Application access tree

Description

> The **entry points** could be to connect to information systems defined on Soffid, or to connect to other applications. These applications can be Web applications or Native applications. Each information systems can have one or more application entry points.

The entry points are managed in a tree structure, that allows creating new menus and new application access.

Each member of the tree can be tied to a list of users, account groups, or roles. Also, you can choose if the application menu entry will be visible or not by unauthorized users.

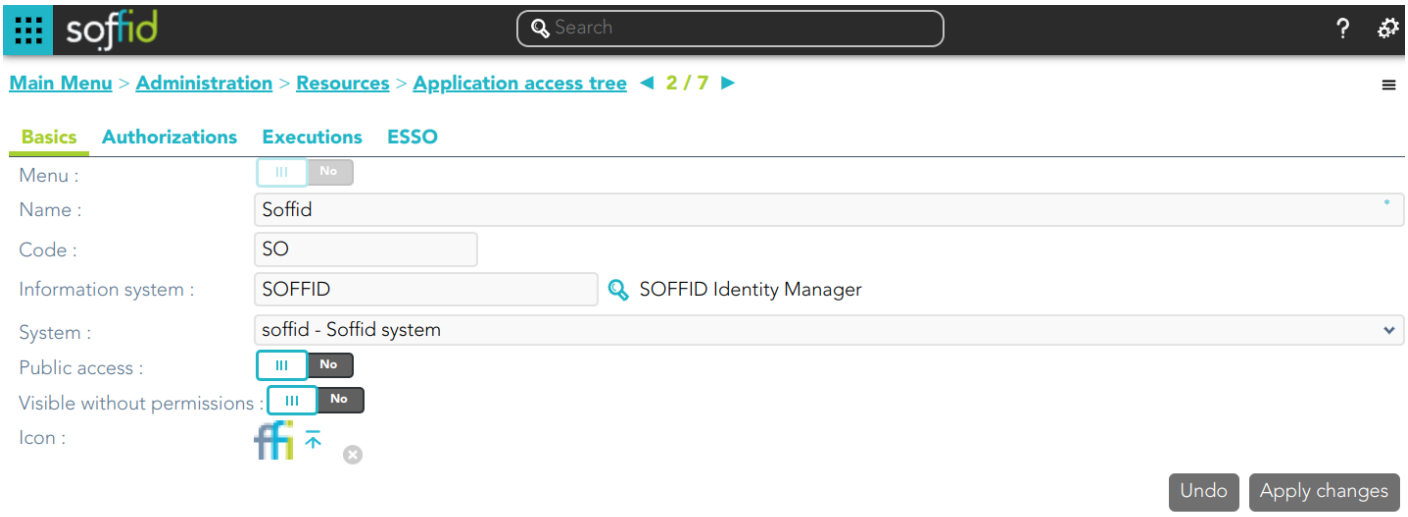
After logging on to a managed workstation, the system will apply such restrictions and will update the Windows or Linux start menu.

Each application entry point will have different execution methods for fully managed workstations, loosely managed workstations, or external devices. Each of them can be a web browser URL or a javascript piece.

Each application entry point can have a single sign on rule. Those roles are fully explained in the ESSO reference guide. For more information, you can visit the ESSO chapter.

The defined entry points allow to final users open applications from the self service portal. For more information can visit My Applications page.

Screen overview



Related objects

1. **Information system**
2. **User**
3. **Group**
4. **Role**
5. **Account**

Standard attributes

Basics

- **Menu**: (yes|no) when the menu is Yes, this application will be like a folder to contain and organize other applications.
- **Name**: application identifier name.
- **Code**: application code.
- **Information System**: asset or application, from a functional point of view, on which the permissions are granted or revoked. For more information visit the Information Systems page.
- **System**: information storage system from a technical point of view (active directory, database, CSV, ...). These systems are the agents configured on Soffid, for more information about these visit the Agents page.
- **Public access**: when it is Yes, this application will be displayed as public at the self-service portal of all users.
- **Visible without permissions**: when it is Yes, this application will be displayed at the self-service portal, but only users with permissions will be allowed to connect.

- **Icon:** application identification icon.

Authorizations

Allows you to grant access permissions to users, groups, roles, or accounts.

To give authorization it is necessary, first of all, to select the grantee type, then to choose the user, group, role, or account, and finally choose the access level. The access level allows two options:

- **Manage**: allows to update the entry point.
- **Execute**:
  - When the entry point has selected the option public access to NO, only users with the assigned access level as execute could execute that entry point.
  - When the entry point has selected the option public access to YES, all users can execute that entry point.

Executions

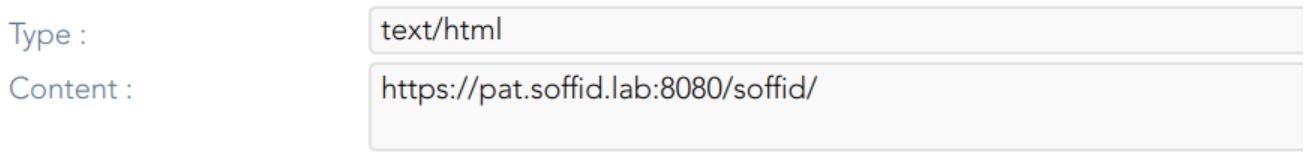
Allows Administrator users to configure the entry point access. It is only available to entry points with the option Menu not selected.

There are three options to configure the executions. Administrator users can configure one or more:

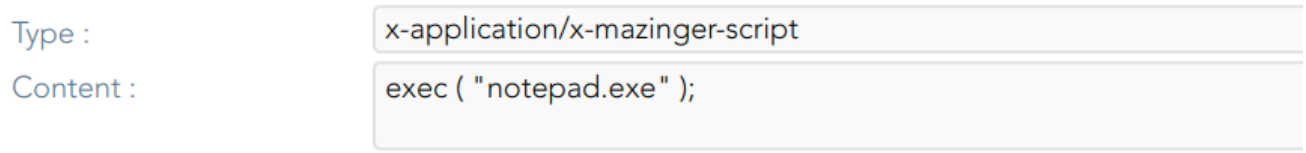
- **Running from Intranet**: if you select the Yes option, Soffid will check if the host that is trying to run this entry is located in a network flagged as internal, if so, Soffid will allow to run the entry.
- **Running from Extranet**: if you select the Yes option, Soffid will check if the host that is trying to run this entry is located in a network NOT flagged as internal, if so, Soffid will allow to run the entry.
- **Running on the Internet**: if you select the Yes option, Soffid will check if the host that is trying to run this entry is located in an unknown network, if so, Soffid will allow to run the entry.

For each execution option it is possible to configure the following parameters:

- **Enabled**: if the option is available to configure.
- **Type**: access connection type.
- **Content**:
  - **text/html**: a URL to access to the application.

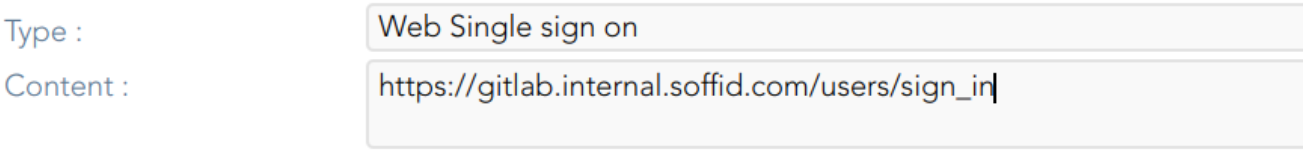


- **x-application/x-mazinger-script:** scripts that will be executed on ESSO clients



- **Recorded session:** configuration to use PAM service.

- **Web Single Sign On:** a URL to access the application with SSO.



ESSO

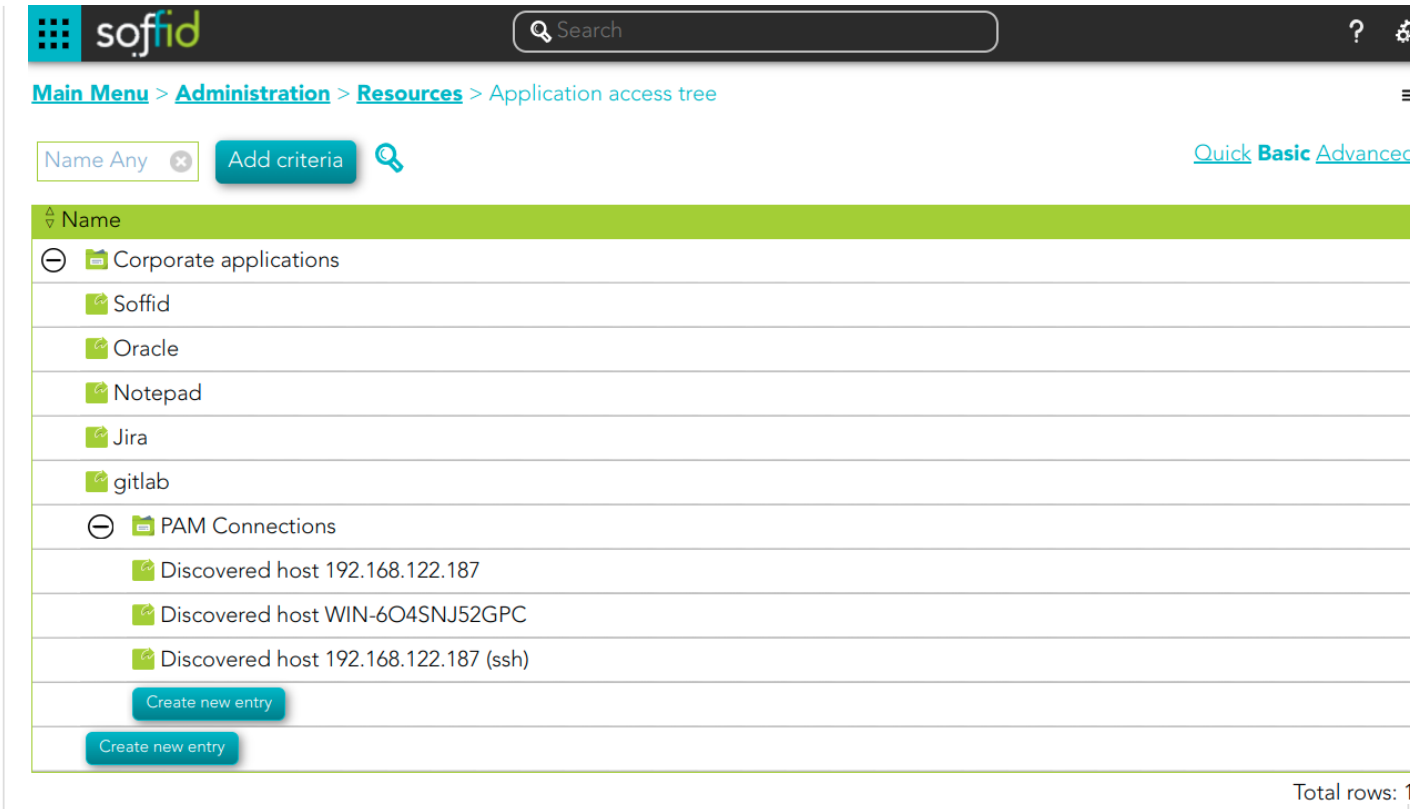
Allows you to customize a script to define a pattern to detect when an application is used and how to inject the credentials.

> For more information, you can visit the ESSO chapter.

Actions

Application query

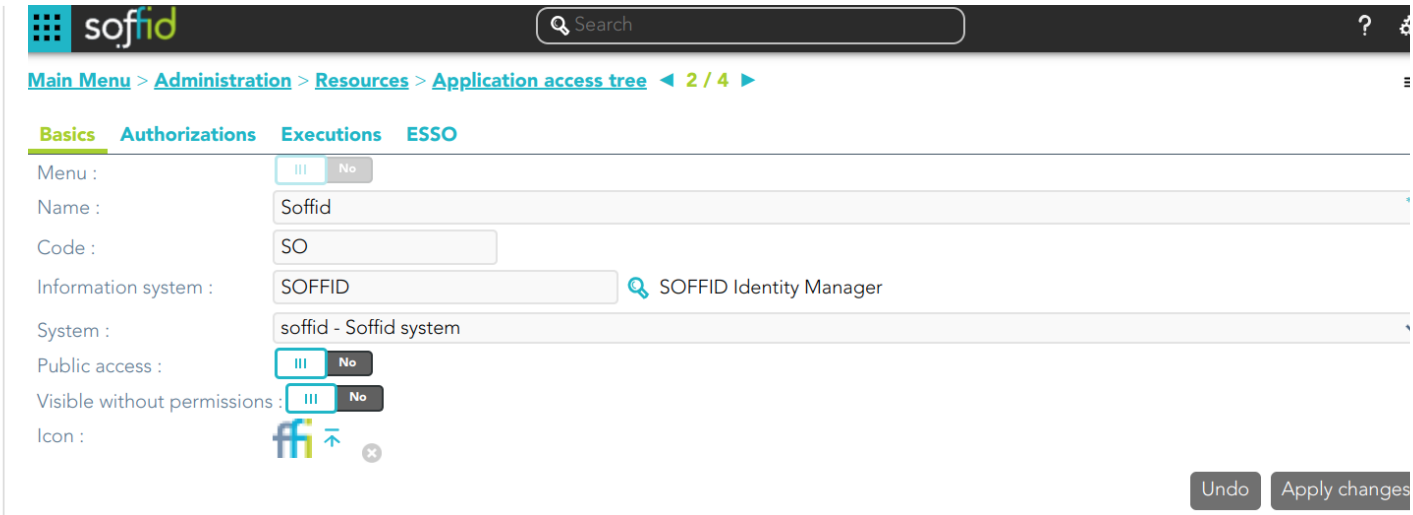
Image



Query	Allows to query the entry points through different search systems, Quick, Basic and Advanced.
Create new entry	Allows you to add a new entry point. To create a new entry point you can click the Create new entry button, then Soffid will display a new window to fill in the entry point data. To add a new entry point it will be mandatory to fill in the required fields.

Application detail

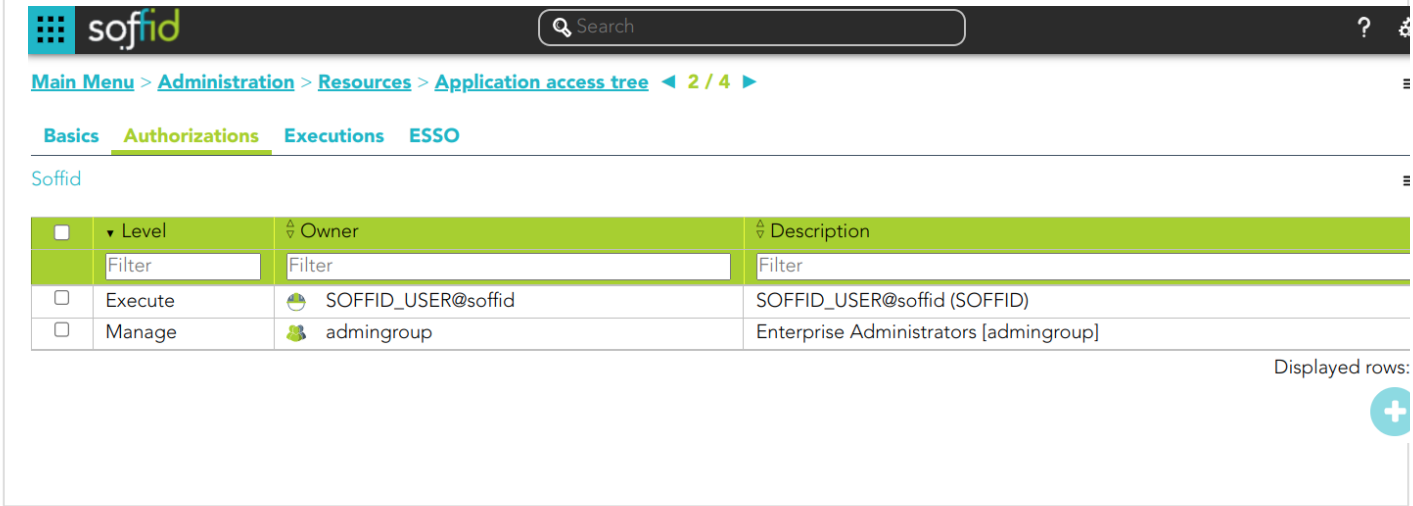
Image

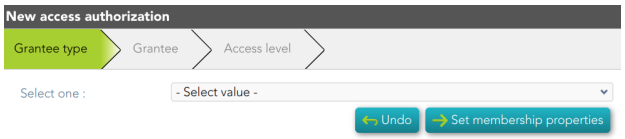


Apply changes	Allows you to save the data of a new entry point or to update the data of a specific entry point. To save the data it will be mandatory to fill in the required fields.
Delete	Allows you to delete the entry point. To delete an entry point, you can click the hamburger icon and then click the delete button (trash icon). 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 made.

Authorizations

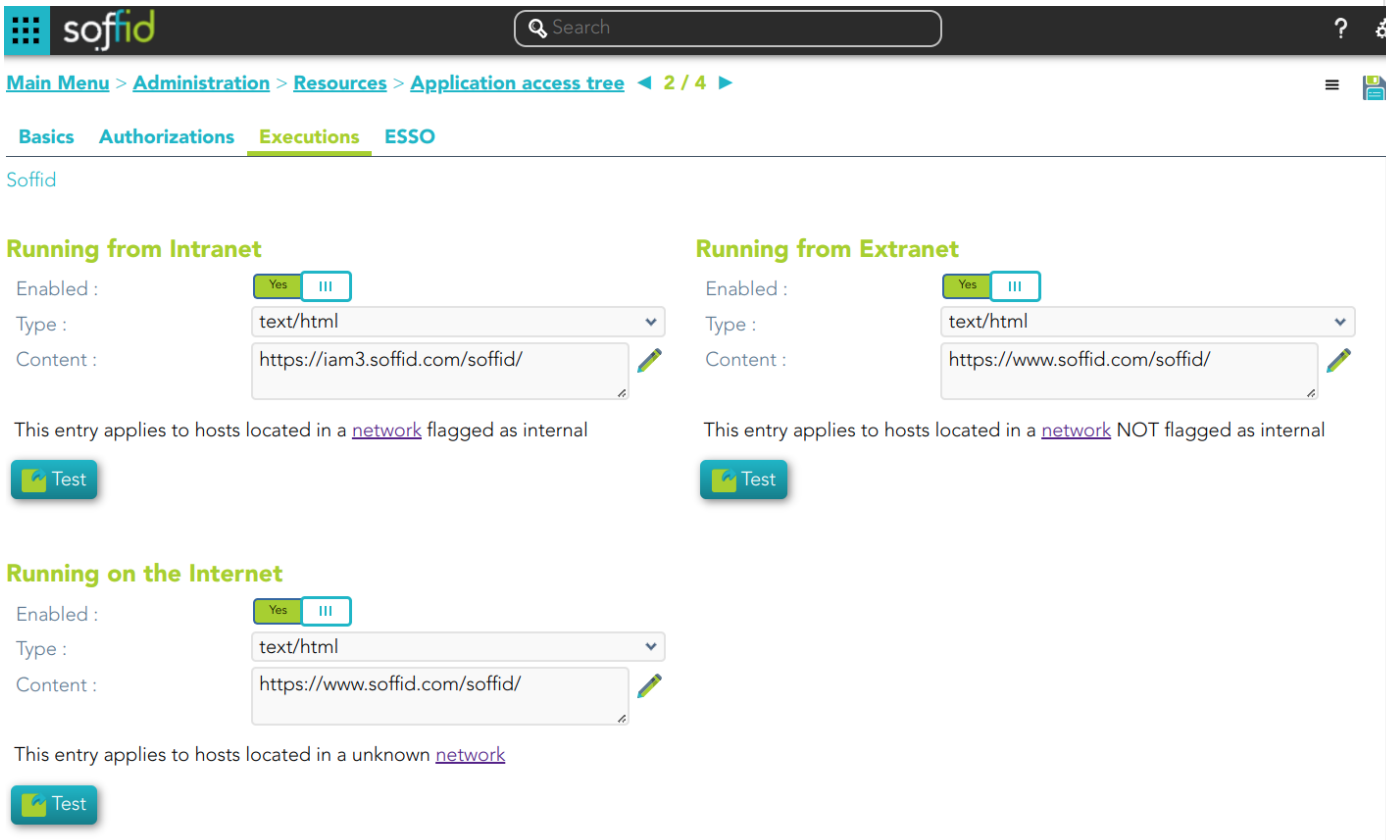
Image



Add new	Allows you to add a new authorization. You can choose that option on the hamburger menu or by clicking the add button (+). **Image**  First, you will select the Grantee type, which could be a role, a user, an account, or a group. Second, you will select the Grantee, it will depend on the Grantee type selected. Then, you will fill in the access level. And finally, you will apply changes.

Executions

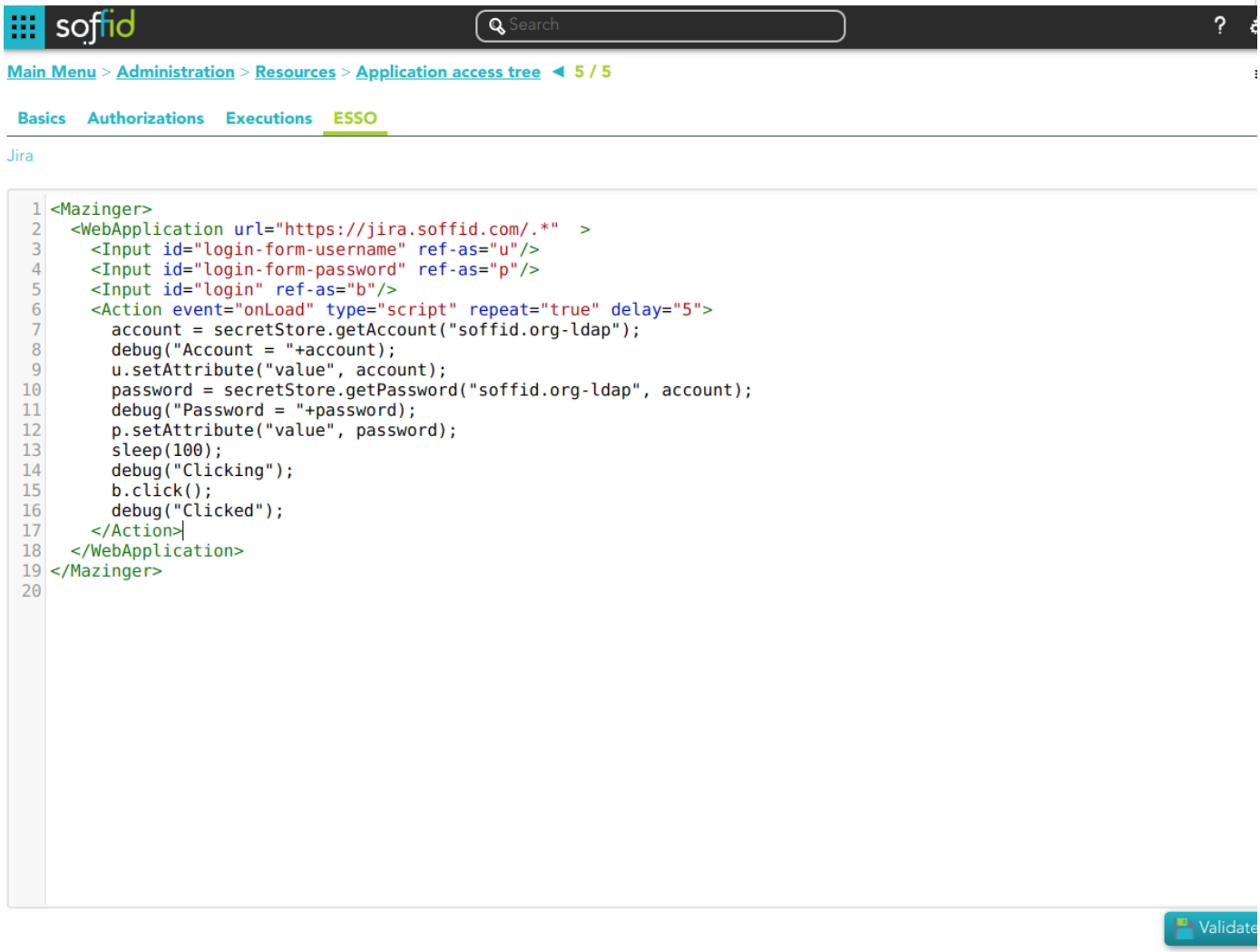
Image



Apply Changes	Allows you to save the execution configuration.
Delete	Allows you to delete the execution configuration.

ESSO

Image



Validate	Allows you to validate and save the script.

Revision #36
Created 7 April 2021 14:49:37 by pgarcia@soffid.com
Updated 25 April 2024 06:52:28 by pgarcia@soffid.com