группы безопасности с областью действия Domain Local (Локальная в домене). Если инфраструктура включает родительские и дочерние домены, при создании экземпляра системы в родительском домене рекомендуется использовать команду **/i: "<путь к экземпляру системы>" /gu**.

Пример: **IndeedID.instance.exe /i:"dc=demo,dc=local" /gu**

Использование этой команды позволяет создать группы безопасности с областью действия Universal (Универсальная) и избежать возможных проблем при последующей активации Indeed-Id Enterprise Server в дочернем домене.

Учетная запись пользователя, под которой выполняется создание экземпляра системы Indeed-Id, также включается в служебные группы (помимо Domain Admins). После создания экземпляра системы, при необходимости, следует настроить членство в группах безопасности Indeed-Id согласно действующим в компании политикам безопасности.

Установка от имени учетной записи с ограниченными правами

Для создания экземпляра системы Indeed-Id от имени учетной записи с ограниченными правами **перед запуском утилиты IndeedID.instance.exe** необходимо:

1. Вручную создать контейнер **Indeed-Id** в целевом домене/подразделении.
2. Для созданного контейнера **Indeed-Id** установить права **Full control** (**Полный контроль**) на учетную запись, от имени которой планируется запускать утилиту IndeedID.instance.exe.
3. В свойствах созданного контейнера **Indeed-Id** на вкладке **Security** (**Безопасность**) нажать **Advanced (Дополнительно)**, далее на вкладке **Permissions (Разрешения**) выбрать нужную учетную запись, нажать **Edit (Изменить)** и в выпадающем списке **Apply onto** (**Применяется к**) выбрать **This object and all child objects** (**Этот объект и все дочерние объекты**).
4. Выполнить выход из системы и повторный вход, чтобы внесенные в настройки прав изменения вступили в силу.
5. Запустить утилиту IndeedID.instance.exe с указанными выше параметрами.

После выполнения команды в созданном вручную контейнере **Indeed-Id** создаются необходимые подконтейнеры и группы.

Для пунктов 1, 2 и 3 необходима учетная запись с правами Администратора домена (Domain Admins)

После выполнения всех указанных действий список прав для созданного контейнера Indeed-Id (Access Control List) будет очищен, и как следствие права на создание/удаление экземпляра системы Indeed-Id у используемой учетной записи могут не сохраниться.

Создание экземпляра системы Indeed-Id вручную

Для создания экземпляра системы Indeed-Id вручную:

1. В консоли Active Directory Users and Computers создайте контейнер **Indeed-Id** и в нем – контейнер **SCPs**.
2. В контейнере **Indeed-Id** создайте локальные и универсальные группы безопасности (Domain Local/Universal Security Groups):
    - **Indeed-ID Server Admins**
    - **Indeed-ID User Admins**
    - **Indeed-ID Password Managers**
    - **Indeed-ID ESSO Admins**
    - **Indeed-ID Security Supervisors**
3. Включите в каждую из созданных групп безопасности группу **Domain Admins**.

Для созданных групп:

- Запрещается наследование списка избирательного управления доступом (DACL) от родительского элемента.
- В список контроля доступа (ACL) необходимо включить записи Everyone – Read, Group member – Full Control. Под Group member понимается действующий член данной группы (таким образом, права Full Control для группы Indeed-Id Server Admins будут даны уже действующим членам группы Indeed-Id Server Admins).

Для созданных контейнеров:

- Запрещается наследование списка избирательного управления доступом (DACL) от родительского элемента.
- В список контроля доступа (ACL) необходимо включить записи Everyone – Read, Indeed-Id Server Admins – Full Control.

Назначение прав

Назначение прав при создании контейнера Indeed-Id происходит следующим образом:

- **Indeed-Id**. Право на чтение объекта Indeed-Id является общим. Права на запись и изменение назначаются только членам группы Indeed-Id Server Admins после их активации.
- **Indeed-ID Server Admins, Indeed-ID User Admins, Indeed-ID Password Managers, Indeed-ID Security Supervisors**. Во все указанные группы включается группа Администраторы домена (Domain Admins). Право на чтение объекта является общим, права на запись и изменение назначаются только членам группы.
- **Objects**. Право на чтение объекта является общим. Полный набор прав назначается группам Администраторы домена (Domain Admins), Indeed-ID Server Admins и учетной записи SYSTEM.

Группы безопасности

Группы безопасности предназначены для распределения прав на управление системой Indeed-Id. Необходимые группы безопасности добавляются в контейнер Indeed-Id при создании экземпляра системы Indeed-Id:

- **Indeed-ID Server Admins**. Участники данной группы обладают правами на управление сервером Indeed-Id (активация сервера, запуск/остановка сервера, генерация и экспорт ключа шифрования).
- **Indeed-ID User Admins**. Участники данной группы обладают правами на управление свойствами пользователей Indeed-Id (разрешение/запрет на использование технологии аутентификации Indeed-Id, изменение настроек Indeed-Id).
- **Indeed-ID Password Managers**. Участники данной группы обладают правами на запуск Менеджера паролей - утилиты автоматической генерации паролей пользователей.
- **Indeed-ID ESSO Admins**. Участники данной группы обладают правами на управление SSO профилями пользователей.
- **Indeed-ID Security Supervisors.** Участники данной группы обладают правами просмотра (без права редактирования) следующих настроек системы: SSO профилей пользователей, ролей SSO, просмотра свойств пользователей, просмотра политики паролей.

Член каждой из встроенных групп безопасности Indeed-Id может проверить статус сервера Indeed-Id (команда IndeedID.srvcfg.exe /state).

Группа **Indeed-ID Security Supervisors** создается автоматически при создании инстанса версией утилиты IndeedID.Instance.exe выше 2.0.3.0. В случаях, когда инстанс был развернут версией утилиты ниже 2.0.3.0, группу можно создать, запустив утилиту IndeedID.instance.exe с ключом /up. Группа является опциональной, и обновленный сервер может стартовать без нее.

При создании экземпляра Indeed-Id командой утилиты IndeedID.instance.exe группы безопасности создаются автоматически.

Для настройки профилей пользователей SSO необходим установленный модуль **Indeed-Id Enterprise SSO**.

Права на управление параметрами системы Indeed-Id могут быть делегированы отдельному пользователю или группе пользователей в рамках домена.

Установка Indeed-Id Enterprise Server

Количество устанавливаемых продуктов Indeed-Id Enterprise Server определяется в соответствии с индивидуальными требованиями к масштабируемости и отказоустойчивости. В качестве типового средства хранения данных и настроек решения используется Active Directory (схема при этом не расширяется).

Оптимальным вариантом развертывания инфраструктуры Indeed-Id в плане обеспечения возможности входа в сеть/приложение является **централизованная установка**. Indeed-Id сервер и инфраструктура Indeed-Id разворачиваются в родительском домене.

Данное инфраструктурное решение оптимально и гарантированно работает (этот вариант уже используется у многих клиентов). На случай плохого канала связи имеются настройки кэширования данных пользователя. При этом при первом входе пользователя в сеть/приложение по аутентификатору при наличии связи с серверами Indeed аутентификационные данные будут кэшированы на локальной машине. В дальнейшем при отсутствии связи с серверами Indeed пользователи смогут входить в сеть/свои целевые приложения.

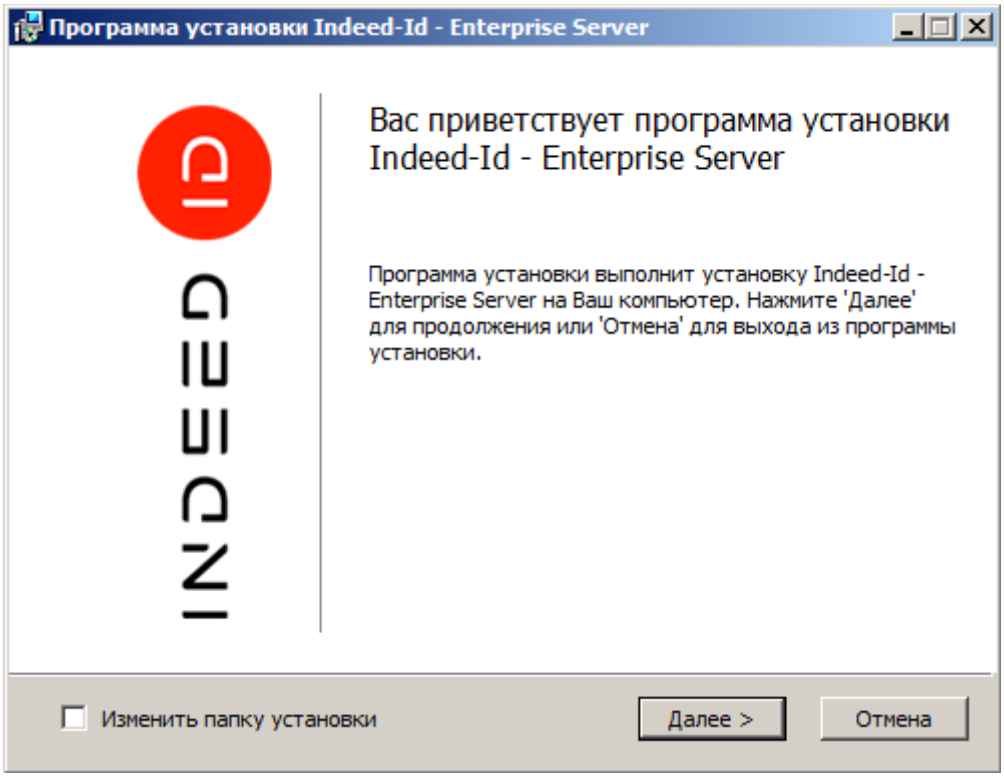
Вариант **децентрализованной установки** (развертывание инфраструктуры Indeed-Id отдельно в каждом районном центре) имеет значительное количество нюансов:

- Компетенция администраторов системы Indeed районных центров, как правило, существенно ниже;
- Необходимость выделения одного-двух серверов для системы в каждом районном центре;
- Необходимость распространения и обновления лицензий Indeed в районных центрах;
- Децентрализация настройки – необходимость настройки пользователей Indeed/ESSO-приложений и учётных записей ESSO в каждом районном центре отдельно;
- В случае отсутствия канала связи до областного центра, меньше возможности воспользоваться функцией кэширования (не будет возможности войти под пользователем родительского домена в дочернем и наоборот).

Установка первого экземпляра Indeed-Id Enterprise Server

Для установки Indeed-Id Enterprise Server выполните следующие действия:

1. Запустите программу установки IndeedID.Enterprise.Server.msi и дождитесь отображения Мастера установки. По умолчанию сервер будет установлен в C:\Program Files\Indeed-Id\Server[2]. Если необходимо изменить путь установки, установите соответствующую опцию и нажмите **Далее**.

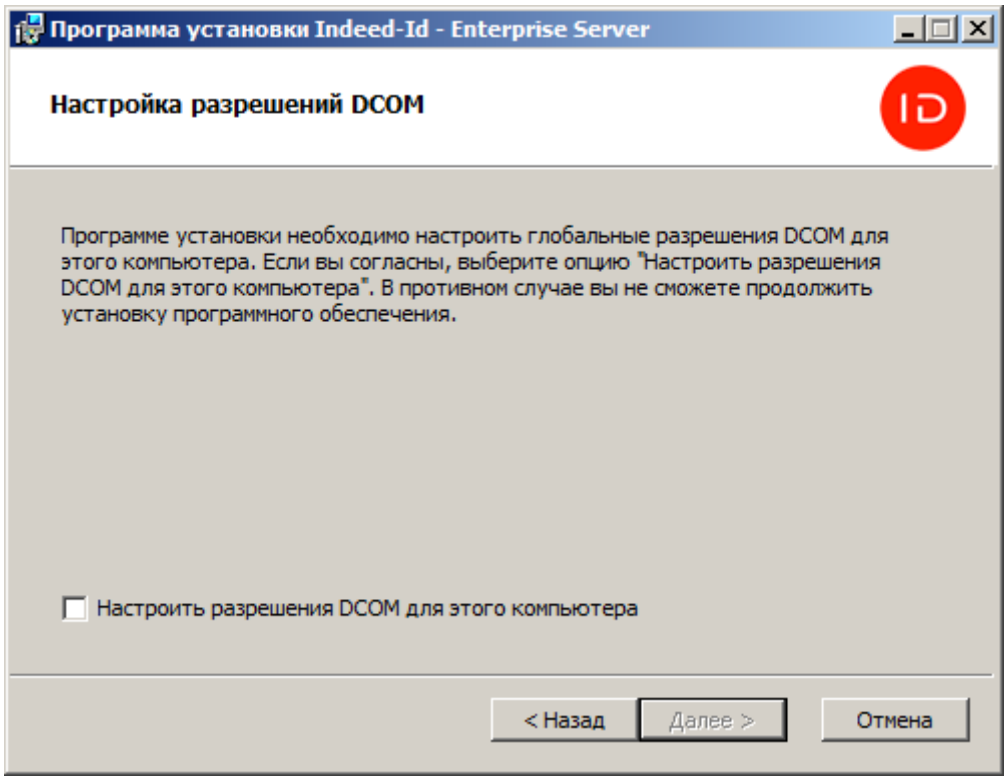


2. Укажите путь для установки сервера если на предыдущем шаге была выбрана опция **Изменить папку установки**.

[2] C:\Program Files (x86)\Indeed-Id\Server – для 64-битных ОС.

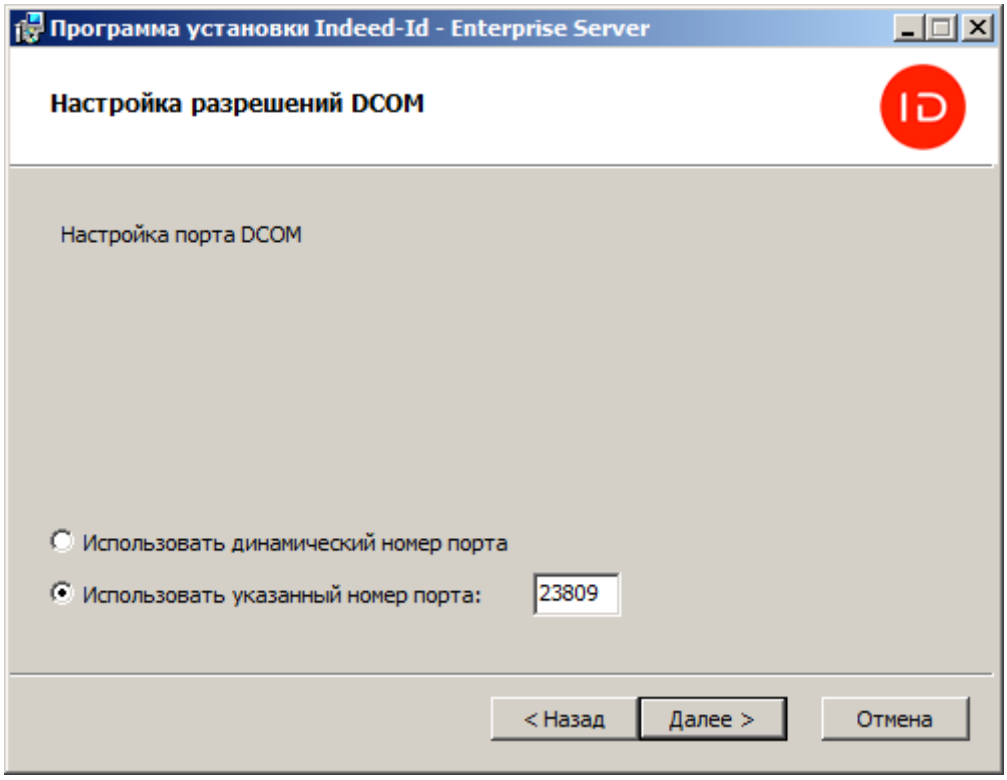
3. Выберите опцию **Настроить разрешения DCOM для этого компьютера** и нажмите **Далее**.

При выборе данной опции будут изменены общие настройки DCOM компьютера: в разделе настроек **COM Security - Launch and Activate Permissions - Limits** для категории **Authenticated Users** будут установлены права **Local Activation** и **Remote Activation**.

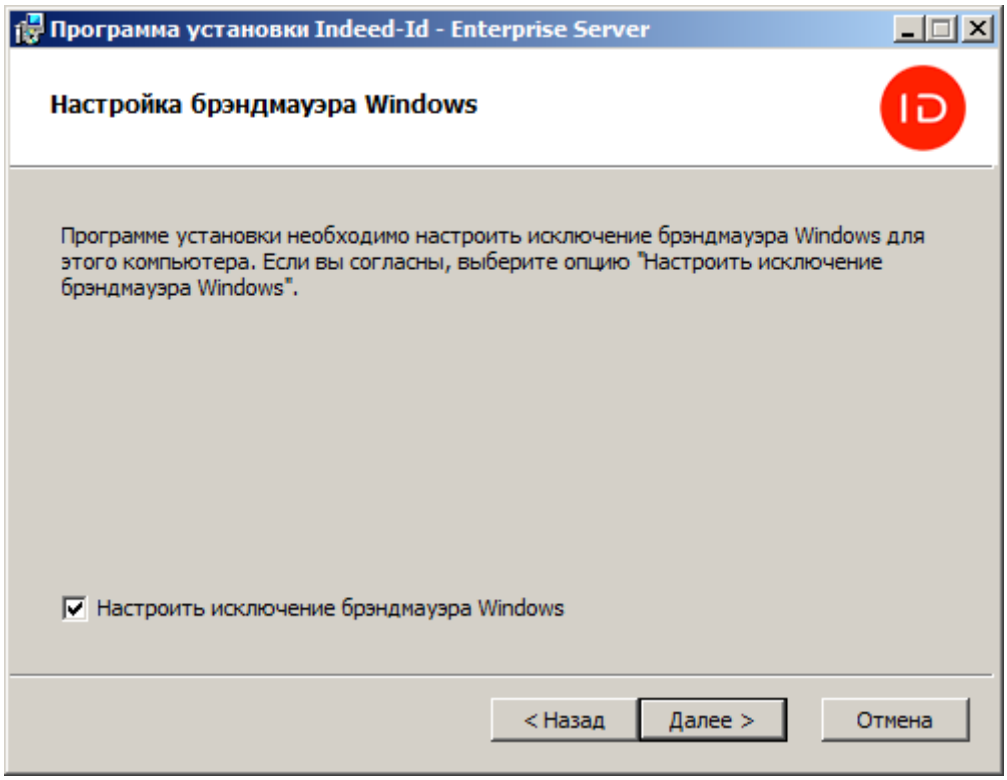


4. Выберите порт DCOM для соединения с Indeed-Id Enterprise Server. Вы можете указать порт самостоятельно (по умолчанию 23809), либо выбрать динамическое определение порта. Для продолжения установки нажмите **Далее**.

После установки Indeed-Id Enterprise Server вы сможете изменить номер порта DCOM с помощью средства **dcomcnfg**.



5. Если в системе включен брандмауэр Windows, выберите опцию **Настроить исключение брандмауэра Windows**. Для продолжения нажмите **Далее**.

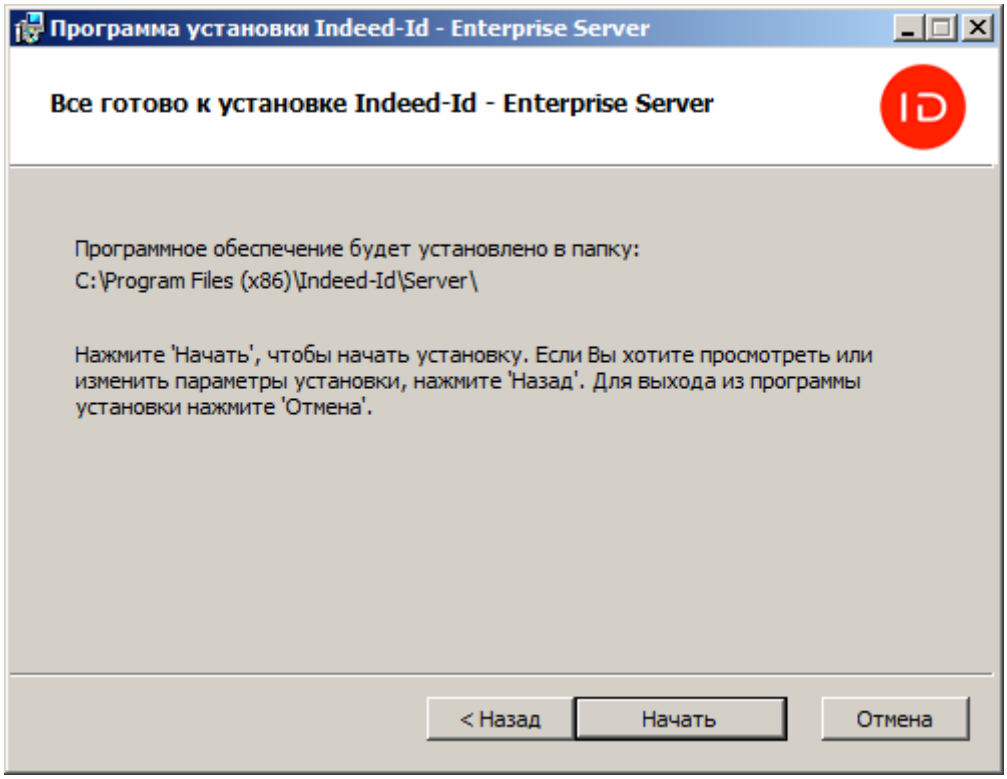


6. В процессе установки будет создан журнал событий системы. В этот журнал будут заноситься все события, регистрируемые компонентами системы Indeed-Id, установленными на рабочей станции. Журнал создается однократно при установке любого продукта, входящего в состав комплекса Indeed-Id Enterprise Authentication/Enterprise SSO за исключением Провайдеров аутентификации Indeed-Id.

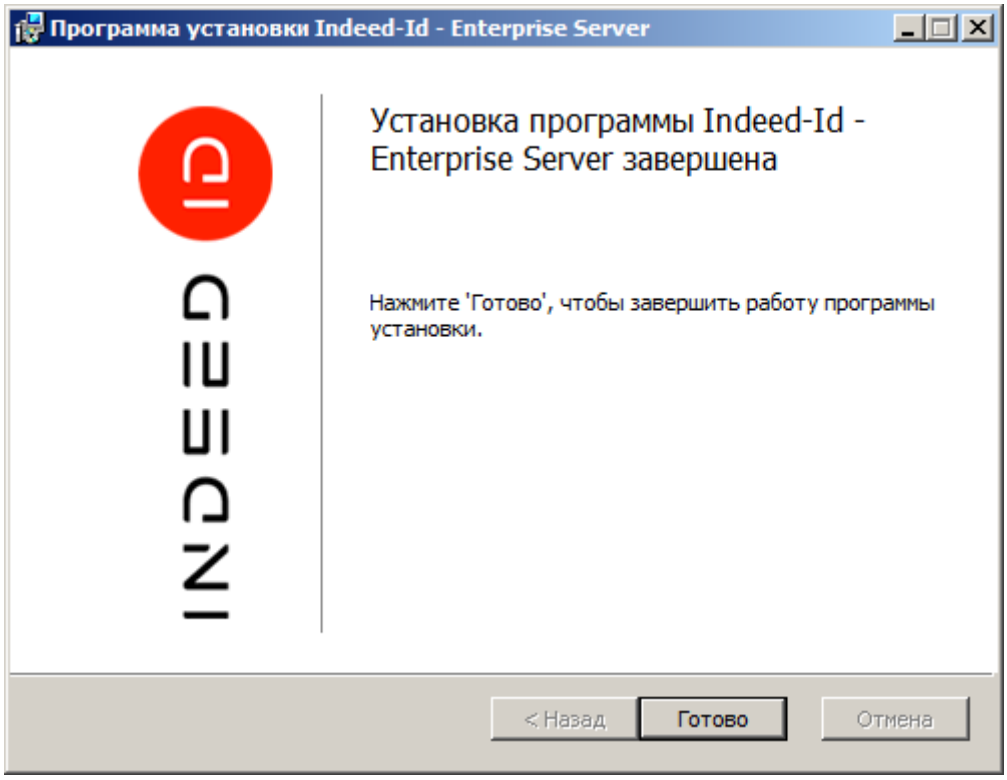
Для просмотра журнала событий перейдите в раздел **Администрирование – Просмотр событий – Журналы приложений и служб – Indeed-ID** (Administration Tools – Event Viewer – Application and Services Logs – Indeed-ID) панели управления Windows. Размер журнала составляет 10Мб.

В версиях Indeed-Id Enterprise Server до 2.0.133 включительно события также могут быть записаны в стандартный журнал Application, если он был выбран на этапе установки компонента. При обновлении на новые версии Indeed-Id Enterprise Server журнал событий не изменится.

7. Нажмите **Начать** для запуска процесса установки или **Отмена** для завершения работы программы установки.



8. Дождитесь завершения установки и нажмите **Готово**.



Для того, чтобы внесенные в систему изменения вступили в силу, необходимо завершить текущую рабочую сессию и выполнить повторный вход в систему.

Смотрите также: **Установка дополнительного экземпляра Indeed-Id Enterprise Server**.

Настройка первого экземпляра Indeed-Id Enterprise Server

Для выполнения настройки Indeed-Id Enterprise Server необходимы права Indeed-Id Server Admins.

После установки первого экземпляра Indeed-Id Enterprise Server необходимо выполнить следующие действия:

1. Активировать Indeed-Id Enterprise Server.
2. Выполнить генерацию ключа шифрования.

При наличии нескольких экземпляров Indeed-Id Enterprise Server необходимо выполнить экспорт ключа шифрования на дополнительные серверы.

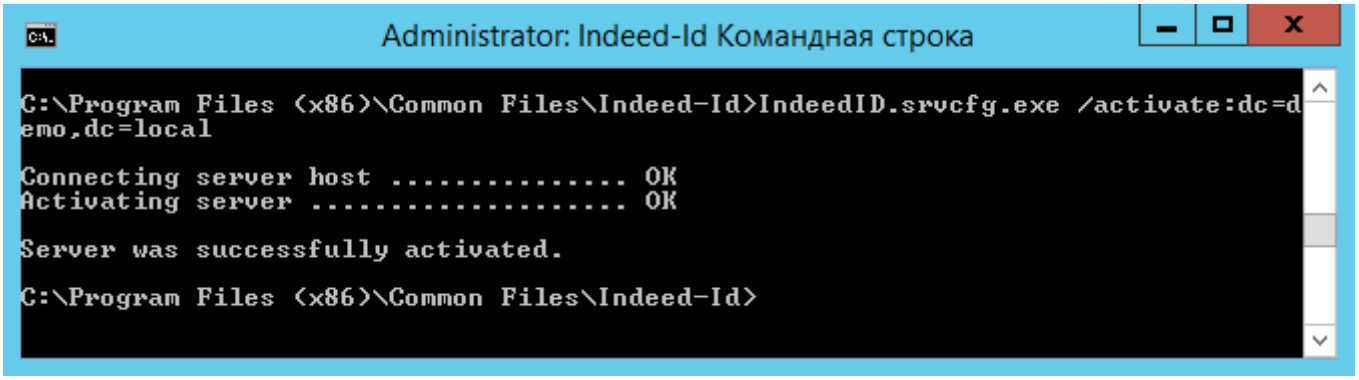
3. Выполнить регистрацию серверной лицензии.
4. Выполнить применение серверной лицензии.
5. Запустить Indeed-Id Enterprise Server.

Настройка Indeed-Id Enterprise Server осуществляется с помощью утилиты IndeedID.srvcfg.exe. После установки модуля Indeed-Id Enterprise Server данная утилита находится в каталоге \Program Files\Common Files\Indeed-Id.

Активация Indeed-Id Enterprise Server

Для активации Indeed-Id Enterprise Server запустите утилиту **IndeedID.srvcfg.exe** с параметрами **/activate: < путь к экземпляру системы >**, где < путь к экземпляру системы >- Distinguished Name (DN) подразделения домена, в котором развернут экземпляр системы. Например, для домена demo.local, в корне которого развернут экземпляр системы Indeed-Id, путь будет выглядеть следующим образом: "dc=demo,dc=local".

Пример: Команда **IndeedID.srvcfg.exe /activate:dc=demo,dc=local** [3] активирует Indeed-Id Enterprise Server для экземпляра системы demo.local.



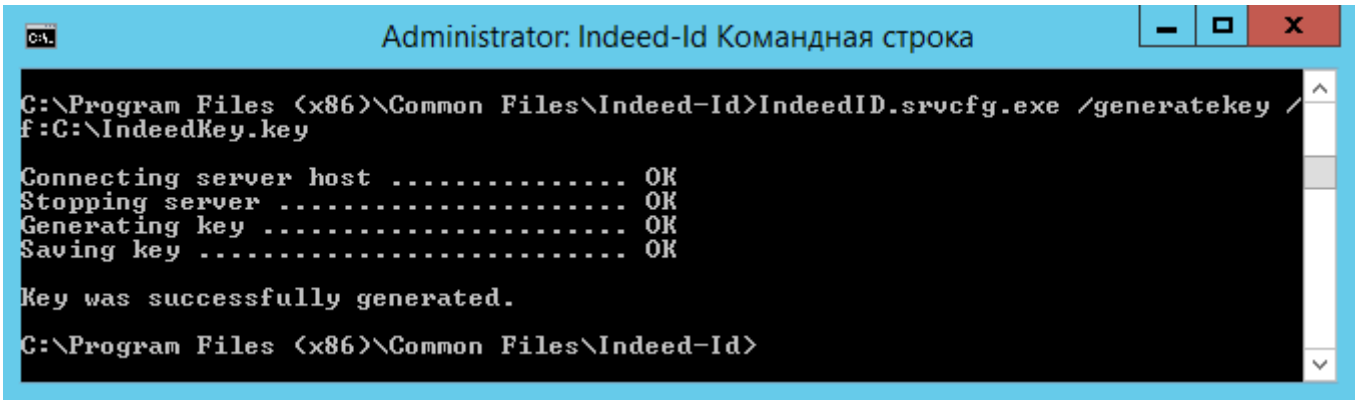
Если экземпляр системы Indeed-Id был создан с уникальными именами контейнера и подконтейнера (имена контейнера и подконтейнера, в которых располагаются данные системы в Active Directory, отличаются от установленных по умолчанию Indeed Identity (Indeed-ID) и Indeed AM соответственно), то при активации сервера необходимо использовать параметры **/company** и **/product**:

IndeedID.srvcfg.exe /activate:"dc=demo,dc=local" /company:"Access Control" /product:"Indeed Enterprise Authentication"

Генерация ключа шифрования и его применение

При установке первого сервера Indeed необходимо создать ключ шифрования данных системы. Для генерации ключа шифрования запустите утилиту IndeedID.srvcfg.exe с параметрами **/generatekey /f:"C:\keyname.key"** (**keyname** - имя файла для сохранения ключа). В результате в указанном каталоге будет создан файл ключа шифрования с заданным именем. Если файл с заданным именем уже существует, будет предложено перезаписать его.

Пример: Команда **IndeedID.srvcfg.exe /generatekey /f:"C:\IndeedKey.key"** создает файл ключа IndeedKey.key на локальном диске C:\.



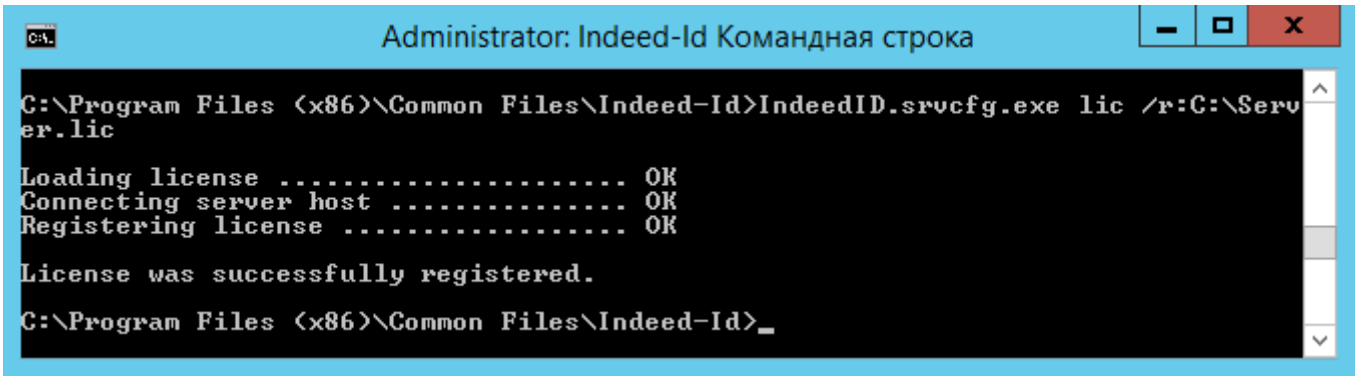
[3] Путь также может быть задан в альтернативном формате: IndeedID.srvcfg.exe /activate:demo.local/.

Настоятельно рекомендуется хранить файл ключа шифрования на внешнем носителе и обеспечить надежность его хранения.

Регистрация серверной лицензии

Для регистрации серверной лицензии запустите утилиту IndeedID.srvcfg.exe с параметрами **IndeedID.srvcfg.exe lic /r:Путь к файлу лицензии**.

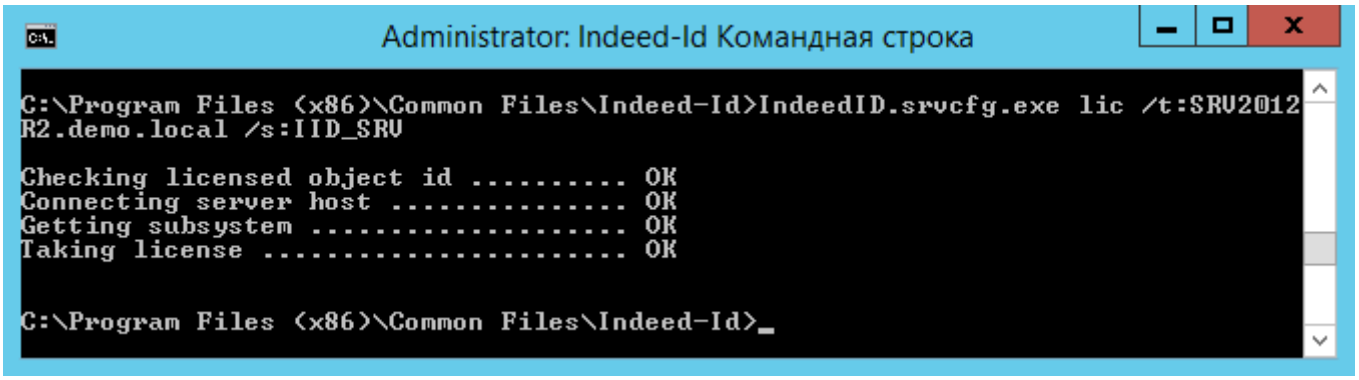
Пример: Команда **IndeedID.srvcfg.exe lic /r:C:\Server.lic** регистрирует лицензию, хранящуюся в файле Server.lic.



Применение серверной лицензии

Для применения серверной лицензии запустите утилиту IndeedID.srvcfg.exe с параметрами **IndeedID.srvcfg.exe lic /t:server1name /s:IID_SRV** (**server1name** – имя Indeed-Id Enterprise Server в формате DNS).

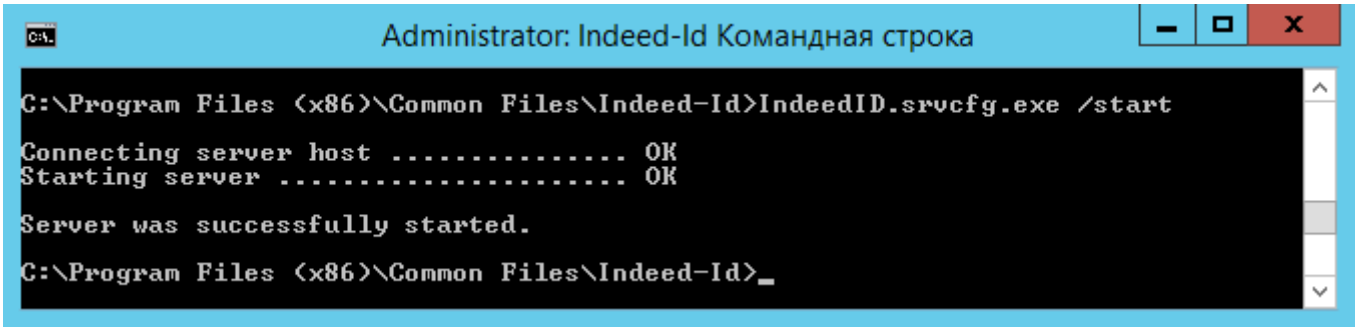
Пример: Команда **IndeedID.srvcfg.exe lic /t:SRV2012R2.demo.local /s:IID_SRV** выполняет применение лицензии для Indeed-Id Enterprise Server с именем SRV2012R2.demo.local.



Запуск Indeed-Id Enterprise Server

Для запуска Indeed-Id Enterprise Server запустите утилиту IndeedID.srvcfg.exe с командой **/start**.

Пример: Команда **IndeedID.srvcfg.exe /start** запускает установленный и активированный Indeed-Id Enterprise Server с примененной для него серверной лицензией.



Дальнейшее **администрирование сервера Indeed-Id** при помощи утилиты IndeedID.srvcfg.exe может осуществляться как непосредственно с самого сервера Indeed, так и с рабочей станции администратора, на которой установлен компонент Indeed-Id Admin Pack. Полное описание параметров утилиты IndeedID.srvcfg.exe приведено в документе **Indeed-Id Admin Pack. Руководство по эксплуатации.pdf**.

Операции активации (/activate), деактивации (/deactivate) и извлечения ключа шифрования (/extractkey) не могут быть выполнены удаленно. Перечисленные команды выполняются исключительно на серверах Indeed.

Установка дополнительного экземпляра Indeed-Id Enterprise Server

Развёртывание дополнительного Indeed-Id Enterprise Server не является обязательным шагом, но настоятельно рекомендуется для обеспечения отказоустойчивости системы.

1. Выполните вход на дополнительный сервер Indeed-Id под учетной записью с правами локального администратора;
2. Выполните запуск инсталлятора IndeedID.Enterprise.Server.msi.
3. Следуя дальнейшим инструкциям инсталлятора выполните установку Indeed-Id Enterprise Server.
4. Выполните вход на сервер Indeed-Id с правами Indeed-ID Server Admins.

Настройка дополнительного экземпляра Indeed-Id Enterprise Server

Для выполнения настройки Indeed-Id Enterprise Server необходимы права Indeed-Id Server Admins.

Для настройки дополнительного экземпляра Indeed-Id Enterprise Server необходимо выполнить следующие действия:

1. Активировать дополнительный Indeed-Id Enterprise Server.
2. Выполнить экспорт ключа шифрования на дополнительный Indeed-Id Enterprise Server.
3. Выполнить применение серверной лицензии для дополнительного Indeed-Id Enterprise Server.
4. Запустить дополнительный Indeed-Id Enterprise Server.

Настройка дополнительного экземпляра Indeed-Id Enterprise Server осуществляется с помощью утилиты IndeedID.srvcfg.exe, находящейся в локальном каталоге C:\Program Files\Common Files\Indeed-Id.

Активация дополнительного экземпляра Indeed-Id Enterprise Server

Активация дополнительного экземпляра Indeed-Id Enterprise Server производится по аналогии с активацией первого экземпляра Indeed-Id Enterprise Server.

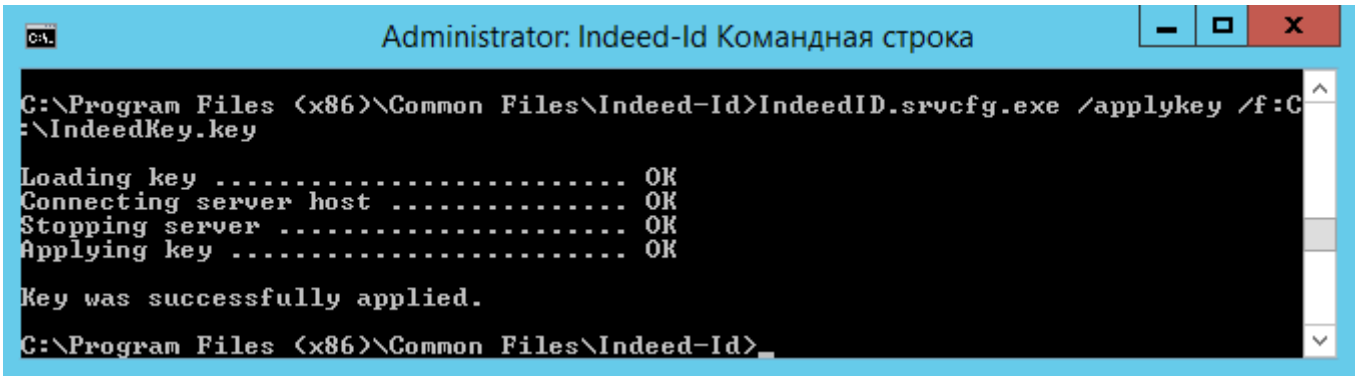
Экспорт ключа шифрования

Для экспорта ключа шифрования на дополнительный Indeed-Id Enterprise Server на первом Indeed-Id Enterprise Server запустите утилиту IndeedID.srvcfg.exe с параметрами **/applykey /h:server2name /f:"C:\keyname.key"** (**server2name –** адрес дополнительного Indeed-Id Enterprise Server в DNS формате; **keyname** – имя файла, в который был сохранен ключ шифрования после его генерации в процессе установки первого сервера).

В версиях сервера ниже 1.5.165.0 для экспорта ключа шифрования использовалась команда **/e**.

Пример: Команда **IndeedID.srvcfg.exe /applykey /h:srv2.demo.local /f:"C:\Key.key"** передает ключ, сохраненный на первом сервер Indeed на локальном диске C:\ в файле Key.key, на дополнительный Indeed-Id Enterprise Server с именем srv2.demo.local.

Также можно скопировать файл ключа шифрования на дополнительный сервер Indeed-Id и выполнить команду **IndeedID.srvcfg.exe /applykey /f:"C:\Key.key"**



Применение серверной лицензии

Применение серверной лицензии для дополнительного сервера производится по аналогии с применением лицензии на первый сервер Indeed. Запустите утилиту IndeedID.srvcfg.exe с параметрами **IndeedID.srvcfg.exe lic /t:server2name /s:IID_SRV** (**server2name** – имя дополнительного сервера в формате DNS).

Пример: Команда **IndeedID.srvcfg.exe lic /t:srv2.demo.local /s:IID_SRV** выполняет применение лицензии для дополнительного Indeed-Id Enterprise Server с именем srv2.demo.local.

Запуск дополнительного Indeed-Id Enterprise Server

Для запуска дополнительного сервера Indeed запустите утилиту IndeedID.srvcfg.exe с параметрами **/h:server2name /start** (**server2name** - имя дополнительного Indeed-Id Enterprise Server в формате DNS).

Дальнейшее **администрирование сервера Indeed-Id** при помощи утилиты IndeedID.srvcfg.exe может осуществляться как непосредственно с самого сервера Indeed, так и с рабочей станции администратора, на которой установлен компонент Indeed-Id Admin Pack. Полное описание параметров утилиты IndeedID.srvcfg.exe приведено в документе *Indeed-Id Admin Pack. Руководство по эксплуатации.pdf*.

Операции активации, деактивации и извлечения ключа шифрования не могут быть выполнены удаленно. Перечисленные команды выполняются исключительно на серверах Indeed.

Использование тестового Indeed-Id Enterprise Server

В целях повышения надежности системы при ее обновлении рекомендуется использовать выделенный тестовый Indeed-Id Enterprise Server. Использование тестового экземпляра сервера позволяет проверить совместимость программного обеспечения на рабочих станциях пользователей с новой версией Indeed-Id Enterprise Server и устранить возможные проблемы, не затрагивая систему в целом. По истечению периода тестовой эксплуатации выполняется обновление модуля Indeed-Id Enterprise Server на всех экземплярах серверных рабочих станциях и отключение тестового сервера до очередного обновления.

Предварительные настройки

Для использования тестового экземпляра Indeed-Id Enterprise Server необходимо выполнить следующие действия:

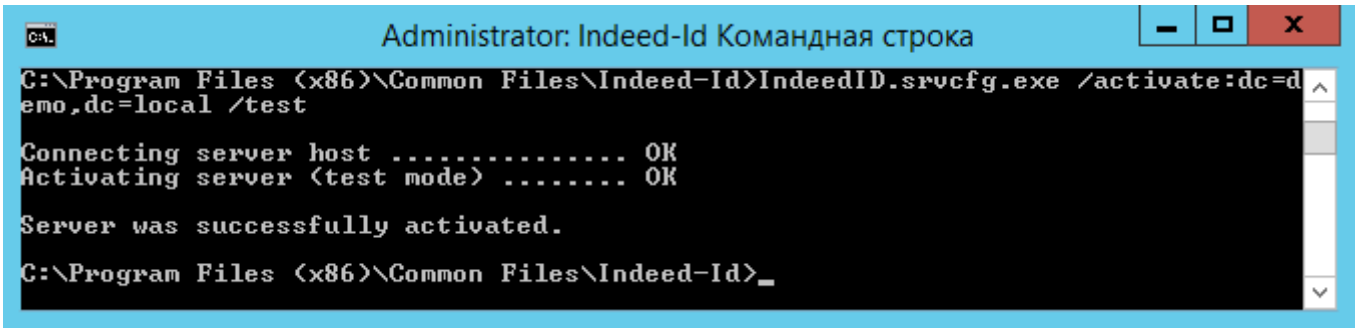
1. С помощью оснастки **Active Directory Пользователи и Компьютеры** (Active Directory Users and Computers) создайте **Подразделение** (Organization Unit) или **Группу** (Group) для компьютеров, взаимодействующих с тестовым экземпляром Indeed-Id Enterprise Server.
2. Включите политику «Использовать для работы только тестовые серверы Indeed-Id». Подробнее о том, как включить данную политику смотрите в разделе *Настройка групповых политик Indeed-Id, политики Test Servers* документа *Indeed-Id Admin Pack. Руководство по эксплуатации.pdf*.
3. Распространите действия политики на созданное в п.1 Подразделение или Группу.
4. Переместите в необходимые рабочие станции в связанное с групповой политикой Подразделение (Группу) и выполните обновление групповых политик.

Перевод Indeed-Id Enterprise Server в тестовый режим использования

Для перевода Indeed-Id Enterprise Server в тестовый режим выполните следующие действия:

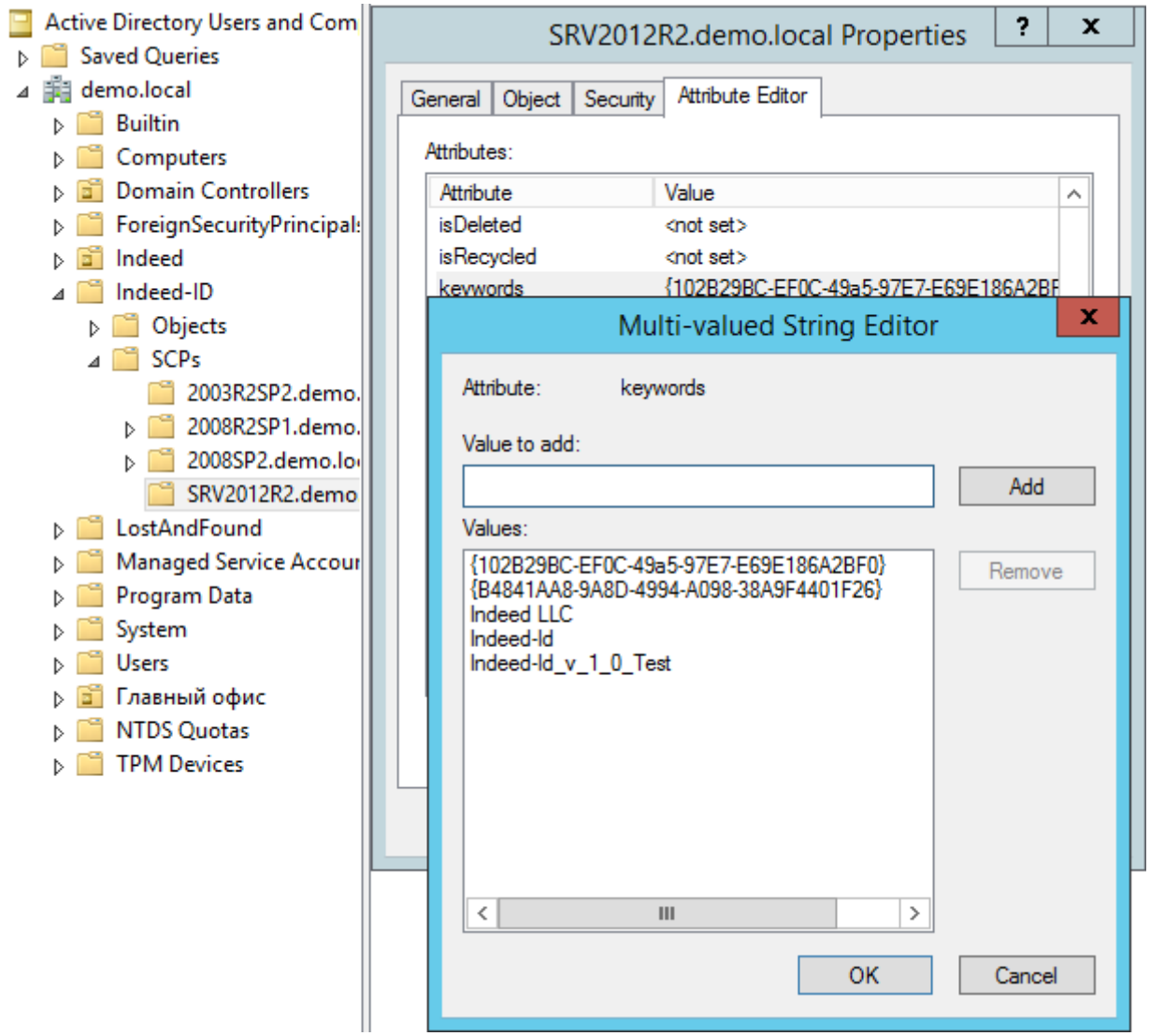
1. Деактивируйте Indeed-Id Enterprise Server.
2. Запустите утилиту IndeedID.srvcfg.exe с параметрами **/activate:<путь к экземпляру системы> /test**.

Пример: Команда **IndeedID.srvcfg.exe /activate:dc=demo,dc=local /test** активирует данный Indeed-Id Enterprise Server в тестовом режиме.



Для возвращения Indeed-Id Enterprise Server в стандартный режим использования необходимо деактивировать его и активировать обычным способом.

Определить, является ли Indeed-Id Enterprise Server тестовым, можно по свойствам записи SCP, соответствующей данному серверу. Для просмотра свойств записи SCP можно использовать стандартные средства администрирования (например, оснастку Active Directory Пользователи и компьютеры (Active Directory Users and Computers).



Если атрибут **keywords** содержит запись с суффиксом Test, данный Indeed-Id Enterprise Server является тестовым.

Настройка автоматической идентификации пользователей

Для удобства аутентификации пользователей на сервере Indeed может быть настроена автоматическая идентификациия. В этом случае пользователю достаточно будет предоставить обученный аутентификатор (например, RFID-карту), а система сама определит, какому пользователю принадлежит предоставленный аутентификатор.

Настройка автоматической идентификации осуществляется на всех серверах Indeed-Id и на рабочих станциях пользователей при помощи пакета кастомизации или групповой политики. Административный файл политики входит в состав дистрибутива компонента Indeed-Id Admin Pack.

Пакет кастомизации, помимо настроек автоматической идентификации может содержать логотип компании клиента, а также параметры установки и настройки продуктов Indeed-Id. Пакет кастомизации разрабатывается индивидуально для каждого клиента. Если Вам необходим пакет кастомизации, обратитесь в службу технической поддержки Indeed-Id за подробной информацией.

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 пользователь должен обучить аутентификатор после того, как будет выполнена настройка автоматической идентификации на всех серверах Indeed-Id и рабочей станции пользователя либо выполнить вход в систему по ранее обученному аутентификатору после включения автоматической идентификации.

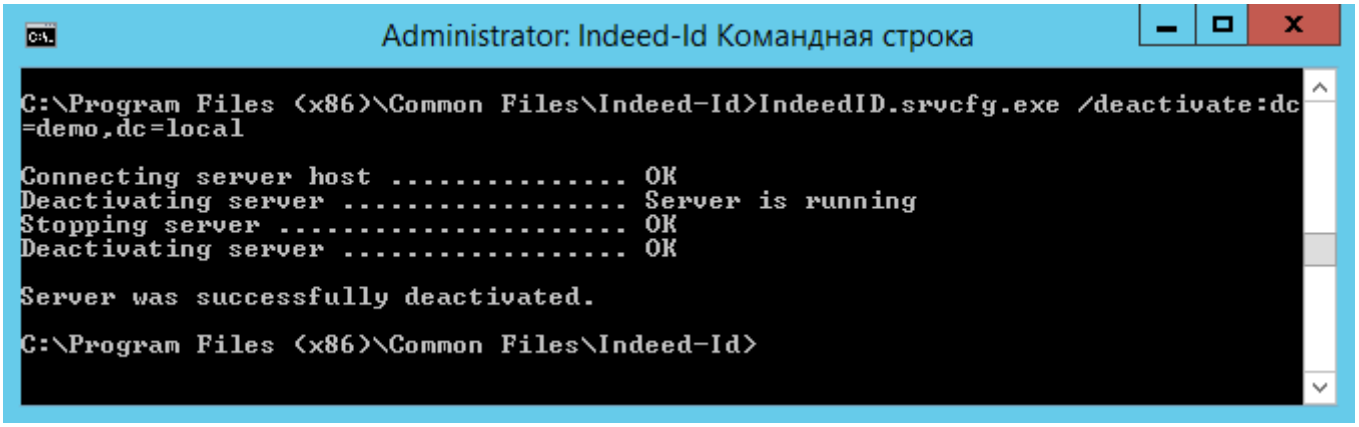
Функция автоматической идентификации может быть использована вместе с функцией автоматического завершения сеанса пользователя, если другой пользователь предоставит свой аутентификатор. Для настройки автоматической идентификации и автоматического завершения сеанса пользователя обратитесь к документу *Indeed-Id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

Удаление и обновление Indeed-Id Enterprise Server

Перед удалением сервера Indeed его необходимо деактивировать. При деактивации сервера необходимо указывать полный путь (Distinguished Name) к экземпляру системы, в котором ранее был активирован удаляемый сервер.

Для деактивации Indeed-Id Enterprise Server запустите утилиту IndeedID.srvcfg.exe с параметрами **/deactivate:< путь к экземпляру системы >**

Пример: Команда **IndeedID.srvcfg.exe /deactivate:dc=demo,dc=local** [4] деактивирует Indeed-Id Enterprise Server для экземпляра системы в корне домена demo.local.



Если экземпляр системы Indeed-Id был создан с уникальными именами контейнера и подконтейнера (имена контейнера и подконтейнера, в которых располагаются данные системы в Active Directory, отличаются от установленных по умолчанию Indeed Identity (Indeed-ID) и Indeed AM соответственно), то при деактивации сервера необходимо использовать параметры **/company** и **/product**:

IndeedID.srvcfg.exe /deactivate:"dc=demo,dc=local" /company: "Access Control" /product: "Indeed Enterprise Authentication"

Для удаления модуля Indeed-Id Enterprise Server выполните следующие действия:

1. В **Панели управления Windows** выберите **Установка и удаление программ**.
2. В списке установленных программ выберите **Indeed-Id – Enterprise Server** и нажмите **Удалить**.
3. Подтвердите действие и дождитесь завершения удаления.
4. При установке новой версии модуля Indeed-Id Enterprise Server автоматически выполняется обновление компонентов текущей версии. При отсутствии особых указаний службы поддержки удаление текущей версии модуля не требуется.

В целях повышения надежности системы установку новой версии модуля Indeed-Id Enterprise Server рекомендуется выполнять на выделенном сервере, переведенном в тестовый режим использования. Использование тестового Indeed-Id Enterprise Server позволяет проверить совместимость программного обеспечения на рабочих станциях пользователей с новой версией Indeed-Id Enterprise Server и устранить возможные проблемы, не затрагивая систему в целом. По истечении периода тестовой эксплуатации выполняется обновление модуля Indeed-Id Enterprise Server на всех серверах и отключение тестового экземпляра Indeed-Id Enterprise Server до очередного обновления. Для получения подробной информации о тестовом режиме

[4] Путь также может быть задан в альтернативном формате: IndeedID.srvcfg.exe /deactivate:demo.local/.

использования Indeed-Id Enterprise Server обратитесь к документу *Indeed-Id Admin Pack. Руководство по эксплуатации.pdf* (см. **Использование тестового Indeed-Id Enterprise Server**).

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 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.