PNMsoft

Business Processes in Motion™

PNMsoft Knowledge Base

Sequence User Guides

Permissions

Microsoft Partner

Gold Application Development

TABLE OF CONTENTS

General Document Information

Purpose

The purpose of this document is to describe how to define permissions in Sequence applications, and to provide several permissions guidelines and best practices.

This guide is primarily geared for process owners and Administrators, but it is important for Developers to be familiar with the information as well.

Prerequisites

- Basic knowledge of developing processes with Sequence.

Overview

Sequence includes a practical and powerful Permissions module which enables you, a project Administrator, to define exactly which users, groups and roles have permissions to access and edit which workflows and activities. This is important for any BPM solution, especially those which include sensitive data.

The Golden Rule: Just Enough, but Not Too Much

On the one hand, you want to provide permissions to those who need it, on the other, you want to protect confidential data or sensitive activities from those who should not have access to them. As the Administrator of the project, it is your responsibility to define permissions in an intelligent manner to achieve this balance. This guide will help you to do so.

Watch a webinar on Sequence Permissions with several examples.

Permissions in Sequence

We'll start by providing some general concepts about how permissions in Sequence work. Firstly, Sequence permissions don't work exactly like Windows permissions. They are specific to the elements of Sequence, such as workflows and activities.

There are three settings which determine what a user can see and do within Sequence's runtime environment, Flowtime:

- Permission type
- Permission level
- Permission sharing

Permission Type:

There are two types of permissions:

- Workflow Permissions
- Activity Permissions

It's important to understand that each of these types are defined separately and have different effects on process execution (more details to follow).

Permission Level:

There are four permission levels:

- No Access
- Read Only
- Read & Write
- Full Control

Each of these levels gives different amounts of control to users and groups over process elements (more details to follow).

Permission Sharing:

Permissions can be shared within a group and between groups (more details on how to define sharing below).

What Elements Requires Permissions?

Permissions are required for:

- Workflows
- Human activities
- Listener activities

There is no harm in granting permissions for other activities, but it is not needed.

Permissions Rules and Guidelines

This section includes some detailed rules guidelines on how permissions work.
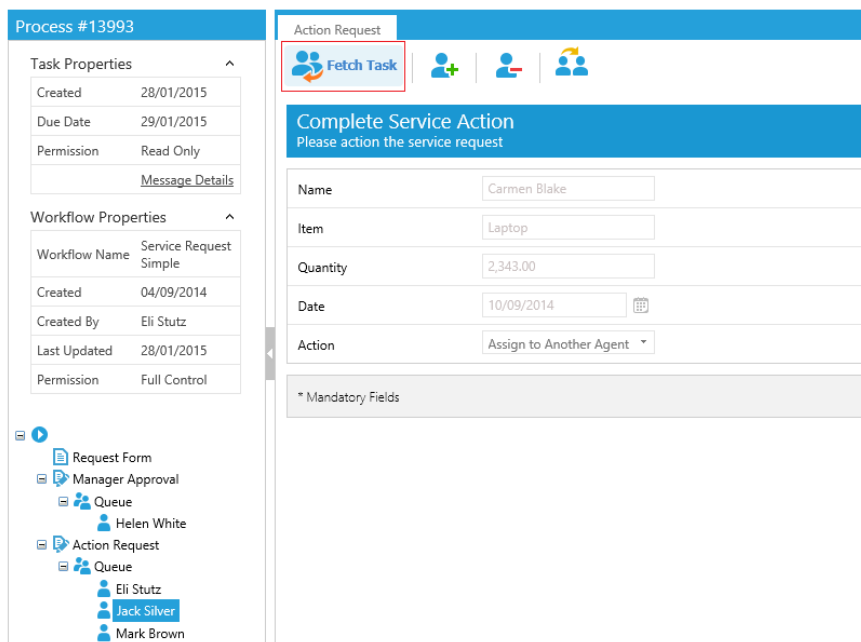
Workflow Permissions vs. Activity Permissions

Workflow and activity permissions affect how users can view and act on elements in Flowtime (Sequence's end user environment).

- Workflow permissions give users access to processes in Flowtime grids. This enables users to view and manage process instances. For example, starting new process instances, opening existing instances and viewing open and closed instances.
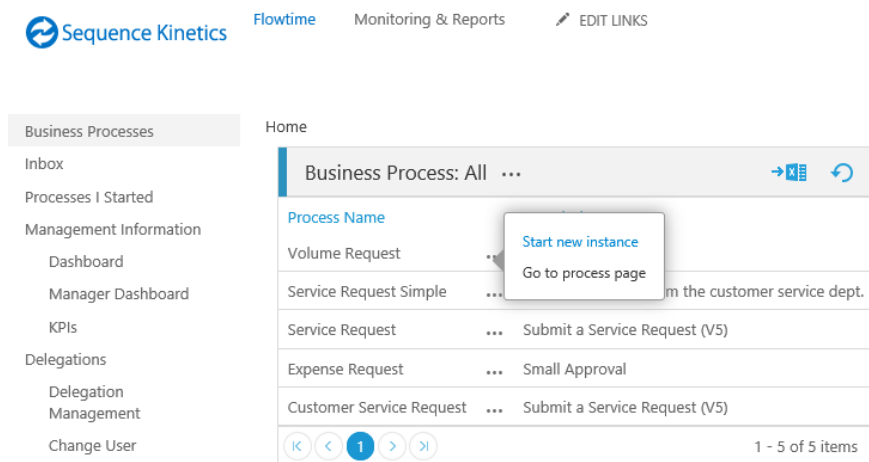
Flowtime - Start New Instance

- Activity permissions give users access to activities within process instances, for example, viewing, fetching and completing tasks.

Flowtime – Fetching a Task

The following tables describes the differences between workflow and activity permissions:

Level	Workflow (grids* and actions)	Activity (Tree view, actions)
No access	Has no access.	Has no access.
Read	Can view the workflow instances.	Can view activity instances.
Read & Write	Can view the workflow instances and create new instances.	Can view and submit activities (tasks are an exception**). Can add/remove recipients and reassign tasks (if these options are enabled).
Full Control	Can view, create instances, abort, rollback and delete.	Can view, submit, submit on behalf of someone else, and resubmit. Can add/remove recipients and reassign tasks (even if these options are disabled).

* Grids include Flowtime web parts: Business Processes, Processes Grid, My Processes, Processes I Started

** Task activity level Read & Write: submit only if assigned to the user.

> *Tip: Full control is a powerful permission level which should only be granted if absolutely necessary, and to a limited number of users. In most cases, Read & Write permission should be sufficient.*

User vs. Group Permissions

You can define permissions for specific users or for groups (you select this from the top drop-down list in the Permissions screen).

User permissions apply to specific users.

> *Tip: It is advisable not to grant specific user permissions. Instead, grant Group or Role permissions, to make processes easier to maintain and more robust.*

Group permissions:

- Are applied to all the users in the direct group.
- Can propagate to subgroups (only when applicable).
- Allow sharing using the Public attribute.

Groups are defined in the **Administration > Edit Organization** tree. The OBS tree can be synchronized from your Active Directory. See the Active Directory Guide for more details.

Role Permissions

You can define permissions for workflows and activities by role (also selected from the top drop-down list in the Permissions screen).

There are two types of roles:

- Creator (of an activity or workflow)
- Recipients (of tasks or messages)

> *Tip: Add Read & Write permissions of a Task to the Recipients of that Task. This ensures that all recipients of the Task will have permission to complete it.*

Public and Cascade Options

Sharing workflows using the Public and Cascade options is an important permissions feature in many BPM projects.

Public and cascade behavior is driven by the process instance creator (the permissions are given in relation to this role). These options are only valid for groups. You select them from the Permissions screen.

Public indicates that members of the same group as the process creator have visibility over each other's workflow instances.

Cascade:

- Is only valid when Public is enabled.

- Allows members of a group to see instances from other groups.

- Defines whose instances the group sees, not who sees the group's instances.

- Cascade options are:

    - Upper Groups
    - Lower Groups
    - Upper and Lower Groups

For example, in an Expense reporting process, each employee should see his report only, management should see all reports. Here, you would set the Management group's permissions to Public and Cascade > Lower Groups.

Permissions and BRS

The BRS (Background Runtime Service) is a Windows Service that performs many time-based Sequence activities. The BRS user is the identity running the Windows service.

The following permission guidelines apply to the BRS:

- The identity running the BRS must be an active Sequence user.

- If a Database Listener activity is used in the workflow, you must define permissions for this user.

- If the Database Listener activity is at the start of the workflow: grant the BRS user Read & Write permissions for the workflow and for the Database Listener activity.

- If the Database Listener is located elsewhere in the workflow: you need only grant the BRS user Read & Write permissions for the Database Listener activity.
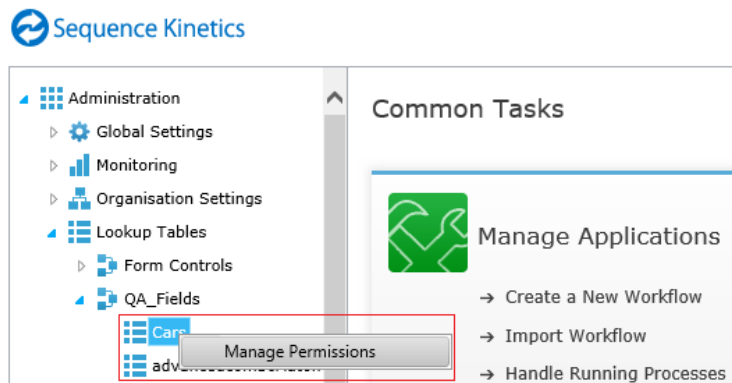
Administrative Permissions

In addition to Workflow/Activity permissions, permissions can also be granted on various tables in the Administration site.

Global Administrator and Developer are NOT process-level permissions, and they do not have an effect on Flowtime operations. These are roles relevant only for the Administration site.

- Global Administrator: Can view and manage all Administration tables, Workflows and Categories.

- Developers: Can view and manage Workflows and Categories only, unless granted permissions manually to specific table(s).

To grant permission to an Administration table, right-click the table, and select **Manage Permissions**.

Administration Tables Permissions

For example, you may want to grant specific employees permissions to add and edit values of a lookup table that is used to populate combo box values in a workflow form:
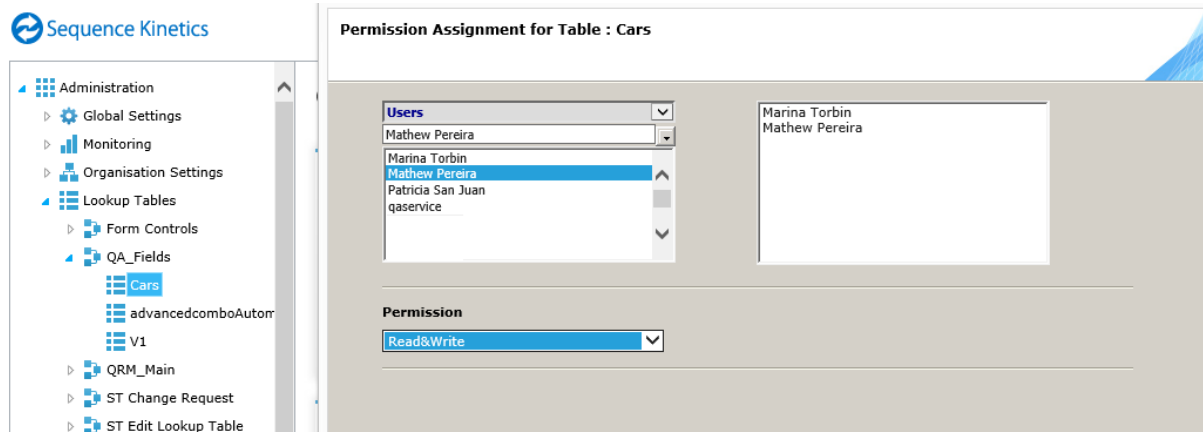
Permissions for Lookup Table

Group Manager Role

The Group Manager role is also not a workflow/activity permission, but it does enable certain operations within Flowtime. It is a group-related role that allows:

- Viewing messages for all group members.
- Adding members to group.
- Performing delegations on behalf of group members.

You can set the Group Manager role for users in the **Organization Settings > Employees** table:

Last Name	First Name	Title	E-mail	Group Manager	Role In Group	Move to Group	Remove
Engineer 3	Lisbon	-	LisbonEn3@PNMTRAINING.com	✓		⇨	✕
Engineer 4	Lisbon	-	LisbonEn4@PNMTRAINING.com	☐		⇨	✕
Engineer 5	Lisbon	-	LisbonEn5@PNMTRAINING.com	☐		⇨	✕
Engineer 6	Lisbon	-	LisbonEn6@PNMTRAINING.com	☐		⇨	✕
Engineer 7	Lisbon	-	LisbonEn7@PNMTRAINING.com	☐		⇨	✕

Users In Lisbon Engineers

1

Group Manager Role

A Standard Scenario

You have created a workflow with several activities. You would now generally define permissions as follows (see the numbered code below):

1. Give the group which needs to start process instances Read & Write permissions on the workflow.

2. Give the Process Creator role Read & Write permission to the first Form of the workflow.

3. Give the Task Recipient role Read & Write permissions to the workflow Tasks.

4. Give the Message recipient role Read permissions on workflow Messages.
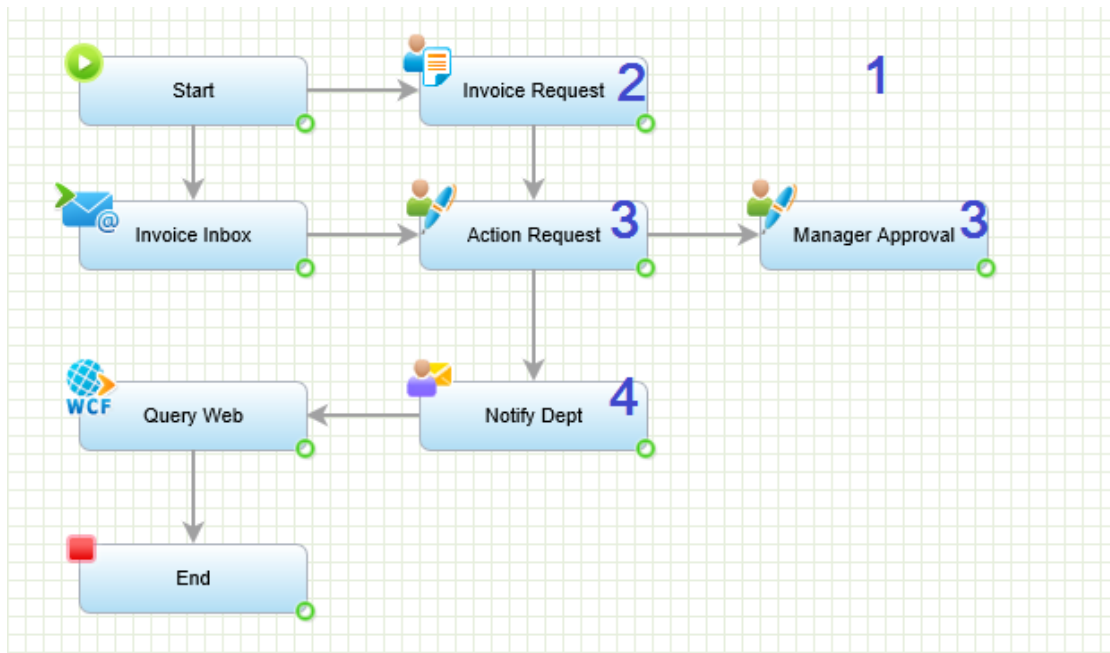
Example Workflow

If you do not properly define these permissions, your users will not be able to use the workflow properly!
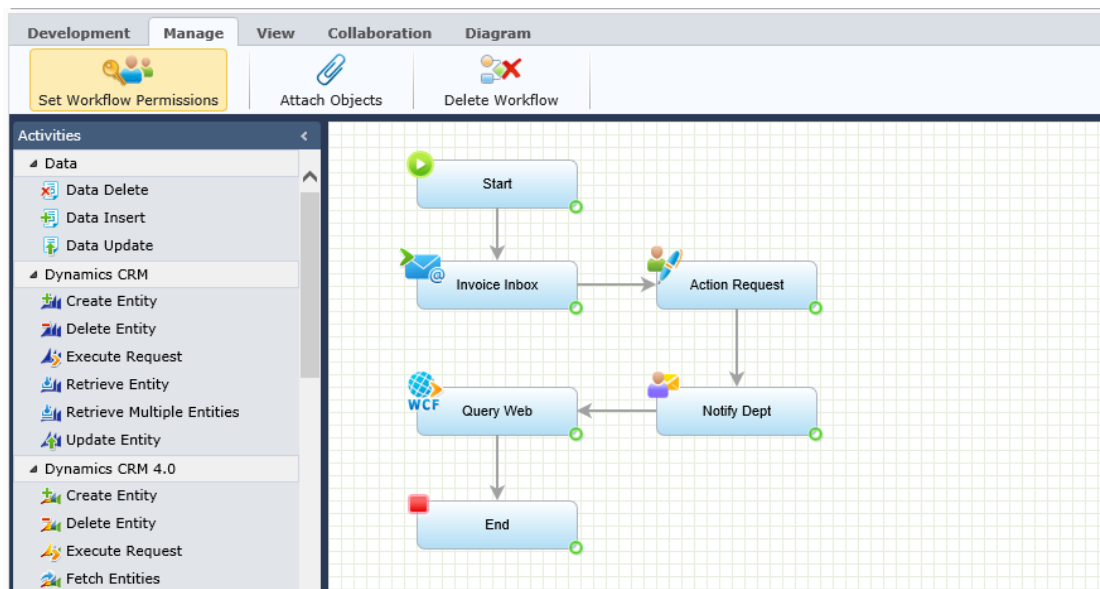
The following section describes how to grant permissions.

Defining Permissions

It's quite simple to define permissions for workflows and activities. Here's how:
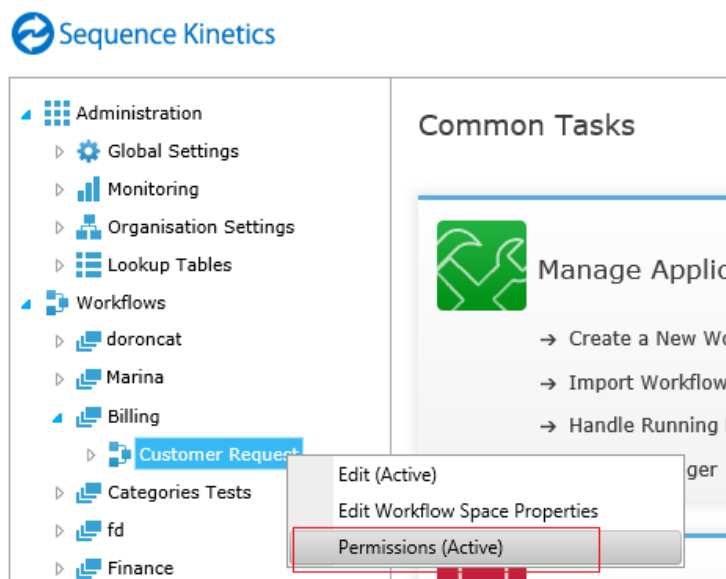
To define workflow permissions:

1. Open the workflow in the App Studio.

2. From the top ribbon, select **Manage > Set Workflow Permissions**.

Set Workflow Permissions

OR

From the **Administration > Workflows** tree, right click the workflow and select **Permissions**.

Set Workflow Permissions

The Workflow Permissions screen opens:

Workflow Permissions Screen

This screen includes the following options:

Field	Description
A list of permissions	This area lists the permissions that have been granted.
Add Group Permissions	Add permissions to a group.
Add Process Role Permissions	Add permissions to a process role.
Add User Permissions	Add permissions to specific users.
Clear only workflow permissions	Remove workflow permissions only.
Clear workflow and activity permissions	Remove workflow and activity permissions.

3. Click **Add Group Permissions** / **Add Process Role Permission** / **Add User Permissions** as required.
   The Assign Permissions screen appears (we will show an example of the Group Permission screen below).

Assign Group Permissions Screen

This screen includes the following options:

Field	Description
Groups	The groups(s) for whom you wish to grant permissions. Click [...] to select groups.
Permission Level	Select the level of permission you would like to grant: Read Only/Read & Write/Full Control/No Access. **Read:** Users see the workflow in the home page workflow list, but cannot create new instances. **Read & Write:** Users see the workflow in the home page workflow list and can create a new instance. **Full Control:** Users see the workflow in the home page workflow list, can create a new instance, and can delete or abort processes. **No Access:** Users cannot see the workflow.
Public	When set (for a group/department), this enables all employees of that group to view each other's workflows in their 'Processes page' in Flowtime.
Cascade Type	Enables users from one group to view workflows created by users from sub groups or parent groups in 'Processes page' in Flowtime. Note: This option is only relevant if you select the Public checkbox below. For example, if you select Lower Groups for a parent group and select Public, this will enable the parent group users to view workflows initiated by sub groups. If users from the parent group have permissions for these workflows, they can also perform actions on them according to their permission level.

Field	Description
Propagate to Subgroups	If selected, the current group's sub groups will inherit the permissions. Note: When granting permissions to a group Sequence does not grant permissions to employees in its sub groups.
Propagate to Activities	If selected, the current workflow activities will inherit the workflow permissions. This can save time – as you then only need to define the workflow permissions and propagate them to all the workflow's activities).

4. Click **Update**. The permissions you have defined are displayed:

Workflow Permissions

You can change permissions for a specific row by clicking ✎ .

You can propagate permission to all activities for a specific row by clicking ≈ .

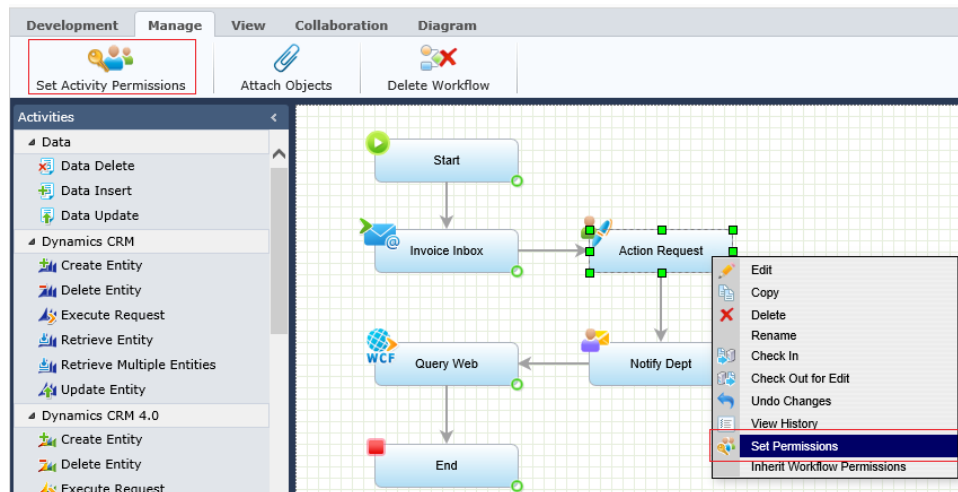You can remove permissions for a specific row by clicking ✘ .

To define activity permissions:

1. Click the desired activity.

2. From the top ribbon, select **Manage > Set Activity Permissions**.

   OR

   Right-click the activity, and select **Set Permissions**.

Set Permissions – Activity

The Activity Permissions screen opens:

Activity Permissions Screen

This screen includes the following options:

Field	Description
A list of permissions	This area lists the permissions that have been granted.
Add Group Permissions	Add permissions to a group.
Add Process Role Permissions	Add permissions to a process role.
Add User Permissions	Add permissions to specific users.
Clear all permissions for this activity.	Remove all activity permissions.

3. Click **Add Group Permissions** / **Add Process Role Permission** / **Add User Permissions** as required.
The Assign Permissions screen appears (we will show an example of the Group Permission screen below).

Assign Group Permissions Screen

This screen includes the following options:

Field	Description
Groups	The groups(s) for whom you wish to grant permissions. Click [...] to select groups.
Permission Level	Select the level of permission you would like to grant: Read Only/Read & Write/Full Control/No Access. This affects how users can see and edit the activity in Flowtime as

Field	Description
	follows:
	Read: Users see the activity.
	Read & Write: Users see and can edit/submit the activity. Users can add/remove recipients and reassign tasks (if these options are enabled).
	Full Control: Users see and can edit/submit the activity and can edit/resubmit the activity after it has been submitted. Users can also submit a task on behalf of another user. Users can add/remove recipients and reassign tasks (even if these options are disabled).
	No Access: Users cannot see the activity.
Public	When set (for a group/department), this enables all employees of that group to view each other's activities in Flowtime.
Cascade Type	Enables users from one group to view activities created by users from sub groups or parent groups in Flowtime. Note: This option is only relevant if you select the **Public** checkbox below. For example, if you select **Lower Group**s for a parent group and select **Public**, this will enable the parent group users to view activities initiated by sub groups. If users from the parent group have permissions for these activities, they can also perform actions on them according to their permission level.
Propagate to Subgroups	If selected, the current group's sub groups will inherit the permissions.

4. Click **Update**. The permissions you have define for the activity are displayed:
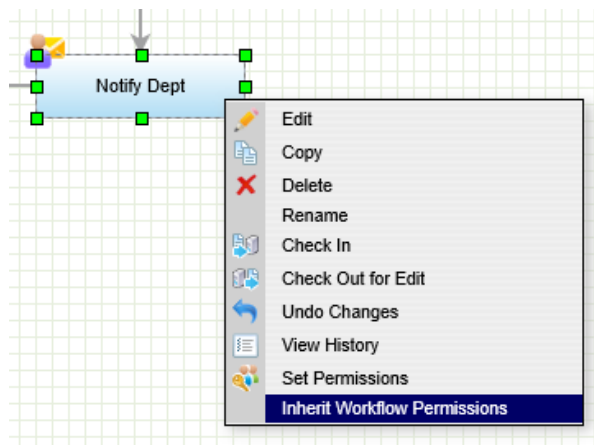

Activity Permissions

You can change permissions for a specific row by clicking ✏ .

You can remove permissions for a specific row by clicking ✖ .

Permissions Best Practices

Here are some best practices for defining permissions in your Sequence projects:

- Include permissions planning in your workflow design. Think of how to grant permission to groups and roles so that they will be able to execute workflows more effectively.

- Use group and role permissions only, avoid granting permissions to specific users. This makes the project more robust and easier to maintain.

- For Tasks, always give the recipient role Read & Write permissions.

- Avoid granting Full Control unless it is absolutely necessary. Use Read & Write instead.

- Administrators usually need to be able to view all instances. Ensure that they are granted Read & Write permissions on all workflows and activities.

- You can quickly apply workflow level permissions to an activity by using the **Inherit Workflow Permissions** option.

Inherit Workflow Permissions