IRC

Identity Risk & Compliance

- Create SoD matrix
- Schedule weekly risk report
- Design a recertification campaign
- Create advanced authorization rules

Create SoD matrix

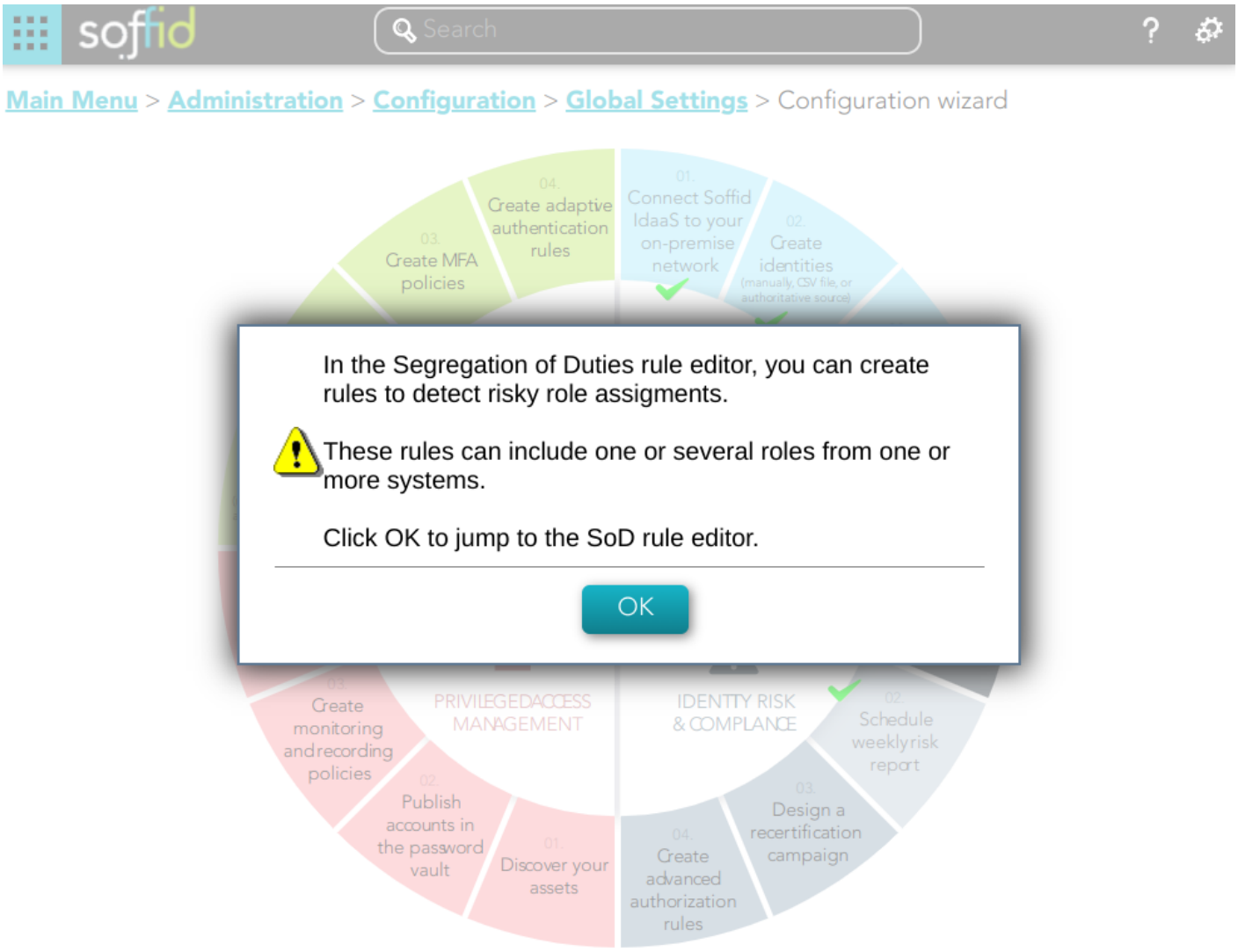
Description

The segregation of duties (SoD) is a fundamental element of internal controls, defined to prevent error and fraud. Segregation of duties ensures that at least two individuals are responsible for the separate parts of any task.

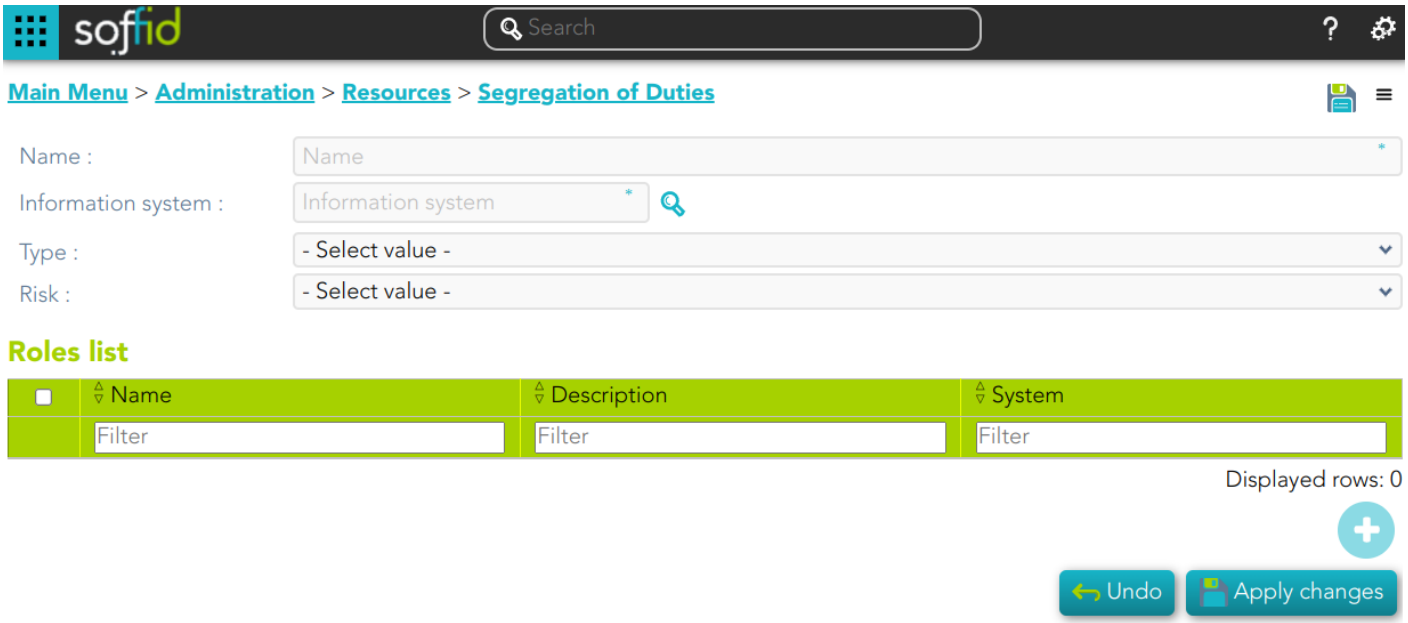
> You can find additional information by visiting **the Segregation of Duties page**.

Step-by-step

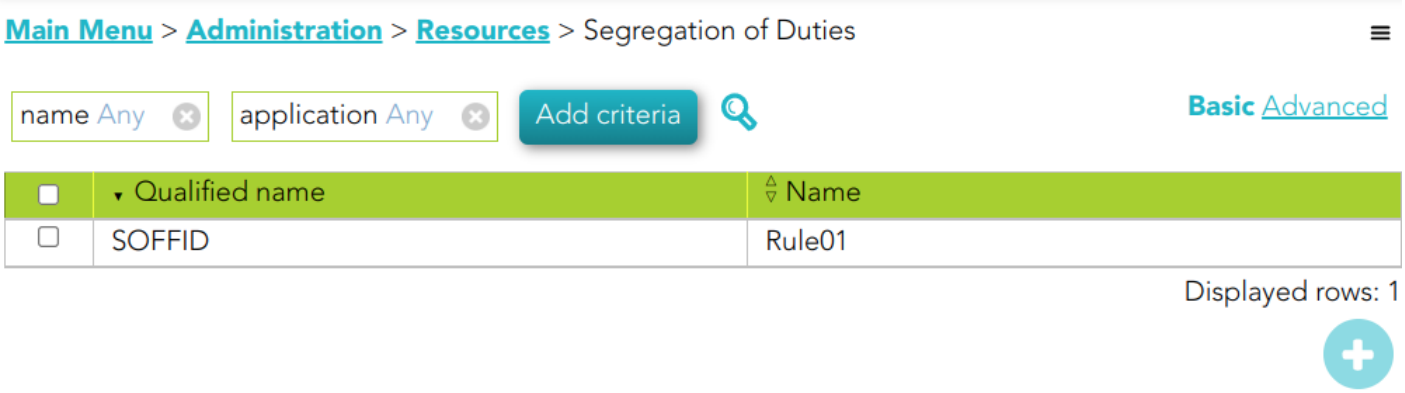
1. First, you must select the Create SoD matrix and click the OK button.



2. Once you click the OK button, Soffid will browse to the Segregation of Duties page in order to add a new SoD



3. Finally you must save or Apply changes to save the SoD.



Standard attributes

- **Name**: name of the segregation separation of duties
- **Information System**: asset or application, from a functional point of view, on which the permissions are granted or revoked.
- **Type**: type of segregation
  - **Trigger on all permissions**: no user can be assigned the roles added to the role list.
  - **Trigger on some permissions**: if you select that option, you have to fill in the number of roles that can not match. Soffid will not allow you to assign to a user more than the number indicated of the roles added to the role list.
  - **Query permissions matrix**: Soffid displays a matrix that allows you to select the risk between pairs of roles, those roles are the roles added to the role list.
- **Risk**: level of risk:
  - **Low**.
  - **High**.
  - **Forbidden**: it is not allowed that one user to have assigned the roles defined on the role list.
  - **None**: there is no risk.
- **Role List**: list of roles to keep in mind on the segregation of duties.

Schedule weekly risk report

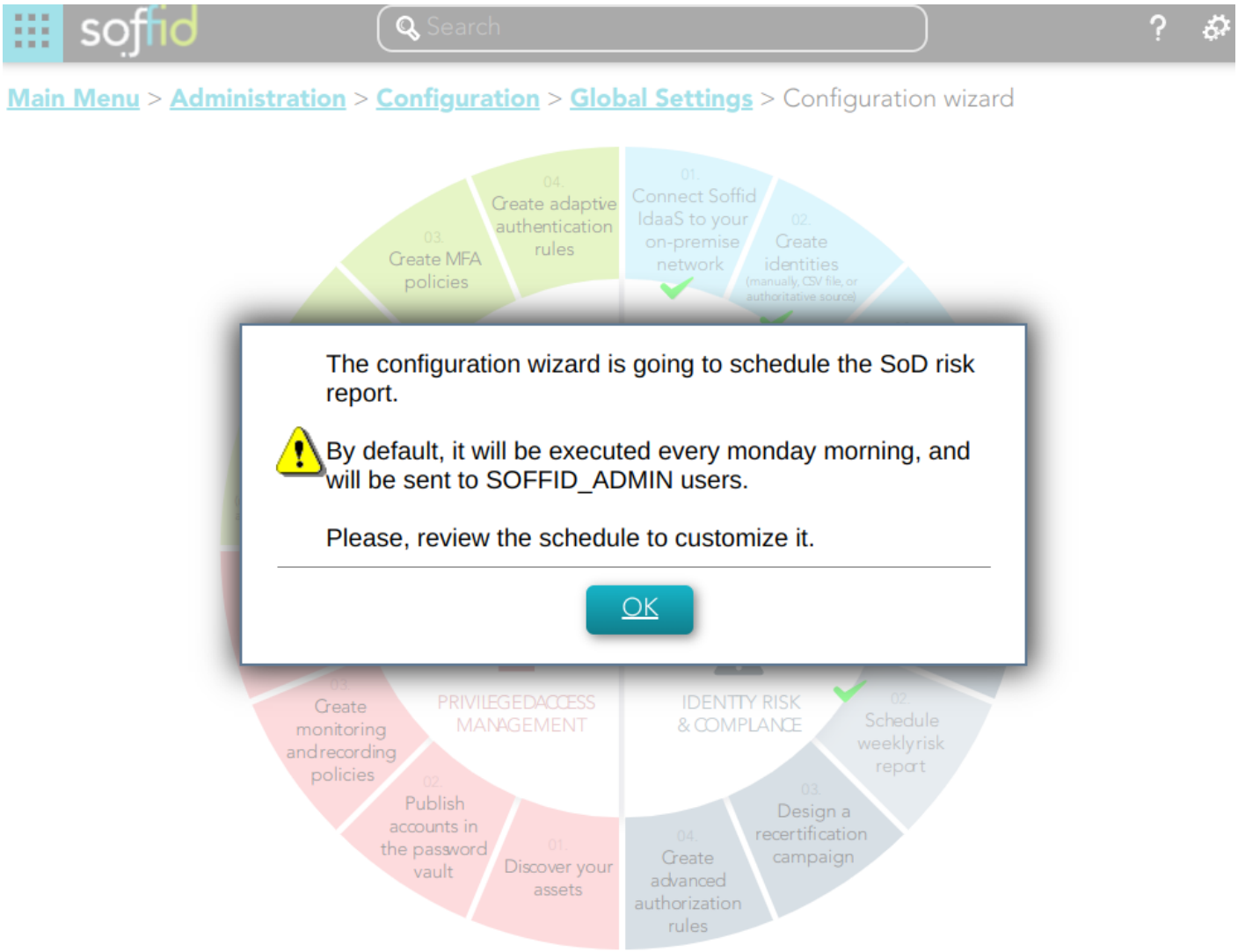
Description

The wizard allows you to schedule a new Weekly risk report. It is a document that provides an overview of the potential risks. The information in this document is related to the rules defined in the SoD.

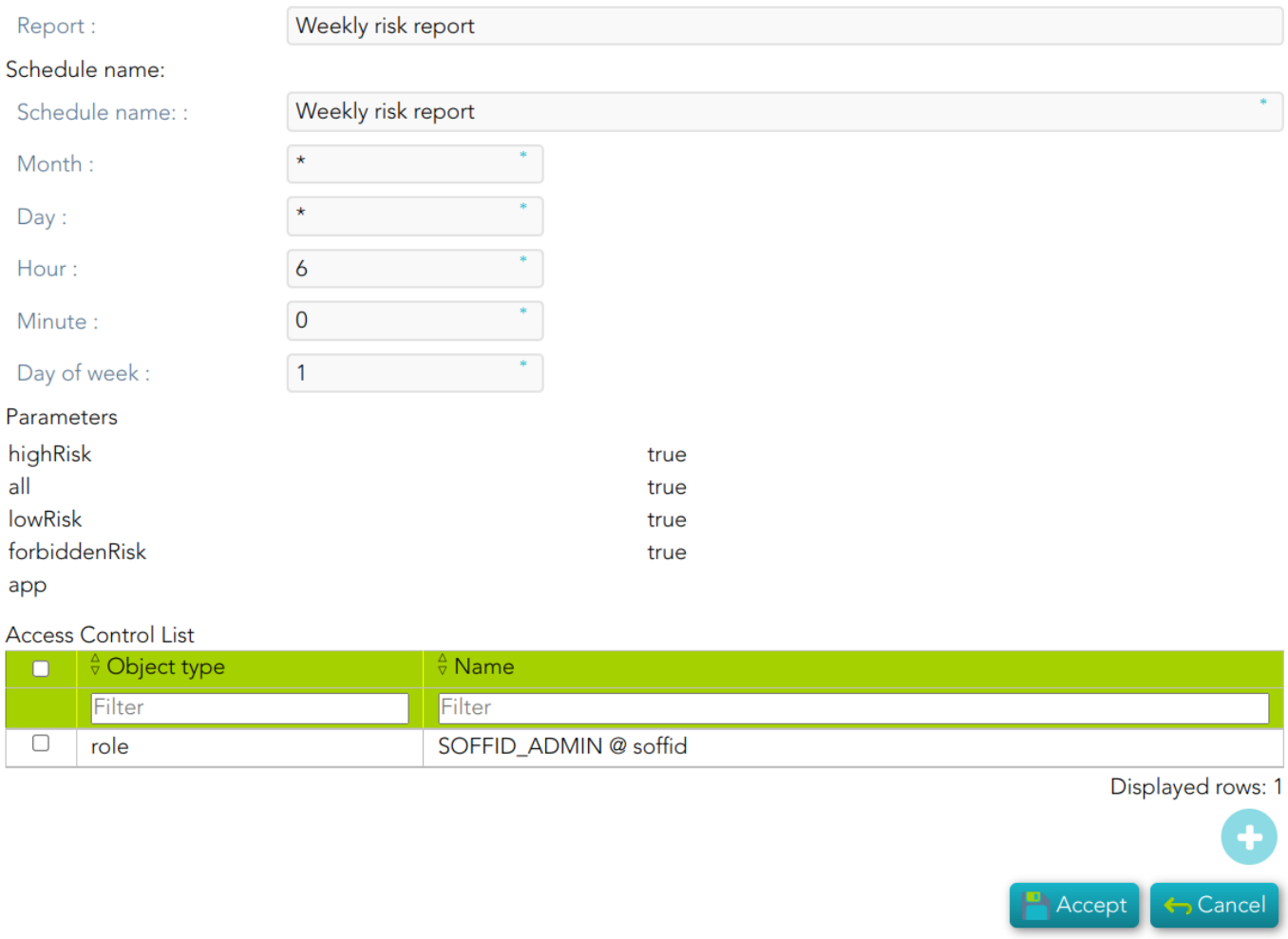
> For more information, you can visit the Scheduled reports page.

Step-by-step

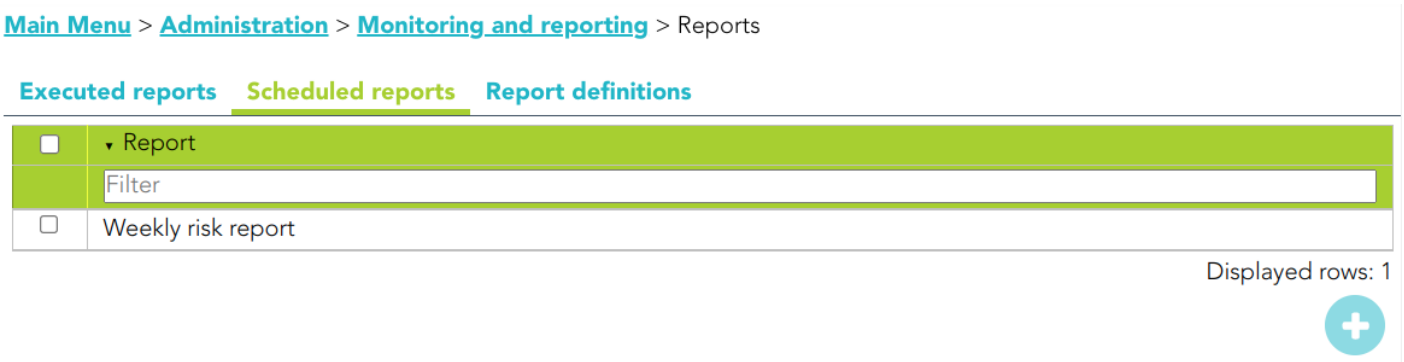
1. First, you must select the Schedule weekly risk report and click the OK button.



2. Then, Soffid will browse to the configure report page and allows you to configure the Weekly risk report.



3. Finally you must accept the changes, and the report will be displayed on the Scheduled reports page



Standard attributes

- **Report**: name of the report.
- **Schedule name**: identified name.
- **Month**: number of the month (1-12) when the task will be performed.
- **Day**: number of the day (1-31) when the task will be performed.

- **Hour**: hour (0-23) when the task will be performed.
- **Minute**: minute (0-59) when the task will be performed.
- **Day of week**: number of the day (0-7 where 0 means Sunday) of the week when the task will be performed.
- **Access Control List**: to prevent unauthorized usage. Will be granted to users, groups or roles.

For each value of month, day, hour, minute, or day of the week:

- * means any month, day, hour, minute, or day of the week. e.g. */5 to schedule every five minutes.
- A single number specifies that unit value: 3
- Some comma separated numbers: 1,3,5,7
- A range of values: 1-5

Design a recertification campaign

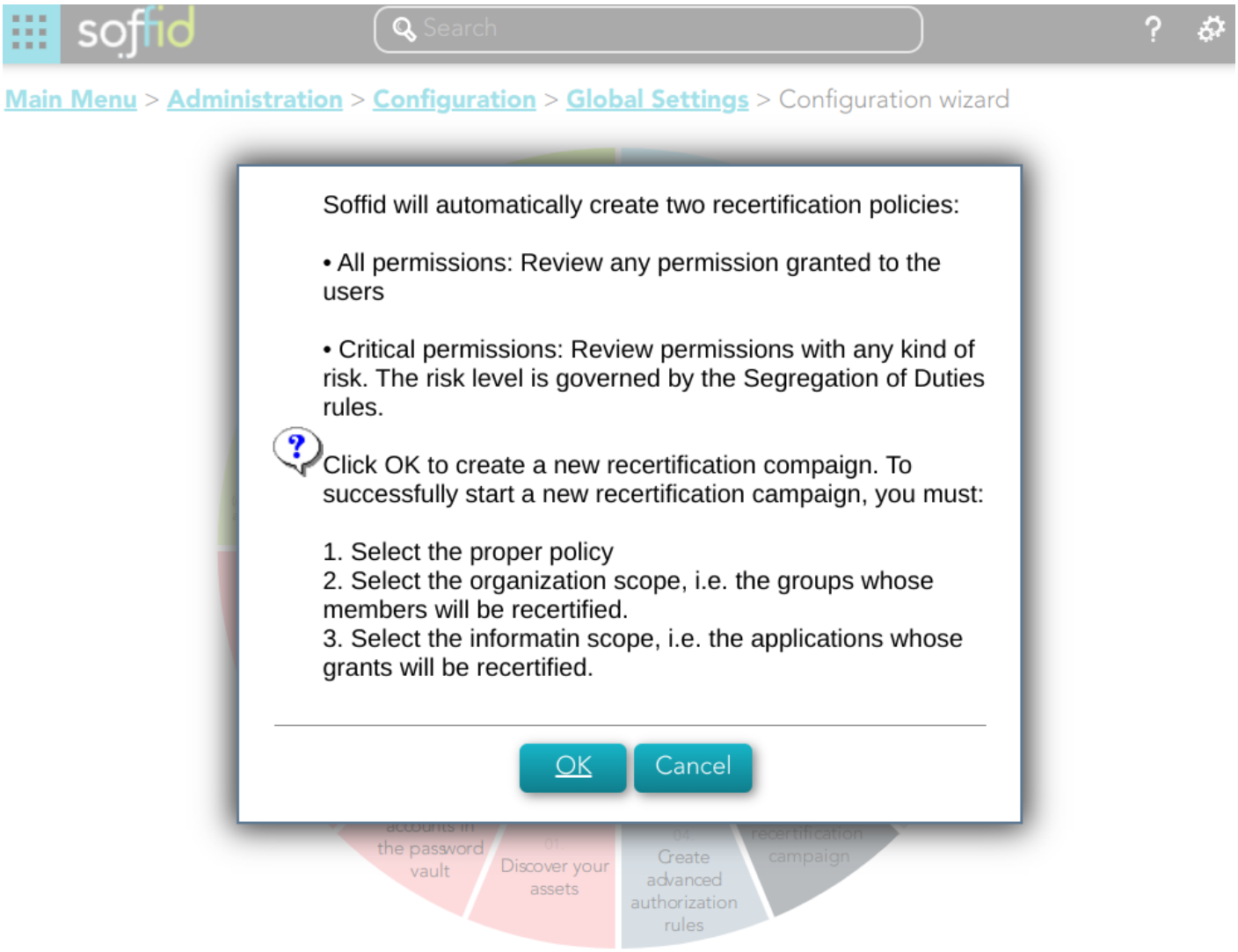
Description

The wizard allows you to create a new recertification campaign. To be able to do this, Soffid has created two recertification policies, *All permissions* and *Critical permissions*.

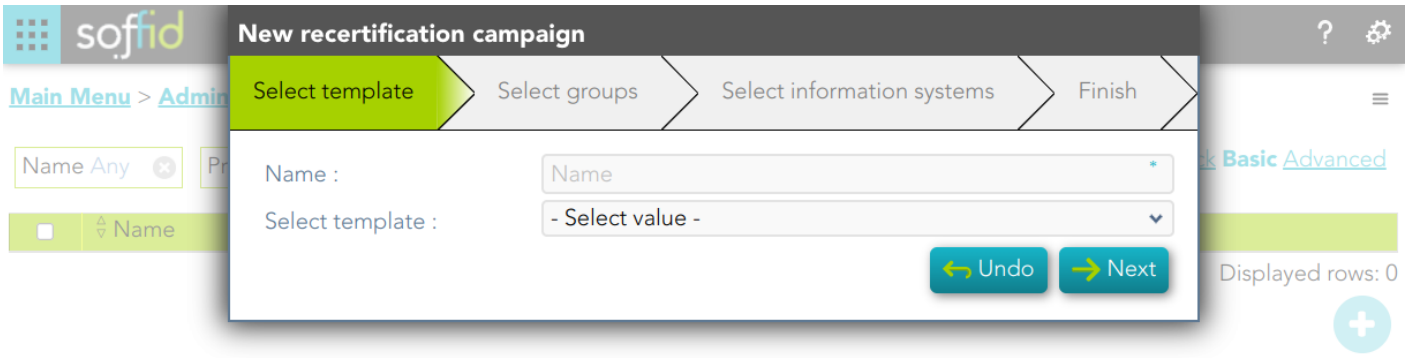
> For more information, you can visit **the Recertification book**.

Step-by-step

1. First, you must select the Design a recertification campaign and click the OK button.



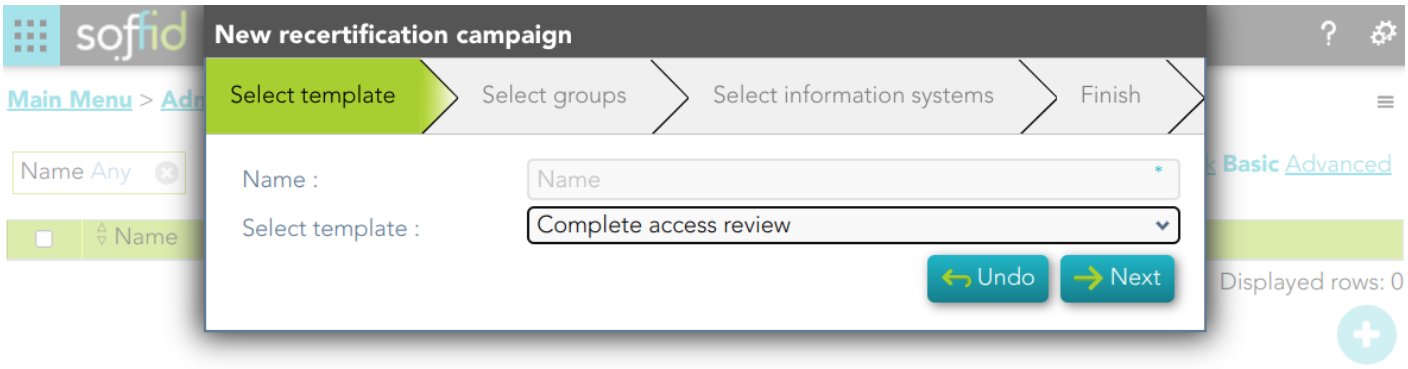
2. Then Soffid will browse the New recertification campaign



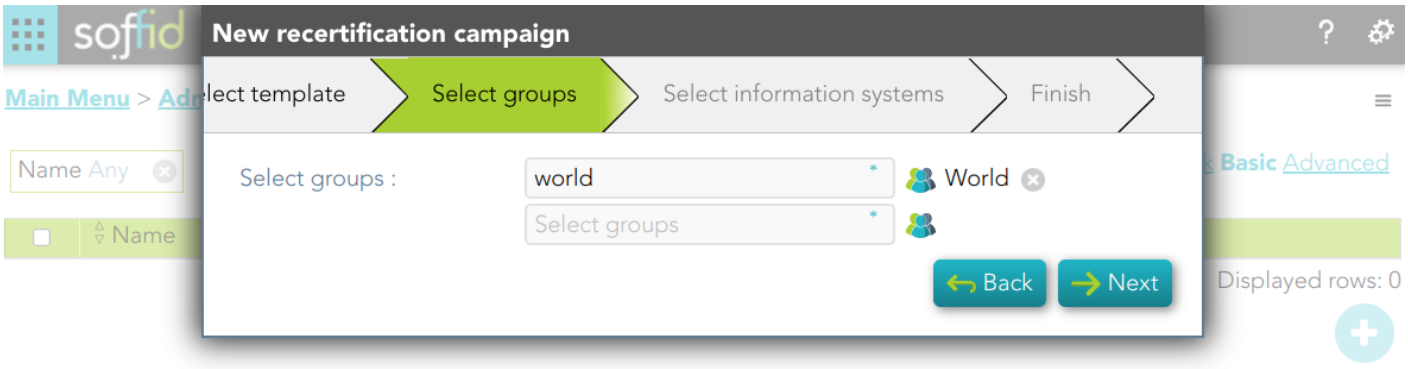
3. In this step you must write a campaign name and select a template.

3.1. Complete access review

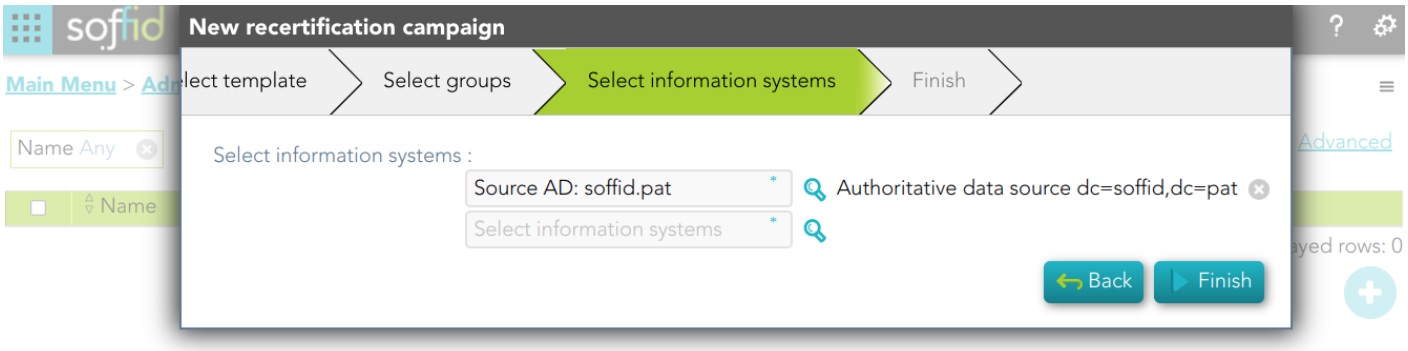
3.1.1. Write a name, select the Complete access review, and click the Next button



3.1.2. Select the group or groups to apply the campaign and click the Next button



3.1.3. Select the Information systems to apply the campaign and click the Finish button



Standard attributes

- **Name**: name to identify the campaign.
- **Template**: select the policy that will be applied. That has to be defined previously on the Recertification policies page.
- **Groups**: list of user groups where the campaign will be applied. You can choose one or more.
- **Information Systems**: list of information systems where the campaign will be applied. You can choose one or more.

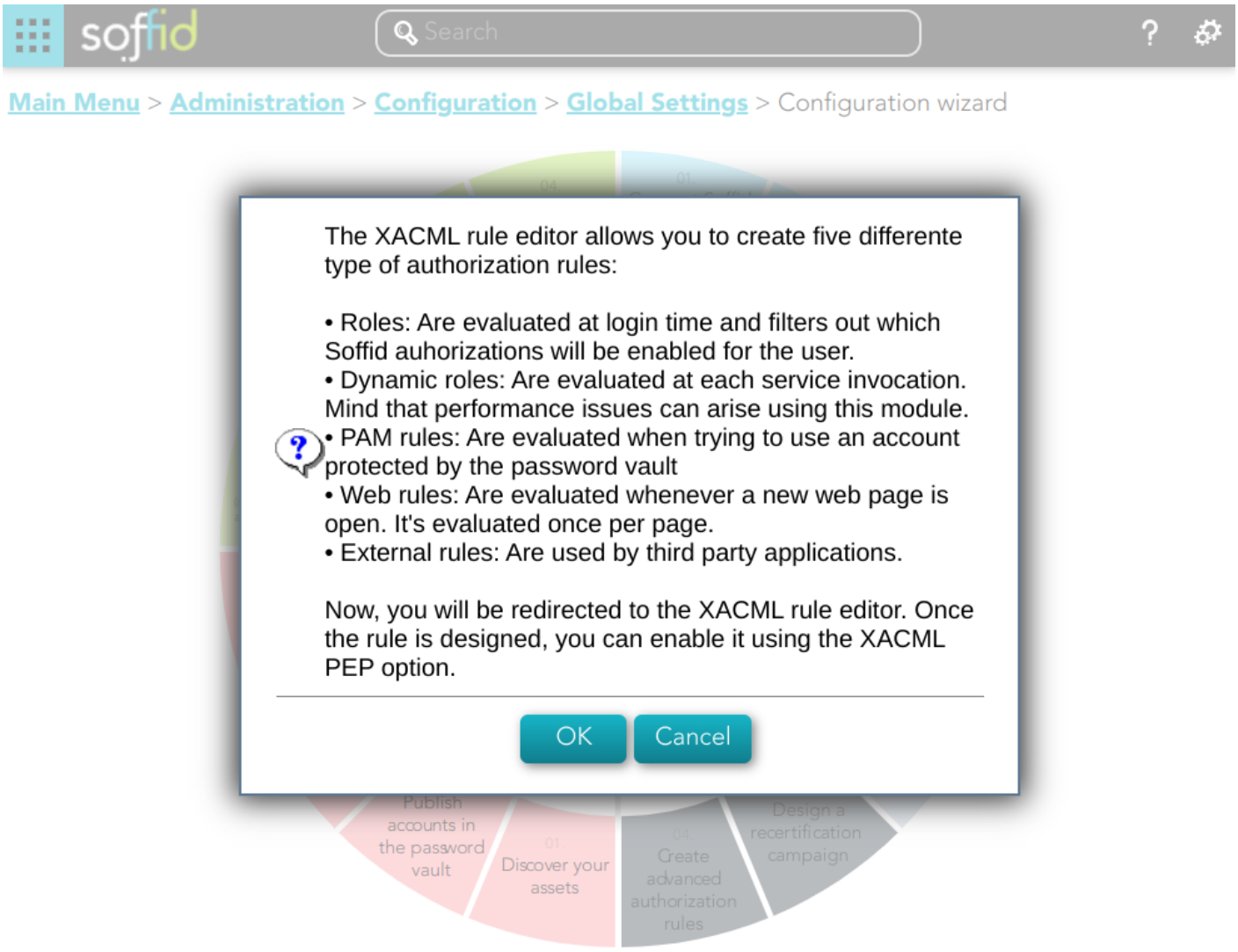
Create advanced authorization rules

Description

This wizard allows you to browse the XACML Policy Management page to create new policies to add more complex and restricted rules to the authorizations.

> For more information, you can visit the XACML page.

Screen overview



Screen overview

https://www.youtube.com/embed/C3LMc4rrEQI?ref=0

Related objects

- Policy set
- Policy
- Policy set reference

- Policy reference