Authorizations

Definition

> Soffid console provides a granular access control system. That granular control system allows the administrator user to assign granular permissions to roles. Be in mind that some permissions may inherit some other permissions.

You cannot assign permissions directly to users. Instead, permissions are assigned to roles and roles are assign to users, either directly or through grant inheritance.

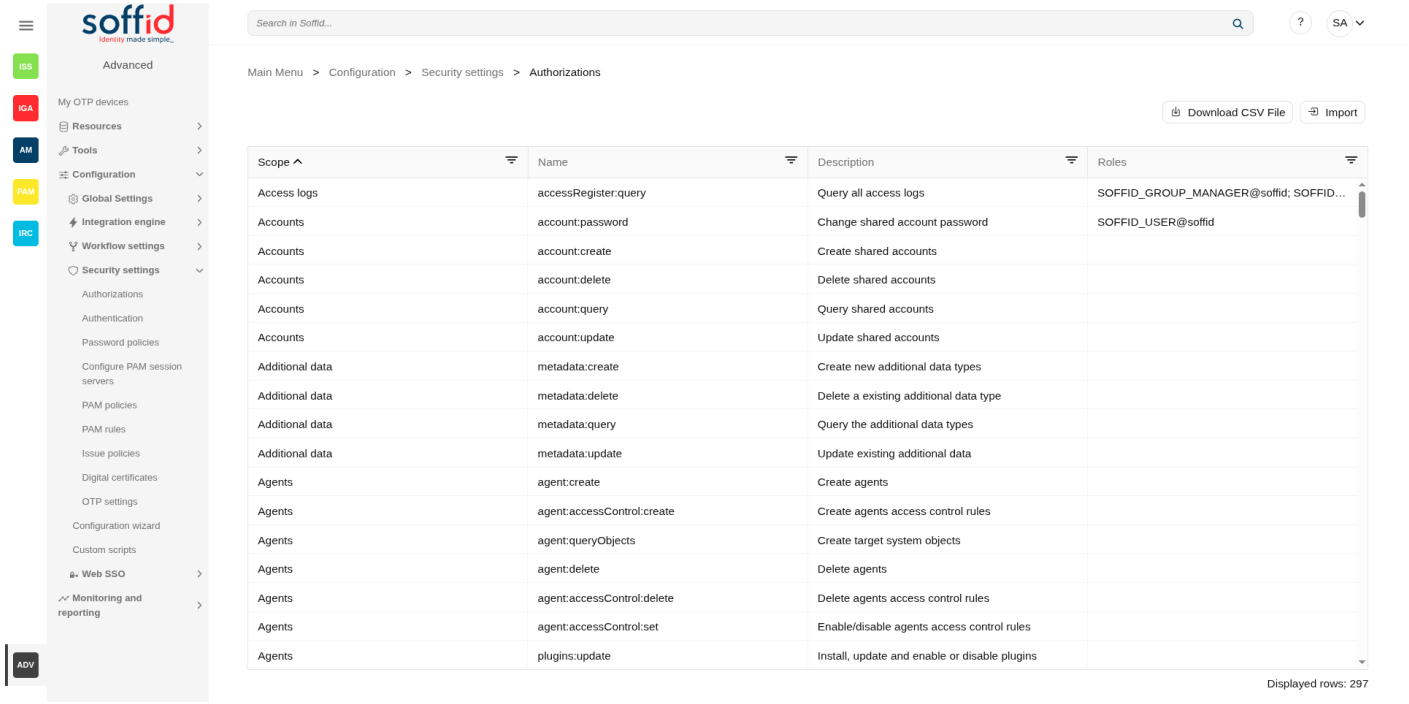
The roles may be created into Soffid application system, but could also be included in any other application system.

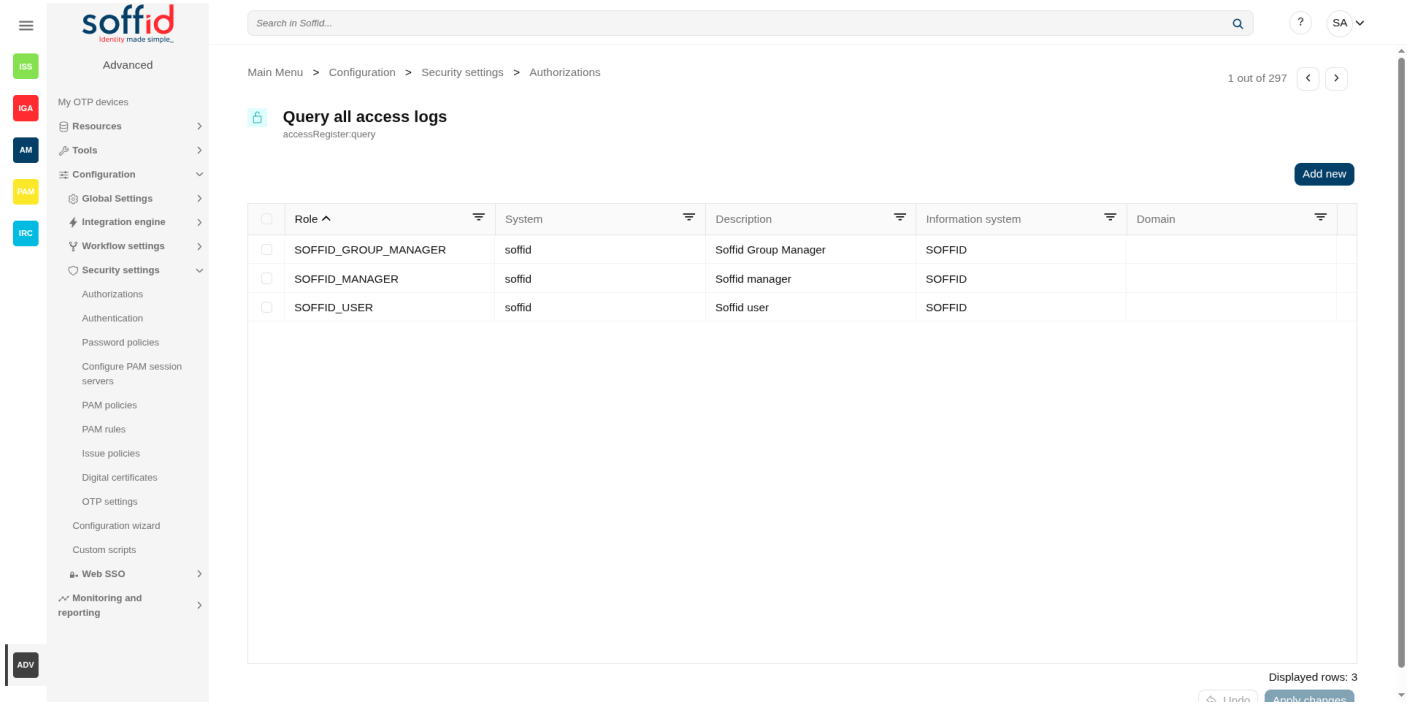
Permissions are grouped into permission scopes. Most scopes are Soffid object types, but there are one special scope named Soffid, that applies to Soffid console web pages.

Addons can create their own authorizations that automatically will appear at this screen. When a new addon has been installed and applied, the first thing to do use to be assign permissions for this new addon. In fact, administrators won't be able to manage the addon unless the log out and log in to get the newly created permissions.

The permissions given to roles and the roles given to users are cached by Soffid. In order to reapply permissions, the user should close its session and log-in again

Screen overview





Related objects

- Users: authorisations are given to users through the roles that have been granted to them.
- Roles : authorisations are granted to roles
- Information systems : roles are gathered into information systems

Standard attributes

Table attributes

- **Scope**: scope of application.
- **Name**: name of the granular permission.
- **Description**: brief description of the granular permission.
- **Roles**: role list assigned to that granular permission.

Authorization attributes

- **Role**: role name.
- **System**: target system name.
- **Description**: role description.
- **Information system**: asset or application, from a functional point of view.
- **Domain**: the role is limited to that scope.

Actions

Table actions

Download CSV file	Allows you to download a CSV file with the authorization data.
Import	Allows you to upload a CSV file with the authorization data to add or to update the granular control system. If they exist, the values of the CSV file will prevail. First, you need to pick up a CSV file, that CSV has to contain a specific configuration. Then you need to check the contents. And finally, you need to select the mappings for each column of the CSV file to import the data correctly and to click the Import button.

Authorization actions

Add new	Allows you to add a new role to the authorization. First, you need to search a role writing the role name on the field, and Soffid will show the values related. Second, you can select one or more roles and accept. And finally, you need to apply changes to save the roles added. If you cancel that action, no role will be assigned.
Delete	Allows you to delete one or more roles from an authorization. To delete one role, you need to click the subtraction symbol (-), located at the end of the row, of the role which you want to delete and then apply changes. To delete more than one role, you can select the roles which you want to delete and there click the subtraction symbol (-) and then apply changes. It is mandatory apply changes to save the roles deleted. Soffid will ask you for confirmation to perform that action, you could confirm or cancel the operation.
Undo	Allows you to quit without applying any changes.
Apply changes	Allows you to update the changes made on the authorization.

Select role actions

Undo	Allows you to quit without applying any changes.
Apply now	Allows you to add the role or roles to the authorization.

Others

Most common authorizations

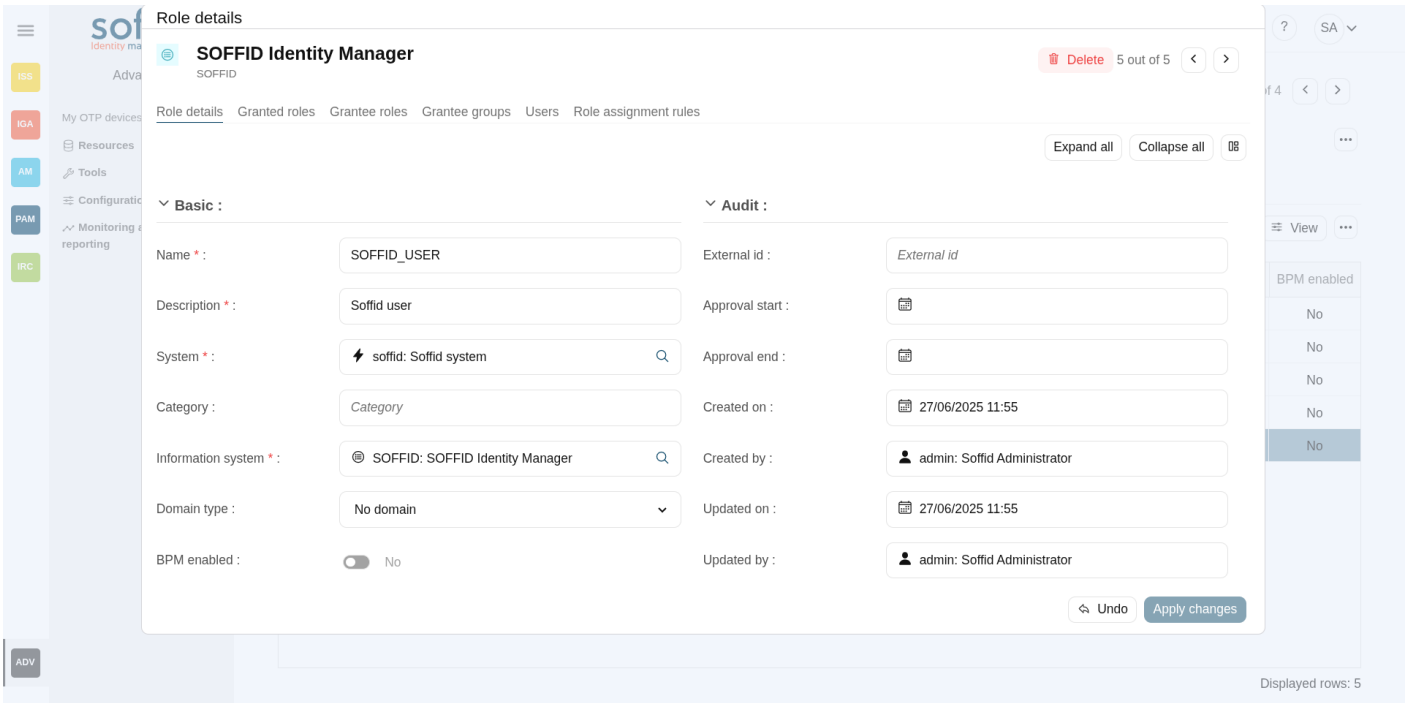
Page	**Code/s**	**Role**
Password vault	sso:manageAccounts agent:query metadata:query	SOFFID_PAM_ADMIN

Password vault, modify Owners, Managers and SSO Users.	account:password account:query account:update metadata:query agent:query role:query customObject:query customObjectType:query group:query networkDiscovery:schedule pamSession:create sso:createSharedFolders sso:passwordManager sso:manageAccounts user:group:delete user:query	SOFFID_PASSWORD_VAULT

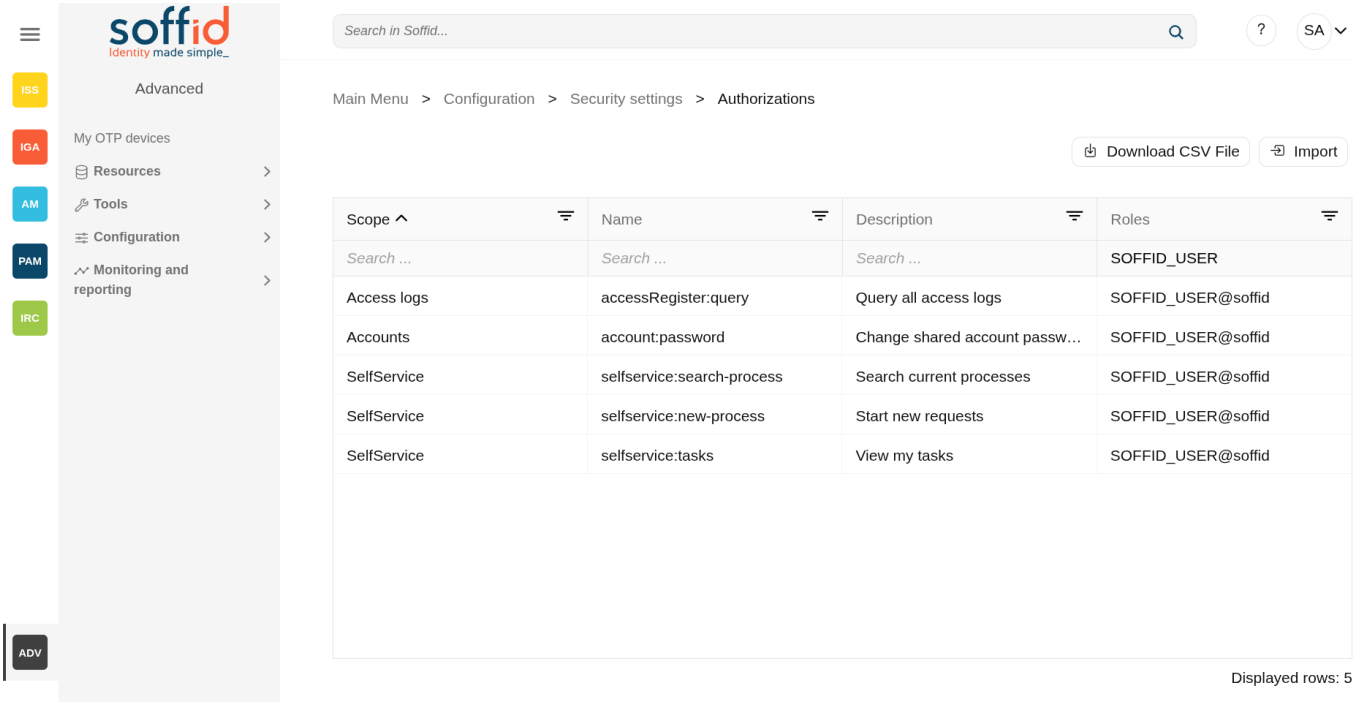
Examples

End user for identity self service.

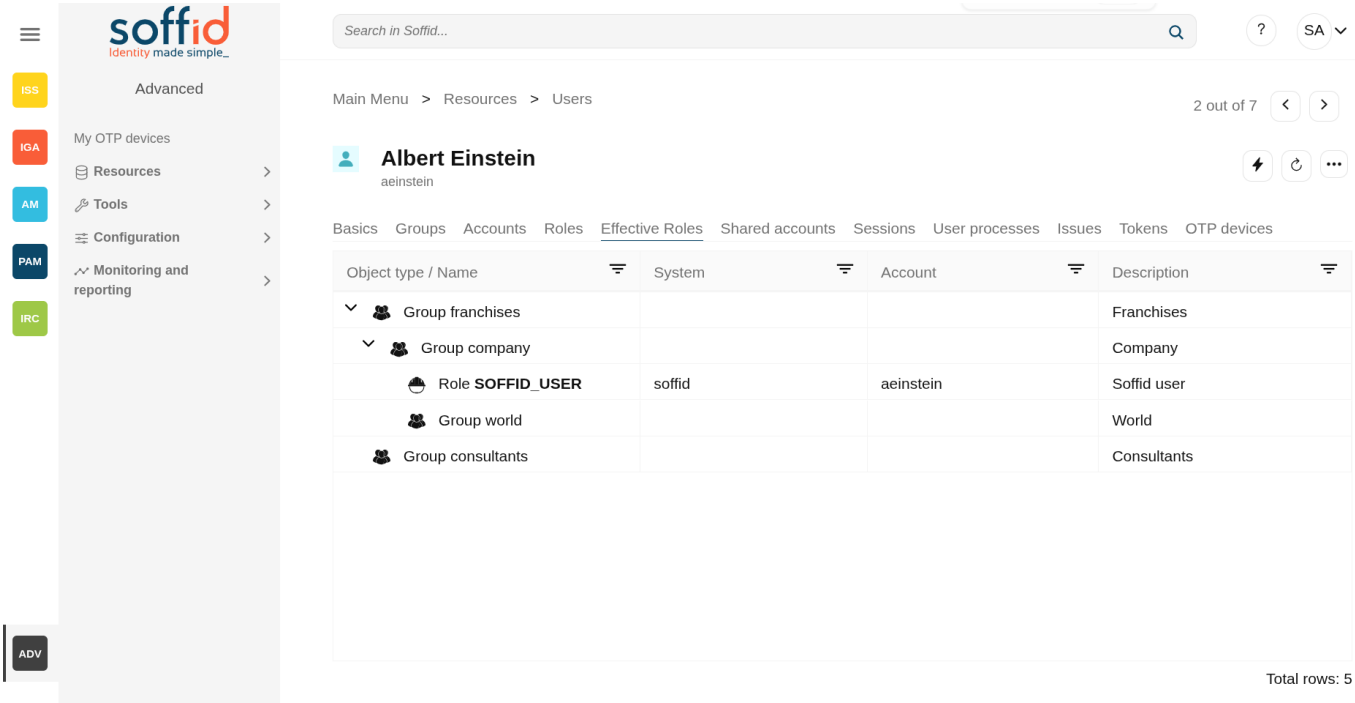
A Soffid role is created for this functionality.



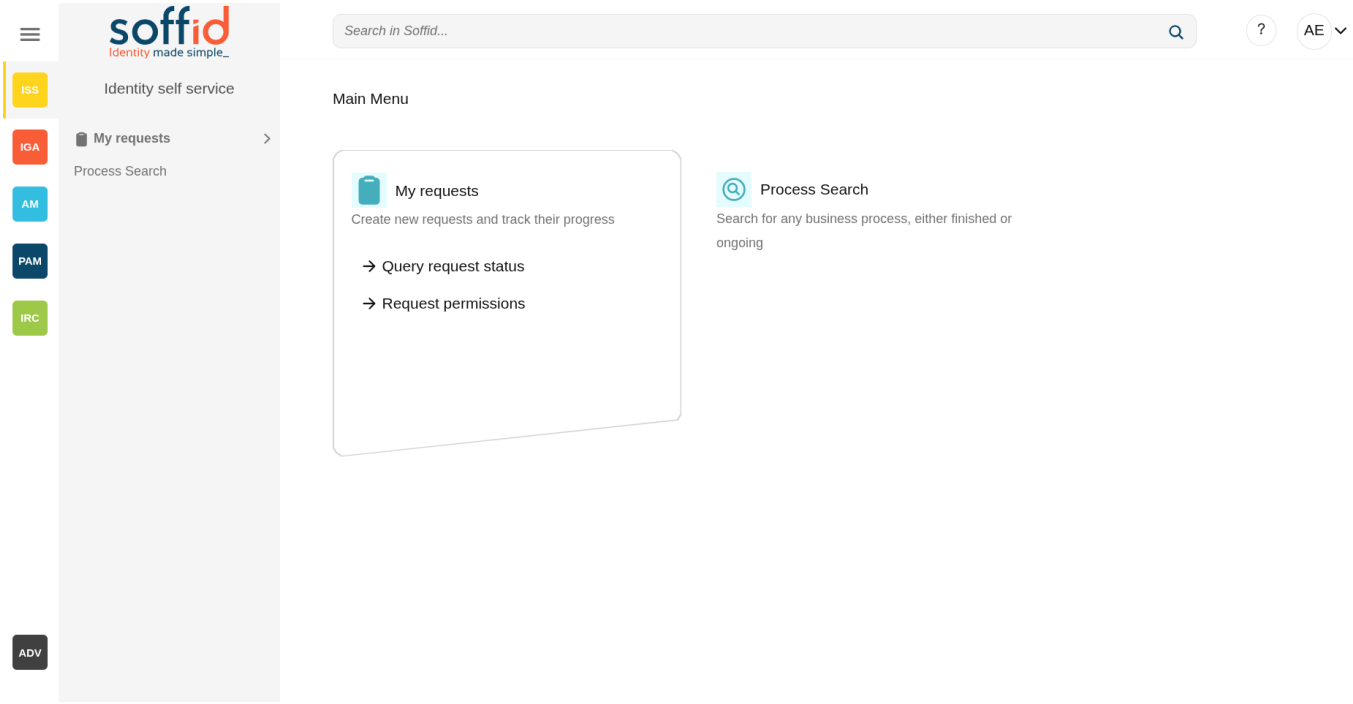
This role is assigned to the authorisations we require.



The role is assigned to a user.



The user will only be able to access the pages and actions permitted by their authorisations.



Revision #12
Created 19 July 2025 12:07:42 by Sion Vives
Updated 20 August 2026 07:32:45 by David Gómez