



# **Contents**

 FIOWX.AI DESIGNER / Designer setup guide / Configuring access rights for Admin

# FIOWX.AI DESIGNER / Designer setup guide / Configuring access rights for Admin

Granular access rights can be configured for restricting access to the Admin component.

Access authorizations are provided, each with specified access scopes:

1. Manage-platform - for configuring access for managing platform details

# Available scopes:

- read users are able to view platform status
- admin users are able to force health check scan
- 2. Manage-processes for configuring access for managing process definitions

# Available scopes:

- import users are able to import process definitions and process stages
- read users are able to view process definitions and stages
- edit users are able to edit process definitions

© FLOWX.AI 2023-07-26 Page 1 / 6



- admin users are able to publish and delete process definitions, delete stages, edit sensitive data for process definitions
- 3. **Manage-configurations** for configuring access for managing generic parameters

#### Available scopes:

- **import** users are able to import generic parameters
- read users are able to view generic parameters
- edit users are able to edit generic parameters
- admin users are able to delete generic parameters
- 4. **Manage-users** for configuring access for access management

#### Available scopes:

- read users are able to read all users, groups and roles
- edit users are able to create/update any user group or roles
- admin users are able to delete users, groups or roles
- 5. **Manage-integrations** for configuring integrations with adapters

#### Available scopes:

- **import** users are able to import integrations
- read users are able to view all the integrations, scenarios and scenarios configuration(topics/ input model/ output model/ headers)
- edit users are able to create/update/delete any values for integrations/scenarios and also scenarios configuration (topics/input model/

© FLOWX.AI 2023-07-26 Page 2 / 6



output model/ headers)

• admin - users are able to delete integrations/scenarios with all children

The Admin service is configured with the following default users roles for each of the access scopes mentioned above:

# · manage-platform

- o read:
  - ROLE ADMIN MANAGE PLATFORM READ
  - ROLE\_ADMIN\_MANAGE\_PLATFORM\_ADMIN
- o admin:
  - ROLE\_ADMIN\_MANAGE\_PLATFORM\_ADMIN

# • manage-processes

- import:
  - ROLE ADMIN MANAGE PROCESS IMPORT
  - ROLE ADMIN MANAGE PROCESS EDIT
  - ROLE\_ADMIN\_MANAGE\_PROCESS\_ADMIN
- read:
  - ROLE\_ADMIN\_MANAGE\_PROCESS\_READ
  - ROLE ADMIN MANAGE PROCESS IMPORT
  - ROLE ADMIN\_MANAGE\_PROCESS\_EDIT
  - ROLE\_ADMIN\_MANAGE\_PROCESS\_ADMIN
- edit:
  - ROLE\_ADMIN\_MANAGE\_PROCESS\_EDIT
  - ROLE\_ADMIN\_MANAGE\_PROCESS\_ADMIN
- admin:
  - ROLE\_ADMIN\_MANAGE\_PROCESS\_ADMIN

© FLOWX.AI 2023-07-26 Page 3 / 6



# manage-configurations

- import:
  - ROLE ADMIN MANAGE CONFIG IMPORT
  - ROLE\_ADMIN\_MANAGE\_CONFIG\_EDIT
  - ROLE\_ADMIN\_MANAGE\_CONFIG\_ADMIN
- o read:
  - ROLE ADMIN MANAGE CONFIG READ
  - ROLE\_ADMIN\_MANAGE\_CONFIG\_IMPORT
  - ROLE\_ADMIN\_MANAGE\_CONFIG\_EDIT
  - ROLE\_ADMIN\_MANAGE\_CONFIG\_ADMIN
- o edit:
  - ROLE\_ADMIN\_MANAGE\_CONFIG\_EDIT
  - ROLE ADMIN MANAGE CONFIG ADMIN
- admin:
  - ROLE\_ADMIN\_MANAGE\_CONFIG\_ADMIN

#### · manage-users

- read:
  - ROLE\_ADMIN\_MANAGE\_USERS\_READ
  - ROLE\_ADMIN\_MANAGE\_USERS\_EDIT
  - ROLE\_ADMIN\_MANAGE\_USERS\_ADMIN
- edit:
  - ROLE\_ADMIN\_MANAGE\_USERS\_EDIT
  - ROLE\_ADMIN\_MANAGE\_USERS\_ADMIN
- admin:
  - ROLE\_ADMIN\_MANAGE\_USERS\_ADMIN

# manage-integrations

© FLOWX.AI 2023-07-26 Page 4 / 6



- import:
- ROLE ADMIN MANAGE INTEGRATIONS IMPORT
- ROLE ADMIN MANAGE INTEGRATIONS EDIT
- ROLE\_ADMIN\_MANAGE\_INTEGRATIONS\_ADMIN
- read:
  - ROLE ADMIN MANAGE INTEGRATIONS READ
  - ROLE\_ADMIN\_MANAGE\_INTEGRATIONS\_IMPORT
  - ROLE ADMIN MANAGE INTEGRATIONS EDIT
  - ROLE\_ADMIN\_MANAGE\_INTEGRATIONS\_ADMIN
- edit:
  - ROLE ADMIN MANAGE INTEGRATIONS EDIT
  - ROLE\_ADMIN\_MANAGE\_INTEGRATIONS\_ADMIN
- o admin:
  - ROLE\_ADMIN\_MANAGE\_INTEGRATIONS\_ADMIN



These roles need to be defined in the chosen identity provider solution. It can be either kyecloak, RH-SSO, or other identity provider solution.

In case other custom roles are needed, you can configure them using environment variables. More than one role can be set for each access scope.

To configure access for each of the roles above, adapt the following input:

SECURITY\_ACCESSAUTHORIZATIONS\_AUTHORIZATIONNAME\_SCOPES\_SCOPENAM E\_ROLESALLOWED: NEEDED\_ROLE\_NAMES

© FLOWX.AI 2023-07-26 Page 5 / 6



Possible values for AUTHORIZATIONNAME: MANAGEPLATFORM, MANAGEPROCESSES, MANAGECONFIGURATIONS, MANAGEUSERS.

Possible values for SCOPENAME: import, read, edit, admin.

For example, if you need to configure role access for read, insert this:

SECURITY\_ACCESSAUTHORIZATIONS\_MANAGEPROCESSES\_SCOPES\_READ\_ROLE!
ROLE\_NAME\_TEST

Was this page helpful?

© FLOWX.AI 2023-07-26 Page 6 / 6