Indeed Enterprise Server с хранилищем данных в AD

> **Информация**
>
> Файлы для indeed EA Server 7 расположены: ***indeed AM 7.0\Indeed Enterprise Server\<Номер версии>***
>
> - **IndeedEA.Server-x64.ru-ru.msi** - Пакет для установки Indeed Enterprise Server 7
> - **/Misc/EA.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.

Установка

1. Выполнить установку Indeed Enterprise Server 7.0 через запуск инсталлятора **IndeedEA.Server-v7.0.x64.ru-ru.msi**.
2. Добавить привязку **https** в настройка **Default Web Site** в IIS Manager.

> **Информация**
>
> **Indeed Enterprise Server 7.0** 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.

Редактирование конфигурационного файла.

> **Информация**
>
> Для генерации ключей шифрования рекомендуется использовать утилиту **EA.KeyGen.exe** выбрав произвольный алгоритм.

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**.
    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 adDbContext в атрибуте id.
    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 EA 7.0,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 (rootUserCatalogProviderId)**; **нижнее подчеркивание**; **идентификатор пользователя в каталоге**".

> **Примечание**
>
> Пользователь должен находится внутри каталога пользователей.

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
> ```

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

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

> **Примечание**
>
> Если используется несколько серверов, указываем адрес балансировщика нагрузки.

b. **CertificateThumbprint** - если закрытый ключ в реестре, а сертификат в хранилище компьютера.
c. **CertificateFilePath** - если ключевая пара в pfx.
d. **CertificateFilePassword** - пароль от pfx.

Пример

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

Настройка первичной конфигурации.

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.**

> **Примечание**
>
> Для использования данных провайдеров у вас должен быть установлен **Indeed Bsp Broker** и используемые провайдеры.

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

3. Установите
4. 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.**