PLATFORM DEEP DIVE / Plugins / Plugins setup guides / Task Manager plugin setup / configuring-access-rights-for-task-management

Contents

PLATFORM DEEP DIVE / Plugins / Plugins setup guides / Task Manager plugin setup / Configuring access rights for Task management

Granular access rights can be configured for restricting access to the Task management plugin component.

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

1. **manage-tasks** - for configuring access for viewing the tasks lists

Available scopes:

- read - users are able to view tasks

2. **manage-hooks** - for configuring access for managing hooks

Available scopes:

- import - users are able to import hooks
- read - users are able to view hooks
- edit - users are able to edit hooks

- admin - users are able to delete hooks

3. **manage-process-allocation-settings** - for configuring access for managing process allocation settings

Available scopes:

- import - users are able to import allocation rules
- read - users are able to read/export allocation rules
- edit - users are able to edit access - create/edit allocation rules
- admin - users are able to delete allocation rules

4. **manage-out-of-office-users** - for configuring access for managing out-of-office users

Available scopes:

- read - users are able to view out-of-office records
- edit - users are able to create and edit out-of-office records
- admin - users are able to delete out-of-office records

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

- manage-tasks
  - read:
    - ROLE_TASK_MANAGER_TASKS_READ
- manage-hooks
  - import:
    - ROLE_TASK_MANAGER_HOOKS_IMPORT

        - ROLE_TASK_MANAGER_HOOKS_EDIT
        - ROLE_TASK_MANAGER_HOOKS_ADMIN
    - read:
        - ROLE_TASK_MANAGER_HOOKS_READ
        - ROLE_TASK_MANAGER_HOOKS_IMPORT
        - ROLE_TASK_MANAGER_HOOKS_EDIT
        - ROLE_TASK_MANAGER_HOOKS_ADMIN
    - edit:
        - ROLE_TASK_MANAGER_HOOKS_EDIT
        - ROLE_TASK_MANAGER_HOOKS_ADMIN
    - admin:
        - ROLE_TASK_MANAGER_HOOKS_ADMIN
- manage-process-allocation-settings
    - import:
        - ROLE_TASK_MANAGER_PROCESS_ALLOCATION_SETTINGS_IMPORT
        - ROLE_TASK_MANAGER_PROCESS_ALLOCATION_SETTINGS_EDIT
        - ROLE_TASK_MANAGER_PROCESS_ALLOCATION_SETTINGS_ADMIN
    - read:
        - ROLE_TASK_MANAGER_PROCESS_ALLOCATION_SETTINGS_READ
        - ROLE_TASK_MANAGER_PROCESS_ALLOCATION_SETTINGS_IMPORT
        - ROLE_TASK_MANAGER_PROCESS_ALLOCATION_SETTINGS_EDIT

        - ROLE_TASK_MANAGER_PROCESS_ALLOCATION_SETTINGS_ADMIN
    - edit:
        - ROLE_TASK_MANAGER_PROCESS_ALLOCATION_SETTINGS_EDIT
        - ROLE_TASK_MANAGER_PROCESS_ALLOCATION_SETTINGS_ADMIN
    - admin:
        - ROLE_TASK_MANAGER_PROCESS_ALLOCATION_SETTINGS_ADMIN
- manage-out-of-office-users
    - read:
        - ROLE_TASK_MANAGER_OOO_READ
        - ROLE_TASK_MANAGER_OOO_EDIT
        - ROLE_TASK_MANAGER_OOO_ADMIN
    - edit:
        - ROLE_TASK_MANAGER_OOO_EDIT
        - ROLE_TASK_MANAGER_OOO_ADMIN
    - admin:
        - ROLE_TASK_MANAGER_OOO_ADMIN

> ⚠ **CAUTION**
>
> These roles need to 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: MANAGETASKS, MANAGEHOOKS.

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

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

```
SECURITY_ACCESSAUTHORIZATIONS_MANAGEHOOKS_SCOPES_READ_ROLESALL
ROLE_NAME_TEST
```

Was this page helpful?