

Авторизация по протоколу OAuth 2.0

Настроить авторизацию интегрированных приложений по протоколу OAuth 2.0

Версия 8.0



Эта документация предоставляется с ограничениями на использование и защищена законами об интеллектуальной собственности. За исключением случаев, прямо разрешенных в вашем лицензионном соглашении или разрешенных законом, вы не можете использовать, копировать, воспроизводить, переводить, транслировать, изменять, лицензировать, передавать, распространять, демонстрировать, выполнять, публиковать или отображать любую часть в любой форме или посредством любые значения. Обратный инжиниринг, дизассемблирование или декомпиляция этой документации, если это не требуется по закону для взаимодействия, запрещены.

Информация, содержащаяся в данном документе, может быть изменена без предварительного уведомления и не может гарантировать отсутствие ошибок. Если вы обнаружите какие-либо ошибки, сообщите нам о них в письменной форме.

Содержание

Настроить авторизацию интегрированных приложений по протоколу OAuth 2.0	4
Установить и настроить Identity Service	4
Настроить интеграцию с Identity Service на стороне Creatio	7
Настроить авторизацию приложений по протоколу OAuth 2.0	8

Настроить авторизацию интегрированных приложений по протоколу OAuth 2.0

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

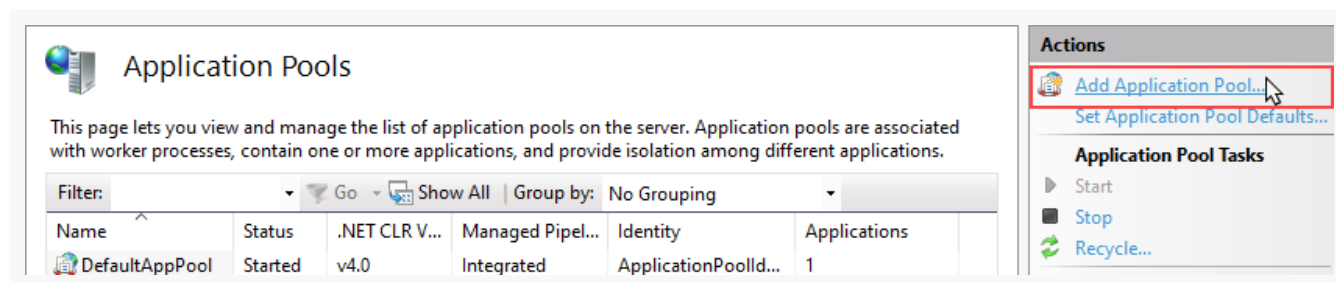
Вы можете настроить для приложений и веб-сервисов, интегрированных с Creatio, безопасную авторизацию по протоколу OAuth 2.0. Эта технология позволяет не передавать сторонним приложениям логин и пароль Creatio, а также ограничить права внешних приложений на действия в Creatio.

Установить и настроить Identity Service

Установка и настройка Identity Service выполняется после развертывания сервера базы данных и сервера приложения Creatio. Чтобы установить Identity Service:

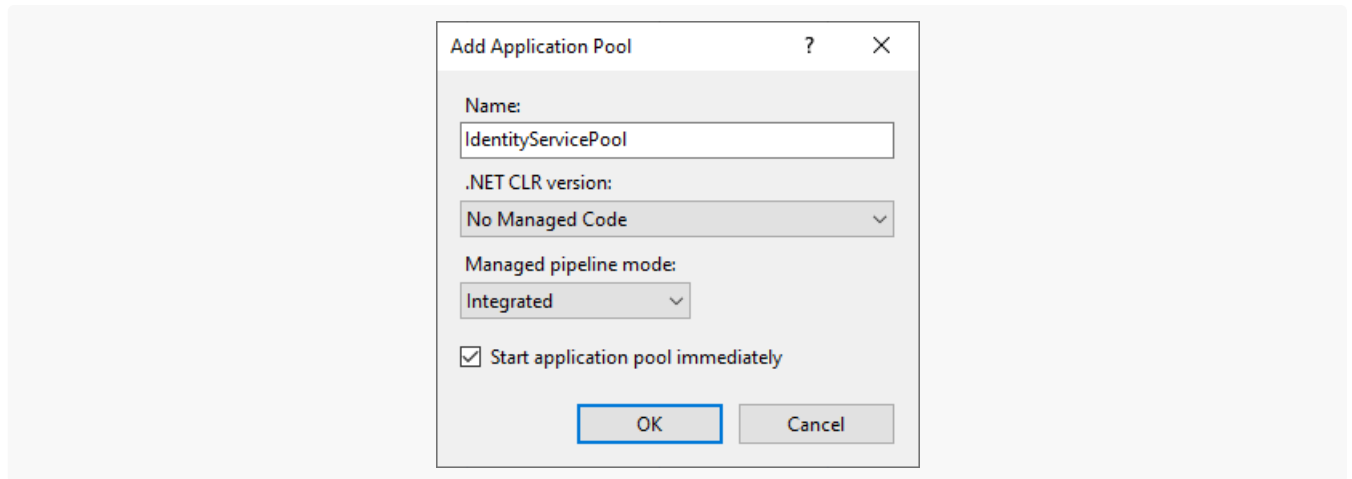
1. Перейдите на сервер приложения.
2. Установите .NET Core runtime 2.2. [Скачать установочный файл](#)
3. Установить .NET Core Hosting Bundle. [Скачать установочный файл](#)
4. Перезапустите IIS.
5. В папке с установочными файлами Creatio найдите архив **IdentityService.zip** и распакуйте его.
6. Добавьте в IIS новый **пул** приложения для Identity Service.
 - a. В области [*Connections*] окна управления IIS перейдите в секцию [*Applications Pools*].
 - b. В области [*Actions*] выберите действие [*Add Application Pool...*].

Рис. 1. — Добавление пула в IIS



- c. В окне настройки пула укажите его название, например, "IdentityServicePool". В поле [*.NET CLR Version*] укажите значение "No Managed Code".

Рис. 2 — Пример настройки пула Identity Service



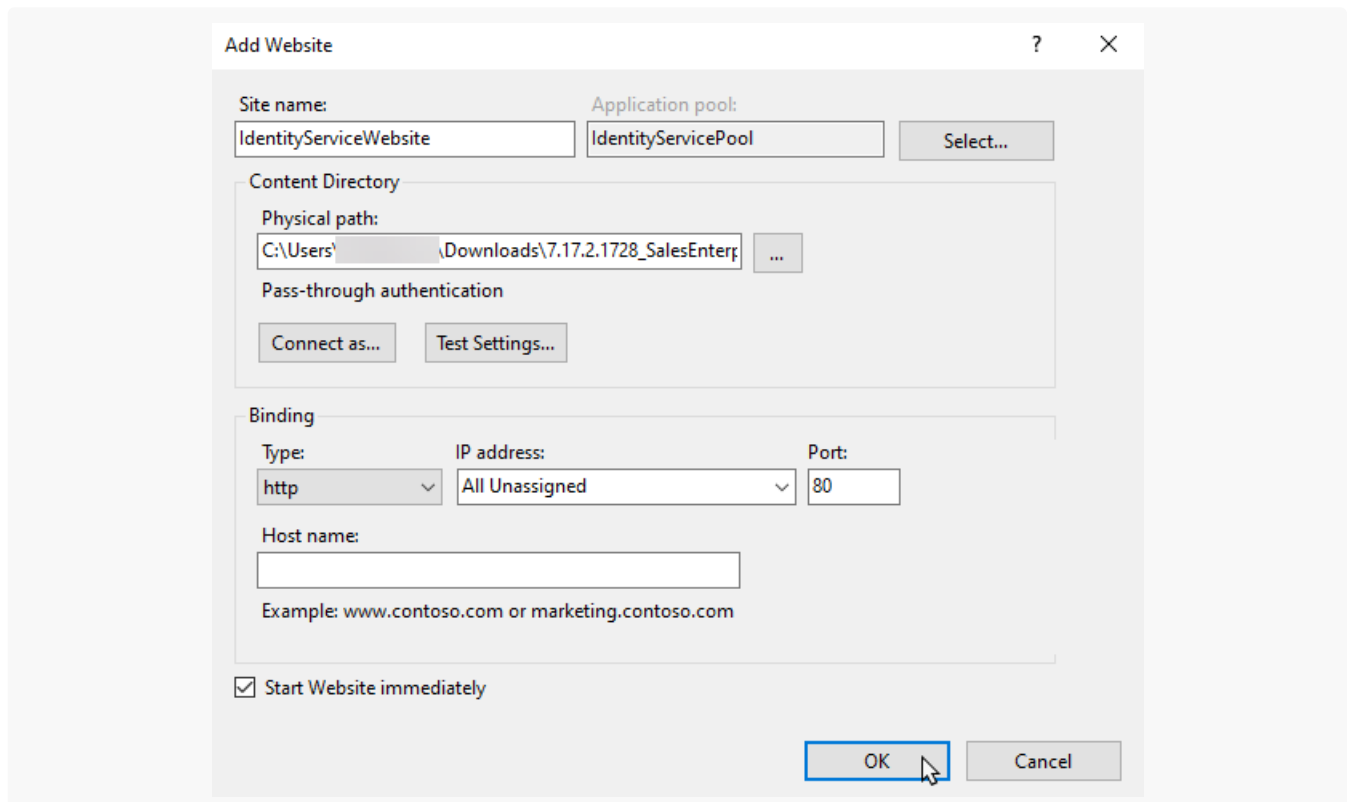
7. Настройте **доступ** к пулу приложения:

- Кликните правой кнопкой мыши по созданному пулу. В контекстном меню выберите [*Advanced Settings...*].
- В открывшемся окне в поле [*Identity*] укажите пользователя для подключения к Identity Service с правом доступа к папке приложения.

8. Создайте в IIS новый **сайт** для Identity Service.

- В окне управления IIS щелкните правой клавишей мыши по [*Sites*] и выберите [*Add Website*] в контекстном меню.
- Укажите название сайта, пул и путь к корневому каталогу с файлами Identity Service.

Рис. 3 — Пример настройки сайта в IIS



9. Настройте сайт на работу с **СУБД** вашего приложения Creatio. Для этого в конфигурационном файле **appSettings.json**, который находится в корневом каталоге Identity Service:

- В параметре “DbProvider” укажите “MsSqlServer” или “Postgres”.
- В настройке MsSqlConnection или PostgresConnection укажите строку соединения. Рекомендуется задавать то же значение строки, что и в основном приложении Creatio. При этом важно, чтобы у пользователя, под которым выполняется подключение к БД, были права на создание и редактирование таблиц.

На заметку. Для подключения Identity Service к приложениям, которые работают с СУБД Oracle, необходимо развернуть дополнительный экземпляр БД на PostgreSQL или Microsoft SQL.

10. Настройте **системного пользователя** Identity Service. Для этого придумайте уникальные значения ClientId, ClientName, ClientSecret и укажите их в блоке “Clients” конфигурационного файла **appSettings.json**, который находится в корневом каталоге Identity Service. Эти значения будут использоваться для настройки взаимодействия между Identity Service и Creatio. Для всех значений можно использовать большие и маленькие буквы, цифры, специальные символы, например, скобки или знаки препинания.

Рекомендуемые параметры:

- ClientId — 16 символов;
- ClientSecret — 32 символа;
- ClientName — произвольное количество символов.

Пример настройки блока “Clients”

```
"[{\"ClientId\":\"{сгенерировать ClientId}\",\"ClientName\":\"{сгенерировать имя}\",\"Secrets
```

На заметку. Во избежание ошибок при запуске Identity Service в файле appsettings.json в настройке “**X509CertificatePath**” необходимо указать полный путь к файлу openssl.pfx, который находится в корневом каталоге папки с Identity Service.

11. Переведите Identity Service на работу по протоколу **HTTPS**. Настройки аналогичны тем, которые необходимо выполнить для приложения Creatio. Подробнее: [Перевести Creatio с HTTP на HTTPS](#).

12. Включите **логирование** работы Identity Service.

- В файле web.config, который находится в папке приложения Identity Service, для параметра “stdoutLogEnabled” установить значение “true”.
- В том же файле для параметра “stdoutLogFile” укажите путь к папке, где будут храниться логи приложения.
- Настройте уровень логирования в appsettings.json, который находится в корневом каталоге Identity Service:

```
"Logging": {
  "LogLevel": {
    "Default": "Error"
  }
}
```

Настроить интеграцию с Identity Service на стороне Creatio

1. **Включите** функциональность интеграции с приложением по протоколу OAuth 2.0. Для этого выполните для базы данных вашего приложения приведенный ниже скрипт. Он универсален и может использоваться для Microsoft SQL и PostgreSQL.

```
UPDATE "AdminUnitFeatureState"

SET "FeatureState" = 1

WHERE "FeatureId" = (

SELECT

  "Id"

FROM "Feature"

WHERE "Code" = 'OAuth20Integration')
```

2. Заполните [системные настройки](#), которые входят в группу “OAuth 2.0”:
- a. **“Адрес сервера авторизации для интеграций по OAuth 2.0”** (код “OAuth20IdentityServerUrl”) — адрес IdentityServer, например, <http://isEnpointExample>.
 - b. **“Идентификатор приложения для интеграций по OAuth 2.0”** (код “OAuth20IdentityServerClientId”) — идентификатор системного пользователя, указанный в параметре “ClientId” файла appSettings.json при настройке IdentityServer.
 - c. **“Секрет клиента для интеграций по OAuth 2.0”** (код “OAuth20IdentityServerClientSecret”) — секретный ключ системного пользователя, указанный в параметре “ClientSecret” файла appSettings.json при настройке IdentityServer.
3. Создайте ресурс приложения по умолчанию. Это действие выполняется один раз при настройке интеграции Identity Service с Creatio.


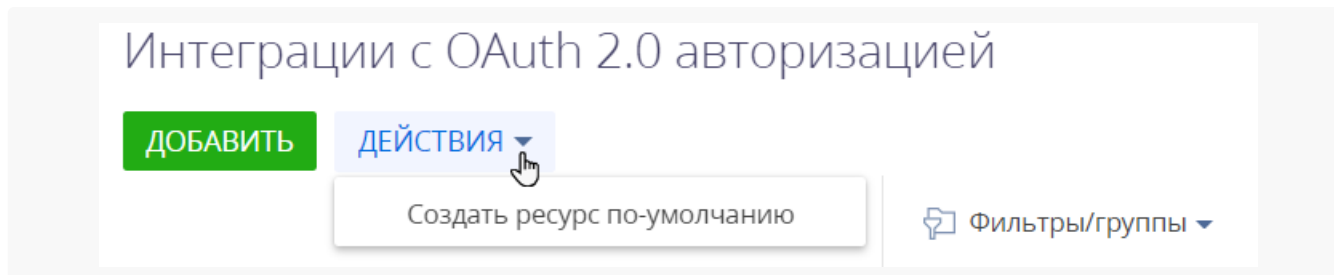
- a. Откройте дизайнер системы по кнопке .
- b. Перейдите в раздел [*Интеграции с OAuth 2.0 авторизацией*].
- c. В меню действий выберите [*Создать ресурс по умолчанию*].

Рис. 4 — Создание ресурса по умолчанию



В результате в приложении будет создана запись ресурса по умолчанию с учетными данными вашего Identity Service.


Настроить авторизацию приложений по протоколу OAuth 2.0

После установки Identity Service и подключения его к Creatio необходимо для каждого из приложений, которые будут авторизоваться в Creatio по протоколу OAuth 2.0, создать запись клиента. Для этого:

1. Откройте дизайнер системы по кнопке .
2. Перейдите в раздел [*Интеграции с OAuth 2.0 авторизацией*].
3. Нажмите [*Добавить*].
4. На открывшейся странице заполните параметры клиента (приложения, которое будет подключаться к Creatio):
 - a. [*Название*] — заголовок, который будет отображаться в реестре интеграций и логах.
 - b. [*URL приложения*] — адрес приложения или веб-сервиса, который интегрируется с Creatio.
 - c. [*Описание*] — задача, которую решает данная интеграция.
 - d. [*Активен*] — признак определяет, используется ли интеграция с данным приложением или веб-сервисом.
 - e. [*Пользователь*] — пользователь системы с требуемым для данной интеграции набором прав. Рекомендуется настроить права доступа для этого пользователя таким образом, чтобы он имел доступ только на чтение и редактирование тех полей, в которые интегрируемое приложение или веб-сервис будут вносить изменения. Например, для веб-сервиса, передающего в Creatio курсы валют, это поля [*Курс*] и [*Начало*] страницы записи справочника [*Валюты*].


Учетные данные клиента (идентификатор и секрет) заполняются автоматически.

Рис. 5 — Пример настройки клиента

 Основные сведения

Название*

integration example

 URL приложения*


http://example.info


Описание


my integration example

Дата создания


06.10.2020 18:21

 Активен ☐


 Учетные данные клиента

 Идентификатор клиента

E78DA10CA8B2A9DEBD88C73BA6126D29

 Секрет клиента

298DFE56921802E77E1048BE2CD5D5784A4D0C98A5CCF9890595435F3D6DA16F

 Пользователь системы*

Федоров Артем

5. Сохраните запись.

6. Повторите шаги 3–6 для всех приложений, которым необходима авторизация по протоколу OAuth 2.0.