FLOWX.AI

FlOWX.AI DESIGNER / Designer setup guide

Contents

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

FlOWX.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

- **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/

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**
  - read:
    - ROLE_ADMIN_MANAGE_PLATFORM_READ
    - ROLE_ADMIN_MANAGE_PLATFORM_ADMIN
  - 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

- **manage-configurations**
  - import:
    - ROLE_ADMIN_MANAGE_CONFIG_IMPORT
    - ROLE_ADMIN_MANAGE_CONFIG_EDIT
    - ROLE_ADMIN_MANAGE_CONFIG_ADMIN
  - read:
    - ROLE_ADMIN_MANAGE_CONFIG_READ
    - ROLE_ADMIN_MANAGE_CONFIG_IMPORT
    - ROLE_ADMIN_MANAGE_CONFIG_EDIT
    - ROLE_ADMIN_MANAGE_CONFIG_ADMIN
  - 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**

- 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
- admin:
  - ROLE_ADMIN_MANAGE_INTEGRATIONS_ADMIN

DANGER

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_SCOPENAME_ROLESALLOWED: NEEDED_ROLE_NAMES
```

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_ROLES
ROLE_NAME_TEST
```

Was this page helpful?