FLOWX.AI

PLATFORM DEEP DIVE / Core components / Core extensions / Integration management

Contents

- PLATFORM DEEP DIVE / Core components / Core extensions / Integration management / Configuring access rights for Integration Management

PLATFORM DEEP DIVE / Core components / Core extensions / Integration management / Configuring access rights for Integration Management

Granular access rights can be configured for restricting access to the Integration Management plugin component. These access rights must be configured in the Designer (admin) deployment.

The following access authorizations are provided, with the specified access scopes:

1. **Manage-integrations** - for configuring access for managing integration management

Available scopes:

- import - users can import integrations
- read - users can view integrations
- edit - users can edit integrations
- admin - users can delete integrations

Integration management is preconfigured with the following default users roles for each of the access scopes mentioned above:

- 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 another identity provider solution. For more details on how to define service accounts, check the Access rights section.

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: MANAGEDOCUMENTTEMPLATES.

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

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

```
SECURITY_ACCESSAUTHORIZATIONS_MANAGEINTEGRATIONS_SCOPES_READ_R
ROLE_NAME_TEST
```

Was this page helpful?