FLOWX.AI

PLATFORM DEEP DIVE / User roles management

Contents

- PLATFORM DEEP DIVE / User roles management / Swimlanes
- PLATFORM DEEP DIVE / User roles management / Business filters

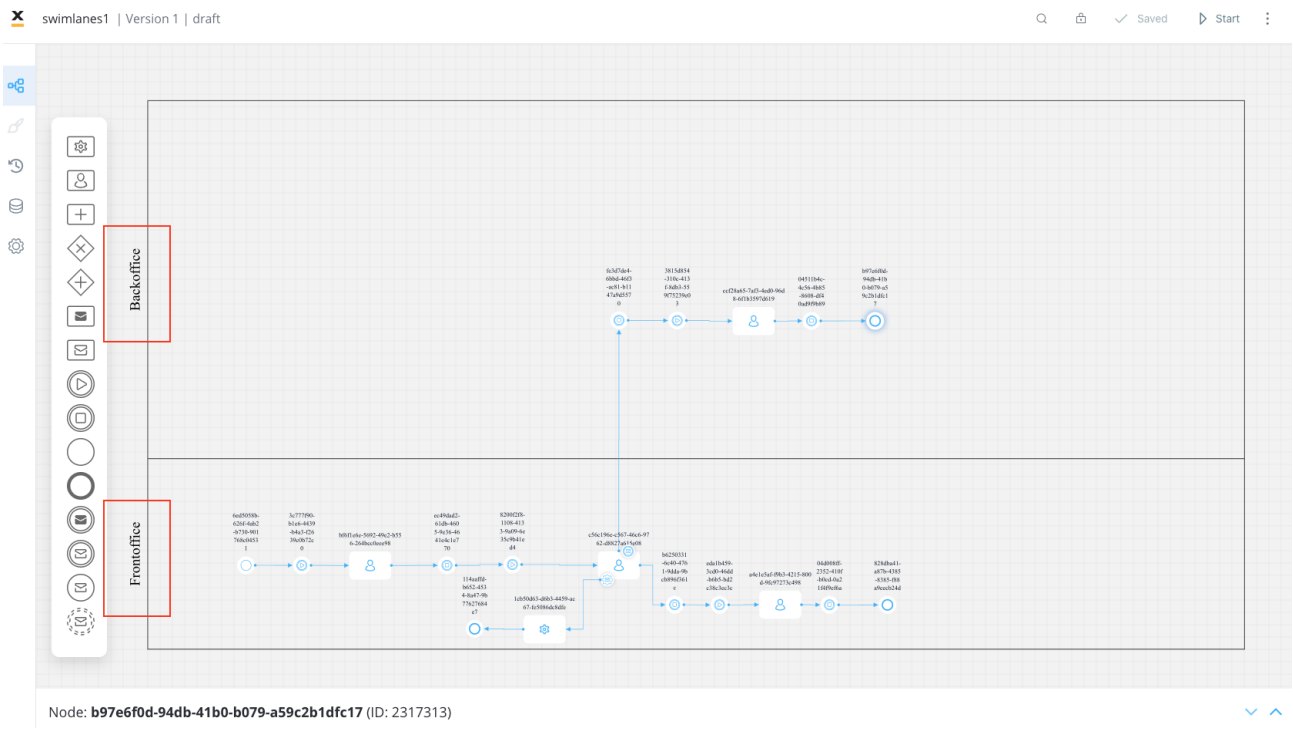
PLATFORM DEEP DIVE / User roles management / Swimlanes

> **INFO**
>
> **What is it?** Swimlanes provide a way of grouping process nodes by process participants.
>
> **Why is it useful?** Using swimlanes we can make sure only certain user roles have access to certain process nodes.

In certain scenarios, it is necessary to restrict access to specific process

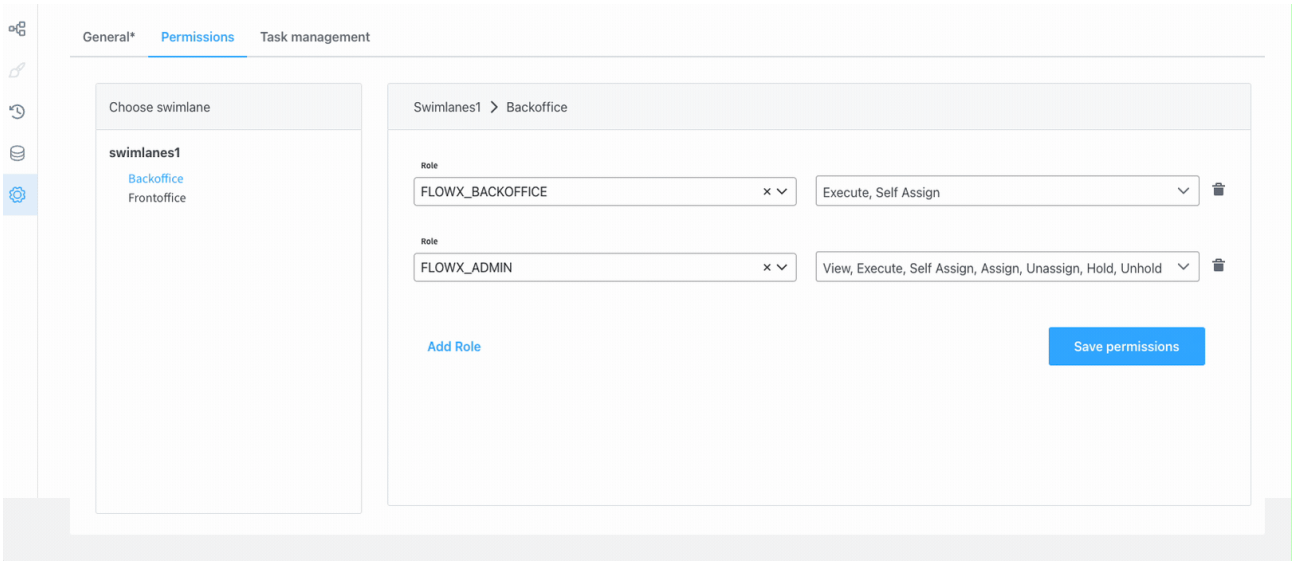
The fallback content to display on prerendering
based on user roles. This can be achieved by organizing nodes into different swimlanes.

Each swimlane can be configured to grant access only to users with specific roles defined in the chosen identity provider platform.

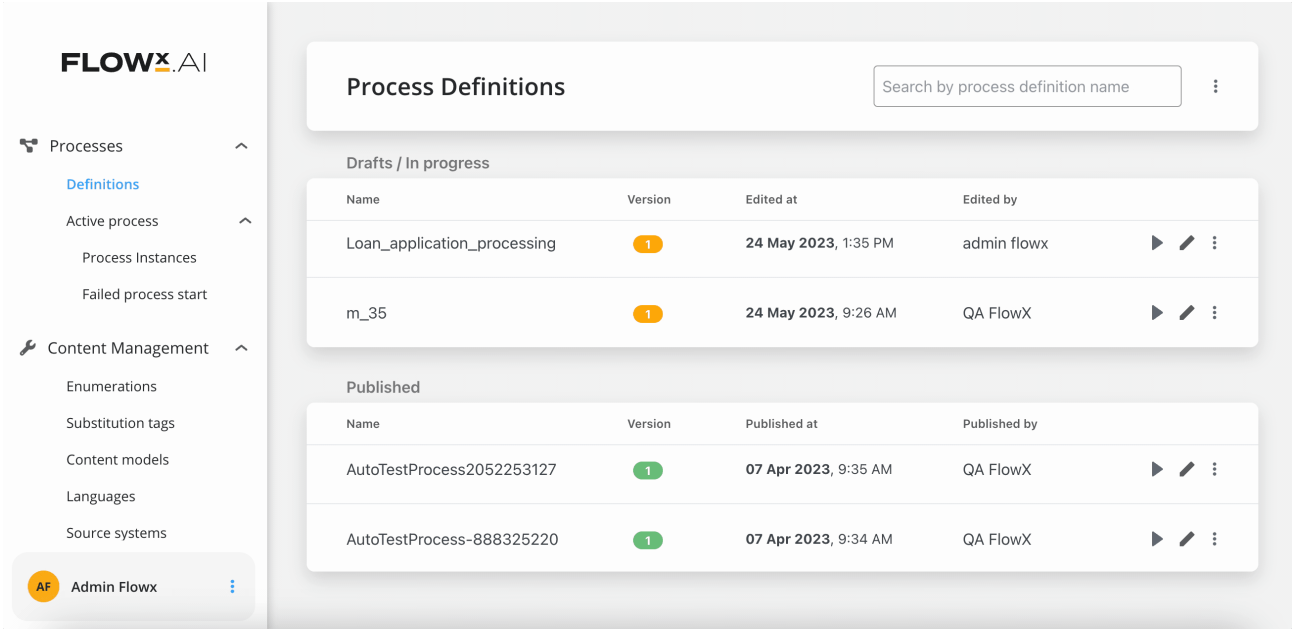


Depending on the type of node added within a swimlane, only users with the corresponding swimlane roles will have the ability to initiate process instances, view process instances, and perform actions on them.

» Click here to view the list of scopes and roles for managing processes



When creating a new process definition, a default swimlane will automatically be added.



As the token moves from one node to the next, it may transition between swimlanes. If a user interacting with the process instance no longer has access to

the new swimlane, they will observe the process in read-only mode and will be unable to interact with it until the token returns to a swimlane they have access to.

Users will receive notifications when they can no longer interact with the process or when they can resume actions on it.

» Configuring access roles for processes

Was this page helpful?

PLATFORM DEEP DIVE / User roles management / Business filters

INFO

What is it? An optional attribute, from the authorization token, that can be set in order to restrict access to process instances based on a business specific value (ex. bank branch name).

Why is it useful? Using business filters we can make sure only the allowed users, with the same attribute, can access a

The fallback content to display on prerendering
.

In some cases it might be necessary to restrict access to process nodes based on certain

The fallback content to display on prerendering
, for example only users from a specific bank branch can view the process instances started from that branch. This can be done by using business filters.

Before they can be used in the process definition the business filter attributes need to be set in the identity management platform. They have to be configured as a list of filters and should be made available on the authorization token. Application users will also have to be assigned this value.

When this filter needs to be applied, the process definition should include nodes with actions that will store the current business filter value to a custom `task.businessFilters` key on process parameters.

If this value is set in the process instance parameters, only users that have the correct business filter attribute will be able to interact with that process instance.

Was this page helpful?