

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:

 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

© FLOWX.AI 2023-07-26 Page 1/3



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



## **M** 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.

© FLOWX.AI 2023-07-26 Page 2 / 3



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

SECURITY\_ACCESSAUTHORIZATIONS\_AUTHORIZATIONNAME\_SCOPES\_SCOPENAM E\_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\_ROLE\_NAME\_TEST

Was this page helpful?

© FLOWX.AI 2023-07-26 Page 3 / 3