FLOWX.AI

PLATFORM SETUP GUIDES / CMS setup guide / configuring-access-rights-for-cms

Contents

- PLATFORM SETUP GUIDES / CMS setup guide / Configuring access rights for CMS

PLATFORM SETUP GUIDES / CMS setup guide / Configuring access rights for CMS

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

Two different access authorizations are provided, each with specified access scopes:

1. **Manage-contents** - for configuring access for manipulating CMS contents

Available scopes:

- import - users are able to import enumeration/substitution tags/ content models
- read - users are able to show enumeration/substitution tags/ content models, export enumeration/substitution tags/ content models
- edit - users are able to create/edit enumeration/substitution tags/ content models
- admin - users are able to delete enumeration/substitution tags/ content models

2. **Manage-taxonomies** - for configuring access for manipulating taxonomies

Available scopes

- read - users are able to show languages/source systems
- edit - users are able to edit languages/source systems
- admin - users are able to delete languages/source systems

3. **Manage-media-library** - for configuring access rights to use Media Library

Available scopes

- import - users are able to import assets
- read - users are able to view assets
- edit - users are able to edit assets
- admin - users are able to delete assets

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

- **manage-contents**
  - import:
    - ROLE_CMS_CONTENT_IMPORT
    - ROLE_CMS_CONTENT_EDIT
    - ROLE_CMS_CONTENT_ADMIN
  - read:
    - ROLE_CMS_CONTENT_EDIT
    - ROLE_CMS_CONTENT_ADMIN
    - ROLE_CMS_CONTENT_READ
    - ROLE_CMS_CONTENT_IMPORT
  - edit:

        - ROLE_CMS_CONTENT_EDIT
        - ROLE_CMS_CONTENT_ADMIN
    - admin:
        - ROLE_CMS_CONTENT_ADMIN
- **manage-taxonomies**
    - import:
        - ROLE_CMS_TAXONOMIES_IMPORT
        - ROLE_CMS_TAXONOMIES_EDIT
        - ROLE_CMS_TAXONOMIES_ADMIN
    - read:
        - ROLE_CMS_TAXONOMIES_READ
        - ROLE_CMS_TAXONOMIES_IMPORT
        - ROLE_CMS_TAXONOMIES_EDIT
        - ROLE_CMS_TAXONOMIES_ADMIN
    - edit:
        - ROLE_CMS_TAXONOMIES_EDIT
        - ROLE_CMS_TAXONOMIES_ADMIN
    - admin:
        - ROLE_CMS_TAXONOMIES_ADMIN
- **manage-media-library**
    - import:
        - ROLE_MEDIA_LIBRARY_IMPORT
        - ROLE_MEDIA_LIBRARY_EDIT
        - ROLE_MEDIA_LIBRARY_EDIT
    - read:
        - ROLE_MEDIA_LIBRARY_READ

        - ROLE_MEDIA_LIBRARY_EDIT
        - ROLE_MEDIA_LIBRARY_ADMIN
        - ROLE_MEDIA_LIBRARY_IMPORT
    - edit:
        - ROLE_MEDIA_LIBRARY_EDIT
        - ROLE_MEDIA_LIBRARY_ADMIN
    - admin:
        - ROLE_MEDIA_LIBRARY_ADMIN

> **CAUTION**
>
> The needed roles should be defined in the chosen 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: MANAGECONTENTS, MANAGETAXONOMIES.

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

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

```
SECURITY_ACCESSAUTHORIZATIONS_MANAGECONTENTS_SCOPES_IMPORT_ROLE
ROLE_CMS_CONTENT_IMPORT
```

Was this page helpful?