Indeed-Id Admin Pack

Руководство по установке и эксплуатации

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 EA/ESSO. Данное Руководство поможет вам выполнить установку компонента Indeed-Id Admin Pack и начать его использование.

Условные обозначения

В Руководстве используются следующие условные обозначения:

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

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

О компоненте Indeed-Id Admin Pack

Компонент позволяет администраторам Indeed EA/ESSO осуществлять конфигурирование системы Indeed EA/ESSO и содержит в себе следующие инструменты администрирования:

- Утилита **IndeedID.srvcfg.exe**. Предназначена для управления Indeed-Id Enterprise Server и просмотра информации по зарегистрированным лицензиями.
- Утилита **IndeedID.ExportImport.exe**. Предназначена для переноса данных и резервного копирования систем Indeed EA/Indeed ESSO из одного домена в другой.
- Утилита **IndeedID.Password.Manager.exe**. Предназначена для генерации случайного пароля пользователям Indeed-Id.
- Утилита **IndeedID.AD.Users.Info.exe**. Предназначена для сбора информации о доменных пользователях.
- Файлы сценариев Windows PowerShell 2.0.
- Шаблоны групповых политик.

Устанавливать Indeed-Id Admin Pack следует на серверы Indeed EA/ESSO и рабочие станции администраторов комплекса Indeed EA/ESSO. Перед установкой компонентов необходимо ознакомиться с разделом **Предварительные условия для установки**.

Предварительные условия для установки

Включение Глобального каталога

Включение Глобального каталога необходимо для успешного поиска Indeed-Id Enterprise Server клиентом (рабочей станцией с установленным Indeed-Id Admin Pack). 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.

Поддерживаемые операционные системы

Для корректной установки Indeed-Id Admin Pack система должна соответствовать следующим требованиям:

- 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
- Windows XP SP3 32bit
- Windows Vista SP2 32/64bit
- Windows 7 SP1 32/64bit
- Windows 8.1 32/64bit
- Windows 10 32/64bit

Аппаратные требования к рабочим станциям

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

Требования к окружению

Для корректной работы Indeed-Id Admin Pack необходимо следующее окружение:

- **Настроенный DNS сервер** (необходимо добавление Reverse lookup zones). **Параметры DNS сервера** необходимо указать **в настройках сетевого подключения** на каждой рабочей станции.
- Права Локального Администратора (Adminstrator) для установки Indeed-Id Admin Pack

Настройки межсетевого экрана

Для корректной работы системы Indeed-Id необходимо изменить следующие настройки межсетевого экрана на Indeed-Id Enterprise Server и на рабочих станциях, на которых установлен компонент Indeed-Id Admin Pack:

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**).
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).

Установка Indeed-Id Admin Pack

Установка пакета Indeed-Id Admin Pack выполняется на рабочей станции администратора системы.

Для установки компонента, пользователь, от имени которого выполняется установка, должен обладать правами администратора (быть членом локальной группы «Администраторы»).

Для установки пакета Indeed-Id Admin Pack выполните следующие действия:

1. Запустите программу установки IndeedID.AdminPack.msi[1] и дождитесь отображения Мастера установки.
2. 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.
3. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.

Средства администрирования Indeed-Id

Управление серверами

Управление Indeed-Id Enterprise Server, лицензиями и ключом шифрования осуществляется с помощью утилиты IndeedID.srvcfg.exe, включенной в состав продукта Indeed-Id Enterprise Server и Indeed-Id Admin Pack по умолчанию находящейся в каталоге C:\Program Files\Common Files\Indeed-Id[2]. Получить доступ к утилите IndeedID.srvcfg.exe можно также через меню **Пуск** > **Программы** > **Indeed-Id** > **Indeed-Id Командная строка**.

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.

Для управления Indeed-Id Enterprise Server и ключом шифрования необходимы права Indeed-Id Server Admins.

[1] Для установки на 64-битных ОС следует использовать инсталлятор IndeedID.AdminPack.x64.msi
[2] C:\Program Files (x86)\Common Files\Indeed-Id – для 64-битных ОС.

Управление Indeed-Id Enterprise Server включает следующие операции:

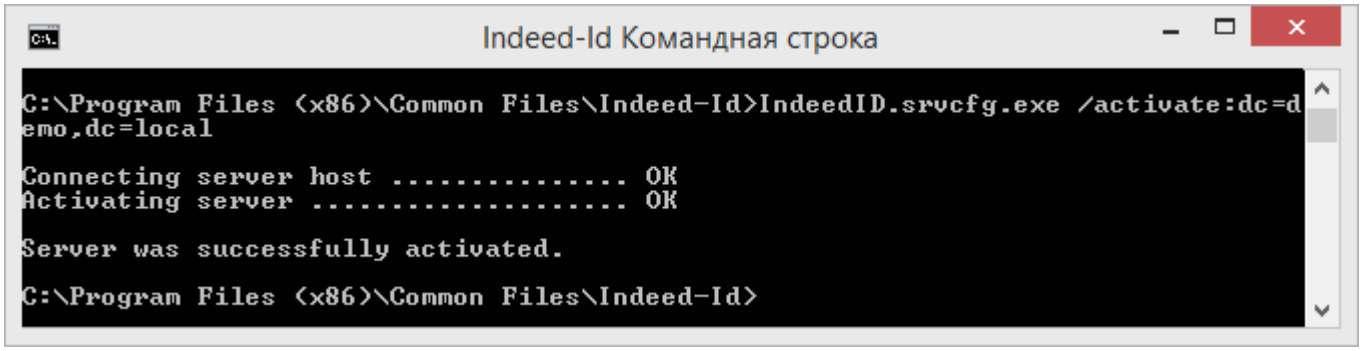
- **Активация и деактивация Indeed-Id Enterprise** Server
- **Запуск, перезапуск, остановка и проверка состояния Indeed-Id Enterprise Server**
- **Управление серверной лицензией**
- **Управление пользовательскими лицензиями в подсистемах**
- **Ошибка! Источник ссылки не найден.**

Активация и деактивация Indeed-Id Enterprise Server

Активация и деактивация Indeed-Id Enterprise Server выполняются непосредственно на сервере.

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.



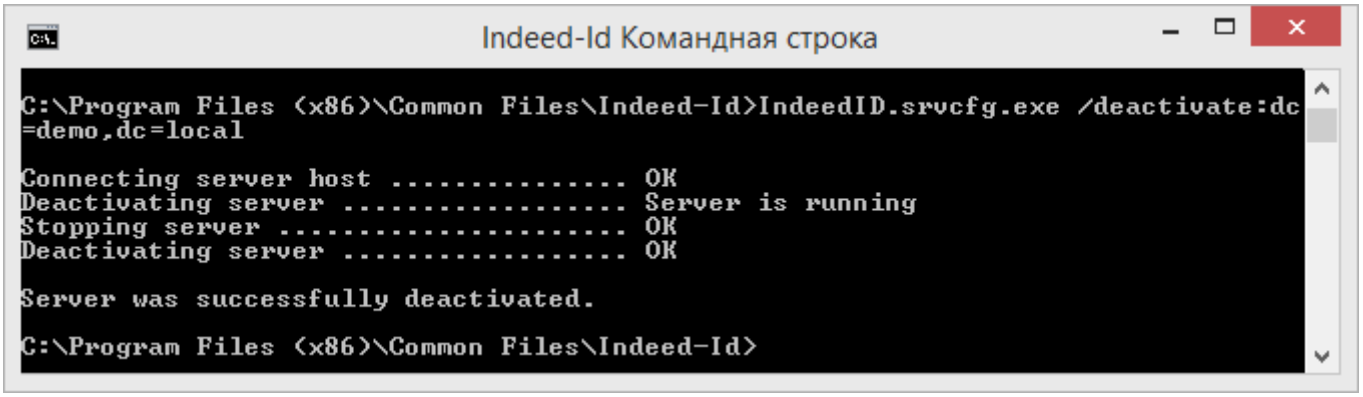
Если экземпляр системы Indeed-Id был создан с уникальными именами контейнера и подконтейнера (имена контейнера и подконтейнера, в которых располагаются данные системы в Active Directory, отличаются от установленных по умолчанию Indeed Identity (Indeed-ID) и Indeed AM соответственно), то при активации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

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

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. По аналогии с командой активации необходимо задавать значения параметров **/company** и **/product**, если экземпляр системы, в котором требуется деактивировать сервер содержит уникальные имена контейнера и подконтейнера.

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



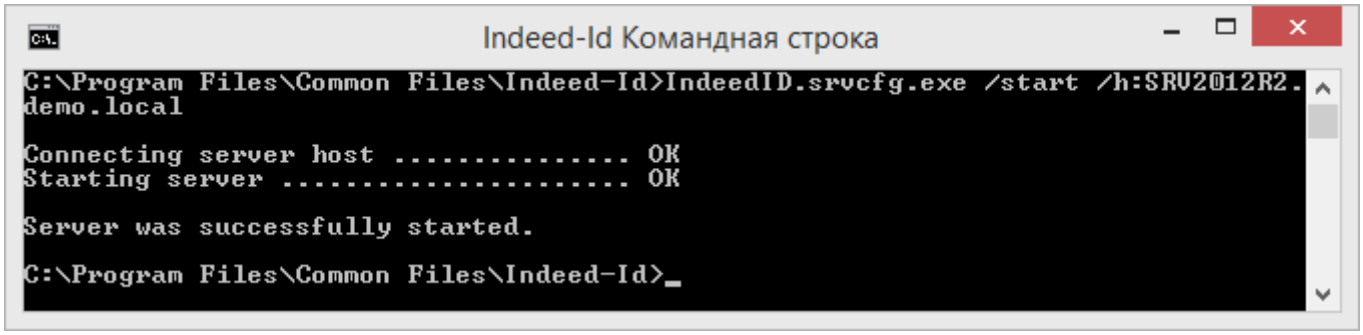
Запуск, перезапуск, остановка и проверка состояния Indeed-Id Enterprise Server

Запуск Indeed-Id Enterprise Server

Функционирование системы Indeed-Id возможно только при запущенном Indeed-Id Enterprise Server.
Для старта Indeed-Id Enterprise Server запустите утилиту IndeedID.srvcfg.exe с параметрами **/start /h:*server_name***, где ***server_name*** – имя сервера Indeed-Id в DNS формате.

Параметр /h необходимо указывать только в случаях, если запуск утилиты осуществляется с рабочей станции администратора. При запуске утилиты IndeedID.srvcfg.exe на сервере Indeed-Id задавать параметр /h не обязательно.

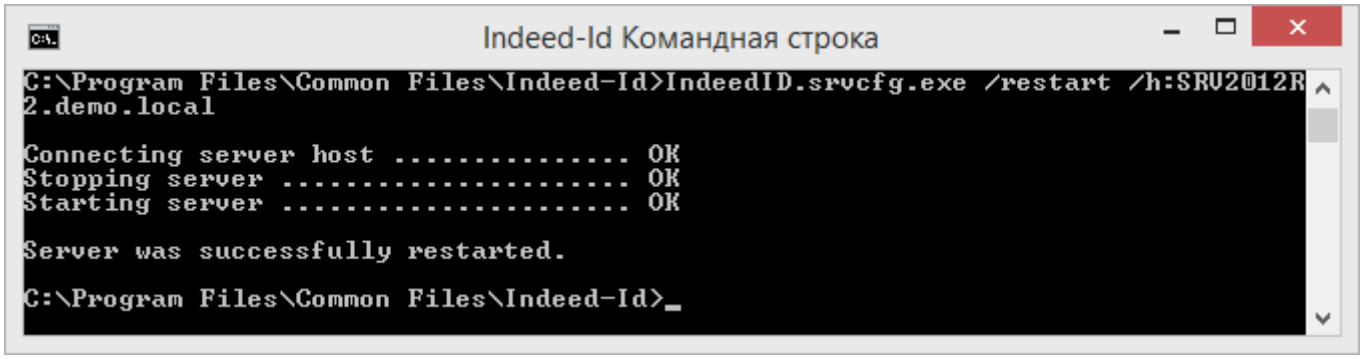
Пример: **IndeedID.srvcfg.exe /start /h:SRV2012R2.demo.local**



Перезапуск Indeed-Id Enterprise Server

Для перезапуска Indeed-Id Enterprise Server запустите утилиту IndeedID.srvcfg.exe с параметрами **/restart /h:*server_name***, где ***server_name*** – имя сервера Indeed-Id в DNS формате.

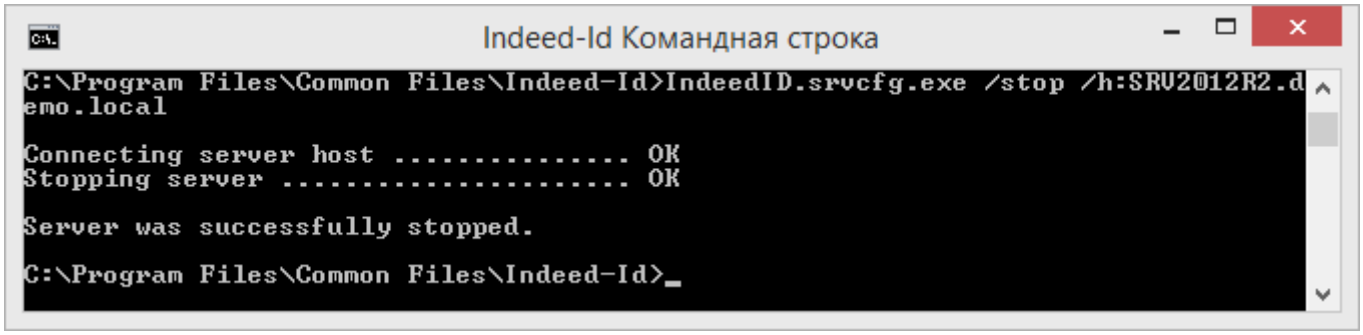
Пример: **IndeedID.srvcfg.exe /restart /h:SRV2012R2.demo.local**



Остановка Indeed-Id Enterprise Server

Для остановки Indeed-Id Enterprise Server запустите утилиту IndeedID.srvcfg.exe с параметрами **/stop /h:*server_name***, где ***server_name*** – имя сервера Indeed-Id в DNS формате.

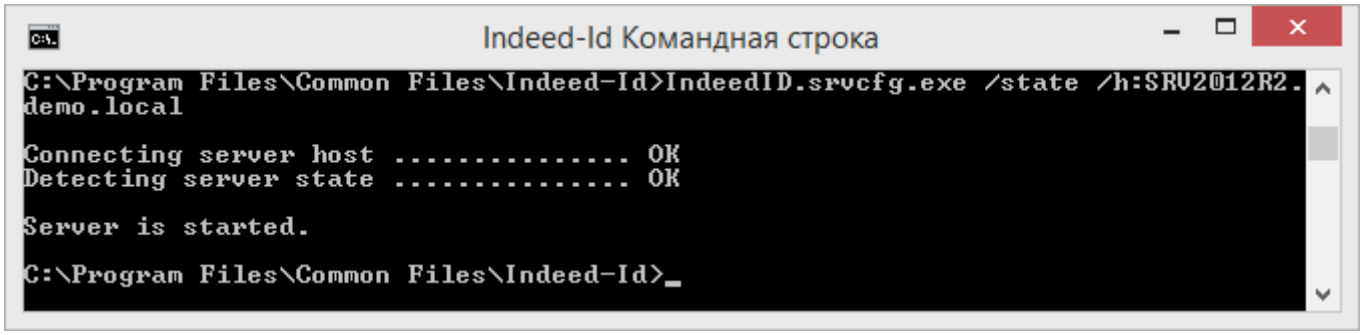
Пример: **IndeedID.srvcfg.exe /stop /h:SRV2012R2.demo.local**



Проверка состояния Indeed-Id Enterprise Server

Для проверки состояния Indeed-Id Enterprise Server запустите утилиту IndeedID.srvcfg.exe с параметрами **/state /h:*server_name***, где ***server_name*** – имя сервера Indeed-Id в DNS формате. Сообщение о состоянии Indeed-Id Enterprise Server выводится в командной строке.

Пример: **IndeedID.srvcfg.exe /state /h:SRV2012R2.demo.local**



Если в случае перезагрузки рабочей станции с установленным Indeed-Id Enterprise Server, серверу не удалось стартовать автоматически в течение 10 минут, то ещё через 10 минут автоматически будет предпринята следующая попытка старта сервера. Всего таких попыток будет 10.

Управление серверной лицензией

Управление серверной лицензией включает регистрацию лицензии и применение на активированных экземплярах Indeed-Id Enterprise Server.

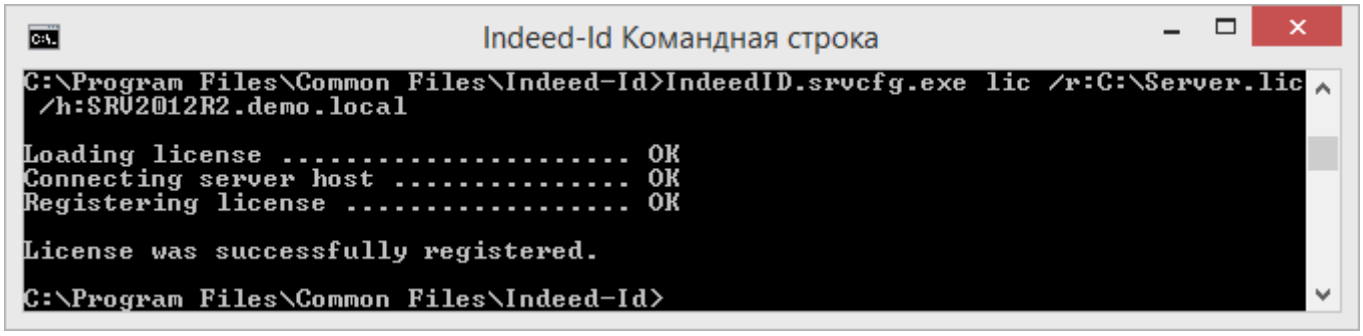
Регистрация серверной лицензии

Для регистрации серверной лицензии запустите утилиту IndeedID.srvcfg.exe с параметрами **IndeedID.srvcfg.exe lic /r:*license_path* /h:*server_name***, где:

license_path – путь к файлу лицензии
server_name – имя сервера Indeed-Id в DNS формате

Параметр /h необходимо указывать только в случаях, если запуск утилиты осуществляется с рабочей станции администратора. При запуске утилиты IndeedID.srvcfg.exe на сервере Indeed-Id задавать параметр /h не следует.

Пример: Команда **IndeedID.srvcfg.exe lic /r:C:\Server.lic /h:SRV2012R2.demo.local** регистрирует лицензию, хранящуюся в файле Server.lic в корне диска C.



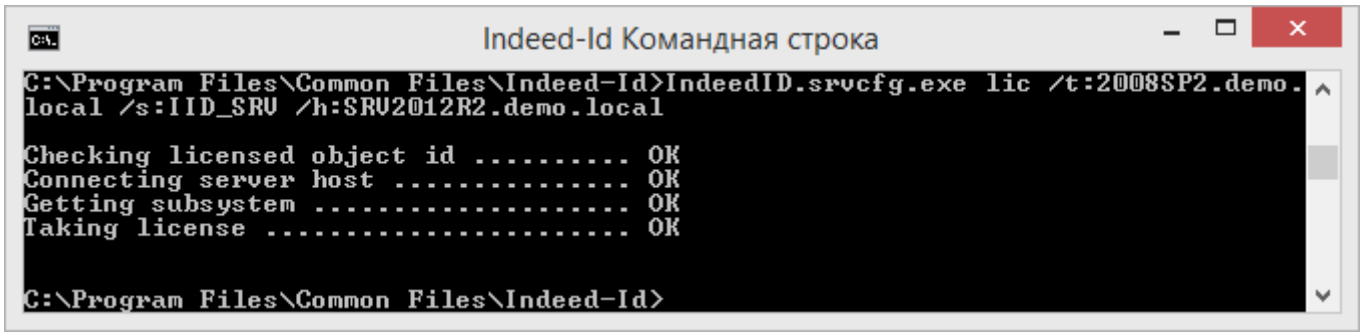
Применение серверной лицензии

Для применения серверной лицензии запустите утилиту **IndeedID.srvcfg.exe** с параметрами **IndeedID.srvcfg.exe lic /t:*server_name* /s:IID_SRV /h:*server_name***, где

/t:server_name – имя сервера Indeed-Id в формате DNS, для которого необходимо применить лицензию
/h:server_name – имя сервера Indeed-Id в формате DNS, к которому необходимо подключиться для выполнения команды.

Администратор со свей рабочей станции может применить лицензию для дополнительного сервера (указав его имя в параметре /t), подключившись к ранее развернутому основному серверу (указав его имя в параметре /h). Поддерживается также и применение лицензии для того сервера, через которой выполняется подключение (т.е. значение *server_name* в параметрах /t и /h может быть одинаковым).

Пример: Команда **IndeedID.srvcfg.exe lic /t:2008SP2.demo.local /s:IID_SRV /h:SRV2012R2.demo.local** выполняет применение лицензии для Indeed-Id Enterprise Server с именем 2008SP2.demo.local через подключение к ранее развернутому серверу Indeed с именем SRV2012R2.demo.local



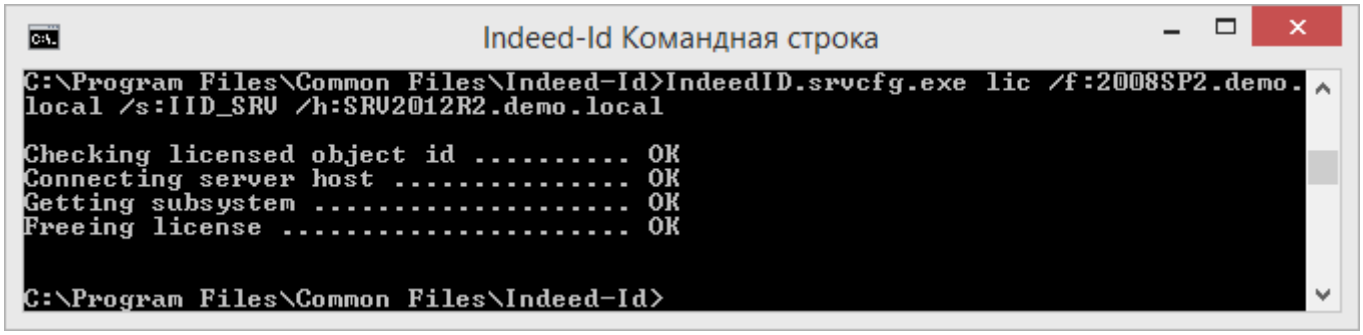
Освобождение серверной лицензии

Для освобождения серверной лицензии запустите утилиту IndeedID.srvcfg.exe с параметрами **IndeedID.srvcfg.exe /f:*server_name* /s:IID_SRV /h:*server_name***, где:

/f:server_name – имя сервера Indeed-Id в формате DNS, для которого необходимо освободить лицензию
/h:server_name – имя сервера Indeed-Id в формате DNS, к которому необходимо подключиться для выполнения команды.

Администратор со свей рабочей станции может отозвать лицензию для дополнительного сервера (указав его имя в параметре /t), подключившись к ранее развернутому основному серверу (указав его имя в параметре /h). Поддерживается также и отзыв лицензии для того сервера, через которой выполняется подключение (т.е. значение *server_name* в параметрах /f и /h может быть одинаковым).

Пример: Команда **IndeedID.srvcfg.exe lic /f:2008SP2.demo.local /s:IID_SRV /h:SRV2012R2.demo.local** выполняет освобождение лицензии Indeed-Id Enterprise Server с именем 2008SP2.demo.local через подключение к ранее развернутому серверу Indeed с именем SRV2012R2.demo.local



Управление пользовательскими лицензиями в подсистемах

Во избежание утраты лицензий перед удалением или блокировкой учетных записей пользователей Active Directory необходимо отключать опции **Разрешить использование Indeed-Id Windows® Logon** и **Разрешить использование Indeed-Id Enterprise SSO** на вкладке **Настройки** в карточке пользователя приложения Indeed EMC.

Для управления пользовательскими лицензиями в подсистемах используйте команду вида

IndeedID.srvcfg lic </r:licfile> </u:licid> </c> </e> </es> </i:subsystem> </fas> </fs> /<fu> </s> [/h:hostname]

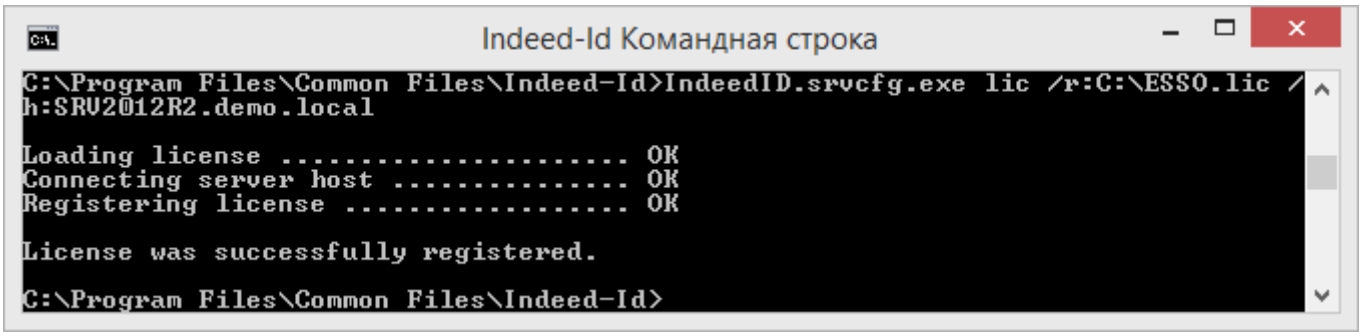
где:

- **/r** – зарегистрировать лицензию;
- **/u** – отозвать лицензию;
- **/c** – очистить данные лицензии;
- **/e** – вывести список зарегистрированных лицензий;
- **/es** – вывести список лицензируемых подсистем;
- **/i** – вывести информацию о подсистеме лицензирования;
- **/h** – установить соединение с указанным хостом;
- **licfile** – имя файла лицензии;
- **licid** – идентификатор лицензии;
- **subsystem** – имя подсистемы (**IID_LFW_USR** для системы Indeed-Id Windows® Logon, **IID_ESSO_USR** для системы Indeed-Id Enterprise SSO, **IID_SRV** для Indeed-Id Enterprise Server);
- **hostname** – имя хоста.
- **/fs** – освобождение неиспользуемых лицензий подсистемы. Необходимо дополнительно указать подсистему опцией /s (поддерживаются подсистемы IID_SRV, IID_LFW_USR и IID_ESSO_USR)
- **/fu** – освобождение всех неиспользуемых пользовательских лицензий из подсистем IID_LFW_USR и IID_ESSO_USR.
- **/fas** - освобождение всех захваченных лицензий указанной подсистемы. Необходимо дополнительно указать подсистему опцией /s (поддерживаются подсистемы IID_SRV, IID_LFW_USR и IID_ESSO_USR)

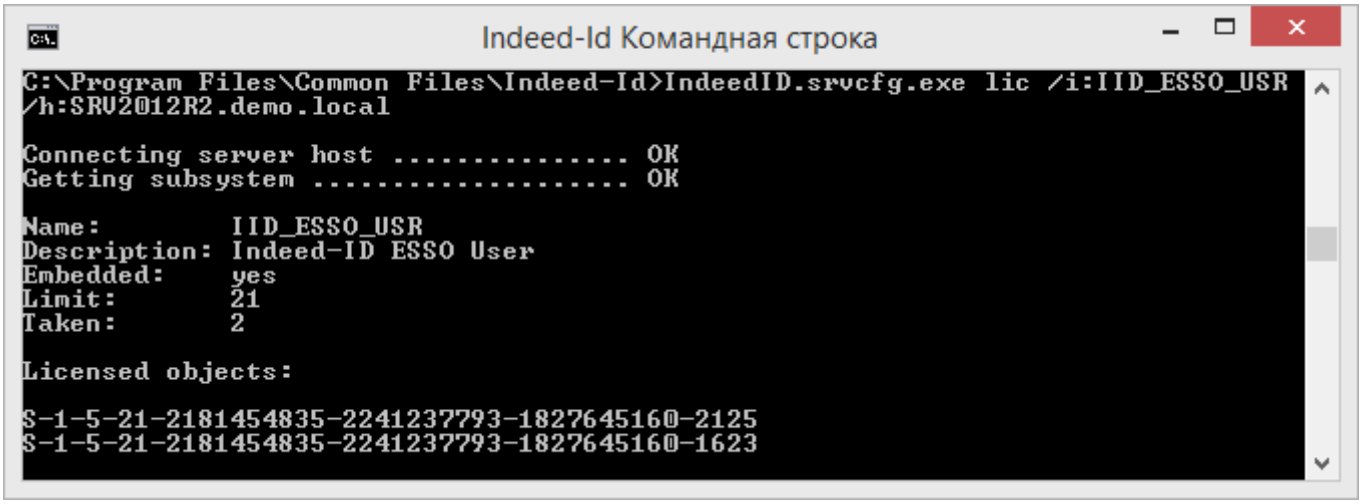
Примеры:

Параметр /h необходимо указывать только в случаях, если запуск утилиты осуществляется с рабочей станции администратора. При запуске утилиты IndeedID.srvcfg.exe на сервере Indeed-Id задавать параметр /h не следует.

a) Регистрация лицензии в подсистеме:



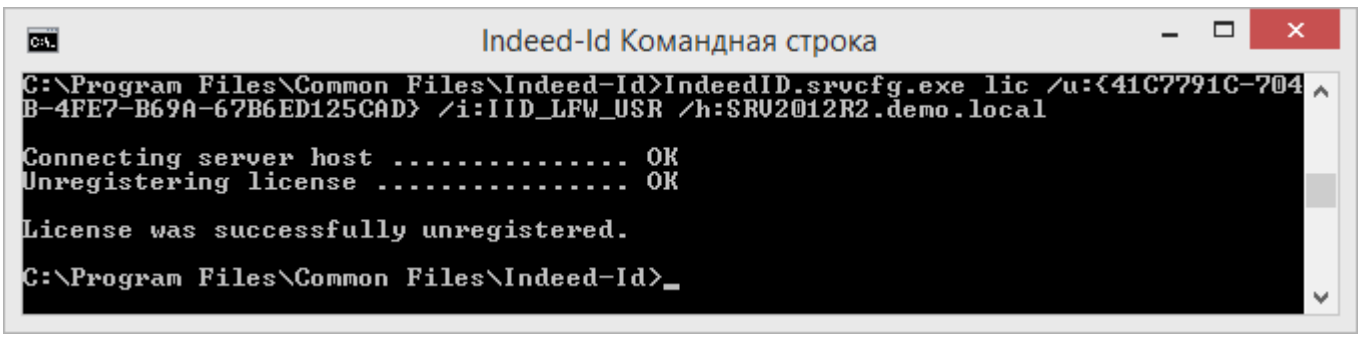
b) Просмотр количества действительных и примененных лицензий в подсистеме:



В командной строке выводятся следующие параметры:

- **Name** – имя лицензируемой подсистемы;
- **Description** – описание объекта лицензирования;
- **Embedded** – тип системы лицензирования (встроенная/не встроенная);
- **Limit** – количество действительных лицензий в подсистеме. Если отсутствуют действительные лицензии, параметр принимает значение 0;
- **Taken** – количество примененных лицензий в подсистеме. Если отсутствуют примененные лицензии, параметр принимает значение 0;
- **Licensed objects** – идентификатор лицензируемого объекта, выводится при наличии примененных лицензий.

c) Отзыв лицензии в подсистеме:

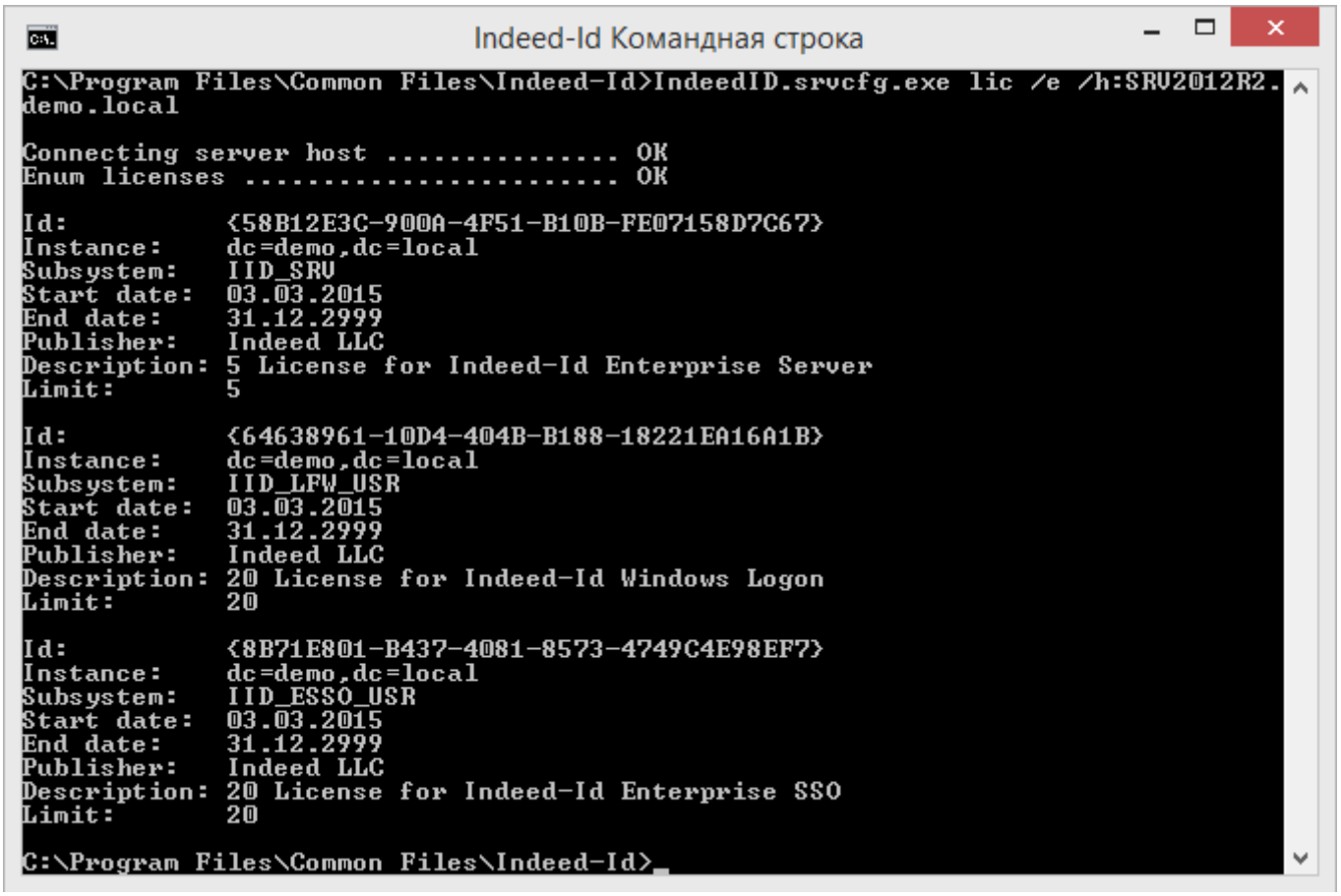


При отзыве лицензии необходимо указывать ее идентификатор. Ниже приведен пример файла лицензии с выделенным идентификатором:

```
<?xml version="1.0" encoding="utf-16"?>
<Indeed-Id>
  <License>
    <Id>{15E663C4-8AC9-47BD-8E6B-0637EA14FD5E}</Id>
    <Instance>dc=demo,dc=local</Instance>
    <SubsystemName>IID_LFW_USR</SubsystemName>
    <StartDate>01.01.2010</StartDate>
    <EndDate>31.12.2010</EndDate>
    <Description>License for local testing</Description>
    <Publisher>Indeed LLC</Publisher>
    <Limit>100</Limit>
  </License>
<Signature>78EE018B1A234ABD07691EDEA295847F501FF138DFB3F7A104A2DD0741328E9C0EAF57F45DC
7F38ADD484A41BFBD4602B33B90DA385AFEC8C2A3D37CD0D5B759</Signature>
</Indeed-Id>
```

Идентификатор лицензии также можно получить, воспользовавшись командой вывода параметров лицензии **lic /e**, как указано в пункте d:

d) Просмотр информации по всем зарегистрированным лицензиям всех подсистем:



Управление ключом шифрования

Генерация ключа шифрования выполняется после установки первого экземпляра Indeed-Id Enterprise Server. В версиях Enterprise Server до 2.0.133 включительно использовался алгоритм шифрования RC4 со 128-битным ключом шифрования. В последующих версиях используется шифрование с использованием AES256 и случайного вектора инициализации (Initialization vector).

При обновлении Indeed-Id Enterprise Server с версии 2.0.133 (и более ранних) алгоритм шифрования остается неизменным - RC4. Если вы хотите перейти на алгоритм шифрования AES в рамках обновления сервера Indeed, обратитесь, пожалуйста, в службу технической поддержки. Специалисты нашей компании дадут необходимые консультации и подготовят инструкцию для выполнения данной операции.

Сгенерированный ключ может быть сохранен в .key-файле и в реестре. В дальнейшем ключ шифрования может быть сгенерирован заново (с созданием нового файла или перезаписью старого) или восстановлен.

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

В случае повреждения или утраты ключа шифрования вы можете выполнить генерацию нового ключа или восстановление ключа. **Восстановление ключа шифрования** позволяет продолжить работу с заданными ранее параметрами системы и прежними аутентификаторами пользователей. После генерации нового ключа шифрования все заданные ранее параметры и обученные аутентификаторы будут недоступны.

При наличии дополнительных экземпляров Indeed-Id Enterprise Server необходимо выполнить экспорт ключа шифрования с первого экземпляра Indeed-Id Enterprise Server на дополнительные.

Генерация ключа шифрования

Для генерации ключа шифрования запустите утилиту IndeedID.srvcfg.exe с параметрами **/generatekey /f:"C:*keyname*.key" /h:server_name**, где:

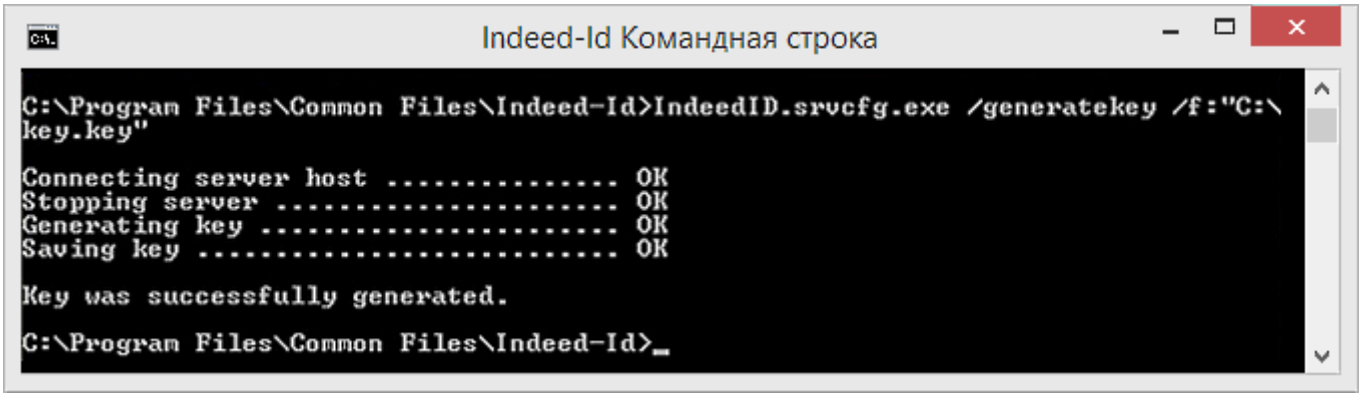
keyname – имя файла для сохранения ключа
server_name – имя сервера Indeed-Id в DNS формате.

Параметр /h необходимо указывать только в случаях, если запуск утилиты осуществляется с рабочей станции администратора. При запуске утилиты IndeedID.srvcfg.exe на сервере Indeed-Id задавать параметр /h не следует.

В результате в указанном каталоге рабочей станции, с которой происходит выполнение команды будет создан файл ключа шифрования с заданным именем. Если файл с заданным именем уже существует, будет предложено перезаписать его. Ключ шифрования будет передан на сервер Indeed-Id, указанный в параметре /h.

В версиях сервера ниже 1.5.165.0 для генерации ключа шифрования использовалась команда **/g.**

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



Экспорт ключа шифрования

Экспорт ключа шифрования требуется в случае установки дополнительных экземпляров Indeed-Id Enterprise Server. Экспорт ключа может быть осуществлён следующими способами:

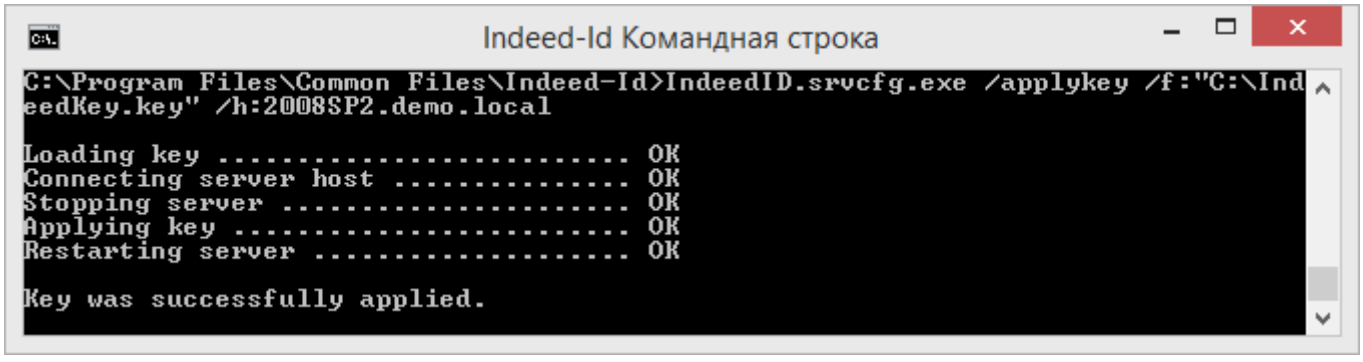
1) Экспорт ключа шифрования с рабочей станции администратора на сервер Indeed-Id.
2) Перенос вручную файла ключа шифрования на сервер Indeed-Id и выполнение команды экспорта на целевом сервере.

Ниже приведены примеры для каждого случая:

Для экспорта ключа шифрования с рабочей станции администратора на сервер Indeed-Id выполните на рабочей станции администратора команду IndeedID.srvcfg.exe с параметрами **/applykey /f:"key_path" /h:*server_name***, где

key_path – путь к файлу ключа шифрования на рабочей станции администратора
server_name – имя того сервера Indeed-Id в DNS формате, на который необходимо экспортировать ключ шифрования

Пример: Команда **IndeedID.srvcfg.exe /applykey /f:"C:\IndeedKey.key" /h:2008SP2.demo.local** передает ключ, хранящийся в файле IndeedKey.key на локальном диске C:\ на сервер Indeed-Id с именем 2008SP2.demo.local.



Для применения ключа шифрования из файла на сервере Indeed-Id выполните команду IndeedID.srvcfg.exe с параметрами **/applykey /f:"key_path"** , где *key_path* – путь к файлу ключа шифрования на целевом сервере Indeed-Id.

Пример: **IndeedID.srvcfg.exe /applykey /f:"C:\IndeedKey.key"**

В версиях Indeed-Id Enterprise Server ниже 1.5.165.0 для экспорта ключа шифрования использовалась команда **/e**.

Восстановление ключа шифрования

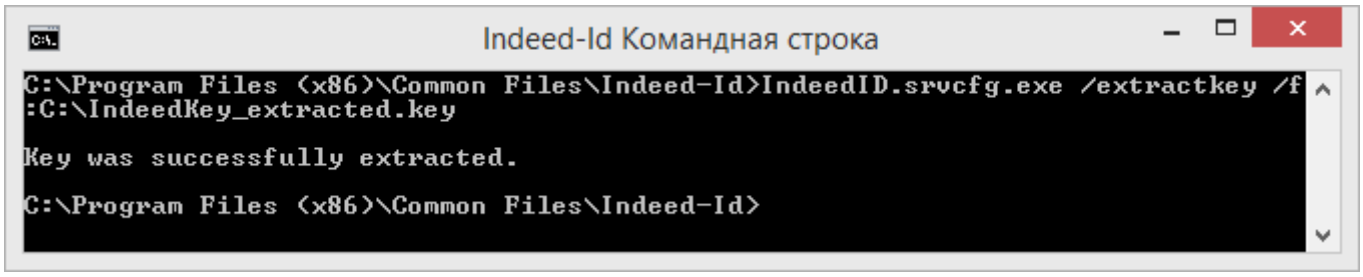
При наличии хотя бы одного функционирующего экземпляра Indeed-Id Enterprise Server вы можете восстановить ключ шифрования из реестра операционной системы, под управлением которой работает данный сервер.

Восстановление ключа шифрования выполняются непосредственно на сервере Indeed-Id. В целях безопасности удаленное выполнение данных команд не поддерживается.

Для восстановления ключа шифрования на сервере выполните команду **IndeedID.srvcfg.exe /extractkey /f:"C:\<Имя_Файла>.key"**. Вы можете указать любое имя файла, независимо от того, какое имя было указано при генерации ключа в процессе установки Indeed-Id Enterprise Server.

В версиях сервера ниже 1.5.165.0 для восстановления ключа шифрования использовалась команда **/i.**

Пример: Команда **IndeedID.srvcfg.exe /extractkey /f:"C:\IndeedKey_extracted.key"** выполняет запись ключа шифрования из реестра в файл IndeedKey_extracted.key на диске C:\.



Полученный файл можно в дальнейшем использовать при установке дополнительных экземпляров Indeed-Id Enterprise Server (см. **Экспорт ключа шифрования**).

Миграция данных Indeed-Id

Утилита **IndeedID.ExportImport.exe** предназначена для переноса всех данных системы (аутентификаторы и SSO-приложения пользователей, настройки пользователей, лицензии) из одного экземпляра системы Indeed-Id в другой.

Запуск утилиты необходимо производить на серверах Indeed-Id. Удаленное выполнение данных команд не поддерживается.

Пользователь, от имени которого выполняется запуск утилиты должен быть членом следующих групп безопасности:

- Локальный администратор
- Indeed-ID ESSO Admins
- Indeed-ID Server Admins
- Indeed-ID User Admins
- Для сброса пароля доменных учетных записей необходимо право **Сброс пароля** (Reset password) в домене, данные пользователей которого были импортированы при помощи утилиты.

Миграция данных состоит из 4 шагов:

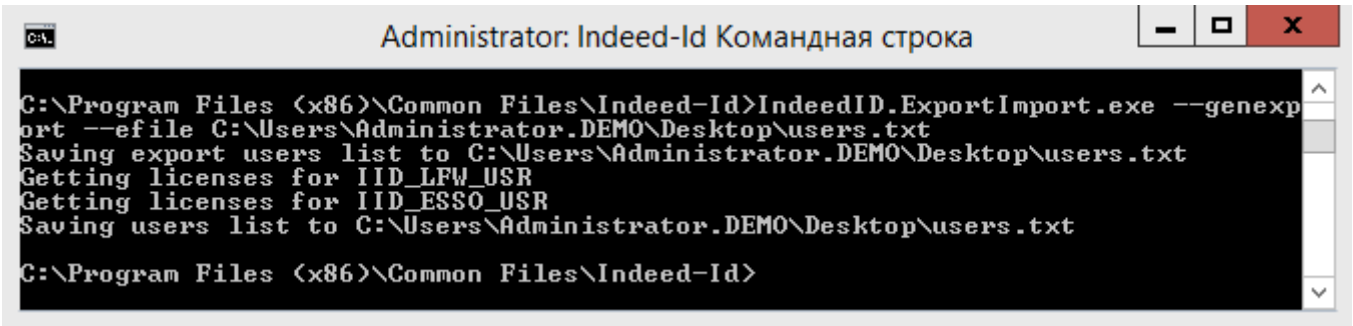
- Генерация файла экспорта пользователей
- Экспорт данных из текущего хранилища Indeed-Id
- Генерация файла импорта пользователей
- Импорт данных в новое хранилище Indeed-Id

Генерация файла экспорта пользователей

Перед извлечением данных о пользователях системы Indeed-Id из хранилища необходимо сформировать список пользователей системы. Для этого запустите в командной строке утилиту IndeedID.ExportImport.exe с параметрами ––**genexport** и ––**efile** с указанием имени текстового файла, в который необходимо вывести информацию о пользователях.

Пример:

IndeedID.ExportImport.exe ––genexport ––efile C:\Users\Administrator.DEMO\Desktop\users.txt



Данная команда создает файл users.txt на рабочем столе пользователя со списком пользователей домена, данные которых будут импортированы. Во время выполнения команды в этот файл записываются пользователи, которым разрешено использование WL или SSO. Чтобы добавить пользователя, которому не разрешено использование WL или SSO, необходимо вручную добавить данного пользователя в список, либо перед генерацией списка разрешить данному пользователю использование SSO или WL.

Пример содержимого файла:

WL:1;ESSO:1;FROM:CN=Анна Березова,CN=Users,DC=demo,DC=local

WL:1;ESSO:1;FROM:CN=Евгений Белов,CN=Users,DC=demo,DC=local

WL:1;ESSO:0;FROM:CN=Администратор,CN=Users,DC=demo,DC=local

где:

WL:1 – пользователю разрешено использование Windows Logon (применена лицензия для пользователя)

ESSO:0 – пользователю запрещено использование ESSO (не применена лицензия ESSO для пользователя)

CN=Анна Березова,CN=Users,DC=demo,DC=local – Уникальное Имя (Distinguished Name)

Экспорт данных из хранилища Indeed-Id

Экспорт данных выполняется при помощи файла со списком пользователей (см. **Генерация файла экспорта пользователей**). Для экспорта данных необходимо запустить утилиту **IndeedID.ExportImport.exe** с параметрами, определяющими файл со списком пользователей, каталог для выгрузки данных, пароль, которым будет защищен каталог с выгруженными данными и сам набор данных, которые необходимо извлечь из хранилища.

Пример:

IndeedID.ExportImport.exe ––export ––efile C:\Users\Administrator.DEMO\Desktop\users.txt ––storage C:\Users\Administrator.DEMO\Desktop\backup ––password Qwerty1 ––system 1 ––users 1 ––key C:\IndeedKey.key

где:

efile – Путь к файлу со списком пользователей

storage – Путь, по которому необходимо создать каталог для выгрузки данных

password – Пароль, который будет использован для защиты каталога с данными

Запомните или запишите этот пароль! Его необходимо будет ввести во время операции импорта данных.

system – Экспорт данных SSO приложений и SSO ролей. Варианты значения: 0 данные не экспортируются, 1 данные экспортируется.

users – Экспорт паролей, настроек, аутентификаторов, SSO аккаунтов, черного списка SSO пользователя. Варианты значения: 0 данные не экспортируются, 1 данные экспортируется.

key – Путь к файлу с ключом шифрования, который необходимо использовать для шифрования экспортируемых данных. Это может быть текущий ключ шифрования, или новый (созданный при развертывании сервера Indeed в новом домене).

Опциональный параметр, если не задан, то для шифрования используется ключ шифрования сервера, на котором происходит выполнение команды.

Пример вывода результата работы команды:

```
Exporting system data from DC=demo,DC=local to C:\Users\Administrator.DEMO\Desktop\backup
Saving system data to C:\Users\Administrator.DEMO\Desktop\backup\DC=demo,DC=local.system\system.sso.apps
Saving system data to C:\Users\Administrator.DEMO\Desktop\backup\DC=demo,DC=local.system\system.sso.roles
Exporting users from DC=demo,DC=local to C:\Users\Administrator.DEMO\Desktop\backup
Loading users list from C:\Users\Administrator.DEMO\Desktop\users.txt
============================================================
Exporting user data from CN=Евгений Белов,CN=Users,DC=demo,DC=local
Getting user data
Saving user data to C:\Users\Administrator.DEMO\Desktop\backup\CN=Евгений Белов,
CN=Users,DC=demo,DC=local.user\user.password
Getting user data
Saving user data to C:\Users\Administrator.DEMO\Desktop\backup\CN=Евгений Белов,
CN=Users,DC=demo,DC=local.user\user.settings
Getting user data
Saving user data to C:\Users\Administrator.DEMO\Desktop\backup\CN=Евгений Белов,
CN=Users,DC=demo,DC=local.user\user.authenticator
Getting user data
Saving user data to C:\Users\Administrator.DEMO\Desktop\backup\CN=Евгений Белов,
CN=Users,DC=demo,DC=local.user\user.sso.accounts
Getting user data
Saving user data to C:\Users\Administrator.DEMO\Desktop\backup\CN=Евгений Белов,
CN=Users,DC=demo,DC=local.user\user.sso.blacklist
Saving plugin data to C:\Users\Administrator.DEMO\Desktop\backup\CN=Евгений
Белов,CN=Users,DC=demo,DC=local.user\PluginData.AuthMethods.{AA612D5B-E708-41CA-B7E3
-7CEDDE28DF45}
Saving plugin data to C:\Users\Administrator.DEMO\Desktop\backup\CN=Евгений
Белов,CN=Users,DC=demo,DC=local.user\PluginData.AuthMethods.{42456525-8EC1-4AB1-97B8
-45AF8635D10F}
Saving plugin data to C:\Users\Administrator.DEMO\Desktop\backup\CN=Евгений
Белов,CN=Users,DC=demo,DC=local.user\PluginData.AuthMethods.{0AF65AD8-DB77-4B64-B489
-958D9B36E28C}
============================================================
Summary report for export operation
============================================================
System data processed successfully.
1 of 1 users processed successfully.
```

Если в процессе экспорта произошли ошибки, связанные с экспортом системных данных или пользовательских данных, то это будет отображено в разделе **Summary report for export operation**. Перед продолжением миграции убедитесь, что все необходимые данные успешно сохранены в файловое хранилище экспортированных данных.

В результате выполнения команды на рабочем столе появился каталог с именем **backup**, содержащий настройки системы и данные пользователей Indeed-Id.

Генерация файла импорта пользователей

Данная команда создает файл со списком пар, состоящих из уникальных имен пользователей домена **из которого переносятся данные** («старый» домен) и уникальных имен пользователей домена, **в который переносятся данные** («новый» домен). Данные пользователей «старого» домена будут мигрированы в данные пользователей «нового» домена.

Выполните вход на сервер Indeed-Id, активированный и запущенный в «новом» домене. Перенесите на сервер из «старого» домена пользовательский файл экспорта (*users.txt* см. **Генерация файла экспорта пользователей**) и хранилище данных Indeed-Id (каталог *backup* см. **Экспорт данных из хранилища Indeed-Id**).

Пары уникальных имён пользователей можно добавлять в файл вручную. Например, если имена пользователей «старого» и «нового» домена не совпадают и соответствие между ними не было установлено автоматически.

Для генерации пользовательского файла импорта запустите утилиту IndeedID.ExportImport.exe с параметрами, определяющими путь к файлам экспорта и импорта пользователей, а также путь к объекту контейнеру или подразделению), в котором располагаются пользователи «нового» домена.

Пример:

IndeedID.ExportImport.exe ––genimport ––efile C:\Users\Administrator.DEMO\Desktop\users.txt ––usersroot "ou=Indeed,dc=newdomain,dc=local" ––ifile C:\Users\Administrator.DEMO\Desktop\users2.txt

где:

efile – Путь к файлу со списком пользователей «старого» домена

usersroot – корневой путь, по которому будет происходит поиск пользователей в новом домене. Поиск также происходит в дочерних объектах.

ifile – Путь с указанием имени текстового файла, в который необходимо вывести информацию о пользователях «нового» домена.

Пример вывода командной строки после успешного выполнения команды:

Generating import users list from users.txt to users2.txt

Loading users list from users.txt

Saving users list to users2.txt

Пример строк в выходном файле users2.txt:

WL:1;ESSO:1;FROM:CN=Анна Березова,CN=Users,DC=demo,DC=local;TO:CN=Анна Березова,OU=Indeed,DC=demo,DC=local

WL:1;ESSO:1;FROM:CN=Евгений Белов,CN=Users,DC=demo,DC=local;TO:CN=Евгений Белов,OU=Indeed,DC=demo,DC=local

Импорт данных в хранилище

В процессе процедуры импорта произойдет копирование данных из каталога backup в хранилище Indeed-Id нового домена. Запустите на сервере Indeed-Id нового домена утилиту IndeedID/ExportImport.exe с параметрами, определяющими путь к файлу импорта пользователей (файл *users2.txt* см. **Генерация файла импорта пользователей**), путь к каталогу с экспортированными данными (каталог *backup* см. **Экспорт данных из хранилища Indeed-Id**), пароль для доступа к экспортируемым данным, параметры экспорта и ключ шифрования, которым необходимо расшифровать данные.

Пример:

IndeedID.ExportImport.exe ––import ––ifile C:\Users\Administrator.DEMO\Desktop\users2.txt ––storage C:\Users\Administrator.DEMO\Desktop\backup ––password Qwerty1 ––system 1 ––users 1 ––resetpwd 1 ––key C:\IndeedKey.key

где:

ifile – Путь к файлу импорта пользователей

storage – Путь к каталогу с экспортированными данными

password – Пароль, который был установлен на этапе экспорта данных из «старого» домена

system – Экспорт данных SSO приложений и SSO ролей. Варианты значения: 0 данные не экспортируются, 1 данные экспортируется.

users – Экспорт паролей, настроек, аутентификаторов, SSO аккаунтов, черного списка SSO пользователя. Варианты значения: 0 данные не экспортируются, 1 данные экспортируется.

resetpwd – Сброс доменного пароля пользователей на пароль, записанный в файловом хранилище Indeed-Id. Данная настройка позволяет избежать рассинхронизации пароля.

Для сброса пароля доменных учетных записей необходимо право **Сброс пароля** (Reset password) в «новом» домене.

key – Путь к файлу с ключом шифрования, который использовался для шифрования данных на этапе экспорта. Это может быть текущий ключ шифрования, или новый (созданный при развертывании сервера Indeed в новом домене).

Опциональный параметр, если не задан, то для расшифровки используется ключ шифрования сервера, на котором происходит выполнение команды.

При экспорте и импорте данных необходимо использовать один и тот же ключ шифрования.

Пример вывода командной строки после успешного выполнения команды:

```
Importing users from backup to DC=New,DC=local
Loading users list from users2.txt
============================================================
Importing user data from CN=Евгений Белов,CN=Users,DC=demo,DC=local to CN=Евгений
Белов,CN=Users,DC=newdomain,DC=local
Loading user data from backup\CN=Евгений Белов,CN=Users,DC=demo,DC=local.user\user.password
Putting user data
Loading user data from backup\CN=Евгений Белов,CN=Users,DC=demo,DC=local.user\user.settings
Putting user data
Loading user data from backup\CN=Евгений Белов,CN=Users,DC=demo,DC=local.user\user.authenticator
Putting user data
Loading user data from backup\CN=Евгений Белов,CN=Users,DC=demo,DC=local.user\user.sso.accounts
Putting user data
```

```
Loading user data from backup\CN=Евгений Белов,CN=Users,DC=demo,DC=local.user\user.sso.blacklist
Putting user data
Taking user license for IID_LFW_USR subsystem
============================================================
Summary report for import operation
============================================================
1 of 1 users processed successfully.
1 WL licenses are required, 1 are applied.
1 ESSO licenses are required, 1 are applied.
```

Если в процессе импорта произошли ошибки, связанные с импортом системных данных или пользовательских данных, то это будет отображено в разделе **Summary report for import operation**. Перед завершением миграции убедитесь, что все необходимые данные успешно перенесены в хранилище AD и необходимые лицензии применены для всех пользователей.

Проверка импортированных данных

Для проверки импортированных данных в «новом» домене установите на рабочих станциях пользователей компонент Indeed-Id Windows Logon и/или Indeed-Id Enterprise SSO Agent и необходимые провайдеры аутентификации Indeed-Id. Провайдеры аутентификации должны быть установлены и на всех серверах Indeed в «новом» домене.

После установки необходимого ПО проверьте вход в систему/приложение SSO с помощью аутентификаторов пользователей, которые использовались в «старом» домене.

Для проверки настроек пользователя (разрешения на обучение аутентификаторов, количество аутентификаторов, применение лицензий) перейдите в карточку пользователя в консоли управления Indeed EMC.

Управление паролями пользователей

Управление паролями пользователей включает генерацию (изменение) доменного пароля или его сброс на случайное значение.

Изменение доменного пароля на случайный

Генерация случайного пароля может осуществляться:

Автоматически:

- Сервером Indeed-Id при обучении первого аутентификатора.
- Компонентом Indeed-Id Windows® Logon по истечению срока действия текущего пароля или при срабатывании настройки **Требовать смену пароля при следующем входе в систему** (**User must change password at next logon**).
- Утилитой IndeedID.Password.Manager.exe (Менеджер паролей) по истечению срока действия текущего пароля после установки расписания смены паролей с помощью стандартного средства Windows "Планировщик заданий".

Автоматическая генерация случайного пароля активируется при выборе опции **Генерировать случайный пароль доменной учетной записи** на вкладке **Учетные записи** в карточке пользователя консоли управления Indeed EMC. При автоматической смене пароля на случайный пользователь получает соответствующее уведомление.

Вручную с помощью утилиты IndeedID.Password.Manager.exe (Менеджер паролей).

Смена текущего пароля на случайный выполняется только для пользователей Indeed-Id с установленным разрешением **Генерировать случайный пароль доменной учетной записи** по истечению срока действия текущего пароля.

Для запуска утилиты IndeedID.Password.Manager.exe необходимы права Indeed-Id Password Managers.

Генерация случайного пароля

С помощью утилиты IndeedID.Password.Manager.exe может выполняться генерация случайного доменного пароля Windows для:

- всех пользователей системы Indeed-Id
- пользователей системы Indeed-Id в указанном подразделении (OU)
- определенных пользователей

По умолчанию утилита IndeedID.Password.Manager.exe находится в каталоге C:\Program Files\Common Files\Indeed-Id[5].

Генерация случайного пароля для всех доменных пользователей

Для генерации случайного пароля всем доменным пользователям запустите утилиту IndeedID.Password.Manager.exe с параметрами **/change:domain.name** (**domain.name** - имя домена).

Пример:
Команда **IndeedID.Password.Manager.exe /change:demo.domain** выполняет генерацию случайного пароля для всех пользователей домена **demo.domain**. Также команду можно ввести без указания имени домена (**/change**).

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

Генерация случайного пароля для пользователей в определенном подразделении (OU)

Для генерации случайного пароля пользователям в определенном подразделении запустите утилиту IndeedID.Password.Manager.exe с параметрами **/change:domain.name/ou** (**ou** - имя подразделения, **domain.name** - имя домена).

Пример:

Команда **IndeedID.Password.Manager.exe /change:demo.domain/Sales** выполняет генерацию случайного пароля для всех пользователей в подразделении **Sales** домена **demo.domain**.

- Для подразделений второго уровня вложенности должно быть указано подразделение первого уровня, например: **/change:demo.domain/Sales1/Sales11**.

Генерация случайного пароля для определенных пользователей

Для генерации случайного пароля определенным пользователям запустите утилиту IndeedID.Password.Manager.exe с параметрами **/change:username@domain.name/ou** (**username** - имя пользователя, **ou** - имя подразделения, **domain.name** - имя домена).

Пример:

Команда **IndeedID.Password.Manager.exe /change:Ivanov@demo.domain/Sales** выполняет генерацию случайного пароля для учетной записи пользователя **Ivanov** в подразделении **Sales** домена **demo.domain**.

- В одной команде могут быть указаны имена нескольких пользователей, например: **/change:Ivanov@demo.domain /change:Petrova@demo.domain**).
- В команде может быть указан список пользователей, например: **/change:@UserAccounts.txt**. Список пользователей должен храниться в текстовом файле формата .txt.

Настройка расписания смены паролей

Настройку расписания смены паролей удобно реализовать с помощью средства ОС Windows «Планировщик заданий» (Task Scheduler). Настройте запуск утилиты IndeedID.Password.Manager.exe в соответствии с нужным периодом смены пароля. В свойствах задачи укажите **Выполнять для всех пользователей** и **Выполнить с наивысшими правами**. В поле **Программа или сценарий** введите путь к утилите IndeedID.Password.Manager.exe и добавьте ключ **/change:** в параметрах которого укажите домен, подразделение и имя пользователя или группы пользователей, которым требуется сменить пароль.

Пример:

"C:\Program Files\Common Files\Indeed-Id\IndeedID.Password.Manager.exe" /change:demo.domain/Users/Ivan Petrov

Сообщения о событиях смены пароля

Результаты работы Менеджера паролей выводятся на экран консоли и сохраняются в виде сообщений в журнале событий.

- По умолчанию в журнале событий сохраняются сообщения обо всех событиях смены паролей, как успешных, так и неуспешных. Для того, чтобы в журнале событий не сохранялись никакие сообщения используйте команду **/QuietLog**.

- На экран консоли по умолчанию выводятся все сообщения, как сообщения об успешно выполненных командах, так и сообщения об ошибках. Для того, чтобы на экран консоли не выводились никакие сообщения, используйте команду **/QuietConsole**.

Примером ошибок, которые будут фиксироваться, если заданы ключи /QuietLog и /QuietConsole, являются запуск утилиты IndeedID.Password.Manager.exe для несуществующего имени домена или подразделения, для несуществующего пользователя, для несуществующего файла со списком пользователей.

Сброс доменного пароля на случайный

С помощью утилиты IndeedID.Password.Manager.exe может выполняться сброс или установка доменного пароля Windows для:

- всех пользователей системы Indeed-Id
- пользователей системы Indeed-Id в указанном подразделении (OU)
- определенных пользователей

По умолчанию утилита IndeedID.Password.Manager.exe находится в каталоге C:\Program Files\Common Files\Indeed-Id[6].

Требования к окружению для сброса доменного пароля пользователей:

Пользователь, запускающий утилиту IndeedID.Password.Manager.:

- Должен обладать правом **Сброс пароля** (Reset Password) для объектов **Пользователь** (User) в Active Directory
- Входить в группу безопасности **Indeed-Id Password Managers**

Пользователи, для которых будет выполняется сброс паролей:

- Должны иметь разрешение на генерацию случайного пароля (Опция **Генерировать случайный пароль доменной учетной записи** на вкладке *Учетные записи* в карточке пользователя Indeed EMC).
- Наличие ранее установленного доменного пароля и зарегистрированных в Indeed EA(ESSO) аутентификаторов не требуется

Сброс пароля на случайный для всех доменных пользователей

Для сброса пароля всем доменным пользователям запустите утилиту IndeedID.Password.Manager.exe с параметрами **/reset:domain.name** (**domain.name** - имя домена).

Пример:
IndeedID.Password.Manager.exe /reset:demo.domain выполняет сброс существующих доменных паролей на случайные пароли для всех пользователей домена **demo.domain**. Также команду можно ввести без указания имени домена (**/reset**).

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

Сброс пароля на случайный для пользователей в определенном подразделении (OU)

Для сброса пароля на случайный пользователям в определенном подразделении запустите утилиту IndeedID.Password.Manager.exe с параметрами **/reset:domain.name/ou** (**ou** - имя подразделения, **domain.name** - имя домена).

Пример:

Команда **IndeedID.Password.Manager.exe /reset:demo.domain/Sales** выполняет сброс существующих доменных паролей на случайные пароли для всех пользователей в подразделении **Sales** домена **demo.domain**.

- Для подразделений второго уровня вложенности должно быть указано подразделение первого уровня, например: **/reset:demo.domain/Sales1/Sales11**.

Сброс доменного пароля для определенных пользователей

Для сброса существующего пароля на случайный определенным пользователям запустите утилиту IndeedID.Password.Manager.exe с параметрами **/reset:username@domain.name/ou** (**username** - имя пользователя, **ou** - имя подразделения, **domain.name** - имя домена).

Пример:

Команда **IndeedID.Password.Manager.exe /reset:Ivanov@demo.domain/Sales** выполняет сброс установленного доменного пароля на случайный учетной записи пользователя **Ivanov** в подразделении **Sales** домена **demo.domain**.

- В одной команде могут быть указаны имена нескольких пользователей, например: **/reset:Ivanov@demo.domain /reset:Petrova@demo.domain**).
- В команде может быть указан список пользователей, например: **/reset:@UserAccounts.txt**. Список пользователей должен храниться в текстовом файле формата .txt.

Команды **\change** и **\reset** могут использоваться одновременно.

Пример:

IndeedID.Password.Manager.exe /reset:Ivanov@demo.domain /change:Petrova@demo.domain

Мониторинг доменных пользователей

Мониторинг доменных пользователей осуществляется с помощью утилиты **IndeedID.AD.Users.Info.exe**.

Утилита IndeedID.AD.Users.Info.exe позволяет:

- Получать сведения обо всех пользователях домена
- Получать сведения только о пользователях Indeed-Id
- Получать сведения о пользователях в указанном подразделении/контейнере
- Сохранять собранные сведения в файл

Параметры и примеры запуска утилиты IndeedID.AD.Users.Info.exe

При запуске утилиты без параметров выполняется сбор сведений обо всех доменных пользователях без сохранения полученной информации в файл.

Доступ к утилите осуществляется при помощи Командной строки Indeed-Id.

При выводе результатов команды в консоль и сохранении результатов в .csv файл сведения о пользователях отображаются в виде таблицы, где первая графа содержит имя пользователя, вторая графа - идентификатор пользователя (значение 1 соответствует пользователю Indeed-Id, значение 0 - обычному пользователю), третья графа отображает количество обученных аутентификаторов пользователя, четвертая содержит user friendly name, пятая – user LDAP name.

Основные параметры запуска:

-target "SomeDomain/SomeOU" – указание подразделения/контейнера

-OnlyIIDUsers – формирование отчета только по пользователям Indeed-Id

-dividor ":" – использование разделителя (вместо двоеточия может быть использован любой другой символ)

-? – вывод справки

> C:\SomeFile.csv – указание файла для сохранения полученной информации (при указании файла результаты команды в консоль не выводятся)

Поддерживается указание всех параметров и с использованием символа **/**.

Примеры команд:

- **IndeedID.AD.Users.Info.exe > C:\Log.csv** – получение сведений обо всех пользователях домена с сохранением в файл Log.csv на локальном диске C:\.
- **IndeedID.AD.Users.Info.exe -onlyIIDUsers** – получение сведений обо всех пользователях Indeed-Id в домене без сохранения информации в файл.
- **IndeedID.AD.Users.Info.exe -target "demo.domain/Users" > C:\log.csv** – получение сведений обо всех пользователях контейнера Users с сохранением в файл Log.csv на локальном диске C:\.
- **IndeedID.AD.Users.Info.exe -OnlyIIDUsers -target "demo.domain/Users" > C:\log.csv** – получение сведений о пользователях Indeed-Id контейнера Users с сохранением в файл Log.csv на локальном диске C:\.

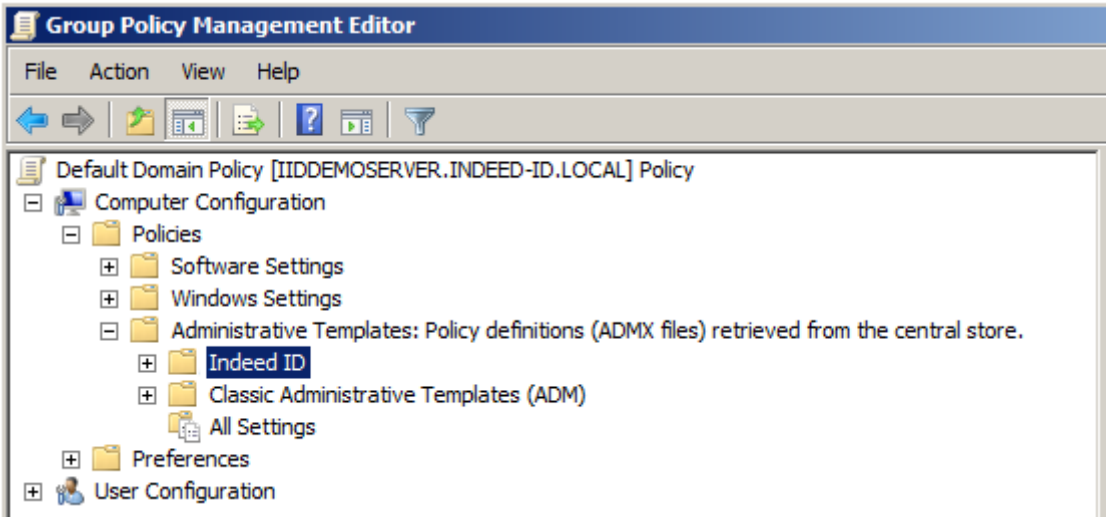
Групповые политики Indeed-Id

Некоторые настройки системы Indeed EA/ESSO задаются групповыми политиками Microsoft. Перед настройкой групповой политики добавьте административные шаблоны Indeed в список шаблонов групповой политики.

Добавление административных шаблонов

Для добавления административных шаблонов Indeed-Id выполните следующие действия:

1. Скопируйте файлы шаблонов из каталога дистрибутива Indeed-Id Admin Pack\version\Misc\GroupPolicyTemplates в центральное хранилище ADMX-файлов на контроллере домена (папка **C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions**)[7].
2. После загрузки они станут доступны в оснастке **Редактор групповых политик** (Group Policy Manager Editor):



3. Шаблоны политик Indeed-Id Paste добавляются в раздел **Конфигурация пользователя** (User Configuration). Шаблоны всех остальных политик и провайдеров аутентификации добавляются в раздел **Конфигурация компьютера** (Computer Configuration).

[7] При использовании локального хранилища ADMX-файлов поместите шаблоны Indeed-Id в C:\Windows\PolicyDefinitions.

Настройка групповых политик

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

Продукт Indeed-Id Admin Pack :

Настройка политик Authenticators

Группа политик **Authenticators**, определяет параметры работы с аутентификаторами пользователей Indeed-Id.

Принудительное переобучение аутентификатора

Политика применяется к рабочим станциям пользователей и позволяет настроить принудительное переобучение аутентификатора при наступлении срока "Предложение о переобучении аутентификатора через (дней)", задаваемого политикой **Срок действия аутентификатора**.

Не задан (Not Configured) или Отключен (Disabled)

Принудительно переобучение аутентификатора при достижении срока предложения переобучения не включено. Пользователь может отказаться от переобучения. Значение по умолчанию – Не задан.

Включен (Enabled)

Пользователь не сможет отказаться по переобучения аутентификатора при достижении срока, когда будет выводиться предложение о переобучении.

Запретить при старте Indeed-Id Enterprise SSO Agent отображать сообщения о сроке действия аутентификаторов

Политика применяется к рабочим станциям пользователей и определяет режим отображения сообщения о сроке действия аутентификаторов отображаться не будут.

Не задан (Not Configured) или Отключен (Disabled)

При старте Indeed-Id Enterprise SSO Agent **будут** отображаться сообщения об истечении срока действия аутентификатора. Значение по умолчанию – Не задан.

Включен (Enabled)

При старте Indeed-Id Enterprise SSO Agent **не будут** отображаться сообщения об истечении срока действия аутентификатора.

Срок действия аутентификатора

Политика применяется к серверам Indeed EA/ESSO и задает параметры срока действия аутентификаторов Indeed-Id.

Не задан (Not Configured) или Отключен (Disabled)

Срок жизни аутентификатора не учитывается. Значение по умолчанию – Не задан.

Включен (Enabled)

Срок жизни аутентификатора учитывается в соответствии с настройками

- **Разрешать переобучение аутентификатора через (дней)**

  Параметр задает минимальный срок жизни аутентификатора в днях до того момента, когда будет возможно его переобучение.

- **Предупреждать об истечении аутентификатора через (дней)**

  Параметр задает срок с момента обучения аутентификатора в днях до того момента, с которого пользователь будет получать уведомление о скором истечении аутентификатора.

- **Предложение о переобучении аутентификатора через (дней)**

  Параметр задает срок с момента обучения аутентификатора в днях до того момента, с которого пользователь будет получать предложение переобучить аутентификатор.

- **Идентификаторы провайдеров, к которым будет применяться политика**

  Список способов входа в виде идентификаторов в системе (GUID), для которых будет учитываться срок жизни аутентификаторов

  Список идентификаторов провайдеров:

  - **Digent** - {89E350C9-4F79-4EB9-988E-FC24161FE2E9}
  - **eTokenPASS** - {EA588135-CED1-4922-B640-924C94A91904}
  - **Futronic** - {A0EF00AD-1EEB-4d48-8BCF-06E19CD5585F}
  - **Z2USB** - {CB5109DA-B575-422C-8805-524FE12B02F5}
  - **Z2USB+PIN** - {1EDFD6E1-FD66-4a5b-971A-CBA0C611BA9B}
  - **OMNIKEY** - {AF1018CD-C275-44c1-9EFF-C7541D1CFC53}
  - **OMNIKEY+PIN** - {199B8FA8-FA9D-4ED8-941D-F86A5C681E0C}
  - **OTM** - {AA612D5B-E708-41CA-B7E3-7CEDDE28DF45}
  - **Smartcard** - {42456525-8EC1-4AB1-97B8-45AF8635D10F}
  - **Smartcard+PIN** - {42456525-8EC1-4AB1-97B8-45AF8635D10F}
  - **OMNIKEY+PalmSecure** - {38219C55-E056-47F2-B365-288A12880872}
  - **Passcode** - {F696F05D-5466-42B4-BF52-21BEE1CB9529}

История аутентификаторов

Политика применяется к серверам Indeed EA/ESSO и задает количество удаленных и перерегистрированных аутентификаторов в истории. Пользователю запрещено регистрировать новые и перерегистрировать существующие аутентификаторы, если они сохранены в истории. Если в качестве размера истории указан '0', то действие, связанное с этой политикой выполнено не будет.

Не задан (Not Configured) или Отключен (Disabled)

История аутентификаторов не сохраняется и не учитывается. Значение по умолчанию – Не задан.

Включен (Enabled)

История аутентификаторов учитывается при обучении/переобучении аутентификаторов

- **Размер истории аутентификаторов**

  Параметр задает максимальное количество аутентификаторов, которые будут храниться в истории.

- **Идентификаторы провайдеров, к которым будет применяться политика**

  Список способов входа в виде идентификаторов в системе (GUID), для которых будет учитываться история при обучении/переобучении аутентификаторов

Список идентификаторов провайдеров:

- **Digent** - {89E350C9-4F79-4EB9-988E-FC24161FE2E9}
- **eTokenPASS** - {EA588135-CED1-4922-B640-924C94A91904}
- **Futronic** - {A0EF00AD-1EEB-4d48-8BCF-06E19CD5585F}
- **Z2USB** - {CB5109DA-B575-422C-8805-524FE12B02F5}
- **Z2USB+PIN** - {1EDFD6E1-FD66-4a5b-971A-CBA0C611BA9B}
- **OMNIKEY** - {AF1018CD-C275-44c1-9EFF-C7541D1CFC53}
- **OMNIKEY+PIN** - {199B8FA8-FA9D-4ED8-941D-F86A5C681E0C}
- **OTM** - {AA612D5B-E708-41CA-B7E3-7CEDDE28DF45}
- **Smartcard** - {42456525-8EC1-4AB1-97B8-45AF8635D10F}
- **Smartcard+PIN** - {42456525-8EC1-4AB1-97B8-45AF8635D10F}
- **OMNIKEY+PalmSecure** - {38219C55-E056-47F2-B365-288A12880872}
- **Passcode** - {F696F05D-5466-42B4-BF52-21BEE1CB9529}

Настройка политик Windows® Logon

Группа политик **Windows® Logon** определяет параметры клиентской части системы и применяется как для рабочих станций, так и для серверов Indeed EA/ESSO.

Автоматическая идентификация пользователей

Политика включает режим автоматической идентификации пользователей. Данный режим позволяет выполнить вход в систему без указания имени пользователя. Имя пользователя определяется автоматически по предоставленному аутентификатору.

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.

Для корректной работы данная политика должна быть включена на всех серверах Indeed-Id и на всех рабочих станциях пользователей. Ниже приведено описание возможных состояний политики.

Не задан (Not Configured) или Отключен (Disabled)

При входе в операционную систему пользователь должен указать свое имя в домене (выбрать из списка последних входивших пользователей или ввести вручную). Значение по умолчанию – Не задан.

Включен (Enabled)

При входе в операционную систему пользователю достаточно предоставить аутентификатор, указание имени пользователя не требуется.

Автоматический выход из системы при смене карты

Включение политики позволяет совершать автоматический выход из операционной системы после извлечения карты текущего пользователя и предоставления карты другого пользователя.

При одновременном использовании с политикой "Автоматическая идентификация пользователей" позволяет реализовать сценарий автоматической смены пользователя в операционной системе при смене карты в считывателе. Политика применяется для рабочих станций пользователей.

Не задан (Not Configured) или Отключен (Disabled)

После извлечения карты из считывателя завершение сеанса работы пользователя производиться не будет.

Если политика выключена, то после извлечения карты из считывателя и прикладывании карты другого пользователя завершение сеанса работы пользователя производиться не будет[8]. Значение по умолчанию – Не задан.

Включен (Enabled)

После извлечения карты из считывателя произойдет заданное политикой действие: завершение или отключение сессии текущего пользователя.

- **Завершение сессии пользователя –** выход из операционной системы пользователя, чья карта была извлечена. Все открытые файлы и приложения текущей сессии будут принудительно закрыты.
- **Отключение сессии пользователя –** смена активной сессии пользователя на сессию пользователя, чья карта была приложена. Все открытые файлы и приложения текущей сессии не будут закрыты.

При одновременном использовании с политикой "Автоматическая идентификация пользователей" позволяет реализовать сценарий автоматической смены пользователя в операционной системе при смене карты в считывателе.

Для корректной совместной работы политик **Автоматическая идентификация пользователей** и **Автоматический выход из системы при смене карты** необходимо включить политику «Разрешить или запретить программам использование специального сочетания клавиш (Disable or enable software Secure Attention Sequence)» и указать значение «Службы и приложения специальных возможностей (Services and Ease of Access Applications)».

Политика «Разрешить или запретить программам использование специального сочетания клавиш (Disable or enable software Secure Attention Sequence)» находится в разделе *Конфигурация компьютера – Политики – Административные шаблоны – Компоненты Windows – Параметры входа Windows* (Computer Configuration - Administrative Templates - Windows Components - Windows Logon Options) оснастки Управление групповой политикой (Group Policy Management).

[8] Поведение при извлечении смарт-карты также зависит от настройки стандартной групповой политики Microsoft «Интерактивный вход в систему: поведение при извлечении смарт-карты».

Выбор автоматической идентификации по умолчанию

Политика включает режим выбора автоматической идентификации по умолчанию. Режим позволяет произвести выбор автоматической идентификации пользователя по умолчанию при входе в операционную систему и в текущей пользовательской сессии (сценарии UAC и т.п.). Политика применяется для рабочих станций пользователей.

Не задан (Not Configured) или Отключен (Disabled)

Способ входа «Автоидентификация» не будет использован как способ входа по умолчанию. В этом случае необходимо будет выбирать способ входа «Автоидентификация» вручную. Значение по умолчанию – Не задан.

Включен (Enabled)

При использовании автоматической идентификации способ входа «Автоидентификация» будет использоваться как способ входа по умолчанию.

При включении политики необходимо определить ситуации, при которых способ входа «Автоидентификация» будет использоваться по умолчанию:

- Выбор автоматической идентификации при входе

  Если опция включена, то при входе в операционную систему способом входа по умолчанию будет «Автоидентификация».

- Выбор автоматической идентификации в существующей сессии

  Если опция включена, то при запросе аутентификации в рамках сессии пользователя (например, при запуске приложения от имени администратора) способом входа по умолчанию будет «Автоидентификация».

Отключить аутентификацию Indeed EA Windows Logon в сессии пользователя

Политика позволяет использовать стандартные способы аутентификации Windows внутри открытой сессии пользователя в операционной системе.

Не задан (Not Configured) или Отключен (Disabled)

Способы аутентификации Indeed будут использоваться в текущей сессии пользователя в операционной системе (например, при RDP-подключении или запуске приложений от имени другого пользователя). Значение по умолчанию – Не задан.

Включен (Enabled)

Внутри сессии пользователя в операционной системе будут использоваться стандартные способы аутентификации Windows, а аутентификация через Indeed будет отключена.

Таймаут выполнения действия при извлечении смарт-карты

Политика определяет продолжительность стандартного и сервисного таймаута после извлечения устройства аутентификации.

Политика задает интервал времени в секундах между извлечением смарт-карты и действием, выполняемым согласно политике Windows "Интерактивный вход: поведение при извлечении смарт-карты" (Interactive logon: Smart-card enhanced removal behavior).

Наличие стандартного таймаута позволяет предотвратить автоматическую блокировку компьютера при случайном извлечении устройства аутентификации.

Наличие сервисного таймаута позволяет предотвратить автоматическую блокировку компьютера в случаях, когда извлечение используемого устройства аутентификации необходимо (обучение дополнительного аутентификатора, получение доступа в систему от имени другой учетной записи по другому аутентификатору и т. п.). Для активации сервисного таймаута перед извлечением устройства необходимо нажать и удерживать комбинацию клавиш **[Ctrl]+[L]**.

Не задан (Not Configured) или Отключен (Disabled)

Таймаут перед автоматической блокировкой рабочей станции не предоставляется. Значение по умолчанию – Не задан.

Включен (Enabled)

При извлечении устройства аутентификации будет использоваться установленный сервисный таймаут.

Принудительное завершение сессии пользователя

Политика позволяет принудительно завершать сессию пользователя, если поведение при извлечении смарт-карты установлено следующим образом: Принудительный выход из системы (Force logoff).

При принудительном завершении возможна потеря несохраненных данных пользовательских приложений.

Не задан (Not Configured) или Отключен (Disabled)

При использовании политики Windows "Интерактивный вход: поведение при извлечении смарт-карты" (Interactive logon: Smart-card enhanced removal behavior) с установленным значением Принудительный выход из системы (Force Logoff) пользователю будет предложено сохранить данные и завершить работу запущенных приложений. Только после этого будет выполнен выход из операционной системы. Значение по умолчанию – Не задан.

Включен (Enabled)

При использовании политики Windows "Интерактивный вход: поведение при извлечении смарт-карты" (Interactive logon: Smart-card enhanced removal behavior) с установленным значением Принудительный выход из системы (Force Logoff) завершение сессии пользователя произойдет мгновенно. Несохраненные данные будут утеряны.

Настройки Credential Provider

Политика применяется для рабочих станций под управлением **Microsoft Windows Vista и более поздних версий** операционных систем, на которых установлен компонент Indeed-Id Windows® Logon. Данная политика определяет отображение способов входа в систему, доступных пользователю.

Не задан (Not Configured) или Отключен (Disabled)

В списке способов входа в операционную систему будут отображаться только способы аутентификации Indeed-Id. Значение по умолчанию – Не задан.

Включен (Enabled)

В списке способов входа в операционную систему будут отображаться указанные способы входа. При установленном значении "**Все способы**" в списке способов входа доступны все возможные способы аутентификации.

При установленном значении "**Только Indeed-Id**" в списке способов входа доступны только способы аутентификации Indeed-Id. Стандартный способ аутентификации "Пароль" недоступен.

При установленном значении "**Все, кроме пароля**" в списке способов входа доступны способы аутентификации Indeed-Id и стандартные способы аутентификации Windows. Способ аутентификации "Пароль" недоступен.

Политика не оказывает влияния на выбор способов аутентификации в приложениях Indeed-Id Windows® Logon, Indeed-Id Enterprise SSO Agent и Indeed-Id Управление аутентификаторами.

Не скрывать системное сообщение о смене пароля пользователя

Политика применяется для рабочих станций под управлением **Microsoft Windows Server 2003 и Windows XP** и определяет, нужно ли скрывать системное сообщение об истечении срока действия пароля пользователя или нет.

Не задан (Not Configured) или Отключен (Disabled)

При входе пользователя в операционную систему с истекающим сроком действия пароля, пароль автоматически меняется. Пользователь получает сообщение «Пароль был автоматически изменен». Сообщение Windows о скором истечении срока действия пароля не отображается. Значение по умолчанию – Не задан.

Включен (Enabled)

При входе пользователя в операционную систему, с истекающим сроком действия пароля отображается сообщение Windows о скором истечении срока действия пароля. Если пользователь подтвердит смену пароля, то пароль изменится на случайный, иначе пароль не будет изменен (смена пароля на случайный произойдет после того как срок действия пароля полностью истечет).

Запрещать использование способа входа «Пароль»

Политика применяется для рабочих станций пользователей и определяет параметры отображения способа входа «Пароль» в списке способов аутентификации Indeed.

Не задан (Not Configured) или Отключен (Disabled)

При входе в операционную систему будет доступна аутентификация по паролю. Значение по умолчанию – Не задан.

Включен (Enabled)

Способ входа «Пароль» будет отображаться в соответствии с заданными параметрами:

- **Запрещать использование способа входа "Пароль" при аутентификации в ОС** – определяет сценарии, при которых пользователю будет недоступен способ аутентификации по доменному паролю:
  - Всегда
  - Только при локальном входе
  - Только при удаленном входе
- **Разрешать использование пароля при недоступности сервера –** действует при отсутствии кэшированных данных пользователя на локальной рабочей станции.

Любой доменный пользователь без разрешения технологии аутентификации Indeed не сможет выполнить вход на рабочую станцию с установленным компонентом Indeed-Id Windows Logon, при отсутствии связи с сервером Indeed EA и настройках политики:

"Запрещать использование способа входа "Пароль" при аутентификации в ОС": **Всегда**

"Разрешать использование пароля при недоступности сервера": **Отключено**

В комбинации:

"Запрещать использование способа входа "Пароль" при аутентификации в ОС": **Только при локальном входе** и "Разрешать использование пароля при недоступности сервера": **Отключено**.

Пользователи без разрешения на использование технологии аутентификации Indeed не смогут войти локально.

В комбинации:

"Запрещать использование способа входа "Пароль" при аутентификации в ОС": **Только при удаленном входе** и "Разрешать использование пароля при недоступности сервера": **Включено**. **Пользователи без разрешения на использование технологии аутентификации Indeed не смогут войти удаленно**.

Настройка политик ESSO

Группа политик ESSO регулирует общие настройки ESSO, параметры работы Indeed-Id Enterprise SSO Agent и Indeed-Id ESSO SAP GUI Module. Политики группы распространяются на рабочие станции пользователей.

Параметры ESSO Agent

Разрешить Indeed-Id Enterprise SSO Agent запускать «Мастер обучения первого аутентификатора» при входе в операционную систему

Данную политику следует использовать в случае, если на рабочей станции установлены компоненты Indeed-Id Windows® Logon и Indeed-Id Enterprise SSO Agent, но в обучении аутентификатора при входе в систему нет необходимости.

Не задан (Not Configured) или Включен (Enabled)

«Мастер обучения первого аутентификатора» будет запускаться при входе в систему компонентами Indeed-Id Windows® Logon и Indeed-Id Enterprise SSO Agent (если у пользователя нет обученных аутентификаторов). Значение по умолчанию – Не задан.

Отключен (Disabled)

«Мастер обучения первого аутентификатора» не будет запускаться приложением Indeed-Id Enterprise SSO Agent при входе в систему.

Защищенный рабочий стол

Разрешить приложению Indeed-Id Enterprise SSO Agent принудительно переключаться на свой рабочий стол, если он был переключен сторонним приложением на стандартный рабочий стол во время процедуры аутентификации пользователя.

Не задан (Not Configured) или Отключен (Disabled)

Indeed-Id Enterprise SSO Agent не будет принудительно переключать рабочий стол пользователя, если он используется другим приложением. Значение по умолчанию – Не задан.

Включен (Enabled)

Indeed-Id Enterprise SSO Agent будет принудительно переключать рабочий стол пользователя на свой собственный, если он используется другим приложением.

Параметры ESSO Common

Включить сжатие данных ESSO

Включение дополнительного сжатия данных SSO, передаваемых между клиентом и сервером. Сжатие данных производится при первом сохранении модифицированных данных ESSO и позволяет уменьшить объем сетевого трафика и занимаемого места в хранилище.

Политику необходимо использовать только в случае ограниченных каналов связи между клиентом и сервером (не более 1Мбит) и большого числа SSO приложений с объемными шаблонами (общий размер файлов шаблонов всех приложений 2Мб и более).

В случае включения данной политики она должна быть применена на всех рабочих станциях с ESSO Agent и всех серверах Indeed EMC, работающих в одном экземпляре системы.

Не задан (Not Configured) или Отключен (Disabled)

Дополнительное сжатие данных отключено. Значение умолчанию - Не задан.

Включен (Enabled)

Дополнительное сжатие данных включено. Все данные, передаваемые на сервер и обратно Агентом ESSO и консолью управления EMC будут дополнительно сжаты.

Параметры ESSO SAP GUI Module

Политики данного раздела необходимо распространять только на те рабочие станции пользователей, на которых установлен компонент Indeed-Id ESSO SAP GUI Module.

Включить предупреждение SAP GUI

Политика включает скрываемое по умолчанию в SAP GUI сообщение о подключении скрипта к приложению.

Не задан (Not Configured) или Отключен (Disabled)

Сообщение о подключении скрипта к приложению SAP не отображается. Значение умолчанию - Не задан.

Включен (Enabled)

Сообщение о подключении скрипта к приложению SAP отображается.

Список SAP System IDs

Политика позволяет задать список System IDs, для которых будет работать Indeed-Id ESSO SAP GUI Module.

Не задан (Not Configured) или Отключен (Disabled)

Indeed-Id ESSO SAP GUI Module будет работать для всех идентификаторов системы. Значение умолчанию - Не задан.

Включен (Enabled)

Indeed-Id ESSO SAP GUI Module будет работать только для указанных в политике идентификаторов системы.

Настройка политик Random Password Policy

Группа политик, определяющих параметры генерации доменного пароля Windows.

Длина генерируемого пароля Windows

Политика применяется к серверам Indeed-Id и рабочим станциям пользователей и позволяет задать длину генерируемого пароля.

Не задан (Not Configured) или Отключен (Disabled)

Используется стандартная длина пароля - 63 символа. Значение по умолчанию – Не задан.

Включен (Enabled)

Длина пароля может быть изменена как в бо̀льшую, так и в меньшую сторону.

Набор символов генерируемого пароля Windows

Политика применяется к серверам Indeed-Id и рабочим станциям пользователей и позволяет задать набор символов генерируемого пароля.

Не задан (Not Configured) или Отключен (Disabled)

При генерации пароля будут использоваться следующие группы символов:

- Латинские символы в верхнем регистре (A - Z)
- Латинские символы в нижнем регистре (a - z)
- Цифры (0 - 9)
- Специальные символы (!, $, #, %)

Значение по умолчанию – Не задан.

Включен (Enabled)

Набор символов, которые будут использоваться при генерации доменного пароля Windows может быть определен вручную. Поддерживаются латинские и кириллические символы, специальные символы и цифры.

Настройка политик Client Connection

Группа политик, определяющих параметры соединения рабочих станций пользователей с серверами Indeed-Id.

Использовать RODC

Политика применяется к рабочим станциям пользователей и позволяет им использовать контроллеры домена только для чтения (Rread-Only Domain Controller) для поиска серверов Indeed EA/ESSO.

Если в инфраструктуре предприятия используются домены только для чтения и при обращении к серверам Indeed-Id с рабочих станций пользователей, находящихся в таких доменах, наблюдаются значительные временные задержки, то включение данной политики может сократить подобные задержки.

Не задан (Not Configured) или Отключен (Disabled)

При поиске контроллера домена в процессе обращения к серверам Indeed-Id с рабочих станцией пользователей контроллеры домена только для чтения учитываться в поиске не будут. Значение умолчанию - Не задан.

Включен (Enabled)

При поиске контроллера домена в результате обращения к серверам Indeed-Id с рабочих станцией пользователей контроллеры домена только для чтения будут учитываться в поиске.

Предпочтительные серверы Indeed EA/ESSO

Политика применяется к рабочим станциям пользователей и позволяет задать список серверов Indeed EA/ESSO к которым необходимо обращаться, если в сайте Active Directory, в котором располагается рабочая станция доступных серверов Indeed EA/ESSO нет.

Не задан (Not Configured) или Отключен (Disabled)

При недоступных серверах Indeed EA/ESSO в «своем» сайте, поиск сервера будет продолжен в других сайтах Active Directory домена. Значение умолчанию - Не задан.

Включен (Enabled)

При недоступных серверах Indeed EA/ESSO в «своем» сайте, запрос с клиентской рабочей станции будет направлен на серверы, указанные в политике. Имена серверов необходимо указывать в полном доменном формате. В качестве разделителя можно использовать символы ";" или ",". Например, при значении политики **IndeedSRV1.demo.local, IndeedSRV2.demo.local; IndeedSRV3.demo.local** пользователь будет равновероятно подключен к одному из приоритетных серверов.

Настройка политик Server

Доверять клиенту при получении от него DNS-имени

Политика применяется к серверам Indeed-Id и определяет, может ли сервер Indeed-Id доверять клиенту при получении от него DNS-имени, если сам сервер по какой-то причине не смог разрешить имя клиента по его IP-адресу.

Эта политика может применяться при наличии установленного модуля Indeed-Id Rules System и может быть полезна, если есть проблемы в работе службы DNS.

Не задан (Not Configured) или Отключен (Disabled)

В случае невозможности сервером Indeed-Id разрешить имя клиента, в аутентификации пользователю будет отказано. Значение по умолчанию – Не задан.

Включен (Enabled)

В случае, если серверу Indeed-Id не удалось самостоятельно разрешить имя клиента по его IP-адресу, будет использоваться имя, сообщенное серверу клиентом.

Блокировка способов входа

Политика применяется к серверам Indeed-Id и позволяет включить и настроить возможность автоматической блокировки способов входа при превышении лимита неверных попыток входа по ним.

Не задан (Not Configured) или Отключен (Disabled)

Блокировка способов входа будет отключена.

Включен (Enabled)

Способы входа пользователей могут быть заблокированы и затем разблокированы в соответствии с определенными в политике параметрами.

Политика задается следующими настройками безопасности:

- **Количество попыток аутентификации до блокировки**. Настройка определяет количество неудачных попыток аутентификации до блокировки способа входа. Заблокированный способ входа становится недоступным для использования до момента разблокировки администратором или до истечения таймаута до разблокировки.
- **Таймаут до разблокировки способов входа**. Настройка задает время таймаута в минутах на которое заданный способ входа будет заблокирован. По истечению таймаута способ входа будет автоматически разблокирован.
- **Сброс счетчика блокировки через.** Настройка задает, сколько минут должно пройти после неудачной попытки входа, прежде чем счетчик неудачных попыток будет сброшен в 0. Может принимать значения от 1 до 99 999 минут.

Если количество попыток аутентификации до блокировки определено, то данный интервал сброса не должен быть больше параметра "Таймаут до разблокировки способа входа".

Разблокировка аутентификатора происходит автоматически по истечению таймаута до разблокировки способа входа.

Настройка политик Test Servers

Политика применяется к рабочим станциям пользователей и позволяет настроить их для работы с тестовыми серверами Indeed-Id.

Использование тестового сервера Indeed-Id позволяет проверить совместимость программного обеспечения на рабочих станциях пользователей с новой версией Сервера и устранить возможные проблемы, не затрагивая систему в целом.

Использовать для работы только тестовые серверы Indeed EA/ESSO

Не задан (Not Configured) или Отключен (Disabled)

Рабочие станции, на которые распространяется политика, будут работать со всеми активными серверами Indeed-Id. Значение по умолчанию – Не задан.

Включен (Enabled)

Рабочие станции, на которые распространяется политика, будут работать только с тестовыми серверами Indeed-Id.

Настройка политик User Enroller

Принудительная проверка аутентификатора

Политика применяется к рабочим станциям пользователей и позволяет включить режим принудительной проверки аутентификатора после его регистрации пользователем.

Не задан (Not Configured) или Отключен (Disabled)

Принудительная проверка аутентификатора после его регистрации производиться не будет. Значение по умолчанию – Не задан.

Включен (Enabled)

После выполнения действий по регистрации аутентификатора пользователю необходимо будет проверить этот аутентификатор.

Настройка политик Indeed-Id Paste

Группа политик Paste регулирует использование функции Indeed-Id Paste. Политики группы распространяются на пользователей.

Разрешить использование Indeed-Id Paste

Политика позволяет разрешить использование функции Indeed-Id Paste.

Не задан (Not Configured) или Отключен (Disabled)

Использование функции Indeed-Id Paste отключено. Значение по умолчанию – Не задан.

Включен (Enabled)

Использование функции Indeed-Id Paste разрешено. При этом функция Indeed-Id Paste может быть разрешена для парольных окон любых приложений. Для этого необходимо включить опцию «Разрешить Indeed-Id Paste для парольных окон любых приложений».
Если опция «Разрешить Indeed-Id Paste для парольных окон любых приложений» выключена, использование функции Indeed-Id Paste будет разрешено для парольных окон только тех приложений, которые указаны в политике «Разрешить Indeed-Id Paste для парольных окон приложений».

Разрешить Indeed-Id Paste для парольных окон приложений

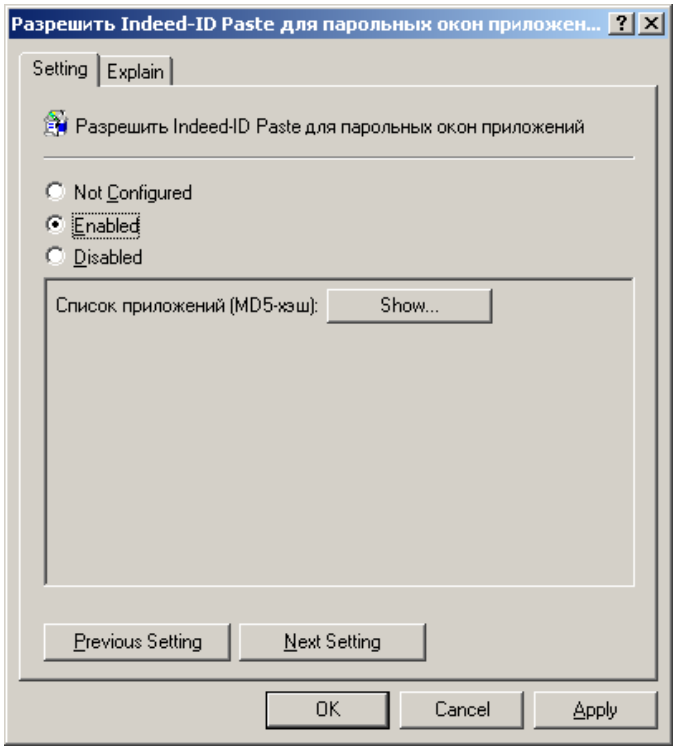
Политика позволяет задать список приложений, для парольных окон которых будет разрешено использование функции Indeed-Id Paste. Принадлежность приложения к списку определяется по значению MD5 хэша.

Не задан (Not Configured) или Отключен (Disabled)

Список приложений, для парольных окон которых разрешено использование функции Indeed-Id Paste, будет пуст. Значение по умолчанию – Не задан.

Включен (Enabled)

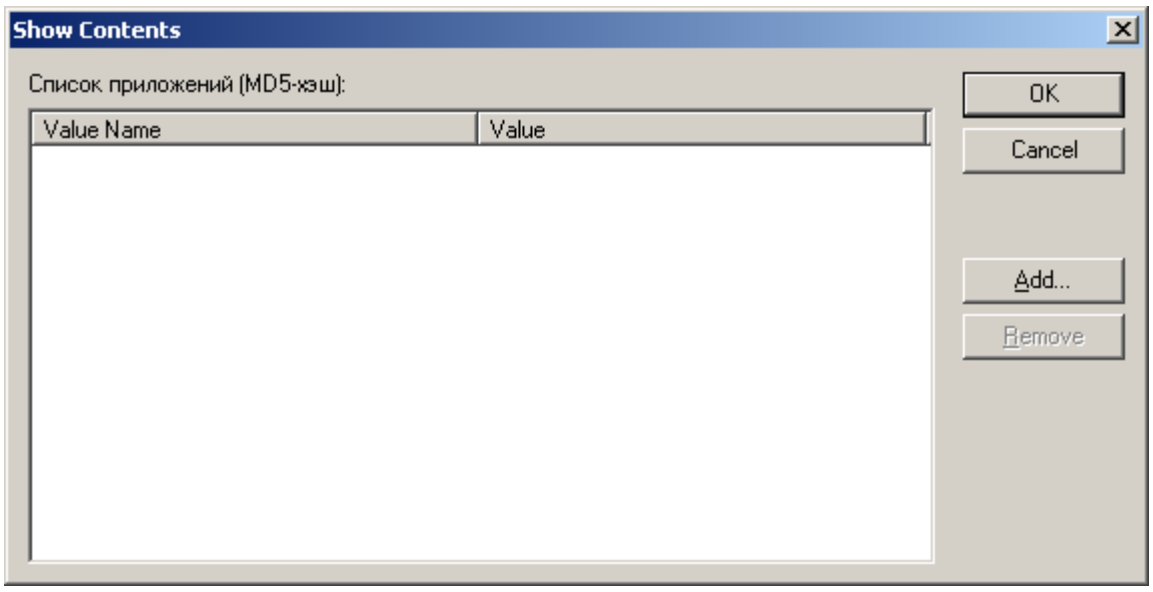
Использование функции Indeed-Id Paste разрешено для парольных окон приложений, заданных в списке приложений.



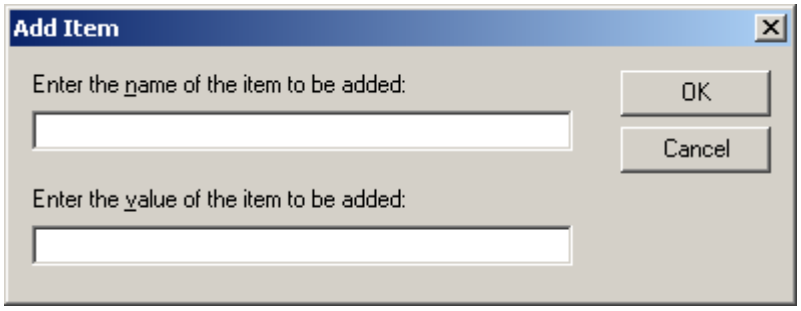
Для получения значения MD5 хэша используются стандартные средства, например, **MD5Summer**.

Значение политики не учитывается в том случае, если в политике «Разрешить использование Indeed-Id Paste» включена опция «Разрешить Indeed-Id Paste для парольных окон любых приложений».

Список приложений открывается при нажатии кнопки **Show** (Показать) в диалоге свойств политики.



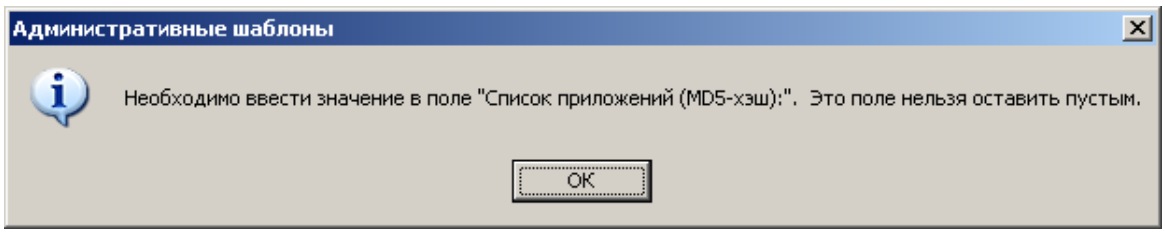
1. Чтобы добавить в список новое приложение, нажмите **Add** (Добавить).
2. В диалоге **Add Item** (Добавление элемента) в поле **Enter the name of the item to be added** (Имя добавляемого элемента) введите значение MD5 хэша приложения.



3. В поле **Enter the value of the item to be added** (Значение добавляемого элемента) вы можете ввести произвольный текстовый комментарий (например, имя приложения).
4. Чтобы сохранить изменения, нажмите **OK**.

Для удаления приложений из списка используйте кнопку **Remove** (Удалить) в диалоге **Show Contents** (Вывод содержания).

Если список приложений пуст, политика не может быть активирована. В этом случае при попытке сохранения изменений или перехода к свойствам другой политики отображается сообщение:



Разрешить Indeed-Id Paste для любых окон приложений

Политика позволяет создать список приложений, при работе с которыми функция Indeed-Id Paste будет разрешена для любых окон.

Не задан (Not Configured) или Отключен (Disabled)

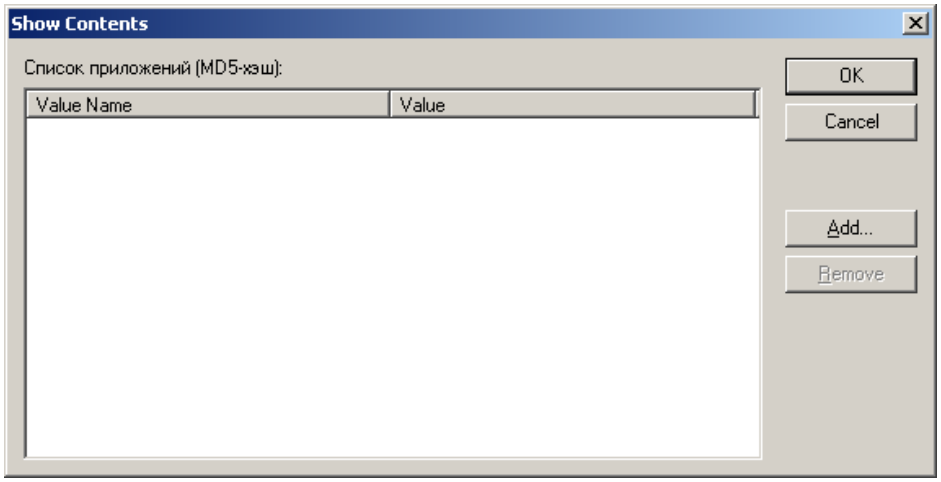
Список приложений, для любых окон которых разрешено использование функции Indeed-Id Paste, будет пуст. Значение по умолчанию – Не задан.

Включен (Enabled)

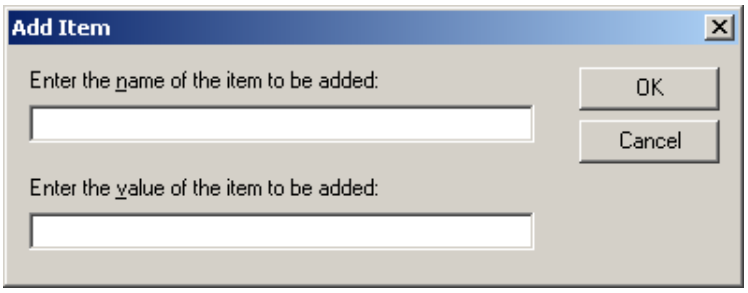
Использование функции Indeed-Id Paste разрешено для любых окон приложений, заданных в списке приложений.

Для получения значения MD5 хэша используются стандартные средства, например, **MD5Summer**.

Принадлежность приложения к списку определяется по значению MD5 хэша.
Список приложений открывается при нажатии кнопки **Show** (Показать) в диалоге свойств политики.



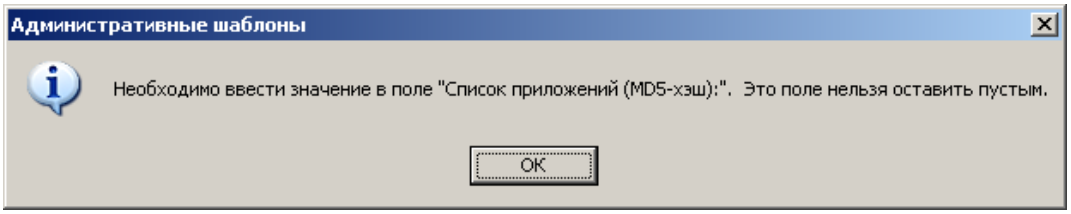
1. Чтобы добавить в список новое приложение, нажмите **Add** (Добавить).
2. В диалоге **Add Item** (Добавление элемента) в поле **Enter the name of the item to be added** (Имя добавляемого элемента) введите значение MD5 хэша приложения.



3. В поле **Enter the value of the item to be added** (Значение добавляемого элемента) вы можете ввести произвольный текстовый комментарий (например, имя приложения).
4. Чтобы сохранить изменения, нажмите **OK**.

Для удаления приложений из списка используйте кнопку **Remove** (Удалить) в диалоге **Show Contents** (Вывод содержания).

Если список приложений пуст, политика не может быть активирована. В этом случае при попытке сохранения изменений или перехода к свойствам другой политики отображается сообщение:



Настройка политик IDM Integration policies

Обходить проблемы репликации

Политика применяется к компьютерам с установленными серверами Indeed-Id и модулями интеграции IDM и позволяет обходить проблемы репликации при создании объектов Active Directory и использовании их непосредственно после создания.

Не задан (Not Configured) или Отключен (Disabled)

Повторное обращение к объекту Active Directory производится не будет. Это означает, что в некоторых сценариях работы (например, создание новой учетной записи пользователя системы Indeed-Id в Active Directory или создание ESSO-профиля этого пользователя) в случае временных задержек репликации данных между контроллерами домена повторное обращение компонентов системы Indeed-Id к Active Directory осуществляться не будет. Значение по умолчанию – Не задан.

Включен (Enabled)

В случае временных задержек репликации данных между контроллерами домена повторное обращение компонентов системы Indeed-Id к Active Directory будет осуществляться в соответствии с определенными в политике параметрами:

- Задержка между повторными попытками обращения к объекту в AD (сек)
  Значение по умолчанию – 5 секунд.
- Количество повторных попыток обращения к объекту AD
  Значение по умолчанию – 50.

Настройка политик провайдеров аутентификации

Помимо политик, относящихся к работе всей системы Indeed-Id, существуют также политики, определяющие параметры работы отдельных провайдеров Indeed-Id. Дополнительная информация по настройке таких политик содержится в руководствах по работе и установке того или иного провайдера Indeed-Id. Файлы административных шаблонов политик входят в состав дистрибутива провайдера.

Пакет сценариев Microsoft Windows PowerShell 2.0

Сценарии, включенные в состав данного пакета, позволяют автоматизировать операции управления свойствами пользователей Indeed-Id и компьютеров в Active Directory. Вы можете использовать готовые сценарии или создавать собственные на основе предоставленных примеров. Для выполнения сценариев необходима установленная среда Microsoft Windows PowerShell 2.0. По умолчанию файлы сценариев находятся в каталоге \Admin Pack\Scripts дистрибутива Indeed-Id. Ниже приведено краткое описание файлов.

Файл constants.ps1

Файл constants.ps1 содержит список констант и включен в состав готовых сценариев. При создании дополнительных сценариев вы можете использовать перечисленные константы, ссылаясь на файл constants.ps1.

Файл constants.ps1 имеет следующий вид (цветом выделены пояснения):

```
# constants.ps1

# constants definition

# Flags for method IDispServerDispatcher::ConnectServer()

Set-Variable CSF_DENY_FIND_SERVER  -option Constant -value 0x00000001  # Do not search Enterprise Server (for example, if client knows that network is unavailable) (Запрет поиска Indeed-Id Enterprise Server (например, если сеть заведомо недоступна))

Set-Variable CSF_DENY_CACHE_SERVER -option Constant -value 0x00000002  # Suppress using Cache Server (Запрет использования кэш-сервера)

# Server state (Состояние Indeed-Id Enterprise Server)

Set-Variable SS_STOPPED -option Constant -value 0x0  # Server stopped (Indeed-Id Enterprise Server остановлен)

Set-Variable SS_STARTED -option Constant -value 0x1  # Server running (Indeed-Id Enterprise Server запущен)

Set-Variable SS_ERROR  -option Constant -value 0x2  # Server error (Ошибка Indeed-Id Enterprise Server)

# User name and computer name formats (Формат имени пользователя и компьютера)

Set-Variable NF_UPN  -option Constant -value 0x0  # username@domain (Формат имени пользователя)

Set-Variable NF_FLAT -option Constant -value 0x1  # DOMAIN\Username or COMPUTERNAME$ (Формат имени пользователя)

Set-Variable NF_LDAP -option Constant -value 0x2  # LDAP (LDAP://CN=User,...) (Формат контейнера)

Set-Variable NF_GUID -option Constant -value 0x3  # GUID of object (GUID объекта)

Set-Variable NF_SID  -option Constant -value 0x4  # object SID (SID объекта)

Set-Variable NF_DNS  -option Constant -value 0x5  # DNS (host.domain.com) (Формат DNS)

# Flags for authenticatiors operations (Параметры операций с аутентификаторами)
```

Set-Variable AOPF_GENERAL -option Constant -value 0x00000001 # Consider general authenticators (Распознавание общих аутентификаторов)

Set-Variable AOPF_ALL -option Constant -value 0xFFFFFFFF # Consider all authenticators (Распознавание всех аутентификаторов)

Flags for change password operation (Параметры операций смены пароля)

Set-Variable CPF_SYSTEM -option Constant -value 0x00000001 # Change password in the system (Смена пароля в системе)

Set-Variable CPF_STORAGE -option Constant -value 0x00000002 # Change password in the database (Смена пароля в базе данных)

Set-Variable CPF_ALL -option Constant -value 0xFFFFFFFF # Change password everywhere (Смена пароля везде)

Logon state (Параметры входа в систему)

Set-Variable LS_LOGGED_OFF -option Constant -value 0x0 # No logon (Вход не выполнен)

Set-Variable LS_LOGGED_ON_AUTH -option Constant -value 0x1 # Logon by authenticator (Вход по аутентификатору)

Set-Variable LS_LOGGED_ON_PASS -option Constant -value 0x2 # Logon by password (Вход по паролю)

Set-Variable LS_LOGGED_ON_COOKIE -option Constant -value 0x3 # Logon by cookie (Вход по cookie) **в текущей версии не поддерживается*

Set-Variable LS_LOGGED_ON_TOKEN -option Constant -value 0x4 # Logon by token (Вход по токену)

Client privileges (Привилегии клиента)

Set-Variable PRIV_USER_C -option Constant -value 0x00000001 # Create User (Создание пользователя)

Set-Variable PRIV_USER_R -option Constant -value 0x00000002 # Read User (general data) (Чтение общих данных пользователя)

Set-Variable PRIV_USER_U -option Constant -value 0x00000004 # Update User (general data) (Обновление общих данных пользователя)

Set-Variable PRIV_USER_D -option Constant -value 0x00000008 # Delete User (Удаление пользователя)

Set-Variable PRIV_USER_PASSWORD_R -option Constant -value 0x00000010 # Read User Password (Чтение пароля пользователя)

Set-Variable PRIV_USER_PASSWORD_W -option Constant -value 0x00000020 # Write User Password (Запись пароля пользователя)

Set-Variable PRIV_USER_SETTINGS_R -option Constant -value 0x00000040 # Read User Settings (Чтение настроек пользователя)

Set-Variable PRIV_USER_SETTINGS_W -option Constant -value 0x00000080 # Write User Settings (Запись настроек пользователя)

Set-Variable PRIV_USER_AUTHENTICATOR_C -option Constant -value 0x00000100 # Create User Authenticators (Создание аутентификаторов пользователя)

Set-Variable PRIV_USER_AUTHENTICATOR_R -option Constant -value 0x00000200 # Read User Authenticators (general data) (Чтение аутентификаторов пользователя (общие данные))

Set-Variable PRIV_USER_AUTHENTICATOR_U -option Constant -value 0x00000400 # Update User Authenticators (general data) (Обновление аутентификаторов пользователя (общие данные))

Set-Variable PRIV_USER_AUTHENTICATOR_D -option Constant -value 0x00000800 # Delete User Authenticators (Удаление аутентификаторов пользователя)

Set-Variable PRIV_USER_AUTH_TEMPLATE_R -option Constant -value 0x00001000 # Read User Authenticators Template (Чтение шаблона аутентификаторов пользователя)

Set-Variable PRIV_USER_AUTH_TEMPLATE_W -option Constant -value 0x00002000 # Write User Authenticators Template (Запись шаблона аутентификаторов пользователя)

Set-Variable PRIV_USER_CACHE_R -option Constant -value 0x00004000 # Read User Cache Data (Чтение кэшированных данных пользователя)

Set-Variable PRIV_USER_CACHE_W -option Constant -value 0x00008000 # Write User Cache Data (Запись кэшированных данных пользователя)

Set-Variable PRIV_SERVER_MANAGEMENT -option Constant -value 0x00010000 # Start/Stop Server (Запуск/останов Indeed-Id Enterprise Server)

Set-Variable PRIV_CRYPTO_KEY_MANAGEMENT -option Constant -value 0x00020000 # Generate/Export/Import Enterprise Key (Генерация/экспорт/импорт ключа шифрования)

Set-Variable PRIV_LICENSE_MANAGEMENT -option Constant -value 0x00040000 # Register/Unregister Licenses & License Subsystems (Регистрация/отмена лицензии и лицензируемых подсистем)

Set-Variable PRIV_USER_PASSWORD_CHANGE -option Constant -value 0x00100000 # Change User Password (Смена пароля пользователю)

Set-Variable PRIV_SYSTEM_SSO_R -option Constant -value 0x01000000 # Read System SSO Data (Чтение системных данных SSO)

Set-Variable PRIV_SYSTEM_SSO_W -option Constant -value 0x02000000 # Write System SSO Data (Запись системных данных SSO)

Set-Variable PRIV_USER_SSO_R -option Constant -value 0x04000000 # Read User SSO Data (Чтение данных пользователя SSO)

Set-Variable PRIV_USER_SSO_W -option Constant -value 0x08000000 # Write User SSO Data (Запись данных пользователя SSO)

User settings IDs (Идентификаторы настроек пользователя)

Set-Variable PROPID_AUTO_PASSWORD_GEN -option Constant -value 0x1 # Generate random password for account (bool) (Генерация случайного пароля для учетной записи)

Set-Variable PROPID_AUTH_MANAGEMENT_PRIV -option Constant -value 0x2 # Authenticatior management privileges (uint) (Привилегии управления аутентификаторами)

Set-Variable PROPID_MAX_AUTH_COUNT -option Constant -value 0x3 # Maximum authenticators count (uint) (Максимальное количество аутентификаторов)

Set-Variable PROPID_CACHE_ENABLE -option Constant -value 0x4 # Cache enabled flag (bool) (Кэширование разрешено)

Set-Variable PROPID_CACHE_EXPIRE -option Constant -value 0x5 # Cache expired date (date) (Дата окончания кэширования)

Set-Variable PROPID_CACHE_BEGIN -option Constant -value 0x6 # Cache begin date (date) (Дата начала кэширования)

Set-Variable PROPID_CACHE_PERIOD -option Constant -value 0x7 # Cache period (date) (Период действия кэширования)

Set-Variable PROPID_CACHE_LOGON_DATE -option Constant -value 0x8 # Cache logon date (date) (Период времени от последнего входа)

Authenticator management privileges (Привилегии управления аутентификаторами)

Set-Variable AUTH_PRIV_ENROLL -option Constant -value 0x00000001 # User can enroll authenticators (Пользователю разрешено обучать аутентификаторы)

Set-Variable AUTH_PRIV_REENROLL -option Constant -value 0x00000002 # User can reenroll authenticatiors (Пользователю разрешено переобучать аутентификаторы)

Set-Variable AUTH_PRIV_REMOVE -option Constant -value 0x00000004 # User can remove authenticatiors (Пользователю разрешено удалять аутентификаторы)

Set-Variable AUTH_PRIV_EDIT_COMMENT_MASK -option Constant -value 0x00000018 # Mask for comment management privileges, 2 bits (3,4 bits) (Маска для привилегий управления комментариями)

Set-Variable AUTH_PRIV_EDIT_COMMENT_ALLOW_ENROLL -option Constant -value 0x00000008 # Comment can be changed only on enrolling (Разрешение на добавление комментария только при обучении аутентификатора)

Set-Variable AUTH_PRIV_EDIT_COMMENT_ALLOW_ALWAYS -option Constant -value 0x00000010 # Comment can be changed at any time (Разрешение на изменение комментария в любое время)

Exception codes and descriptions (Коды и описания исключений)

Set-Variable SERVER_E_NOT_BIOUSER -description "User is not allowed to use Indeed-Id authentication technology." -option Constant -value 0xC1000064 (Пользователь не имеет разрешения на использование технологии аутентификации Indeed-Id)

Set-Variable SERVER_E_ALREADY_BIOUSER -description "User was already allowed to use Indeed-Id authentication technology" -option Constant -value 0xC1000065 (Пользователь уже имеет разрешение на использование технологии аутентификации Indeed-Id)

Set-Variable SERVER_E_WRONG_AUTHENTICATOR_LIMIT -description "Invalid maximum number of authenticators." -option Constant -value 0xC1000069 (Недопустимое максимальное количество аутентификаторов)

Set-Variable SERVER_E_SERVER_NOT_FOUND -description "Indeed-Id Enterprise Server not found." -option Constant -value 0xC100006D (Indeed-Id Enterprise Server не найден)

Set-Variable SERVER_E_SERVER_UNAVAILABLE -description "Indeed-Id Enterprise Server is unavailable." -option Constant -value 0xC1000070 (Indeed-Id Enterprise Server недоступен)

Set-Variable SERVER_E_SERVER_NOT_ACTIVATED -description "Indeed-Id Enterprise Server is not activated." -option Constant -value 0xC1000073 (Indeed-Id Enterprise Server не активирован)

Set-Variable SERVER_E_LICENSE_EXPIRED -description "Your license has expired. Contact your reseller for new license." -option Constant -value 0xC1000076 (Срок действия лицензии истек. Для получения новой лицензии обратитесь к поставщику лицензии)

Set-Variable SERVER_E_LIC_LIMIT_REACHED -description "No free licenses." -option Constant -value 0xC1000082 (Отсутствуют свободные лицензии)

helpers for converting cache period in days to date value and vice-versa (функции для преобразования значения "период кэширования" из дней в дату и наоборот)

```
function to-date([int] $periodInDays)

{

  return [DateTime]::FromOADate($periodInDays)

}

function to-days([DateTime] $period)

{

  return ($period - [DateTime]::FromOADate(0)).Days

}
```

Файлы сценариев

- **enable.disable.IndeedID.cn.ps1**

Сценарий enable.disable.IndeedID.cn.ps1 используется для установки и отмены разрешения на использование технологии аутентификации Indeed-Id для всех пользователей в группе.

- **enable.disable.IndeedID.OU.ps1**

Сценарий enable.disable.IndeedID.OU.ps1 используется для установки и отмены разрешения на использование технологии аутентификации Indeed-Id для всех пользователей в контейнере (CN) и подразделении (OU).

- **enable.disable.IndeedID.user.ps1**

Сценарий enable.disable.IndeedID.user.ps1 используется для установки и отмены разрешения на использование технологии аутентификации Indeed-Id для учетной записи пользователя (можно указать только одну учетную запись).

- **import.key.ps1**

Сценарий import.key.ps1 используется для импорта ключа шифрования.

- **install.license.ps1**

Сценарий install.license.ps1 используется для установки лицензии.

- **free.license.OU.ps1**

Сценарий free.license.OU.ps1 используется для освобождения лицензий Windows® Logon и Enterprise SSO у заблокированных учетных записей.

- **licensed.users.ps1**

Сценарий licensed.users.ps1 предназначен для получения списка пользователей Indeed-Id, обладающих лицензиями Windows® Logon или Enterprise SSO, и определения количества лицензированных пользователей.

- **ChangeProperties\set.caching.options**

Сценарии, находящиеся в данном каталоге, используются для установки параметров кэширования данных пользователей:

  - set.IndeedID.caching.options.ps1 – установка параметров кэширования для пользователя Indeed-Id (можно указать только одну учетную запись);
  - set.IndeedID.caching.options.cn.ps1 – установка параметров кэширования для всех пользователей Indeed-Id в контейнере;
  - set.IndeedID.caching.options.OU.ps1 – установка параметров кэширования для всех пользователей Indeed-Id в подразделении (OU).

- **ChangeProperties\set.random.password**

Сценарии, находящиеся в данном каталоге, используются для установки параметров генерации случайного пароля:

  - set.IndeedID.user.randompassword.ps1 – установить параметры генерации случайного пароля для пользователя Indeed-Id (можно указать только одну учетную запись);
  - set.IndeedID.user.randompassword.cn.ps1 – установить параметры генерации случайного пароля для всех пользователей Indeed-Id в контейнере;
  - set.IndeedID.user.randompassword.OU.ps1 – установить параметры генерации случайного пароля для всех пользователей Indeed-Id в подразделении (OU);

- **ChangeProperties\set.user.rights**

Сценарии, находящиеся в данном каталоге, используются для управления правами пользователей Indeed-Id:

  - set.IndeedID.user.rights.ps1 – установить права пользователя Indeed-Id (можно указать только одну учетную запись);
  - set.IndeedID.user.rights.cn.ps1 – установить права всех пользователей Indeed-Id в контейнере;
  - set.IndeedID.user.rights.OU.ps1 – установить права всех пользователей Indeed-Id в подразделении (OU).

Под правами пользователя Indeed-Id подразумеваются: разрешение на управление аутентификаторами (обучение, переобучение, удаление), добавление комментария при обучении и переобучении аутентификатора.

- **DeleteAuthenticators**

Сценарии, находящиеся в данном каталоге, используются для удаления аутентификаторов пользователей.

  - delete.IndeedID.user.authenticators.ps1 – удалить аутентификаторы пользователя Indeed-Id (можно указать только одну учетную запись).
  - delete.IndeedID.user.authenticators.cn.ps1 – удалить аутентификаторы всех пользователей Indeed-Id в контейнере.
  - delete.IndeedID.user.authenticators.OU.ps1 – удалить аутентификаторы всех пользователей Indeed-Id в подразделении (OU).

- **SetAuthenticatorsMaxCount**

Сценарии, находящиеся в данном каталоге, используются для установки максимального количества аутентификаторов пользователя Indeed-Id.

  - set.IndeedID.user.authenticators.count.ps1 – установить максимальное количество аутентификаторов для пользователя Indeed-Id (можно указать только одну учетную запись).
  - set.IndeedID.user.authenticators.count.cn.ps1 – установить максимальное количество аутентификаторов всех пользователей Indeed-Id в контейнере.
  - set.IndeedID.user.authenticators.count.OU.ps1 – установить максимальное количество аутентификаторов всех пользователей Indeed-Id в подразделении (OU).

- **Search**

Сценарии, находящиеся в данном каталоге, используются для поиска пользователей Indeed-Id.

  - search.IndeedID.users.in.cn.ps1 – найти всех пользователей Indeed-Id в контейнере.
  - search.IndeedID.users.randompassword.in.cn.ps1 – найти всех пользователей Indeed-Id с установленным разрешением на генерацию случайного пароля в контейнере.

- **LfW Enterprise SSO Users**

Сценарии, находящиеся в данном каталоге, используются для применения и отзыва пользовательских лицензий в подсистемах Indeed-Id Windows® Logon и Indeed-Id Enterprise SSO.

  - enable.disable.IndeedID.ESSO.cn.ps1 – применить/отозвать пользовательские лицензии Indeed-Id Enterprise SSO для всех пользователей в контейнере.
  - enable.disable.IndeedID.ESSO.OU.ps1 – применить/отозвать пользовательские лицензии Indeed-Id Enterprise SSO для всех пользователей в подразделении (OU).
  - enable.disable.IndeedID.ESSO.user.ps1 - применить/отозвать пользовательскую лицензию Indeed-Id Enterprise SSO для пользователя (можно указать только одну учетную запись).
  - enable.disable.IndeedID.LFW.cn.ps1 – применить/отозвать пользовательские лицензии Indeed-Id Windows® Logon для всех пользователей в контейнере.
  - enable.disable.IndeedID.LfW.OU.ps1 – применить/отозвать пользовательские лицензии Indeed-Id Windows® Logon для всех пользователей в подразделении (OU).
  - enable.disable.IndeedID.LfW.user.ps1 - применить/отозвать пользовательскую лицензию Indeed-Id Windows® Logon для пользователя (можно указать только одну учетную запись).

Примеры использования сценариев

Для выполнения сценариев требуется ввод параметров. Справка по параметрам выводится в командной строке при запуске сценария. При вводе недопустимых значений параметров выводится сообщение об ошибке.

Далее приведены примеры использования некоторых сценариев с описанием обязательных параметров:

- **setIndeedID.caching.options.ps1**
- **enable.disable.IndeedID.LFW.OU.ps1**
- **enable.disable.IndeedID.ESSO.user.ps1**
- **free.license.OU.ps1**

Кроме обязательных параметров, в ряде сценариев предусмотрены опциональные параметры.

- l Уровень поиска пользователей Indeed-Id. Может использоваться во всех сценариях с постфиксом *.OU. Если значение данного параметра равно 1, поиск пользователей Indeed-Id осуществляется только в корневом подразделении (OU). Если параметр не задан, поиск выполняется в корневом OU и во всех дочерних.

Пример:

.\enable.disable.IndeedID.OU.ps1 -ou 'ou=*Office*,dc=demo,dc=domain' –l 1.

- lf Имя файла для записи лога. Может использоваться во всех сценариях с постфиксами *.cn и *.OU. Если параметр не задан, запись лога не производится.

Пример:

.\search.IndeedID.users.in.cn.ps1 –g 'cn=*Security*,ou=*Office*,dc=demo,dc=domain' –lf *logfile*.

setIndeedID.caching.options.ps1

Параметры команд

-u Имя пользователя в формате user@domain. Для сценариев set.IndeedID.caching.options.cn.ps1 и set.IndeedID.caching.options.OU.ps1 необходимо указывать также контейнер и подразделение (OU). Если параметр не задан, в командной строке выводится сообщение об ошибке.

-c Параметр операции. Возможные значения: 0 - кэширование запрещено, 1 – кэширование разрешено. Если параметр не задан, значение считается равным 0.

-sd Дата начала кэширования в формате MM.DD.YYYY. Для запрета начальной даты необходимо ввести параметр 0. Если параметр не задан, в командной строке выводится сообщение об ошибке.

-ed Дата завершения кэширования в формате MM.DD.YYYY. Для запрета конечной даты необходимо ввести параметр 0. Если параметр не задан, в командной строке выводится сообщение об ошибке.

-p Период времени от последнего входа в систему (в днях). Для запрета периода времени от последнего входа необходимо ввести параметр 0. Если параметр не задан, значение считается равным 0.

Примеры команд:

- **.\set.IndeedID.caching.options.ps1 -u *user@domain* -c 1 -sd *'01.20.2011*' -ed '*02.12.2011*' -p** 10 - данная команда разрешает кэширование данных пользователя, устанавливает начальную и конечную дату кэширования и период с последнего входа в систему. При успешном выполнении сценария будут автоматически заданы соответствующие настройки в диалоге **Кэширование данных пользователя** (вкладка свойств пользователя **Indeed-Id** > **Параметры кэширования**).
- **.\set.IndeedID.caching.options.ps1 -u *user@domain* -c 1 -sd '0' -ed '0' -p 0** – данная команда разрешает кэширование данных пользователя без установки начальной/конечной даты и периода с последнего входа. При успешном выполнении сценария будет автоматически выбрана опция **Разрешить кэшировать данные пользователя на локальном компьютере** в диалоге **Кэширование данных пользователя** (вкладка свойств пользователя **Indeed-Id** > **Параметры кэширования**).

- **.\set.IndeedID.caching.options.ps1 -u *user@domain* -c 0 -sd '0' -ed '0' -p 0** – данная команда запрещает кэширование данных пользователя. При успешном выполнении сценария будет автоматически выключена опция **Разрешить кэшировать данные пользователя на локальном компьютере** в диалоге **Кэширование данных пользователя** (вкладка свойств пользователя **Indeed-Id** > **Параметры кэширования**).

enable.disable.IndeedID.LFW.OU.ps1

Параметры команд

-ou Имя подразделения (указывается в формате ou=OU name,dc=domain name).

-f Флаг операции. Возможные значения: 0 – отозвать лицензию, 1 – применить лицензию.

Примеры команд

- **.\enable.disable.IndeedID.LFW.OU.ps1 -ou 'ou=*Office*,dc=demo,dc=domain' -f 1** – данная команда применяет лицензии Indeed-Id Windows® Logon для всех пользователей в подразделении Office. При успешном выполнении сценария на вкладках свойств впользователей **Indeed-Id** будет автоматически выбрана опция **Разрешить использование Windows® Logon**.
- **.\enable.disable.IndeedID.LFW.OU.ps1 -ou 'ou=*Office*,dc=demo,dc=domain' -f 0 -** данная команда выполняет отзыв лицензии Indeed-Id Windows® Logon для всех пользователей в подразделении Office. При успешном выполнении сценария на вкладках свойств пользователей **Indeed-Id** будет автоматически выключена опция **Разрешить использование Windows® Logon**.

enable.disable.IndeedID.ESSO.user.ps1

Параметры команд

-u Имя пользователя (указывается в формате user@domain).

-f Флаг операции. Возможные значения: 0 – отозвать лицензию, 1 – применить лицензию.

Примеры команд

- **.\enable.disable.IndeedID.ESSO.user.ps1 -u *Anna.Ivanova@demo.domain* -f 1** – данная команда применяет лицензию Indeed-Id Enterprise SSO для пользователя Anna Ivanova. При успешном выполнении сценария на вкладке свойств пользователя **Indeed-Id** будет автоматически выбрана опция **Разрешить использование Enterprise SSO**.
- **.\enable.disable.IndeedID.ESSO.user.ps1 -u *Anna.Ivanova@demo.domain* -f 0** – данная команда выполняет отзыв лицензии Indeed-Id Enterprise SSO для пользователя Anna Ivanova. При успешном выполнении сценария на вкладке свойств пользователя **Indeed-Id** будет автоматически выключена опция **Разрешить использование Enterprise SSO**.

free.license.OU.ps1

Параметры команд

-ou Имя подразделения

-l Имя освобождаемой лицензии (IID_LFW_USR – лицензия пользователя Windows® Logon, IID_SSO_USR – лицензия пользователя Enterprise SSO).

-r Тип поиска. Возможные значения: 0 – нерекурсивный (поиск только в заданном подразделении), 1 – рекурсивный (поиск в заданном подразделении и всех входящих в него подразделениях). Значение по умолчанию – 0.

Примеры команд

- **.\free.license.OU.ps1 -ou 'ou=*ou1*,dc=demo,dc=domain' -l 'IID_ESSO_USR'** – данная команда освобождает лицензии Enterprise SSO для заблокированных пользователей подразделения ou1.

free.license.no.auth.OU.ps1

Параметры команд

-ou Имя подразделения

-l Имя освобождаемой лицензии (IID_LFW_USR – лицензия пользователя Windows® Logon, IID_SSO_USR – лицензия пользователя Enterprise SSO).

-r Тип поиска. Возможные значения: 0 – нерекурсивный (поиск только в заданном подразделении), 1 – рекурсивный (поиск в заданном подразделении и всех входящих в него подразделениях). Значение по умолчанию – 0.

Примеры команд

- **.\free.license.no.auth.OU.ps1 -ou 'ou=*ou1*,dc=demo,dc=domain' -l 'IID_LFW_USR' -r 1** – данная команда освобождает лицензии Windows® Logon у пользователей подразделения ou1, не имеющих обученных аутентификаторов.

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 пользователя.pdf*.

Часто задаваемые вопросы

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