Issue policies

Definition

Soffid has defined automatic events by default. For each of these events, it is possible to define the tasks to be performed and configure them.

You can find this functionality in the following path:

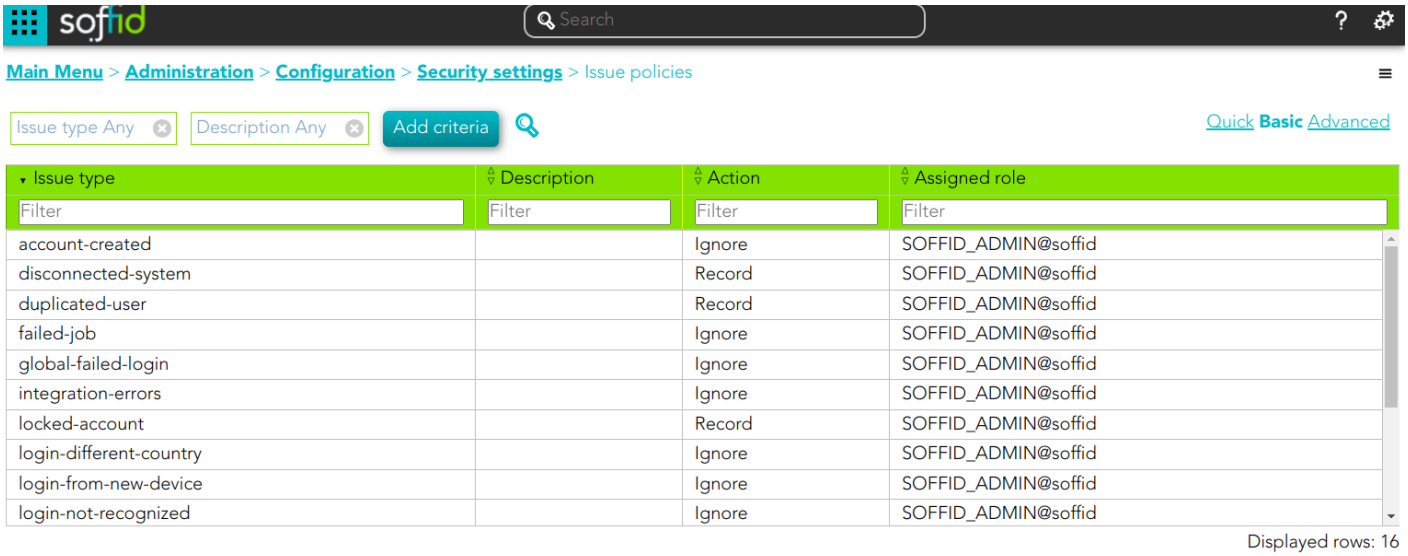
`Main Menu > Administration > Configuration > Security settings > Issue policies`

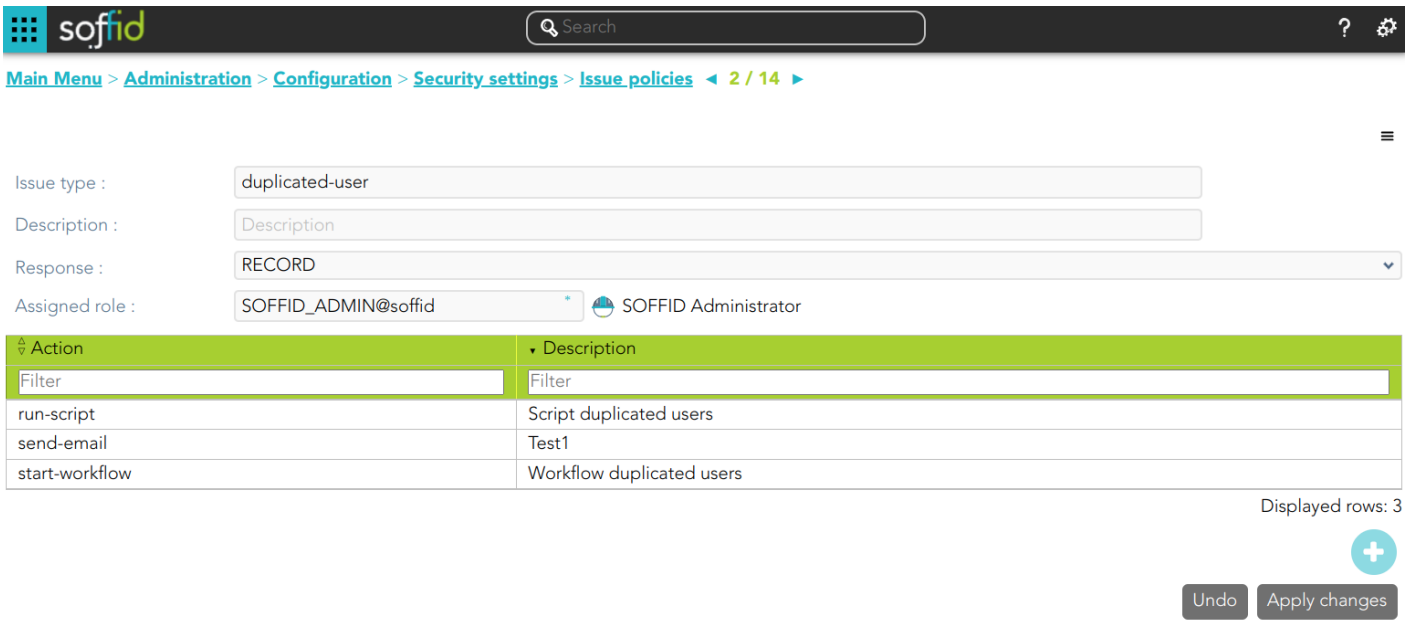
The default events are the following;

Issue Type	Description
account-created	This issue is created when the Sync Server detects when a new account is created. This may occur after the Reconciliation process has been executed.
disconnected-system	This issue is created when the Sync Server detects that some target system is offline.
discovered-host	This issue is created when the Sync Server detects a new host in the network. This only occurs after the Network Discovery process has been executed.
discovered-system	This issue is created when the Sync Server detects a new system in a host. This only occurs after the Network Discovery process has been executed.
duplicated-user	This issue is created the system detects that there are duplicate users, or when the task is generated manually from the user management.
enabled-account-on-disabled-user	This issue is created when an enabled account is detected on a disabled user. This may occur after the reconciliation process has been executed.
failed-job	This issue is created when the system detects job failures. This may occur by running any scheduled task.
global-failed-login	This issue is created when the number of session start failures exceeds the threshold of 0.8.

integration-errors	This issue is created when the Sync Server detects an integration error between Soffid and an end system. You can check the task in the Monitoring & Reporting.
locked-account	This issue is created when an account has been blocked for exceeding the maximum number of login attempts. You can configure the property *Lock after failures* in the Password policies settings. Even if it is temporarily locked, the incident will be generated.
login-different-country	This issue is created when Soffid detects a new login from a different country. It only works with the Identity Provider and it is necessary to have the geolocation database updated.
login-from-new-device	This issue is created when Soffid detects a new login from a new device. It only works with the Identity Provider.
login-not-recognized	This issue is created when Soffid detects a login not recognized (disabled user or user does not exist) in the Soffid Console or in Soffid as an Identity Provider.
otp-failures	This issue is created when an OTP is blocked for exceeding the number of attempts. Currently blocked with 10 unsuccessful attempts.
pam-violation	This issue is created when any of the rules of the PAM are violated. You can define the PAM rules and the PAM policies. Be in mind, that you must check the "Open issue" option in the PAM policies you wish to control.
password-changed	This issue is created when a Password change is detected. These changes come from the end system (Active Directory or Soffid OpenLDAP) and Soffid has been notified. The issue is not created if it is the operator or a script that changes the password in Soffid.
permissions-granted	This issue is created when it is detected that permissions have been given to a user on the end system. This may occur after the reconciliation process has been executed.
risk-increase	This issue is created when it is detected the risk level of a user is increased. You can configure the risks in the Segregation of Duties option.
robot-login	This issue is created when it is detected is detected that someone who has not passed the CAPTCHA is trying to log in to the Identity Provider.
security-exception	This issue is created when unauthorized access to the console via WebService or admin console occurs.

Screen Overview





Related Objects

1. **Roles**

Standard attributes

- **Issue type**: by default, some issues type are defined in Soffid Console.
- **Description**: a brief description of the issue.
- **Action**:
  - **Ignore**: the action will be ignored, and no additional actions will be run.
  - **Record**: the action will be recorded and an issue with the status Acknowledged will be created. The actions configured for the Acknowledged status will be run.

    - **Manage**: a new issue will be created in the New status and the action configured for this status will be run.
- **Assigned role**: the role who will be the owner of the created issues.
- **Actions list**: list of actions to be taken when this issue occurs. You can choose one or more actions from the list and configure them:
    - **Issue status**: it is used to determine the point when the action will be launched.
        - New.
        - Acknowledged.
        - Solved.
        - Solved - Not a duplicate.
    - **Actions**:
        - **Notify affected user**: this allows you to configure an email that will be sent to the affected users.
        - **Send custom email:** this allows you to configure a custom email that will be sent to specific users.
        - **Run script**: allows you to type a script that will be performed
        - **Look affected accounts**: allows you to configure an email that will be sent to the owner user.
        - **Look affected host**.
        - **Notify issue owner by email**.
        - **Acknowledge**.
        - **Start new process**.: allows you to configure the workflow that will be run.
    - **Description**: a brief description of the action you are defining.

> Note that it will be necessary to restart the Sync Server when changing the action of an issue.

Actions

Issue policies query action

Download CSV file	Allows you to download a CSV file with the issue policies data.

Issue policy detail

Add new	Allows you to add a new action to the issue policy. You can choose the action from the action list. Depending on the selected action, you must fill in different information. Once the information will be filled in, you need to close the window and Apply the changes.

Delete	Allows you to delete one or more actions from the actions list.
Apply changes	Allows you to update the changes made to the issue policy.
Undo	Allows you to quit without applying any changes.

Revision #39
Created 7 June 2023 14:55:40
Updated 1 April 2024 10:48:08