

Workflow access control

The workflow access control rules define what workflow operations a user can perform, in other words it is about the authorization of various workflow operations.

NOTE

Currently the access control rules are not configurable. In the current implementation, there is already an interface (WorkflowAuthorizer) which could be replaced by a custom implementation, however there is no way yet to register such custom implementation.

These are the current workflow authorization rules:

- process definitions:
 - deploying, deleting, getting instance counts: users in Administrator role
 - read access: everyone
- starting a new process instance: everyone
- read access to a process instance:
 - users in Administrator role
 - the process owner
 - if the process is associated with a document using the daisy_document process variable, and the user has read access on the document
 - the user is assigned as actor for a task in the process
 - the user belongs to a pool for a task which is associated with a pooled actor. In case the process is associated with a document, the user should also have read access on the document.
 - in all other cases, no access
- update/end a task:
 - users in the Administrator role
 - the process owner
 - the actor for the task
- assign a pooled task to oneself:
 - users in the Administrator role
 - the process owner
 - users belonging to one of the pools, except if the process is associated with a document through the daisy_document process variable and the user has no read permission on the document.
- assign a task to an arbitrary actor:
 - users in the Administrator role
 - the process owner
- unassign task:
 - users in the Administrator role
 - the process owner
 - the task actor (only if the task will fall back to pooled actors)
- delete, suspend or resume a process:
 - users in the Administrator role
 - the process owner

Task and timers are only accessible if one has read access to the process to which they belong.

The results of [workflow queries](#)¹ are automatically filtered according to these access rules.

1. [daisy:353-cd \(Workflow query system\)](#)