Indeed Access Manager Server с хранилищем данных в AD

Информация

Файлы для indeed AM Server расположены: ***indeed AM\Indeed Access Manager Server\<Номер версии>***

- **IndeedAM.Server-x64.ru-ru.msi** - Пакет для установки Indeed AMprise Server 7
- **/Misc/Templates** - Шаблоны политик.
- **/Misc/AM.KeyGen.exe** - Утилита для генерации ключей шифрования.
- **/Misc/AccessControlInitialConfig/EA.Server.AccessControlInitialConfig.exe** - Утилита первичной конфигурации.
- **/Misc/AccessControlInitialConfig/EA.Server.AccessControlInitialConfig.exe.config** - Файл для настройки утилиты конфигурации.
- **/Misc/AM.Config.Encryptor/EA.Config.Encryptor.exe** - Утилита для шифрования конфигурационного файла.
- **/Misc/AM.Config.Encryptor/EA.Config.Encryptor.exe/encryptConfigs.bat** - Скрипт для шифрования всех секций конфигурационного файла.
- **/Misc/AM.Config.Encryptor/EA.Config.Encryptor.exe/decryptConfigs.bat** - Скрипт для расшифровки всех секций конфигурационного файла.

Установка

Информация

После установки сервера Indeed AM будет предложено выполнить настройку с помощью мастера конфигурации для этого не отключайте параметр "Запустить мастер настройки Indeed EA".

1. Выполнить установку Indeed AM Server через запуск инсталлятора **IndeedAM.Server-x64.ru-ru.msi**.

2. Добавить привязку **https** в настройках **Default Web Site** в IIS Manager.

   Информация

   Indeed AM Server является Web приложением, которое работает на базе IIS, в процессе установки для него по умолчанию включается обязательно требование SSL в настройках, что в свою очередь требует включенной привязки https.

   Если вы не намерены использовать протокол https, необходимо отключить требование SSL в настройках IIS для easerver и в конфигурационном файле сервера (C:\inetpub\wwwroot\easerver\Web.config) изменить значение параметра "**requireHttps**" на "**false**".

Пример
<appSettings> <add key="requireHttps" value="false" /> </appSettings>

   a. Запустите **IIS Manager** и раскройте пункт **Сайты** (Sites).
   b. Выберите сайт **Default Web Site** и нажмите **Привязки** (Bindings) в разделе **Действия** (Actions).
   c. Нажмите **Добавить** (Add):
      i. **Тип** (Type) - https.
      ii. **Порт** (Port) - 443.
      iii. Выберите **SSL-сертификат** (SSL Certificate).
   d. Сохраните привязку.

Настройка с помощью мастера конфигурации

Информация

Мастер конфигурации по умолчанию запускается автоматически после установки Indeed AM Server, если запуск не был отключен пользователем.

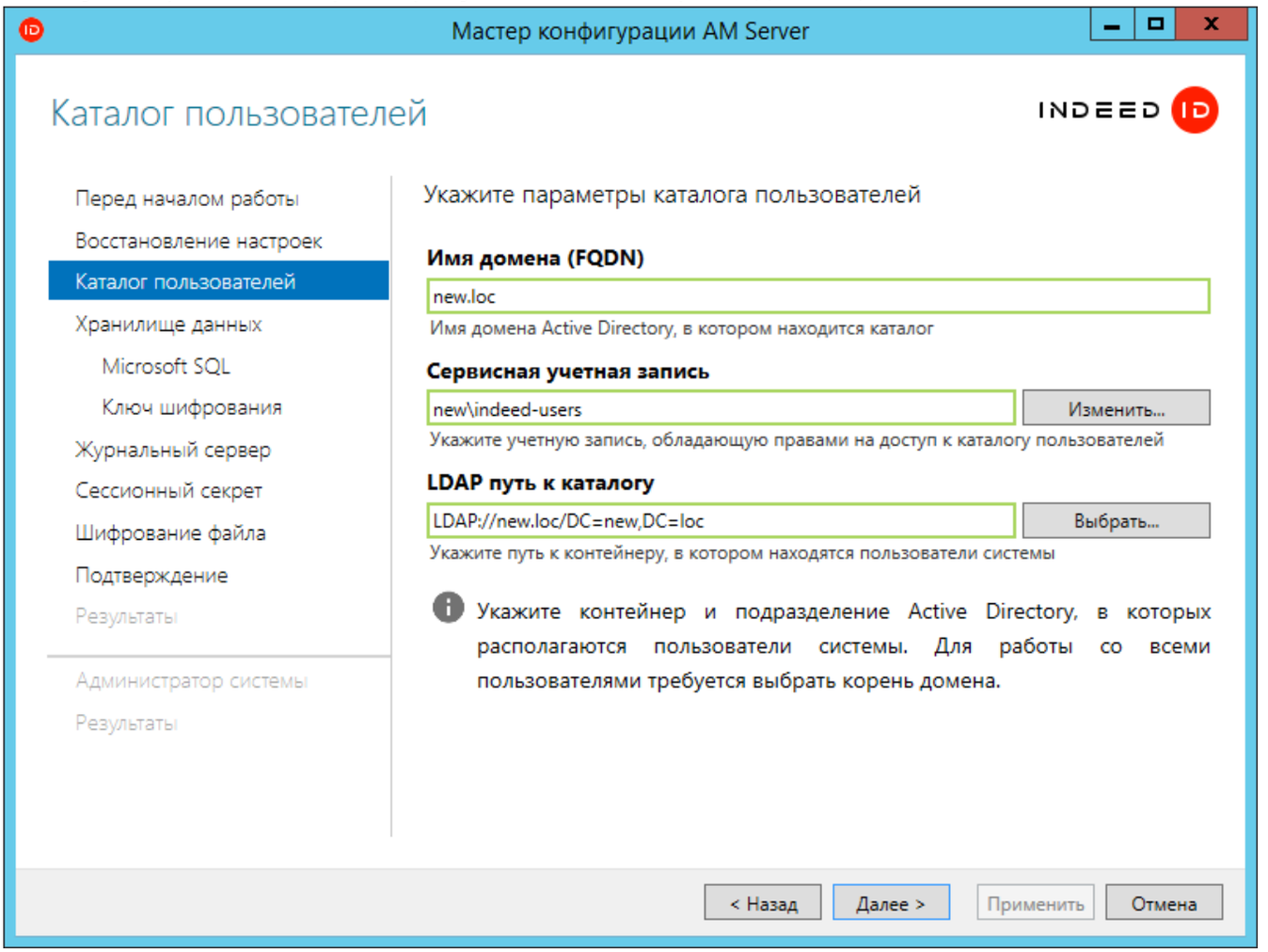
Для запуска мастера вручную откройте файл: C:\Program Files\Indeed EA\Wizard\EA.Server.Wizard.exe

Информация

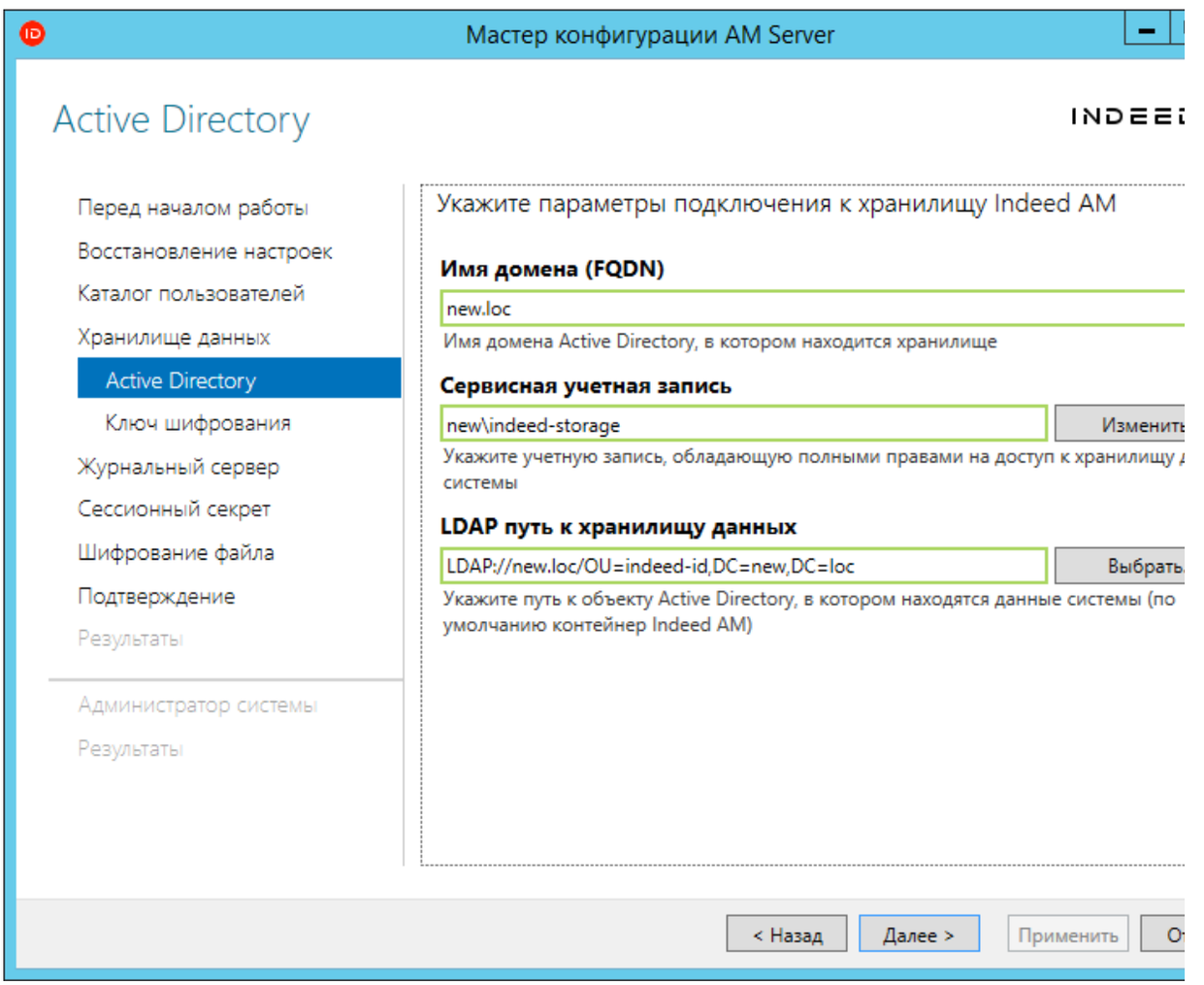
В мастер включена автоматическая проверка введенных данных, в случае успешного ввода - поля будут подсвечены зеленым цветом, и вы сможете перейти к следующему шагу, если данные введены некорректно, то поля будут подсвечены красным, и вы не сможете перейти к следующему шагу пока не укажете корректные данные.

1. На шаге "**Перед началом работы"** нажмите “Далее”.

2. На шаге "**Восстановление настроек**" нажмите “Далее”.
3. На шаге "**Каталог пользователей**" укажите следующие параметры:
    a. **Имя домена (FQDN)** - Укажите полное имя домена, например: *domain.local.*
    b. **Сервисная учетная запись** - Укажите сервисную учетную запись, обладающую правами доступа к пользовательскому каталогу. Нажмите кнопку "**Изменить**" и укажите требуемые данные учетной записи.
    c. **LDAP путь к каталогу** - Укажите путь к каталогу с пользователями. Нажмите кнопку "Выбрать" и выберете требуемый контейнер или домен целиком.



4. На шаге "**Хранилище данных**" выберете тип хранилища Active Directory.
    a. **Имя домена (FQDN)** - Укажите полное имя домена, например: *domain.local.*
    b. **Сервисная учетная запись** - Укажите сервисную учетную запись, обладающую полными правами на контейнер, который будет использоваться в качестве хранилища данных Indeed. Нажмите кнопку "Изменить" и укажите требуемые данные учетной записи.
    c. **LDAP путь к каталогу** - Укажите путь к каталогу с пользователями. Нажмите кнопку "Выбрать" и выберете требуемый контейнер или домен целиком.



5. Шаг "**Ключ шифрования**". Выберете алгоритм шифрования, нажмите "**Сгенерировать**" и нажмите "**Далее**".

    Информация

    Настоятельно рекомендуется выполнить резервную копию ключа шифрования и сохранить в защищенном месте.

6. На шаге "**Журнальный сервер**" укажите следующие данные:

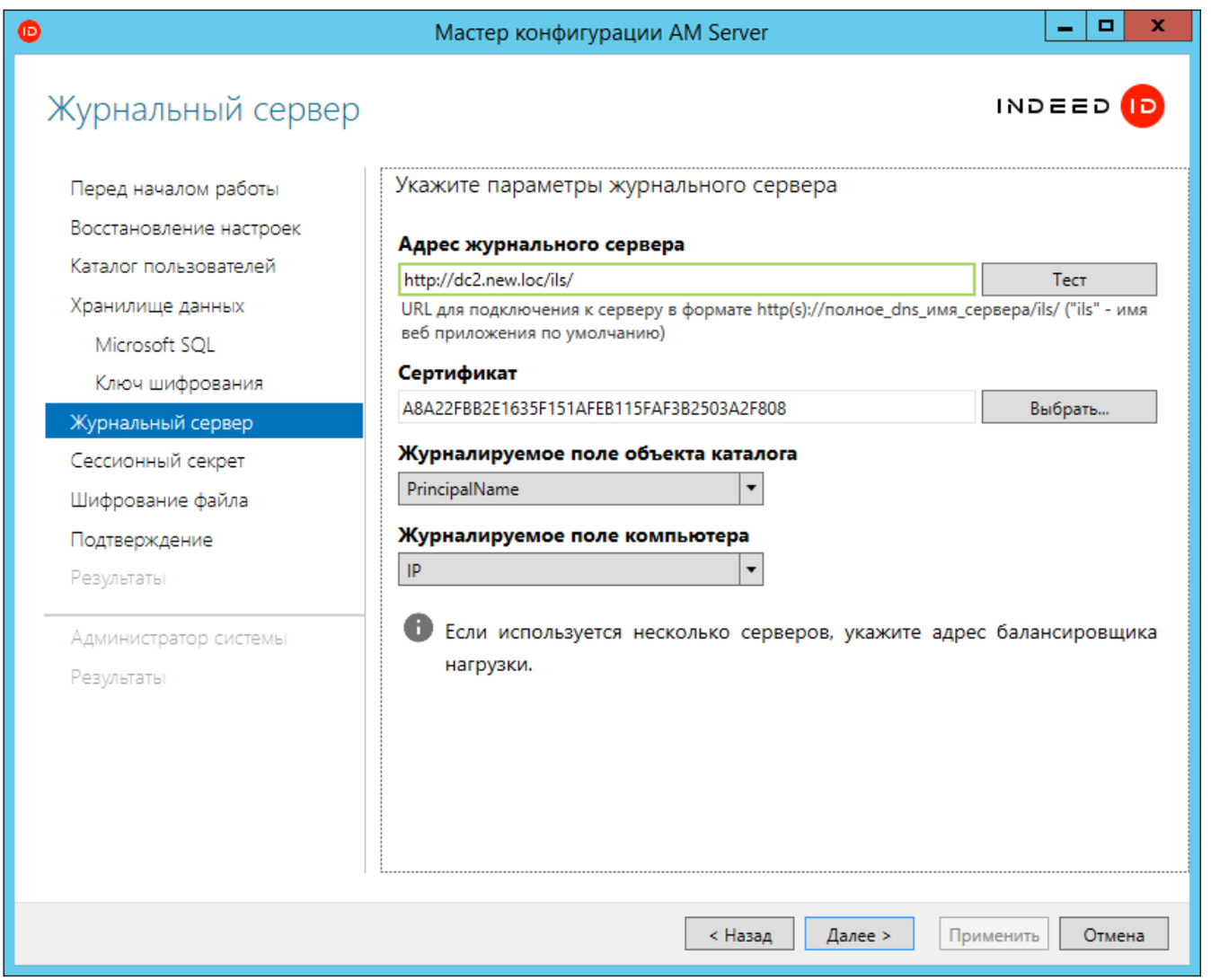
   Информация

   Чтобы при тестировании соединения не возникало ошибок, требуется полностью настроенный лог-сервер, с настроенной базой данных или установленным компонентом EventLog. Если журнальный сервер не готов к работе, вы можете пропустить этот шаг.

   a. **Адрес журнального сервера** - URL для подключения к серверу в формате http(s)://полное_dns_имя_сервера/ils/ , например: http://logserver.demo.local/ils/
   b. **Сертификат** - Выберете сертификат для настройки двухстороннего TLS соединения.
   c. **Журналируемое поле объекта каталога** - Укажите формат в котором будет осуществляться логирование имени пользователя.
   d. **Журналируемое поле компьютера** - Укажите формат в котором будет осуществляться логирование поля **"Компьютер"**.

      Информация

      Для логирования в формате DNS потребуется дополнительная настройка



7. Шаг "**Сессионный секрет**". Сгенерируйте секрет для подписи токена, для этого нажмите **"Сгенерировать"**. После генерации нажмите **"Далее"**.
8. Шаг **"Шифрование файла"**. Вы можете выполнить шифрование настроек конфигурационного файла.

   Информация

   В целях повышения безопасности рекомендуется выполнить шифрование конфигурационного файла.
9. Шаг **"Подтверждение"**. Убедитесь в корректности указанных данных и нажмите **"Применить"**.

   Информация

   Рекомендуется сделать резервную копию конфигурационного файла, по умолчанию параметр "**Сохранить резервную копию параметров конфигурации**" активен.
10. Шаг "**Результаты**". Осуществляется проверка настроек и тестирование подключения к Indeed AM Server.

Настройка администратора системы

Информация

Пользователь, который указывается в качестве администратора системы должен находится в пользовательском каталоге.

1. На шаге "**Администратор системы**" задайте учетную запись администратора Indeed. Указанной учетной записи будут выданы первичные права администратора системы.

   Информация

   Для настройки администратора требуется установленный Indeed AM Windows Password, так как при выдаче первичных прав указанному пользователю, осуществляется аутентификация на сервере Indeed AM
2. На шаге "**Результаты**" отображается статус настройки конфигурационного файла и статус настройки администратора системы.

Ручная настройка системы

Редактирование конфигурационного файла

Информация

Для сохранения изменений в конфигурационном файле приложения, требуется запустить редактор с правами администратора.

Ошибки, возникшие при развертывании сервера АМ (Например ошибка в конфигурационном файле), будут логироваться исходя из настроек LogServer.

Для генерации ключей шифрования рекомендуется использовать утилиту **AM.KeyGen.exe**, выб рав необходимый алгоритм из предложенного списка.

Информация

Если в пароле для сервисных пользователей используются следующие символы: **&**, **"**, **<**, **пробел** , то пароль следуют указывать так:

Символ “амперсанд” (&) - При указании пароля для пользователя символ требуется заменить на: **&** Пример: **password="Q1q2E3e4&"**

Символ “двойные кавычки” (") - При указании пароля для пользователя символ требуется заменить на: **"** Пример: **password="Q1q2E3e4""**

Символ “меньше” (<) - При указании пароля для пользователя символ требуется заменить на: **<** Пример: **password="Q1q2E3e4<"**

1. Откройте конфигурационный файл сервера **Web.config** (**C:\inetpub\wwwroot\easerver\Web.config**).
2. Добавить секретный ключ для подписи токена для параметра "**secretKey**" тега "**logonSettings**". Параметр "**secretKey**" используется для создания токена пользователя в формате **"jwt"**.

Пример
<logonSettings secretKey=" 67d7e6caec61d61239dc0b05f86063ed899931b581fa1ed8140d7843b320fe02"/>

3. Задать каталог пользователя системы, для этого необходимо отредактировать параметры в теге **adUserCatalogProvider**:

    a. **id** - произвольный уникальный идентификатор каталога.
    b. **serverName -** имя домена Active Directory, в котором находится каталог.
    c. **containerPath -** путь к контейнеру в виде Distinguished Name или весь домен, если для хранения пользователей используется весь домен.
    d. **userName** - имя сервисной учетной записи для подключения к каталогу пользователей.
    e. **password** - пароль сервисной учетной записи каталога пользователей в AD.

Пример
<adUserCatalogProviders> <adUserCatalogProvider id="UserId" serverName="indeed-id.local" containerPath="DC=indeed-id,DC=local" userName="IndeedCatalogUser" password="Q1q2E3e4"/> </adUserCatalogProviders>

4. Указать корневой идентификатор провайдера работы с каталогом, необходимо отредактировать атрибут **rootUserCatalogProviderId** в теге **userCatalogProviderSettings**.

    Информация

    При использовании нескольких пользовательских каталогов в параметре **rootUserCatalogProviderId** указывается общий идентификатор каталогов, заданный в параметре **id** тега **orUserCatalogProvider.**

    a. **rootUserCatalogProviderId** - задать значение, которое уже было задано в тэге **adUserCatalogProvider** в атрибуте ***id.***

Пример
<userCatalogProviderSettings rootUserCatalogProviderId="UserId">

5. Задать хранилище данных системы. Для хранилища данных в Active Directory редактируем параметр **rootDbContextId** в теге **dbContextSettings** и параметры в тэге **adDbContext.**
    a. **rootDbContextId** - задать произвольно уникальное значение идентификатора хранилища.
    b. **id** - задать значение, которое уже было задано в тэге **rootDbContextId**.
    c. **path** - LDAP путь к контейнеру с данными в Active Directory. Рекомендуется указывать в формате **"serverless binding"**(Без жесткой привязки к серверу).
    d. **userName** - имя сервисной учетной записи для подключения к хранилищу.
    e. **password** - пароль сервисной учетной записи каталога пользователей в AD.

Пример
<dbContextSettings rootDbContextId="IDRepository"> <adDbContexts> <adDbContext id="IDRepository" path="LDAP://indeed-id.local/OU=Indeed AM 7,DC=indeed-id,DC=local" userName="IndeedDataUser" password="Q1q2E3e4" /> </adDbContexts> </dbContextSettings>

6. Задать ключ шифрования данных системы. Редактируем параметры в теге **encryptionSettings**.
    a. **cryptoAlgName -** указать использованный алгоритм шифрования.
    b. **cryptoKey -** значения ключа, сгенерированного утилитой.
    c. **certificateThumbprint -** Thumbprint сертификата, которым зашифрован ключ (чтобы не учитывать - нужно удалить атрибут).

Пример
<encryptionSettings cryptoAlgName="Aes" cryptoKey=" 90ce7dbc3ff94a7867abc6672c23cce2c3717d38af42f04293130cb68a34ecc2"/>

7. Задать администратора системы. Редактируем параметр **userId** тега **accessControlAdminSettings.**

    a. **userId -** идентификатор пользователя в формате: “<**Идентификатор каталога><нижнее подчеркивание>**<**GUID Администратора Системы>**”.

    Примечание

    Пользователь должен находится внутри каталога пользователей.

    При использовании нескольких пользовательских контейнеров для <**Идентификатор каталога>** указывается **id** контейнера в котором находится администратор системы.

Пример
<accessControlAdminSettings userId="UserId_84e9ccd9-73a2-43c7-abc6-604a16902037"/>

    Информация

    Получить GUID можно с помощью команды **PowerShell**. Предварительно необходимо установить компонент **Remote Server Administration Tools**:

Пример
Get-ADUser YouUserName -Properties * | Select ObjectGUID

Задаем url для подключения к лог серверу. Редактируем тег **logServer**.

1. **URL** - url для подключения к log серверу в формате **http(s)://полное_dns_имя_сервера /ils/api.**

    Примечание

    Если используется несколько серверов, указываем адрес балансировщика нагрузки.
2. **CertificateThumbprint** - если закрытый ключ в реестре, а сертификат в хранилище компьютера.
3. **CertificateFilePath** - если ключевая пара в pfx.
4. **CertificateFilePassword** - пароль от pfx.

Пример
<logServer Url="http://log.indeed-id.local/ils/api/" CertificateThumbprint="" CertificateFilePath="" CertificateFilePassword=""/>

Настройка первичной конфигурации

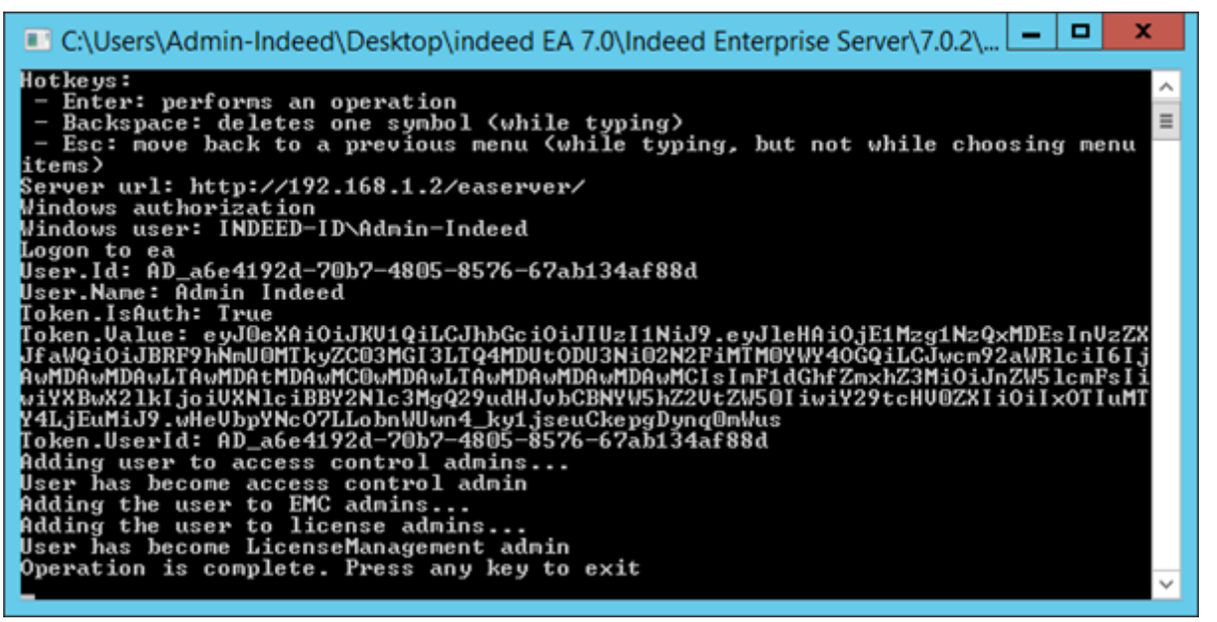
Информация

Пользователь, который указывается в качестве администратора системы должен находится в пользовательском каталоге.

1. Открыть для редактирования файл **EA.Server.AccessControlInitialConfig.exe.config**.
2. Редактировать атрибут **key** - параметр value необходимо поставить в значение **true**, если для авторизации мы хотим использовать **Windows Token**.
   Если сервер находится не в домене, есть вариант использовать один из следующих провайдеров: ***windows password, emailOTP, smsOTP***. Для этого **value** должно быть в положении **false.**

   ```
   <appSettings> <add key="eaServerUrl" value="http://192.168.1.2/easerver/"/> <add key="
   isWindowsAuth" value="true"/> </appSettings>
   ```

3. Запустить на доменной машине утилиту **EA.Server.AccessControlInitialConfig.exe** под пользователем, которого необходимо сделать администратором системы и который прописан в качестве администратора в тэге **accessControlAdminSettings.**



Настройка нескольких пользовательских каталогов

Информация

Если настройка нескольких каталогов осуществляется в уже используемой системе Indeed (После выдачи первичных прав для администратора системы), и изменяется расположение администратора системы или префикс заданный в параметре "**accessControlAdminSettings**" , то потребуется удалить выданные ранее права и выполнить повторный запуск утилиты первичной конфигурации.

Для удаления прав необходимо удалить все данный из таблицы **DbAccessGroupMembers**, расположенной в базе данных системы **Indeed.**

Информация

Если контейнеры находятся в разных доменах/лесах, то требуется создать пользователя для чтения данных с контейнера в своем домене/лесе.

1. Добавьте внутри тега **adUserCatalogProviders** строки для подключения к контейнерам.

Пример

```
<userCatalogProviderSettings rootUserCatalogProviderId="user">
  <userCatalogProviders>
   <sqlUserCatalogProviders></sqlUserCatalogProviders>
   <adUserCatalogProviders>
    <adUserCatalogProvider id="Ad1" serverName="demo.local" containerPath="OU=Indeed_Users,
DC=demo,DC=local" userName="demo\ind-user" password="Q1q2E3e4" />
    <adUserCatalogProvider id="Ad2" serverName="demo.local" containerPath="OU=inDomainUsers,
DC=demo,DC=local" userName="demo\ind-user" password="Q1q2E3e4" />
    <adUserCatalogProvider id="Ad3" serverName="inforest.demo.local" containerPath="
OU=UsersInForest,DC=inforest,DC=demo,DC=local" userName="inforest\cataloguser1" password="
Q1q2E3e4" />
    <adUserCatalogProvider id="Ad4" serverName="newforest.local" containerPath="
OU=Usersoutforest,DC=newforest,DC=local" userName="newforest\cataloguser2" password="
Q1q2E3e4" />
     </adUserCatalogProviders>
  </userCatalogProviders>
```

2. Добавьте внутри тега **orUserCatalogProviders** тег **orUserCatalogProvider** с параметром **id.**

Информация

Значение параметра **id** должно соответствовать значению заданному в параметре **rootUserCatalogProviderId**

3. Добавьте внутри тега **orUserCatalogProvider** тег **userCatalogProviders.** Внутри тега **userCatalogProviders** добавьте теги **userCatalogProvider** с параметром **id,** в котором указывается идентификатор пользовательского контейнера и **ignoreExceptions** со значением **true**, данный параметр игнорирует ошибку подключения к каталогу, если данный каталог не доступен.

Информация

⚠️

Данные теги могут отсутствовать в конфигурационном файле, если ранее было выполнено шифрование конфигурационного файла с не заданными параметрами. Если теги отсутствуют, то добавьте их вручну, полная структура файла представлена ниже.

Пример

```
<orUserCatalogProviders>
  <orUserCatalogProvider id="user">
    <userCatalogProviders>
      <userCatalogProvider id="Ad1" ignoreExceptions="true" />
      <userCatalogProvider id="Ad2" ignoreExceptions="true" />
      <userCatalogProvider id="Ad3" ignoreExceptions="true" />
      <userCatalogProvider id="Ad4" ignoreExceptions="true" />
    </userCatalogProviders>
  </orUserCatalogProvider>
</orUserCatalogProviders>
```

Пример структуры файла

Пример

```
<accessControlAdminSettings userId="UserId_891f2b6c-9a55-4e1a-b69b-b4d6418f4c4c"/>
 <logonSettings secretKey="*****"/>
 <userCatalogProviderSettings rootUserCatalogProviderId="user">
      <userCatalogProviders>
          <sqlUserCatalogProviders>
          </sqlUserCatalogProviders>
          <adUserCatalogProviders>
               <adUserCatalogProvider id="UserId" serverName="new.loc" containerPath="DC=new,
DC=loc"
                    userName="indeed-users" password="Q1q2E3e4" />
               <adUserCatalogProvider id="UserId1" serverName="test.new.loc" containerPath="DC=test,
DC=loc"
                    userName="indeed-users" password="Q1q2E3e4" />
          </adUserCatalogProviders>
      </userCatalogProviders>
      <combineRules>
          <orUserCatalogProviders>
              <orUserCatalogProvider id="user">
                <userCatalogProviders>
                    <userCatalogProvider id="UserId" ignoreExceptions="true" />
                    <userCatalogProvider id="UserId1" ignoreExceptions="true" />
                </userCatalogProviders>
              </orUserCatalogProvider>
          </orUserCatalogProviders>
          <andUserCatalogProviders>
          </andUserCatalogProviders>
      </combineRules>
 </userCatalogProviderSettings>
```

Шифрование/Расшифрование конфигурационного файла

1. Запустите командную строку от имени "**Администратора**".
2. В командной строке перейдите в папку с утилитой для шифрования.

   Информация

   Утилита шифрует секции: **logServer**, **logonSettings**, **userCatalogProviderSettings**, **encryptionSettings**, **dbContextSettings**. Рекомендуется зашифровать все секции.

a. Шифрование/Расшифрование отдельных секций.
   Для **шифрования отдельной секции** необходимо выполнить команду вида: EA.Config.Encryptor /encrypt "Путь к конфигурационному файлу сервера" "Имя секции"

Пример
EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\easerver\Web.config" "logServer"

   Для **расшифровки отдельной секции** необходимо выполнить команду вида: EA.Config.Encryptor /decrypt "Путь к конфигурационному файлу сервера" "Имя секции"

Пример
EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\easerver\Web.config" "logServer"

b. Шифрование/Расшифрование всех секций.

Для **шифрования всех секций** необходимо запустить скрипт **encryptConfigs.bat**.

```
C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>encryptConfigs.bat

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem logServer

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "logServer"
Configuration section has been encrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem logonSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "logonSettings"
Configuration section has been encrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem userCatalogProviderSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "userCatalogProviderSettings"
Configuration section has been encrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem encryptionSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "encryptionSettings"
Configuration section has been encrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem dbContextSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "dbContextSettings"
Configuration section has been encrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>pause
Для продолжения нажмите любую клавишу . . .
```

Для **расшифровки всех секций** необходимо выполнить скрипт **decryptConfigs.bat**

```
C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>decryptConfigs.bat

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem logServer

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "logServer"
Configuration section has been decrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem logonSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "logonSettings"
Configuration section has been decrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem userCatalogProviderSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "userCatalogProviderSettings"
Configuration section has been decrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem encryptionSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "encryptionSettings"
Configuration section has been decrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem dbContextSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "dbContextSettings"
Configuration section has been decrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>pause
Для продолжения нажмите любую клавишу . . .
```