

Additional setup

Set up OAuth 2.0 authorization for integrated applications

Version 7.17



This documentation is provided under restrictions on use and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this documentation, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

Table of Contents

Set up OAuth 2.0 authorization for integrated applications	4
Install and set up the Identity Service	4
Set up the Identity Service integration on Creatio's end	7
Set up the OAuth 2.0 authorization	8

Set up OAuth 2.0 authorization for integrated applications

PRODUCTS: [ALL CREATIO PRODUCTS](#)

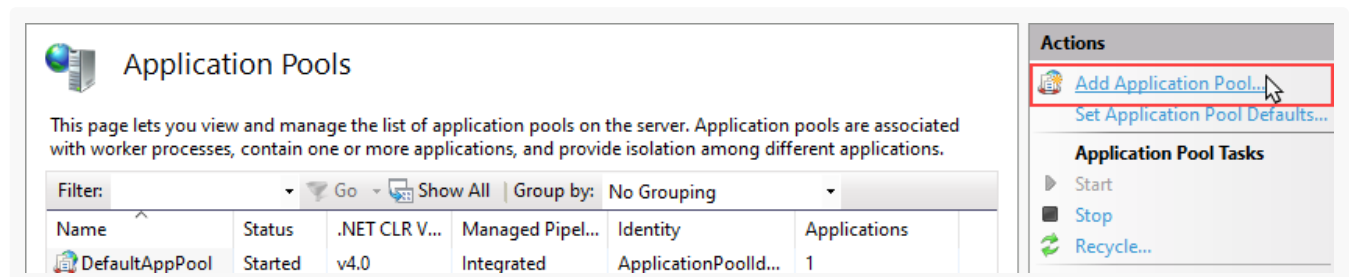
Use OAuth 2.0 protocol to securely authorize third-party applications and web services you integrate with Creatio. This technology does not pass Creatio logins and passwords to third-party applications. OAuth 2.0 also lets you restrict Creatio permissions for the integrated applications.

Install and set up the Identity Service

Deploy the database and Creatio application servers before installing and configuring the Identity Service. To install the Identity Service:

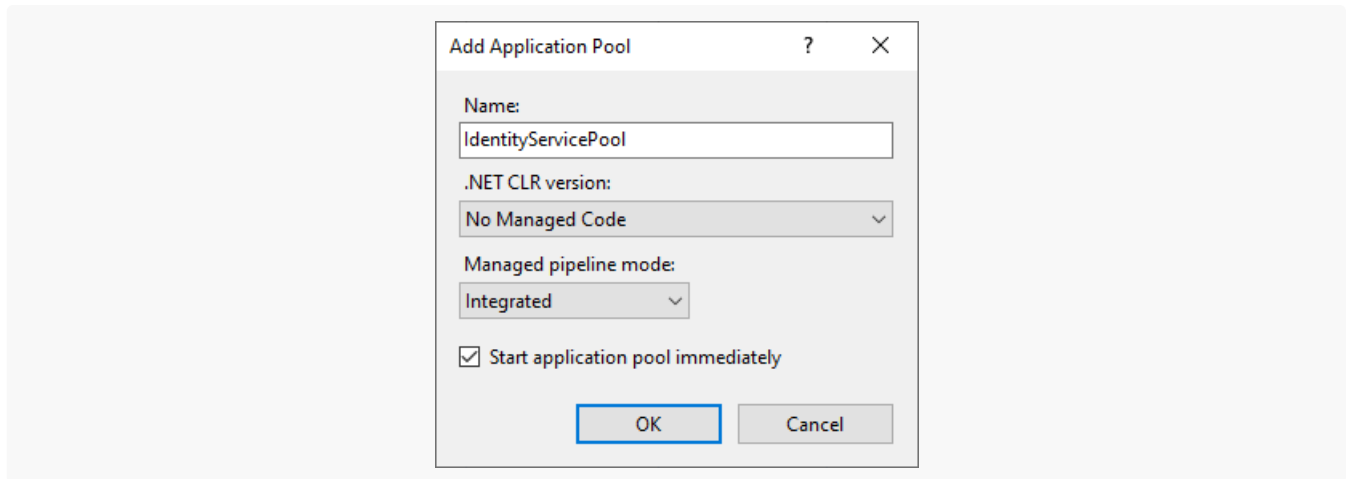
1. Access the Creatio application server.
2. Install the .NET Core Hosting Bundle [Download the install file](#)
3. Restart the IIS.
4. Navigate to the Creatio install file folder, find the **IdentityService.zip** archive, and unzip it.
5. Add the Identity Service application **pool** to the IIS.
 - a. Go to the [*Application Pools*] section in the [*Connections*] area of the IIS management window.
 - b. Select [*Add Application Pool...*] in the [*Actions*] area.

Fig. 1 Adding the pool to the IIS



- c. Specify the pool name in the pool settings window, for example, "IdentityServicePool". Set the [*.NET CLR Version*] field to "No Managed Code".

Fig. 2 Setting up the Identity Service pool



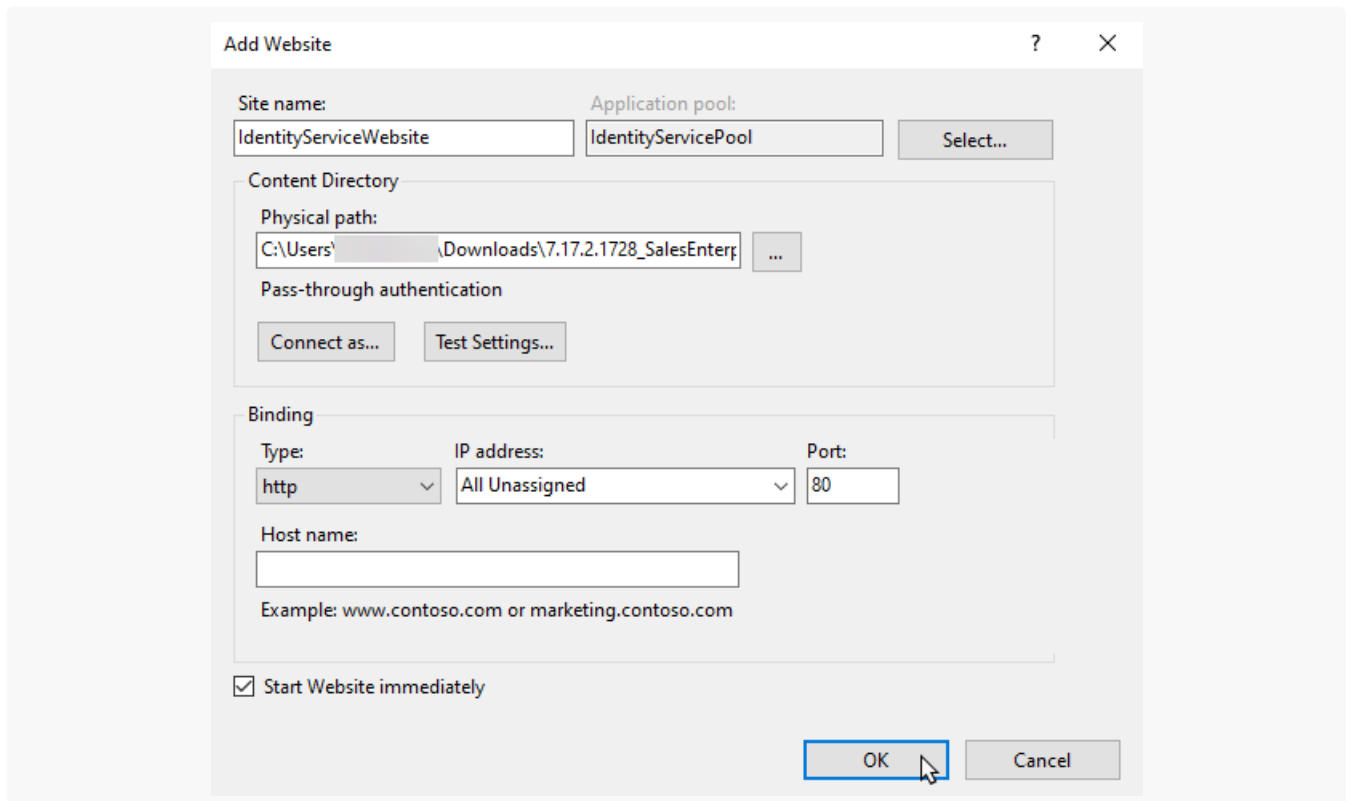
6. Set up **access** to the application pool:

- a. Right-click the newly-created pool. Select [*Advanced Settings...*] in the context menu.
- b. Specify the user with Identity Service directory access permissions in the [*Identity*] field of the newly-opened window.

7. Create a new Identity Service **site** in the IIS.

- a. Click [*Sites*] on the IIS control panel and select [*Add Website*] from the context menu.
- b. Specify the site name, the pool and the path to the Identity Service root directory.

Fig. 3 Setting up the site in the IIS



8. Connect the site to your Creatio **DBMS**. To do so, edit the **appSettings.json** configuration file in the Identity Service root directory:

- a. Set the “DbProvider” parameter to “MsSqlServer” or “Postgres”.
- b. Specify the connection string in the “MsSqlConnection” or “PostgresConnection” setting. We recommend using the same connection string you specified in Creatio. The user that connects to the database must have permissions to create and update the tables.

Note. To connect the Identity Service to Creatio with Oracle DBMS, deploy an additional PostgreSQL or MSSQL database instance.

9. Set up the Identity Service **system user**. To do so, specify the unique ClientId, ClientName, and ClientSecret values in the “Clients” block of the **appSettings.json** configuration file. The file is located in the Identity Service root catalog. Creatio and the Identity Service will use these values to interact with each other. All parameters support uppercase and lowercase letters, numbers, and special characters, for example, brackets or punctuation marks.

Recommended parameters:

ClientId — 16 characters.

ClientSecret — 32 characters.

ClientName — any number of characters.

“Clients” block setup example:

```
"[{"ClientId\":\"{generate ClientId}\",\"ClientName\":\"{generate name}\",\"Secrets\":[\"{ge
```

10. Switch the Identity Service to **HTTPS**. The setup process is similar to switching Creatio to HTTPS. Read more: [Switch Creatio website from HTTP to HTTPS](#).

11. Enable the Identity Service **logging**.

- a. Navigate to the Identity Service directory, open the web.config file, and set the “stdoutLogEnabled” parameter to “true”.
- b. Specify where you would like to store the Identity Service logs in the file’s “stdoutLogFile” parameter.
- c. Open the appsettings.json file in the Identity Service root directory and configure the log level:

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

Set up the Identity Service integration on Creatio's end

1. **Enable** the OAuth 2.0 integration in Creatio. To do so, execute this script in your Creatio database. Use it for both MSSQL and PostgreSQL.

```
UPDATE "AdminUnitFeatureState"

    SET "FeatureState" = 1

WHERE "FeatureId" = (

    SELECT

        "Id"

    FROM "Feature"

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


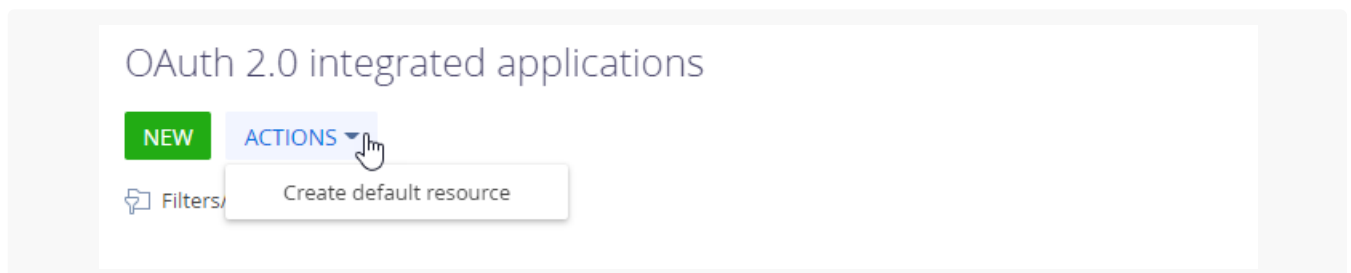
2. Fill in the [system settings](#) in the “OAuth 2.0” group:
 - a. **“Authorization server Url for OAuth 2.0 integrations”** (“OAuth20IdentityServerUrl” code) — the IdentityServer URL, for instance, http://isEndpointExample.
 - b. **“Client id for OAuth 2.0 integrations”** (“OAuth20IdentityServerClientId” code) — the Identity Service user id you specified in the “ClientId” parameter of the appSettings.json file when setting up the IdentityServer.
 - c. **“Client secret for OAuth 2.0 integrations”** (“OAuth20IdentityServerClientSecret” code) — the Identity Service user's secret key you specified in the “ClientSecret” parameter of the appSettings.json file when setting up the IdentityServer.
3. Create a default resource. You only need to perform this action once when setting up the Identity Service integration.
 - a. Click  to open the System Designer.
 - b. Open the [*OAuth 2.0 integrated applications*] section.
 - c. Select [*Create default resource*] in the [*Actions*] menu.

Fig. 4 Adding a default resource



This will create a default resource record with your Identity Service account details.

Set up the OAuth 2.0 authorization

Once you install the Identity Service and connect it to Creatio, add a client record for each application you are going to authorize with OAuth 2.0. To do so:


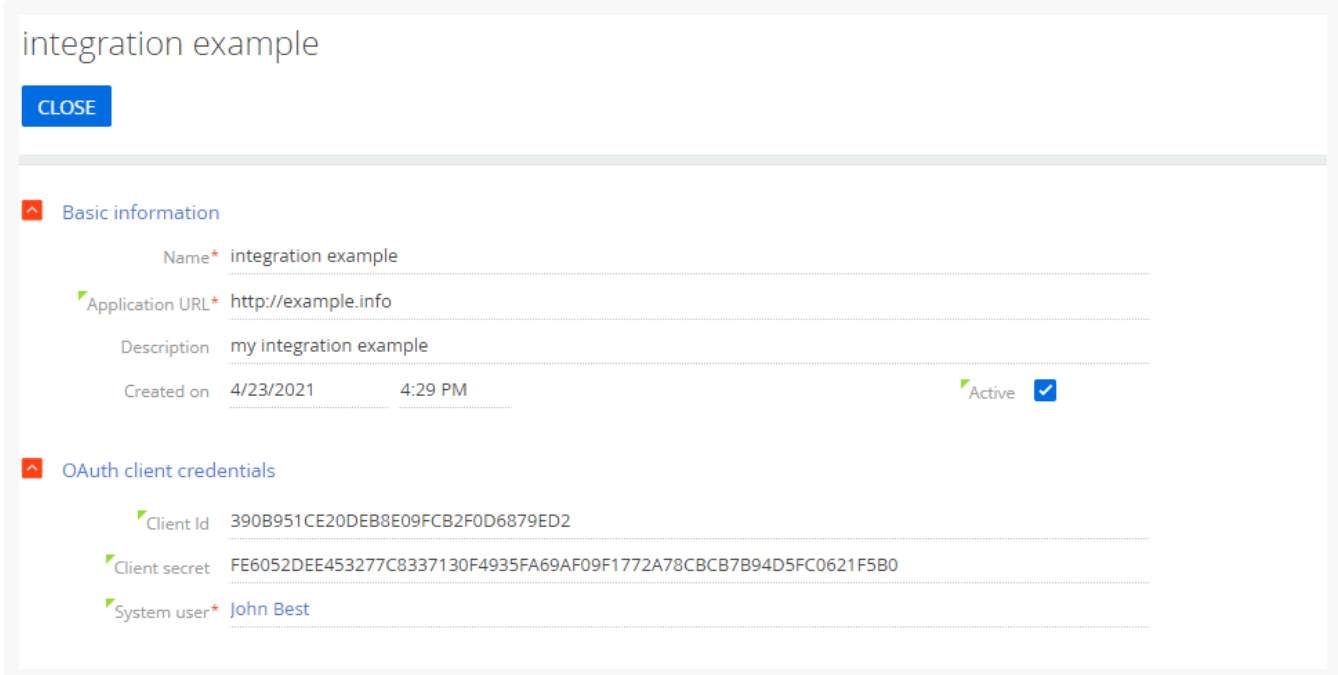
1. Click  to open the System Designer.
2. Open the [*OAuth 2.0 integrated applications*] section.
3. Click [*New*].
4. Fill in the client parameters for the relevant application on the newly-opened page.
 - a. [*Name*] — the title that the integration list and the logs will use.
 - b. [*Application URL*] — the URL of the integrated application or the web service.
 - c. [*Description*] — the purpose of the integration.
 - d. [*Active*] — enables and disables the integration.
 - e. [*System user*] — the Creatio user with sufficient permissions for this integration. We recommend permitting this user to only read and edit the fields the integrated application or the web service need to change. For example, if you are integrating a web service that passes the currency exchange rates to Creatio, grant permissions to only read and edit the [*Rate*] and [*Start*] fields of the [*Currency*] lookup. Creatio automatically populates the **client account details** (the Id and the secret).

Fig. 5 Setting up the client



integration example

CLOSE

Basic information

Name* integration example

Application URL* http://example.info

Description my integration example

Created on 4/23/2021 4:29 PM Active

OAuth client credentials

Client Id 390B951CE20DEB8E09FCB2F0D6879ED2

Client secret FE6052DEE453277C8337130F4935FA69AF09F1772A78CBCB7B94D5FC0621F5B0

System user* John Best

5. Save the record.
6. Repeat steps 3-6 for all applications you need to authorize with OAuth 2.0.