

PLATFORM SETUP GUIDES / FLOWX.AI Engine setup guide / configuring-access-roles-for-processes



Contents

 PLATFORM SETUP GUIDES / FLOWX.AI Engine setup guide / Configuring access roles for processes

PLATFORM SETUP GUIDES / FLOWX.AI Engine setup guide / Configuring access roles for processes

Access to a process definition

Setting up user role-based access on process definitions is done by configuring swimlanes on the process definition.

» Swimlanes

By default, all process nodes belong to the same swimlane. If more swimlanes are needed, they can be edited in the process definition settings panel.

Swimlane role settings apply to the whole process, the process nodes or the actions to be performed on the nodes.

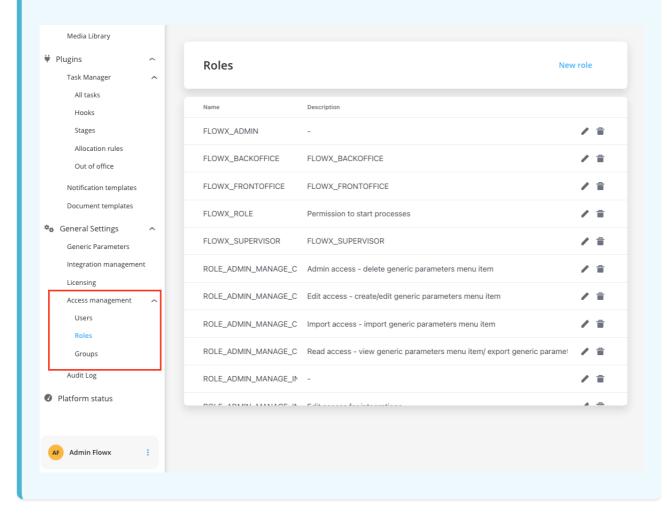
First, the desired user roles need to be configured in the identity provider solution and users must be assigned the correct roles.

© FLOWX.AI 2023-07-26 Page 1/9





You can use the **Access management** tab under **General Settings** to administrate all the roles.



DANGER

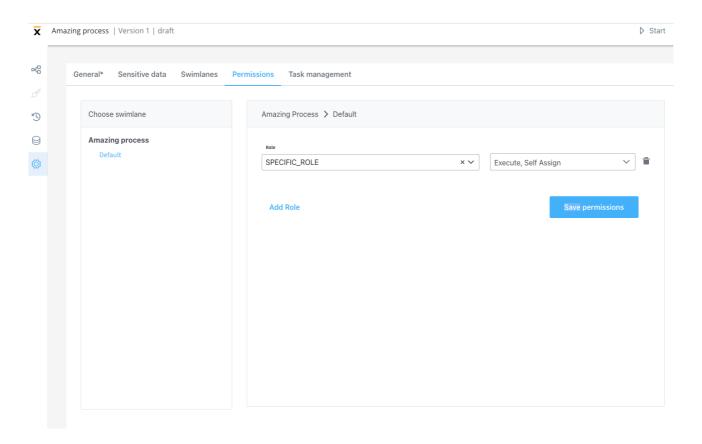
To be able to access the roles defined in the identity provider solution, a **service account** with appropriate permissions needs to be added in the identity provider. And the details of that service account **need to be set up in the platform configuration**.

© FLOWX.AI 2023-07-26 Page 2 / 9



The defined roles will then be available to be used in the process definition settings (**Permissions** tab) panel for configuring swimlane access.

A **Default** swimlane comes with two default permissions assigned based on a specific role.



- execute the user will be able to start process instances and run actions on them
- self-assign the user can assign a process instance to them and start working on it



This is valid for > 2.11.0 FLOWX.AI platform release.

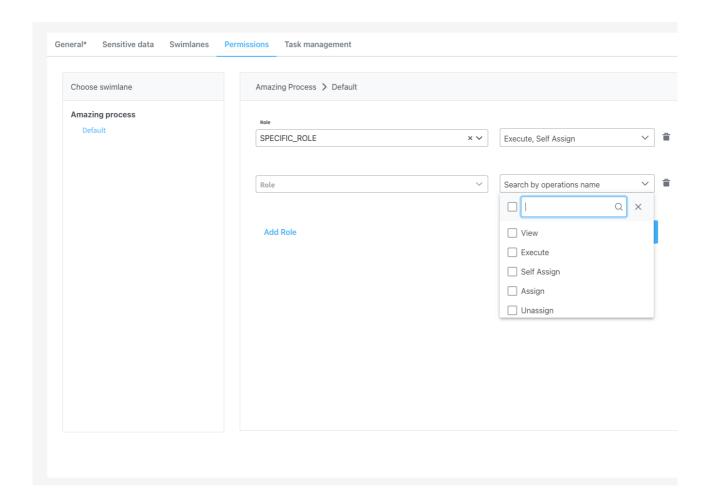


Other **Permissions** can be added manually, depending on the needs of the user. Some permissions are needed to be configured so you can use features inside Task Management plugin. Specific roles need to be assigned separately on a few available process operations. These are:

- **view** the user will be able to view process instance data
- assign user can assign tasks to other users (this operation is only accessible through the Task management plugin)
- unassign user can unassign tasks from other users (this operation is only accessible through the Task management plugin)
- hold user can mark the process instance as on hold (this operation is only accessible through the Task management plugin)
- unhold user can mark the process instance as not on hold (this operation is only accessible through the Task management plugin)

© FLOWX.AI 2023-07-26 Page 4 / 9







< 2.11.0 platform release - if no role is configured on an operation, no restrictions will be applied.

Configuration examples



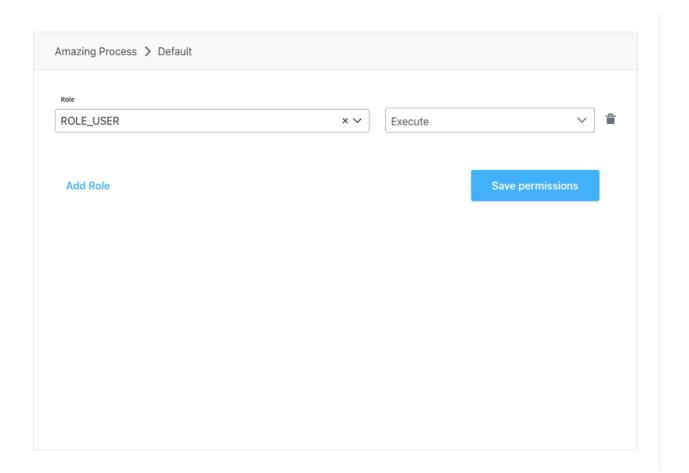
A CAUTION

Valid for < 2.11.0 release version.



Regular user

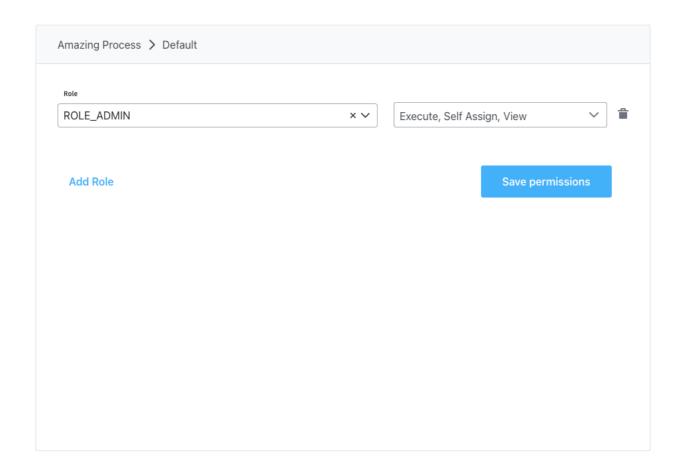
Below you can find an example of configuration of roles for a regular user:



Admin

Below you can find an example of configuration of roles for an admin user:







A CAUTION

! Starting with 2.11.0 release, specific roles are needed, otherwise, restrictions will be applied.

After setting up your preferred identity provider solution, you will need to add the desired access roles in the application configuration for the FLOWX Engine (using environment variables):

» Authorization & access roles



Restricting process instance access based on business filters

» Business filters

Before they can be used in the process definition the business filter attributes need to be set in the identity management platform. They have to be configured as a list of filters and should be made available on the authorization token. Application users will also have to be assigned this value.

Viewing processes instances

Active process instances and their related data can be viewed from the FLOWX Designer. A user needs to be assigned to a specific role in the identity provider solution to be able to view this information.

By default, this role is named FL0WX_R0LE, but its name can be changed from the application configuration of the Engine by setting the following environment variable:

FLOWX_PROCESS_DEFAULTROLES

When viewing process instance-related data, it can be configured whether to hide specific sensitive user data. This can be configured using the FLOWX_DATA_ANONYMIZATION environment variable.

Access to REST API

© FLOWX.AI 2023-07-26 Page 8 / 9



To restrict API calls by user role, you will need to add the user roles in the application config:

Was this page helpful?