

Set permissions from Identity Manager users or roles

This article describes how to view, assign and withdraw permissions for users and roles in [Smart ID Identity Manager](#).

This article is valid for Smart ID 20.11.2 and later.

[Expand/Collapse All](#)

Step-by-step instruction

1. Log in to Identity Manager Admin as Administrator.

To view or edit permissions of an individual **user**:

1. In Identity Manager Admin, go to **Home > User Administration**.
2. Double-click a user name in the list.
The user settings are shown.

To view or edit permissions of a **role**:

1. In Identity Manager Admin, go to **Home > Roles**.
2. Double-click a role name in the list.
The role settings are shown.

Roles in Identity Manager can be configured to only access certain Identity Manager instances, by using the instance ID setting.

To limit a role to access only certain instances:

1. In **Instance Ids**, enter a comma-separated list of **instanceIDs** as configured in the **system.properties** of each instance.

Example: Instance Ids

Instance Ids = internet, intranet

If the field is left empty, then all instances are allowed.
For information on how to configure **instanceIDs** in **system.properties**, see [Limit role to access certain instances of Identity Manager client](#).

To edit permissions of individual users or roles:

1. In the user or role settings, select tab. For more information, see the table below.
2. Check or uncheck permissions as needed.
3. Click **Save**.

Permissions are grouped in these tabs:

Tab	Description
General	Here you can assign and withdraw permissions to access larger functional areas of Identity Manager Admin and Identity Manager operator UI. Functional areas for which a user has no permission are hidden.

Related information

- [Smart ID Identity Manager](#)
- [Limit role to access certain instances of Identity Manager client](#)

Process Permissions	Here you can assign and withdraw permissions to start individual processes in Identity Manager operator UI (that is, Execute) and to edit their configuration in Identity Manager Admin (Update or Delete).
Forms	Here you can assign and withdraw permissions to read (Read) and edit (Update or Delete) the configuration of individual forms in Identity Manager Admin.
Identity Templates	Here you can assign and withdraw permissions to access (Read) data objects of particular categories in Identity Manager operator UI. The categories are determined by the identity templates.
Search Configurations	Here you can assign and withdraw permissions to use (that is, Execute) the individual search configurations in Identity Manager operator UI.