Step 7. Just in time privileges

Introduction

Once the discovery process has been run, the critical accounts have been detected and saved on the password vault, and the password rotation process has been defined, the next step would be to define the necessary approval process to manage the use of the critical accounts.

Using the approval process, Soffid allows you to define, step by step on the **BPM Editor,** the workflow for critical accounts use, and define who has to be the manager or authorized user who will approve or deny to use of those critical accounts. To define and configure the workflow you must know some information like:

- Who or whom can start the process of making a request.
- Who or whom must approve or deny the request.
- If the approved email will be available.
- Which fields must see or fill in the users whom requests.
- Which fields must see or fill in the users whom approve or deny.
- How many approval levels the workflow will need.
- And other requirements.

Then, Soffid can be able to add more complex and restricted rules to the authorizations using **XACML**. With the XACML tool, you will be able to define policy sets and policies to describe general access control requirements. Also, you will be able to define some obligations as actions that have to be returned with response XACML. To define the policy sets and policies, you need to know some relevant information like:

- On which resources, policy set, or policies should be applied
- On which users, a set of policies or policies should be implemented.
- The actions which will be executed
- In which environments the policy sets or policies will be implemented.
- The rules will be applied.
- And other.

Revision #15
Created 26 August 2021 06:27:19
Updated 1 December 2022 09:02:23