Accounts

Description

> An account is the way an user is presented on a target system. There can be user accounts as well as system-purpose accounts.

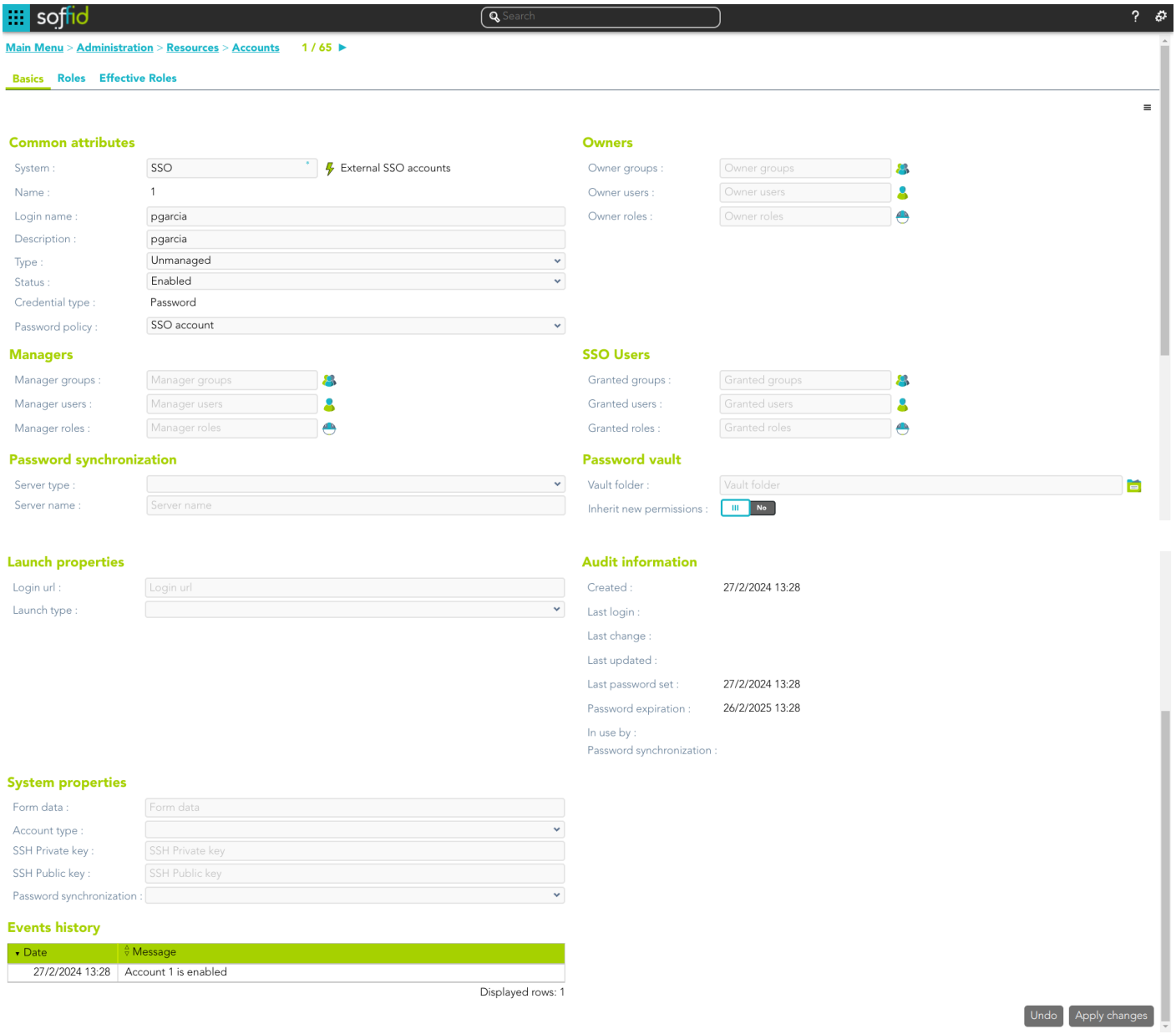
An account belongs to a system and that account can have specific permissions assigned to it. An account must have defined the account type, that is if the account is a single user, privileged, shared, or unmanaged.

The password policy is also mandatory to create an account. That password policy determines the conditions that the password must meet.

It is allowed to set a password for an account, which can be a generated password by the system, or a password set by the administrator user. That password must comply with the password policies defined. When the account is unmanaged, if the password change, it will not be sent to the target system.

The account can be displayed in **black** or **gray** color. The gray color is used to indicate that the account is unmanaged, that is because the agent is disconnected or because the agent is in Read-Only Mode.

Screen overview



Related objects

An account is related, in Soffid, to other objects:

1. **User:** users related to this account.
2. **Groups**: groups to which the account belongs.
3. **Roles**: the permissions that this account has associated with the system in which it is used. They can be assigned or revoked by users with administrator privileges.
4. **System**: the environment in which that account is used (AD, Exchange, etc).

Standard attributes

Basic

On the basic account tab, you can view all the account attributes. It is allowed to add new accounts, update or delete existing accounts and other options.

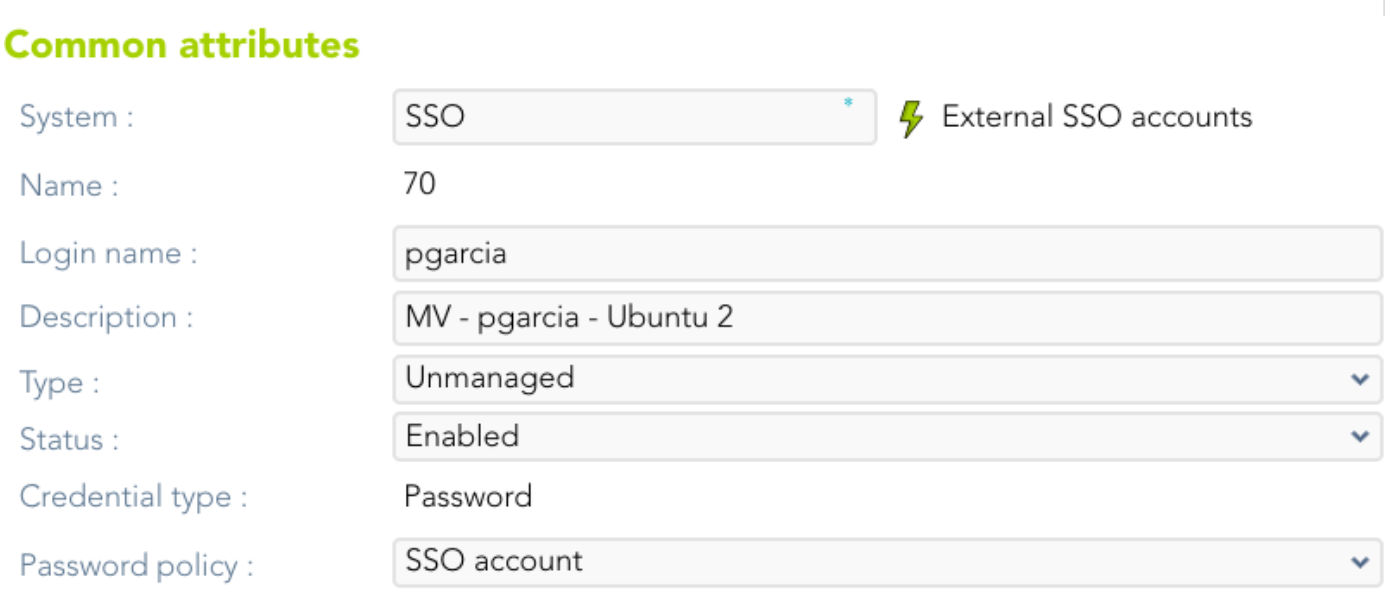
Commons attributes

- **System**: target system to which the account will be connected. When SSO is the system selected, the account name is assigned by Soffid, that is because SSO is a multi-system connector and can be many accounts with the same login name.
- **Name**: name used to identify the account.
- **Description**: plain text with information about the account.
- **Type**: there are four kinds of accounts:
  - **Single user account**: accounts should normally be user accounts and bound to a single user. We can see user accounts on the user management screen, and will mostly be created by Soffid.
  - **Shared accounts**: these accounts are shared among multiple users. They have an access control list to prevent unauthorized usage. Will be granted to users, groups or roles. Passwords on shared accounts might be set by operators or by the user. It depends on the password policy definition. A shared account could have related services.
  - **High privilege accounts**: shared among users, but only one user possesses it at one time. Through self-service portal, a high privilege account owner can check-in and check-out them. Will be granted to users, groups or roles. Passwords on these accounts will be set only by the user using the self-service portal. The user can set it for a period of time. After that, the system will change the password by a temporary one.
  - **Unmanaged accounts**: ignored by Soffid. They can be populated based on existing system accounts. Soffid will be able track any changes applied to this type of accounts on the managed system, but Soffid will not apply any change to the actual system. You should have a limited number of unmanaged accounts, but they are extremely useful during deployment phase.
- **Credential type**: this field will be available when the system is filled with the SSO option.
  - **Password**: this is the default value. This option will allow you to set the account password.
  - **SSH key**: this option will allow you to add a SSH key. This SSH key could be an existing key or a generated new key.
  - **Kubernetes key**: this option will allow you to enter a Yaml descriptor to configure the access.
- **Status**:

- **Enabled**: the account can be used by the user. Soffid engine will disable it when the user does not match the access requirement policy.
- **Manually enabled**: the account can be used by the user. Soffid engine will keep it enabled, even when the user does not match the access requirement policy.
- **Disabled**: the account cannot be used by the user. Soffid engine will enable it when the user does matches the access requirement policy.
- **Manually enabled**: the account cannot be used by the user. Soffid engine will keep it disabled, even when the user matches the access requirement policy.
- **Removed**: the account no longer exists in the target system, but its image is kept in Soffid for audit purposes.
- **Locked**: the account is locked when a user tries to access with a fail password too many times (5 times). The account will be enabled in a specific period of time (5 minutes).
- **Archived**:

- **Password policy**: the policy applied to this account. It is mandatory select a password policy. You can see more information on the User Type and Password policies pages.

Image



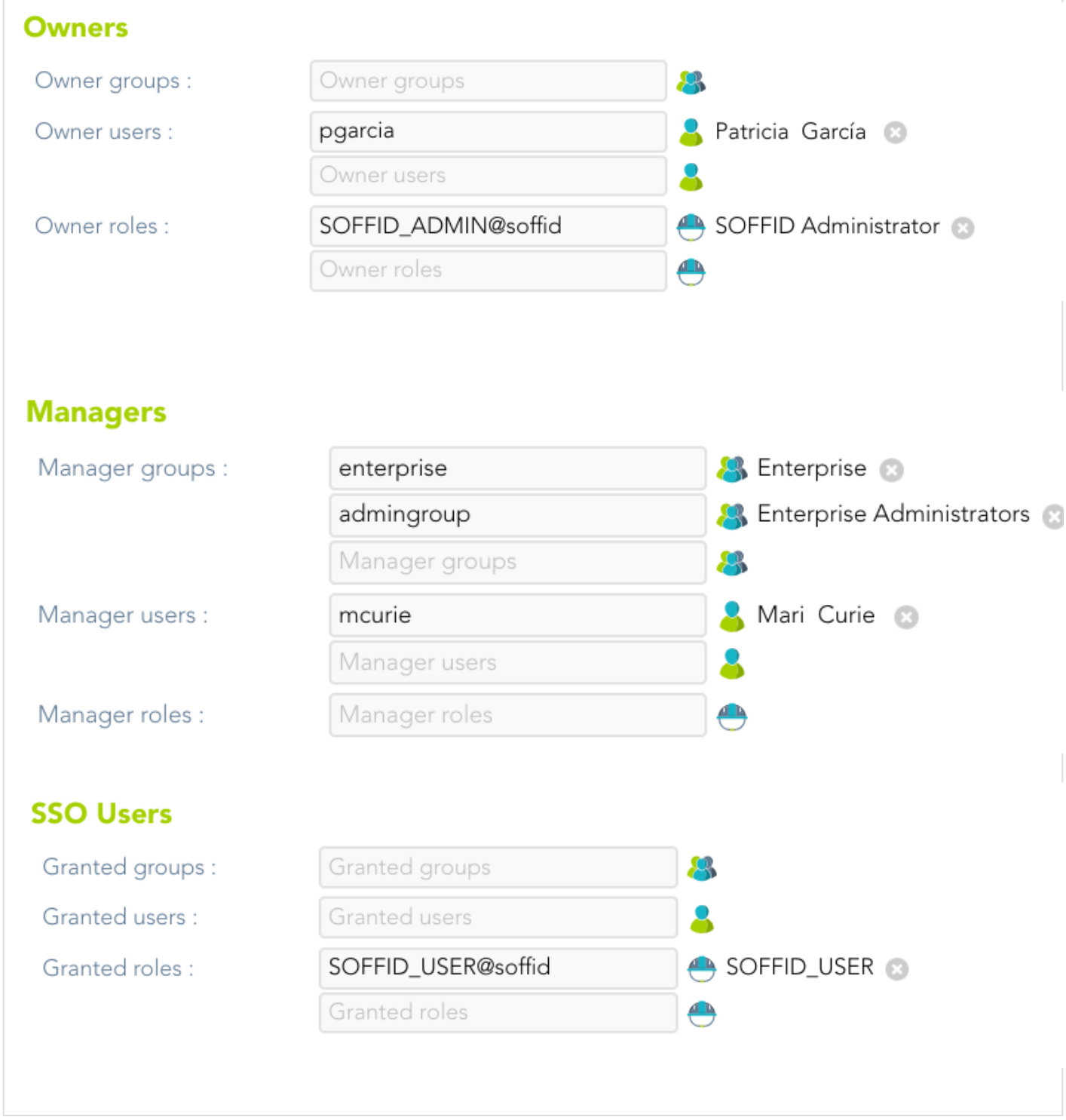
Owners, Managers, and SSO users

Specify the list of users authorized to use this account. For accounts of type "single user", only one user can be specified. Other accounts can have more than one user. The users that can use this account can be specified either directly, by entering the user name, or indirectly, by entering a group or role name. At the latest, any user having that group or role will automatically be entitled to use this account.

There are three access levels for each account and user:

- **SSO User**: can use it by means of the SSO or PAM engines. They cannot change their password, not even through single sign on engine.
- **Manager**: can use it, and set or query the password (using self-service portal), depending on the password policy restriction.
- **Owner**: can use it, modify the access control list, and set or query the password sing self-service portal or single sign-on engine.

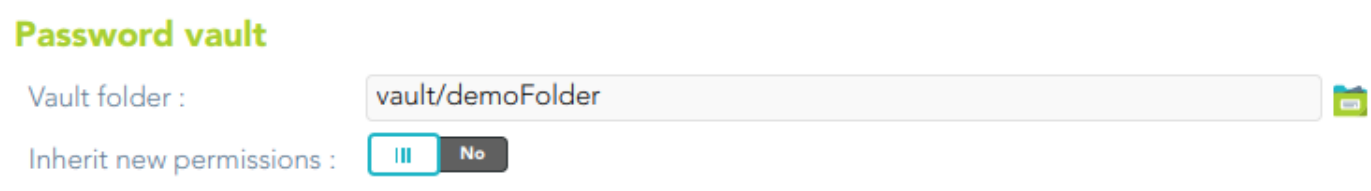
Image



Password vault

- **Vault folder**: personal or shared folder, depending on the account type, in which account data are stored.
- **Inherit new permissions**: determines if the account will inherit the permissions granted to the folder that contains it.

Image



Password synchronization

- **Server type**:
  - Linux
  - Windows
  - Database
- **Server name**
- **SSH Public key**

Image

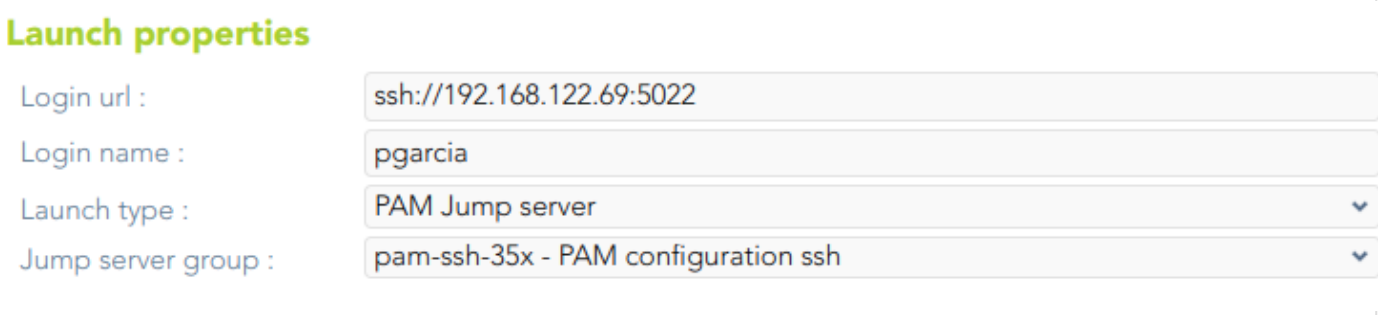


Launch properties

Defines the properties to connect to the target system.

- **Login URL**: URL to connect. You can add the port when you need it
- **Login name**: account name to connect.
- **Launch type**: connection type.
  - **Simple**
  - **WebSSO**
  - **PAM Jump server**: it is mandatory to select the Jump server group.

Image



Audit information

- **Created on**: account creation date.
- **Last login**: last registered access.
- **Last updated**: last modified.
- **Last password set**: date of last password change.
- **Password expiration**: password expiry date.
- **In use by**: account owner
- **Password synchronization**.

System properties

- **SSH Private key**: private key that establishes trust to be able to access the system without requiring a password.
- **SSH Public key**: public key that establishes trust to be able to access the system without requiring a password.

Events history

List of events on this account

Image

Events history

Date	Message
22/4/2024 12:46	Account janis is enabled
02/5/2024 08:04	Account janis is disabled
29/5/2024 08:08	Account janis is enabled
19/6/2024 08:33	Account janis is disabled

Displayed rows: 4

Services

List of services on this account. The account type must be shared to view those services. All these services appear after agent reconciliation.

Image

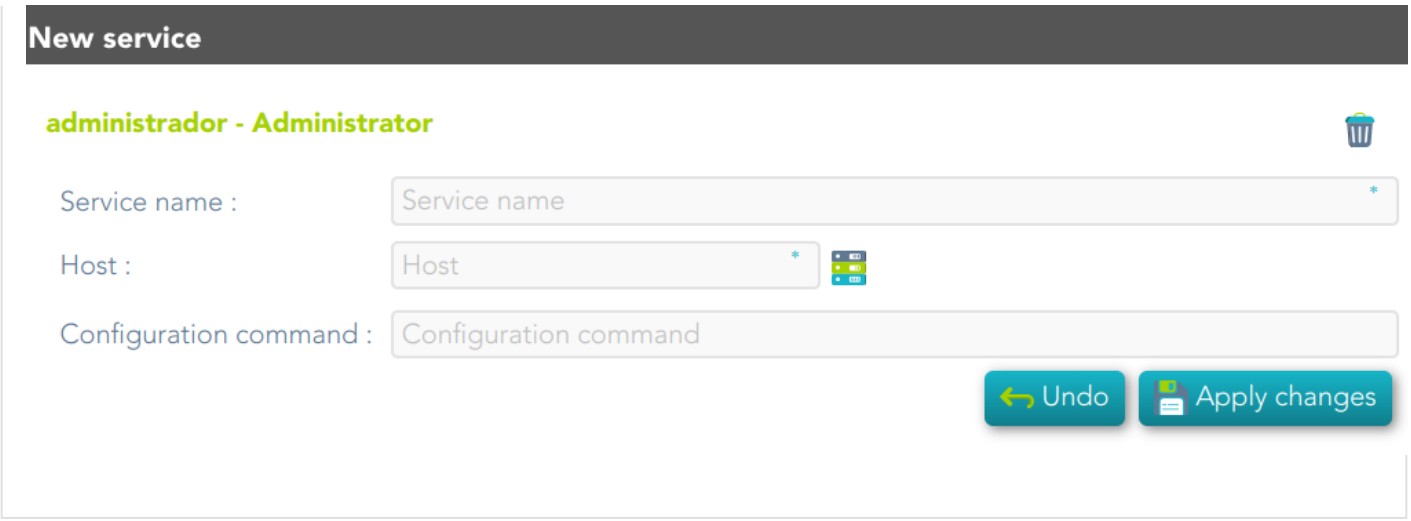
Services

Host	Service name	Configuration command
win-4m3u4hego85	TASK: \CreateExplorerShellUnelevatedTask	
win-4m3u4hego85	TASK: \tarea002	
win-4m3u4hego85	TASK: \User_Feed_Synchronization-{52C824CE-58B1-48FF-909A-2738F98B5580}	
win-4m3u4hego85	TASK: \Mozilla\Firefox Background Update S-1-5-21-456173643-2999096561-4028482310-500 E7CF176E110C211B	
win-4m3u4hego85	TASK: \Mozilla\Firefox Default Browser Agent E7CF176E110C211B	

Displayed rows: 5

Soffid allows you to manage the existing services, you can add, update or remove services as well. This makes sense in the case of Linux machines.

Image



Roles

A role is a collection of permissions that can be granted.

On the roles tab, you can view the roles assigned to the account, it is shown information about the role name, description, application or start (and, if proceed, end) date of the role assignment.

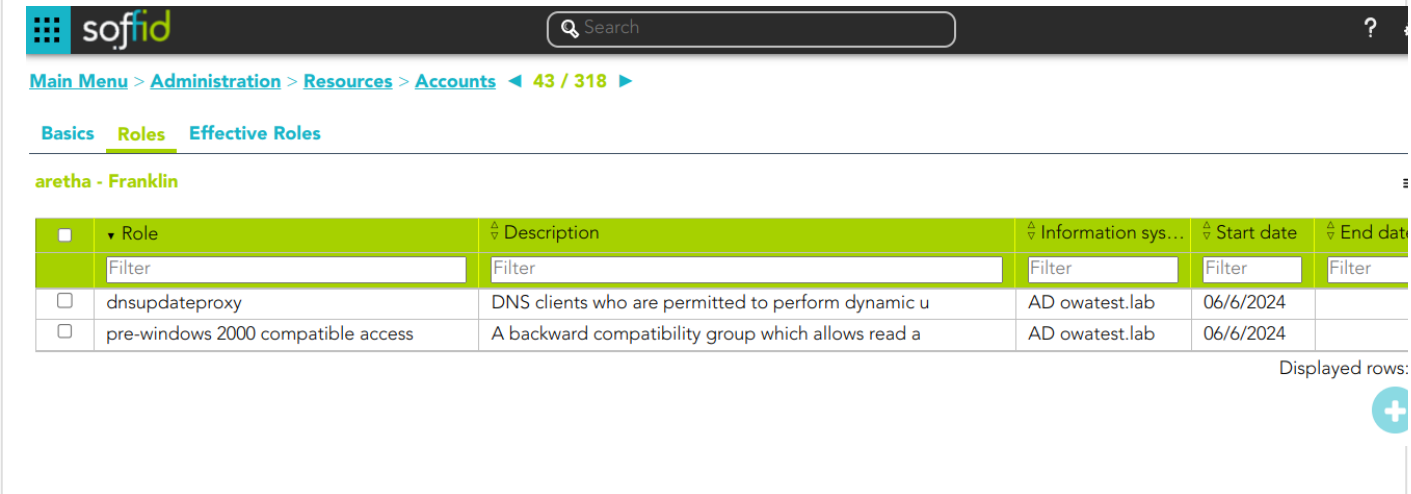
You can also **assign roles** to the account, you can click the add symbol (+), select the role that you want to assign, depending on the role you must fill the scope, and finally set memberships properties.

It is also possible to **revoke roles** to the account from the entitlement details or by selecting one or more records from the list and clicking the button with the subtraction symbol (-).

By clicking on a record, it is shown the detail role assignment information.

Additionally, you can **download a CSV file** with the roles information and you can also **upload a CSV file** to assign or revoke roles.

Image



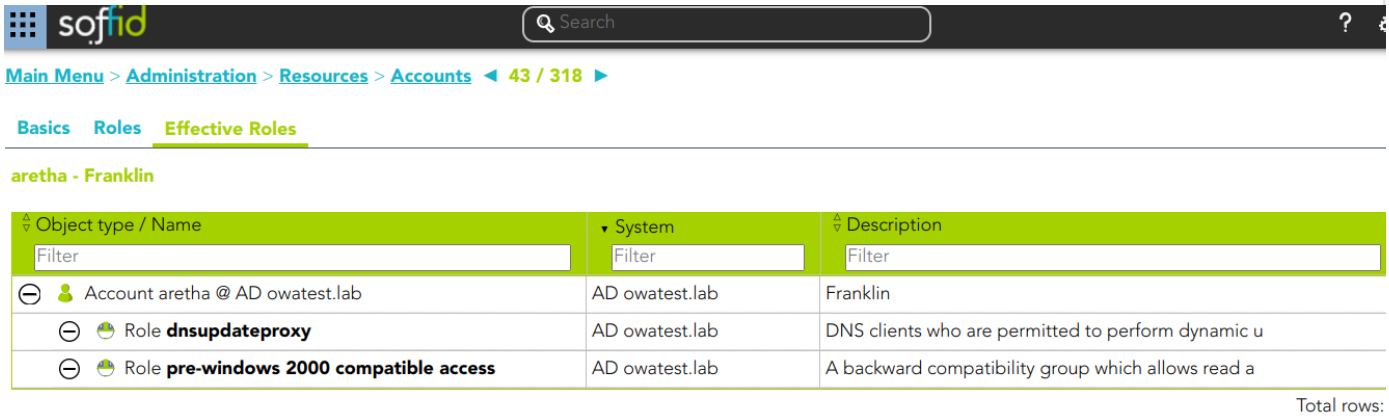
Effective roles

Hierarchy of permissions assigned to or inherited.

This screen details the effective roles for the selected account.

- By direct assignment of the role: when you assign a role to an account, you are assigning to the account all the permissions defined for that role.
- By belonging to a group: when you add a user to a group, the user will have all the roles assigned to the group.
- By rules defined in the system: when a rule is satisfied for a user, the system assigns the roles defined in the rule to the user.

Image



Actions

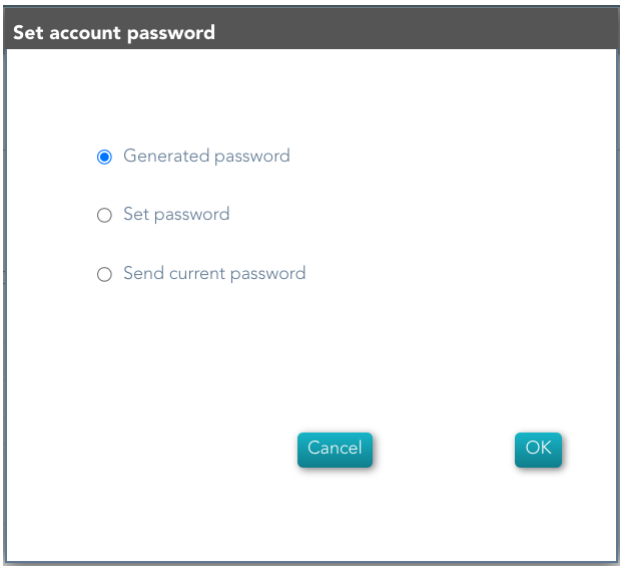
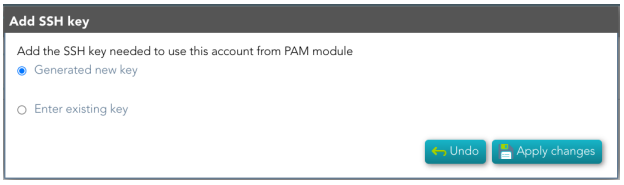
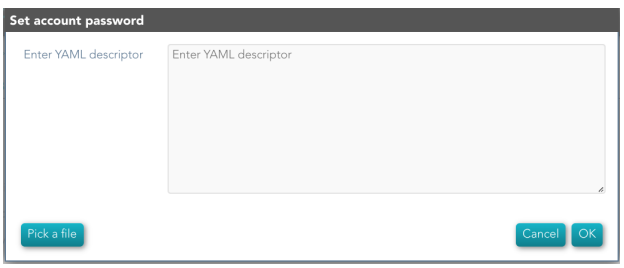
Account query actions

Query	Allows you to query accounts through different search systems, Quick, Basic and Advanced.
Add or remove columns	Allows you to show and hide columns in the table. You can also set the order in which the columns will be displayed. The selected columns and order will be saved for the next time Soffid displays the page to the user.
Add new	Allows you to add a new account in the system. You can choose that option on the hamburger icon or click the add button (+).To add a new account it will be mandatory to fill in the required fields

Delete	Allows you to remove one or more accounts 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.
Download CSV file	Allows you to download a CSV file with the basic information of all accounts.
Bulk actions	Allows massive operations to be performed on all system accounts. With that operation, updates can be made to any of the account's parameters. First of all, you must select the records that you want to update, once you have selected them, you must choose the bulk action on the hamburger icon. For more information visit the Bulk action page.

Account detail actions

Apply changes	Allows you to save the data of a new account or to update the data of a specific account. To save the data it will be mandatory to fill in the required fields
Delete	Allow you to remove the account. You can choose that option on the hamburger icon To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.
Undo	Allows you to quit without applying any changes.

Set password	This option depends on the credential type selected. **Password**: • Allows you to set a new password to the account or a SSH key. • The password can be generated automatically, or you can set the password. • It will be mandatory the password complies with the Password policies defined for the domain. • If an account is unmanaged, the password will not be sent to the target system. **Image**  **SSH key**: • Allows you to generate a new key or enter an existing key. **Image**  **Kubernetes key**: • Allows you to add a YAML descriptor **Image** 

Show actual account properties	Display the account attributes at the target system. To perform that action, Soffid needs to connect with the target system and get the account attributes that will be shown.

Roles

Assign Role	Allows you to assign a new role to the account. You can choose that option on the hamburger menu or click the add button (+). Then you need to select a role from the role list. If it is necessary, the next step will be to set the scope. Then you need to check and fill in the membership properties. And finally, apply changes.
Revoke Role	Allows you to revoke one by one or to revoke some roles at the same time. To revoke some roles at the same time, you need to select the roles, and then click the button with the subtraction symbol (-). To revoke one role, you can click the role, and then Soffid will show a form with the details. Then you can click the delete button (trash icon). Soffid will ask you for confirmation to perform that action, you could confirm or cancel the operation.
Import	Allows you to upload a CSV file with the role list to assign permission. 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 load a specific attribute. And finally, you need to select the mappings for each column of the CSV file to import the data correctly and to click the Import button.
Download CSV file	Allows you to download a CSV file with all the information about account roles.

Revision #68
Created 24 March 2021 12:21:18
Updated 11 November 2024 07:29:08