PAM Policies

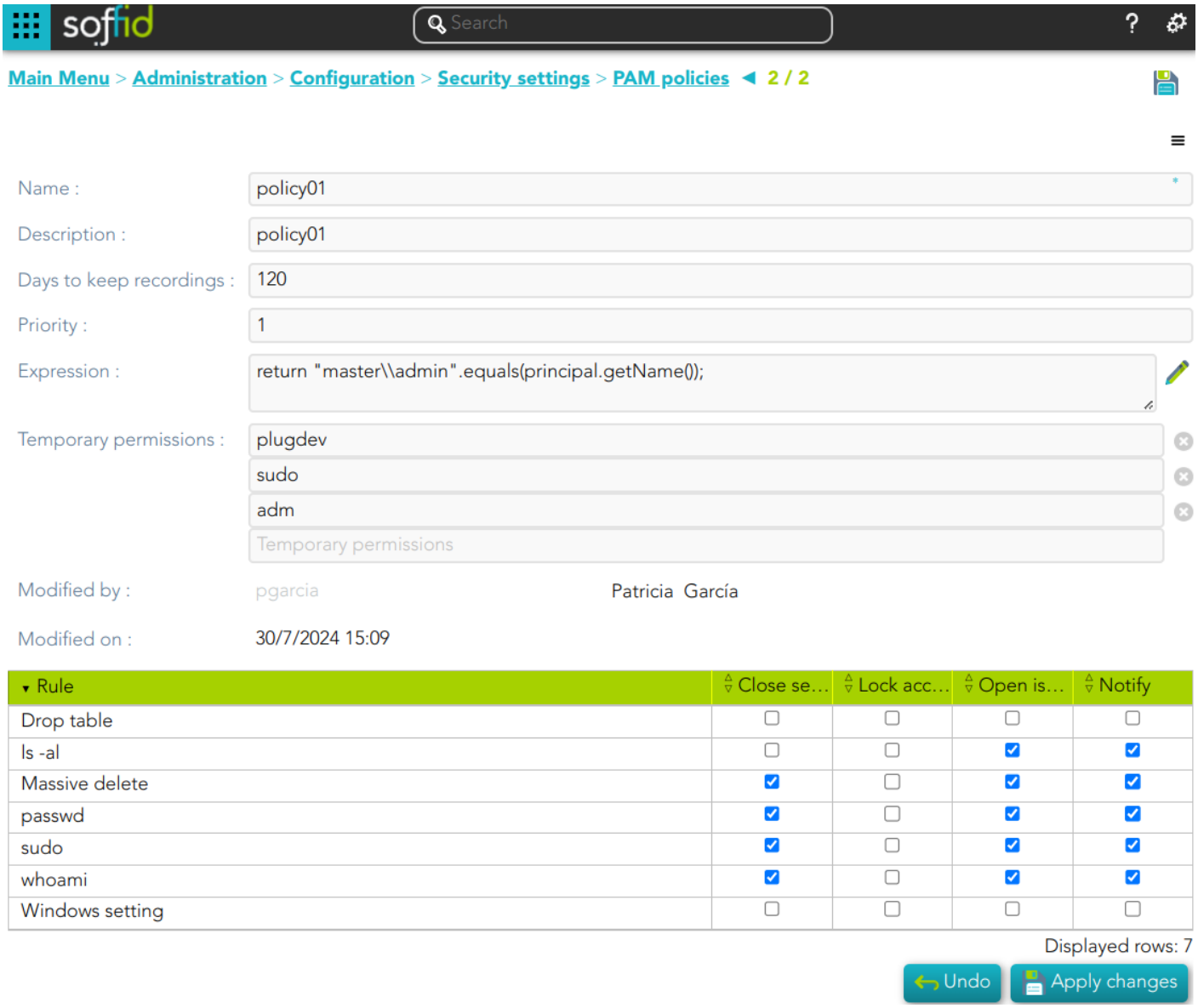
Definition

Privileged Access Management (PAM) policies are a set of guidelines and controls that dictate how privileged access is granted, managed, and audited within an organization.

Soffid allows you to define policies, those policies can be made up of several rules. For each rule, you could select the action to perform when Soffid detects that rule is accomplished.

To use those policies you need to define how policies will be used by each folder in the password vault. For more information, you can visit the Password Vault page.

Screen overview



Standard attributes

- **Name**: name to identify the policy.
- **Description**: a brief description of the policy.
- **Days to keep recordings**: number of days that recordings will be kept.
- **Priority**: allows you to set the priority between the different PAM policies configured. When there are several policies, the policy to be applied is evaluated according to priority and expression.
- **Expression**: this expression is evaluated to determine the priority of the policy to be applied. When there are several policies, the policy to be applied is evaluated according to priority and expression.
- **Temporary permissions**: these permissions will be assigned to the user's account on the target system. The permissions will be maintained for the duration of the session. Once the session is over, the permissions will be revoked. The account must be a managed account.

- **Modified by**: user who modified that rule.
- **Modified on**: the date and time of the update.

When you save the standard attributes of a PAM policy and edit the policy again, the rule list will be shown. Here you can customize the policy depending on the existing rules.

- **Rule list**: show a list of the PAM rules defined. You can check/uncheck the available options. You can choose zero, one, or several:
  - **Close session**: when the rule is met, Soffid will close the session.
  - **Lock account**: when the rule is met, Soffid will lock the account.
  - **Open issue**: when the rule is met, Soffid will open a new issue (*).
  - **Notify**: when the rule is met, Soffid will send a notification about the action.

> (*) You can visit the following page for more information about the issues:
> https://bookstack.soffid.com/books/soffid-3-reference-guide/page/issue-policies and
> https://bookstack.soffid.com/link/1153#bkmrk-pam-violation

> The PAM policies configuration is sent to the user-console.policies to the Store container. You can find this file at /opt/soffid/tomee/data/ips

Image


```
root@77bc37f3629d:/opt/soffid/tomee/data/ips# cat user-console.policies
[{"policyName":"policy002","actions":[{"shortName":"ls -al","description":"ls -al","type":"keyboard","content":"ls
-al","author":"pgarcia","date":1720074500000,"actions":["N"]},{"shortName":"Drop table","description":"Drop table"
"type":"keyboard","content":"[dD][rR][oO][pP].*[tT][aA][bB][lL][eE]","author":"pgarcia","date":1730303556000,"acti
ns":["N"]},{"shortName":"Windows setting","description":"User opens windows settings app","type":"screen","content
:"Panel de Control","author":"pgarcia","date":1731939483000,"actions":["N"]},{"shortName":"whoami","description":"
hoami","type":"keyboard","content":"whoami","author":"pgarcia","date":1720073853000,"actions":["N"]},{"shortName":
sudo","description":"sudo","type":"keyboard","content":"sudo","author":"admin","date":1709047462000,"actions":["N"
"C"]},{"shortName":"Massive delete","description":"Massive delete","type":"keyboard","content":"rm.*-.*r","author"
"admin","date":1709047492000,"actions":["N"]},{"shortName":"apt-get","description":"apt-get","type":"keyboard","co
tent":"apt-get","author":"pgarcia","date":1725440932000,"actions":["N","C"]},{"shortName":"passwd","description":"
asswd","type":"keyboard","content":"passwd","author":"admin","date":1715332681000,"actions":["N"]}],"author":"pgar
ia","date":1734011609000,"maxSessionMinutes":null},{"policyName":"policy001","actions":[{"shortName":"ls -al","des
ription":"ls -al","type":"keyboard","content":"ls -al","author":"pgarcia","date":1720074500000,"actions":["I"]},{"
hortName":"whoami","description":"whoami","type":"keyboard","content":"whoami","author":"pgarcia","date":172007385
000,"actions":["I"]},{"shortName":"Massive delete","description":"Massive delete","type":"keyboard","content":"rm.
-.*r","author":"admin","date":1709047492000,"actions":["I"]},{"shortName":"Windows setting","description":"User op
ns windows settings app","type":"screen","content":"Panel de Control","author":"pgarcia","date":1731939483000,"act
ons":["I","N"]},{"shortName":"passwd","description":"passwd","type":"keyboard","content":"passwd","author":"admin"
"date":1715332681000,"actions":["I"]},{"shortName":"apt-get","description":"apt-get","type":"keyboard","content":"
pt-get","author":"pgarcia","date":1725440932000,"actions":["I","N"]},{"shortName":"sudo","description":"sudo","typ
":"keyboard","content":"sudo","author":"admin","date":1709047462000,"actions":["I"]},{"shortName":"Drop table","de
cription":"Drop table","type":"keyboard","content":"[dD][rR][oO][pP].*[tT][aA][bB][lL][eE]","author":"pgarcia","da
root@77bc37f3629d:/opt/soffid/tomee/data/ips#
```


Actions

PAM rules query

Query	Allows you to query PAM policies through different search systems, Quick, Basic and Advanced.
Add or remove columns	Allows you to show and hide columns in the table.
Add new	Allows you to create a new PAM policy. You can choose that option on the hamburger menu or click the add button (+). To add a new PAM policy it will be mandatory to fill in the required fields.
Delete	Allows you to remove one or more PAM policies by selecting one or more records and next clicking the button with the subtraction symbol (-). To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.
Import	Allows you to upload a CSV file with the PAM policies list to add or update PAM policies to Soffid. First, you need to pick up a CSV file, that CSV has to contain a specific configuration. Then you need to check the content to be loaded, it is allowed to choose if you want or not to load a specific attribute. Finally, you need to select the mappings for each column of the CSV file to import the data correctly and click the Import button.
Download CSV file	Allows you to download a CSV file with the PAM policies information.

PAM rules detail

Apply changes	Allows you to create a new configuration PAM policy or to update an existing one. To save the data it will be mandatory to fill in the required fields.
Undo	Allows you to quit without applying any changes made.
Delete	Allows you to delete a PAM policy. To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.

Revision #18
Created 16 August 2021 13:09:03 by pgarcia@soffid.com
Updated 13 December 2024 10:49:23 by pgarcia@soffid.com