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.

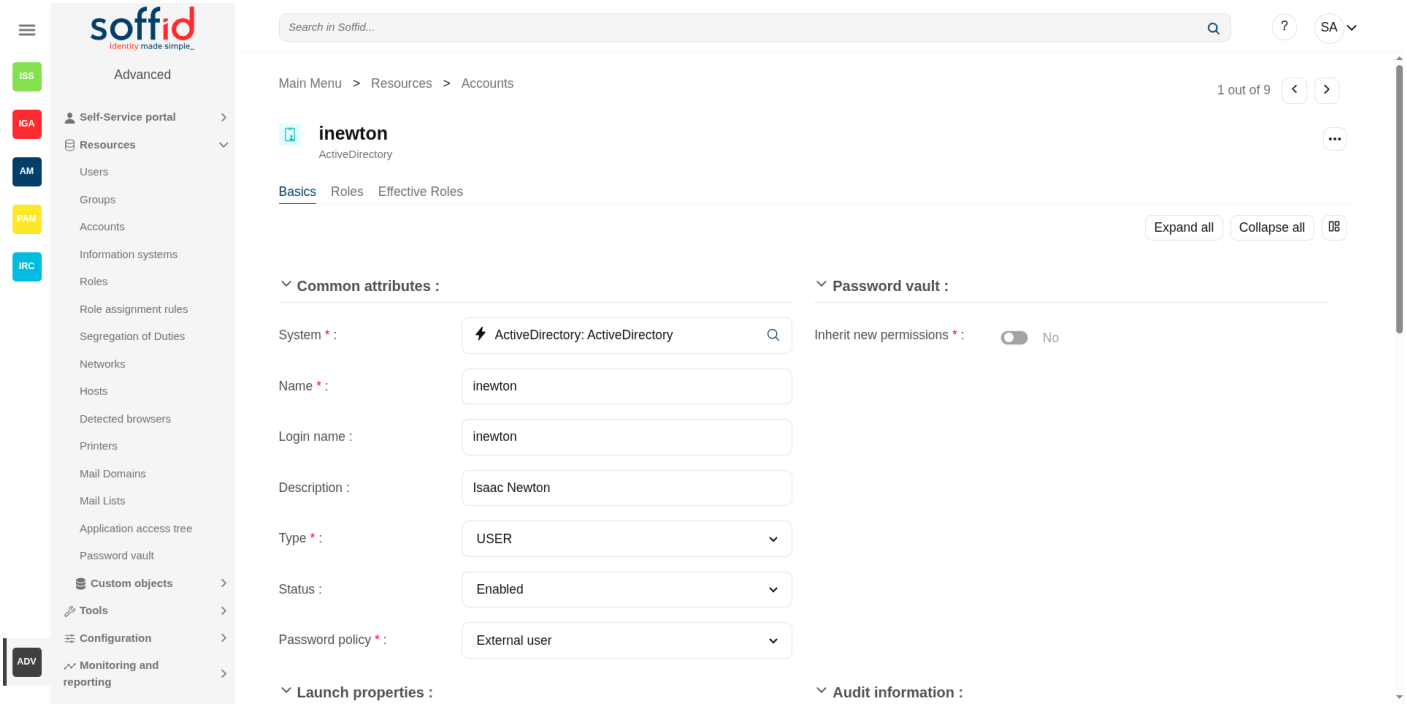
An account belongs to a system and that account can have specific permissions assigned to it. An account must have defined the account type, that is if the account is a single user, privileged, shared, or unmanaged.

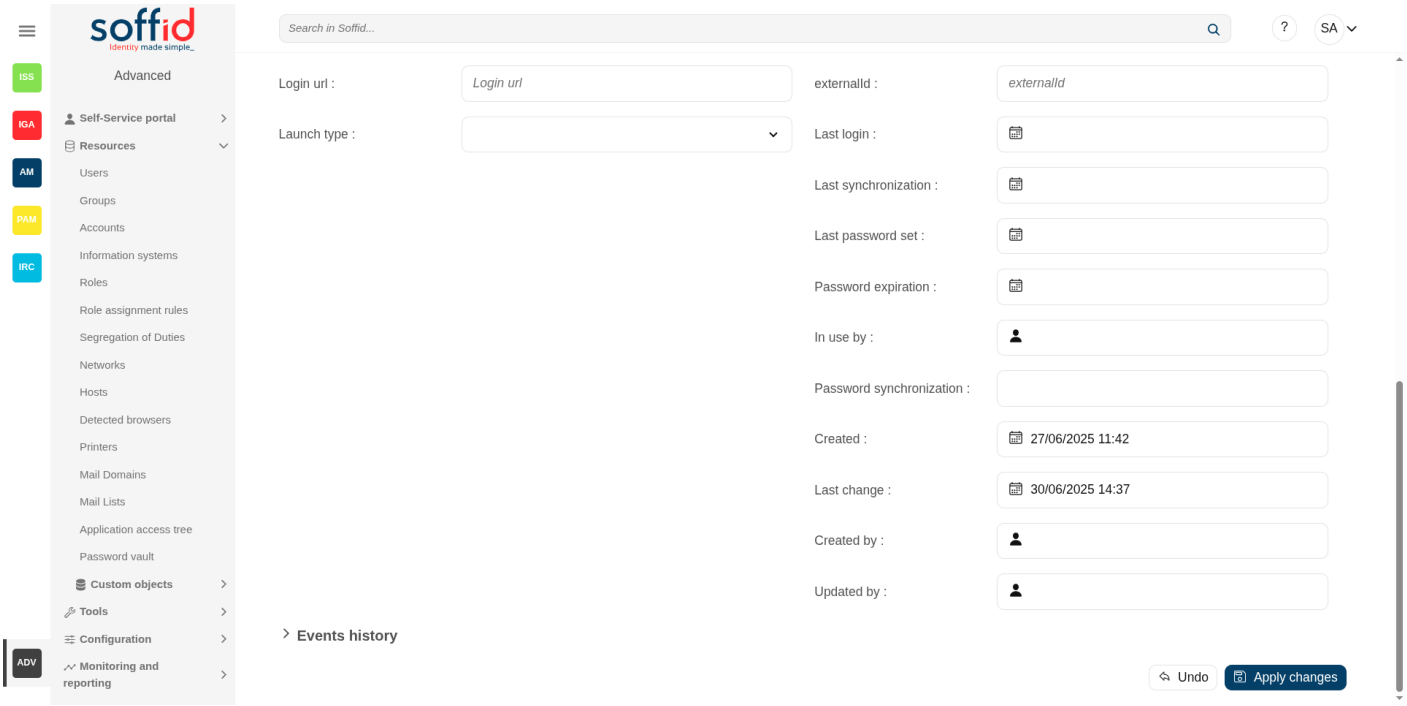
The password policy is also mandatory to create an account. That password policy determines the conditions that the password must meet.

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

- Users : owner users to the accounts
- Agents : the target system in which that account is used (AD, Exchange, etc).
- User type : user type of the onwer user or another one selected in the other account types
- Password policies : password policy of the onwer user or another one selected in the other account types

- 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.
- Information systems : where the roles are gathered
- Password vault : password vault information

Standard attributes

Basic

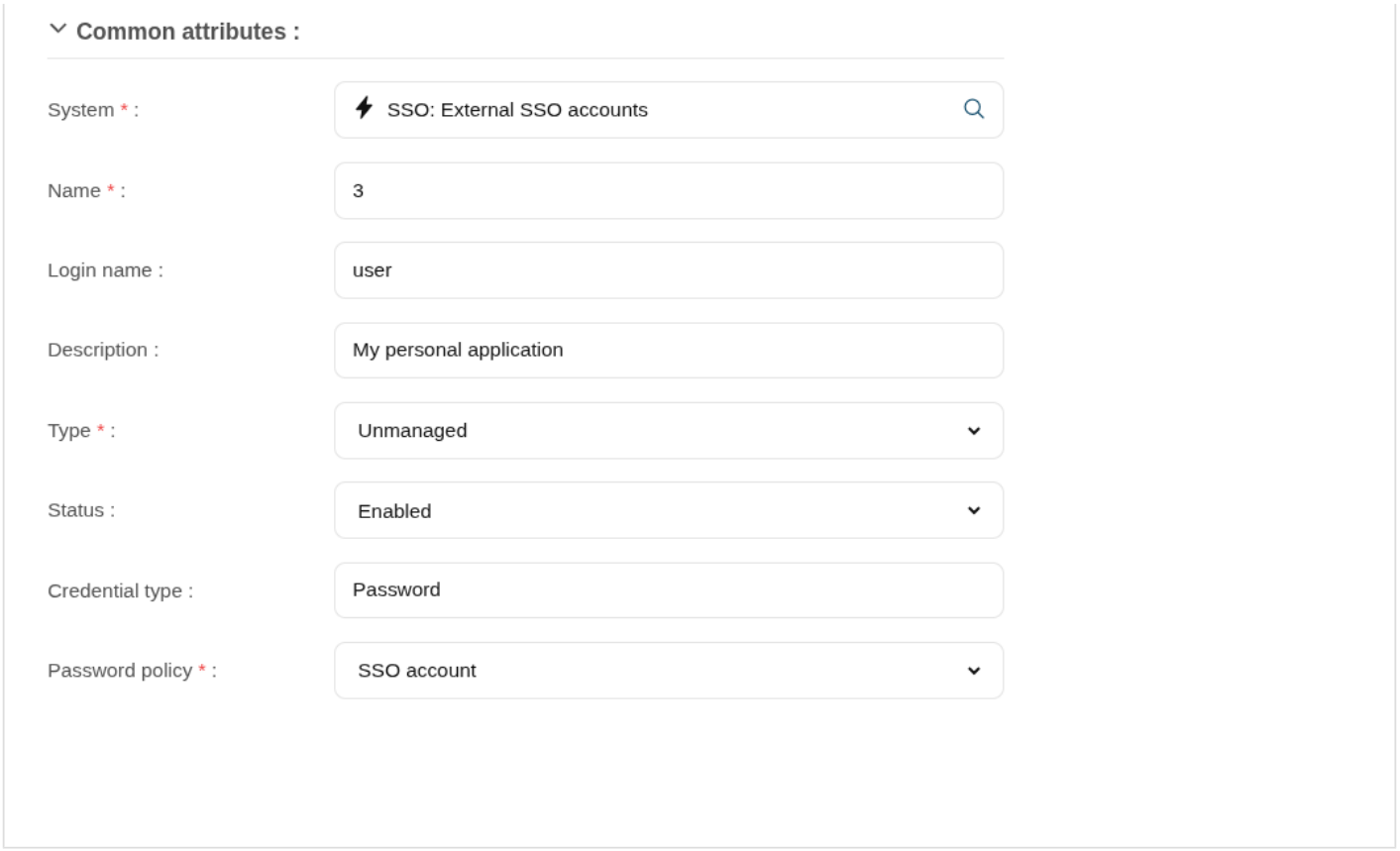
On the basic account tab, you can view all the account attributes. It is allowed to add new accounts, update or delete existing accounts and other options.

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.
- **Login name**: login name used in PAM navigations
- **Description**: plain text with information about the account.
- **Type**: there are four kinds of accounts:
  - **Single user**: these are accounts with a single use owner; we also refer to them as linked accounts. As these accounts are linked to a user, they are part of the user's lifecycle; when the user is modified, the account can also be updated and synchronised, and if the user is desabled, so too is the account. We can also view these accounts on the users page, under the accounts tab; all of them are single user accounts.
  - **Shared**: these are accounts that may be associated with no users or with multiple users. Unlike single user accounts, these are not part of a user's lifecycle and are not linked to them. They have an access control list to prevent unauthorised use. These accounts may also be referred to as service accounts and may have their own roles assigned to them. These accounts have their own password; even if they are associated with a user, password management is handled separately.
  - **Privileged**: these are typically administrator accounts, specific to a particular system and with no associated users by default. Users who need to use these accounts can do it via the Identity Self-Service module; when they log in with this account, a specific password is set, and when the session ends, it is randomised to prevent unauthorised use. Consequently, a privileged account is usually used by only one user at a time. These accounts are usually associated with the PAM module and may require additional steps, such as requesting access via a workflow or adding an authentication factor

    - **Unmanaged**: these are accounts that Soffid does not manage; if changes are made to them, these changes are not synchronised with the end system. Although they can be created manually, these accounts are usually created in Soffid when performing a reconciliation with an end system. This status exists as a preliminary step before deciding what to do with them: either link them to users and convert them to single user accounts, or change them to shared or privileged accounts. Unmanaged accounts in Soffid that exist in an end system represent a potential risk; they must be monitored or permanently deleted.
- **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.
    - **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).
    - **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.
    - **Archived**: same status as "Removed" but useful if you need to differentiate it for a business process
- **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.
- **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



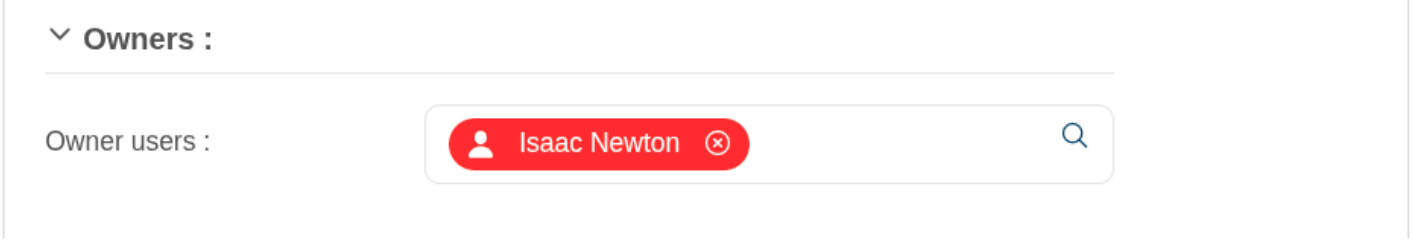
Owners, Managers, and SSO users

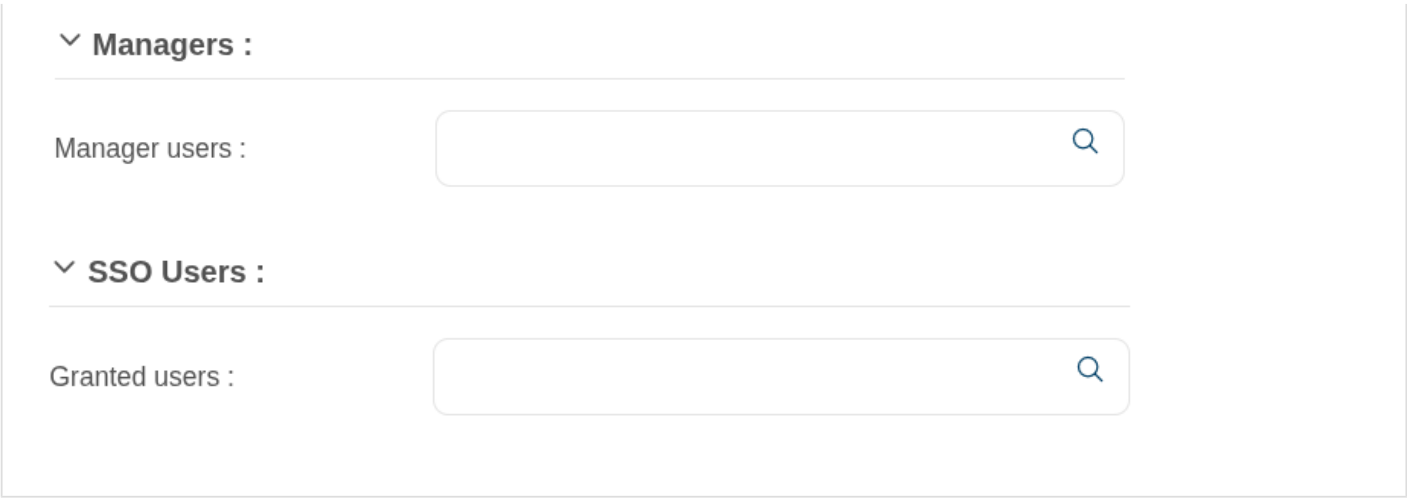
Specify the list of users authorized to use this account. For accounts of type "single user", only one user can be specified. Other accounts can have more than one user. The users that can use this account can be specified either directly, by entering the user name, or indirectly, by entering a group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

- **Owner**: can use it, modify the access control list, and set or query the password sing self-service portal or single sign-on engine.
- **Manager**: can use it, and set or query the password (using self-service portal), depending on the password policy restriction.
- **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.

Image

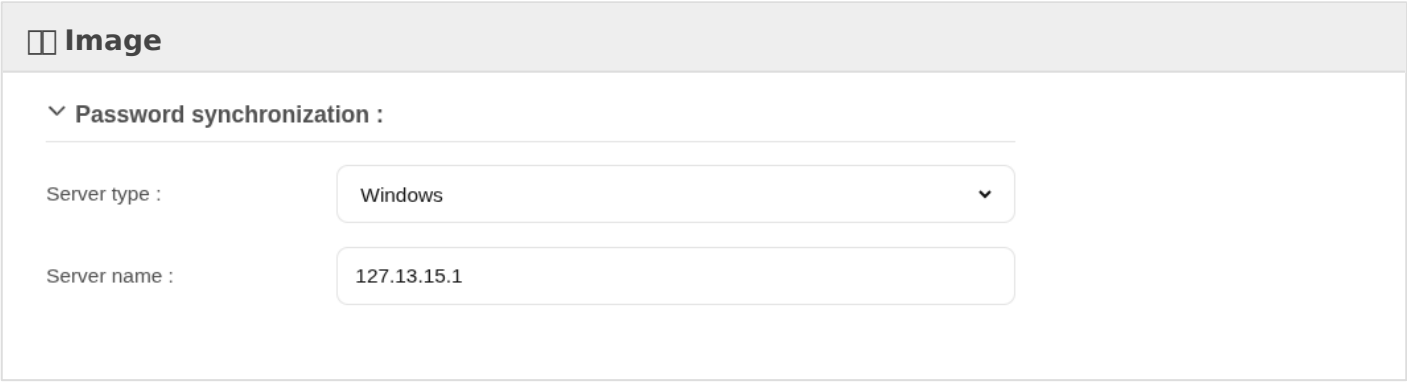




Password synchronization

- **Server type**: type of the server.
  - Linux
  - Windows
  - Database
- **Server name**: descriptive name of the server
- **SSH Public key**: SSH key for linux servers

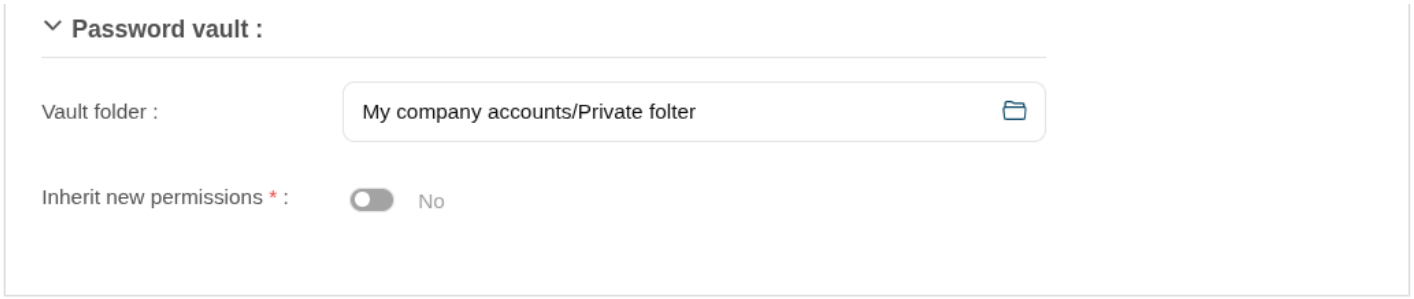
Image



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.

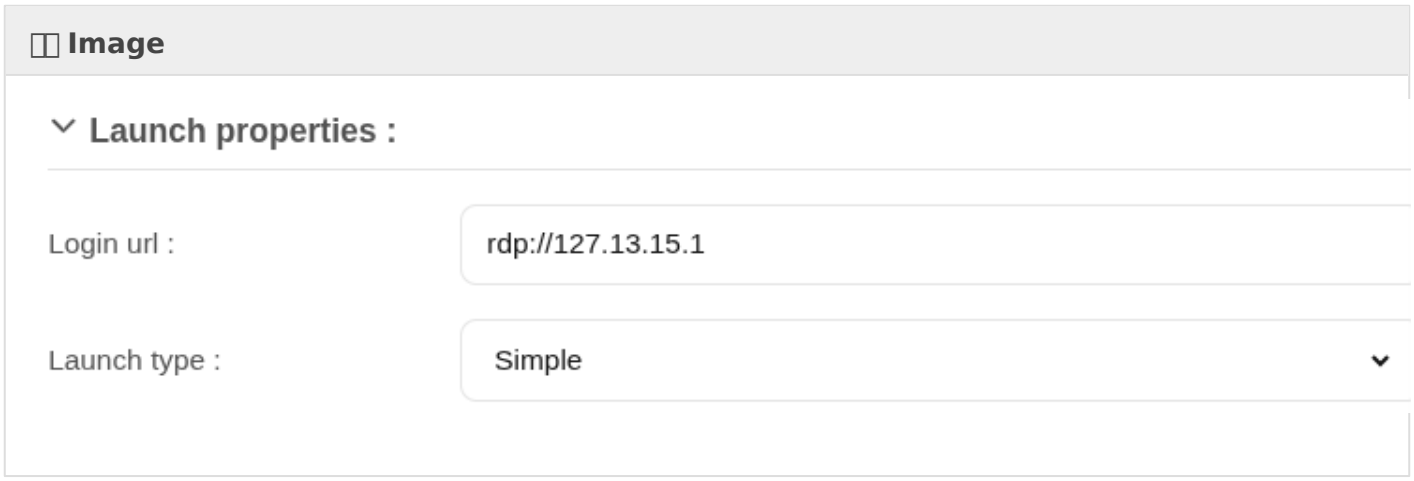
Image



Launch properties

Defines the properties to connect to the target system.

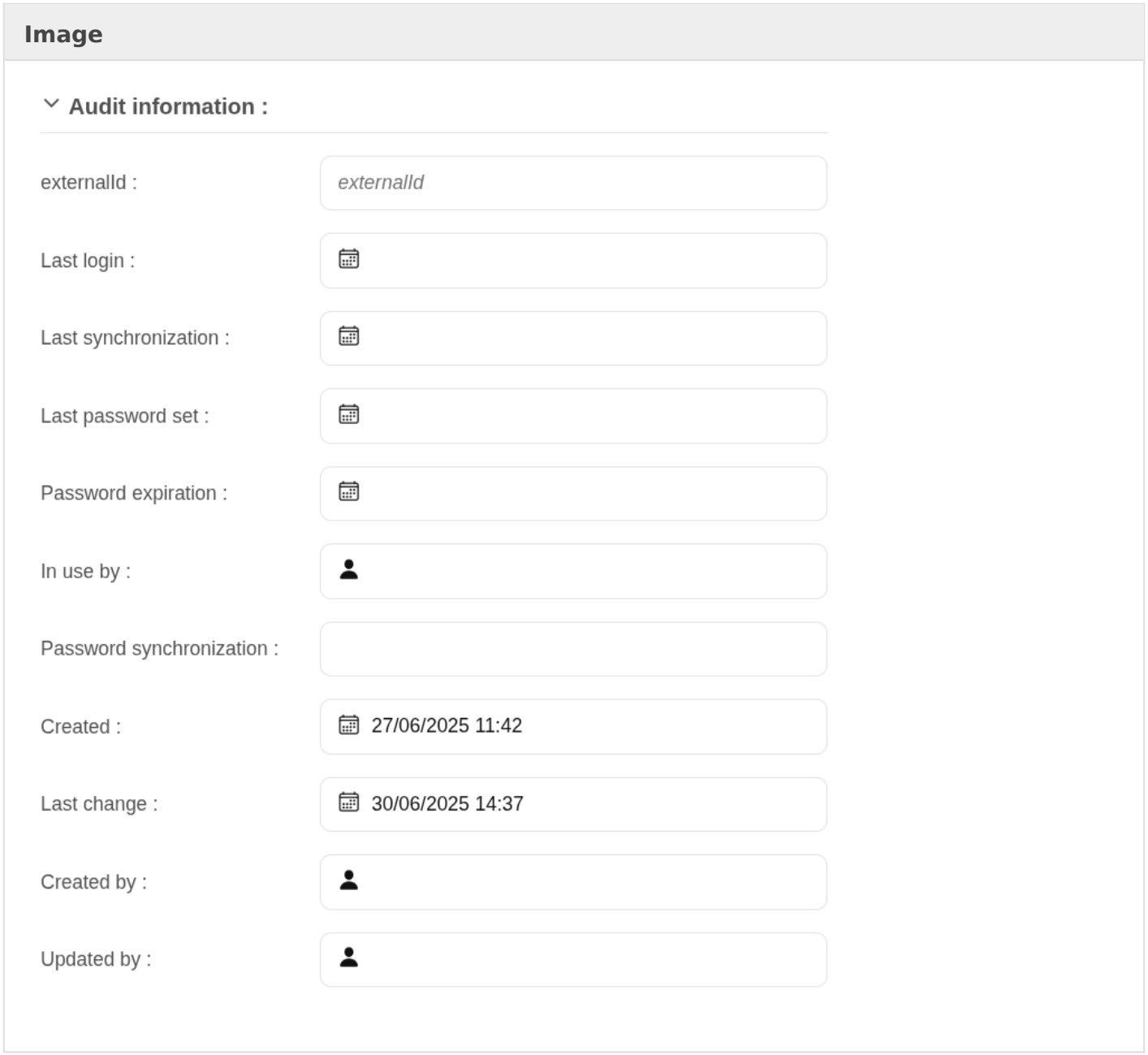
- **Login URL**: URL to connect. You can add the port when you need it
- **Launch type**: connection type.
  - **Simple**
  - **WebSSO**
  - **PAM Jump server**: it is mandatory to select the Jump server group.



Audit information

- **ExternalId**: new attribute in Soffid 4 to keep a record of the unique identifier of the object in the final system (useful for synchronisation and renaming).
- **Last login**: last registered access.
- **Last synchronization**: last registered synchronization.
- **Last password set**: date of last password change.
- **Password expiration**: password expiry date.
- **In use by**: account owner
- **Password synchronization**: password synchronization date.
- **Created**: account creation date.
- **Last change**: last modified.
- **Created by**: user who created the account
- **Updated by**: last user who updated the account

Image



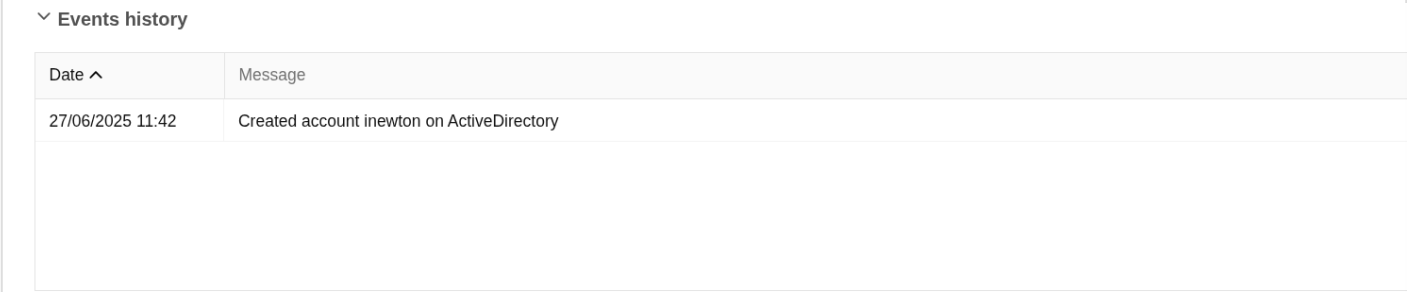
System properties

- **From data**: to add parameters
- **Type:** possible values:
  - Windows
  - Linux
  - Database
- **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.
- **Password synchronization**: possible values:
  - Valid
  - Expired
  - Invalid

Events history

List of events on this account

Image



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

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

The roles are 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 new" button, 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 "Delete role" button.

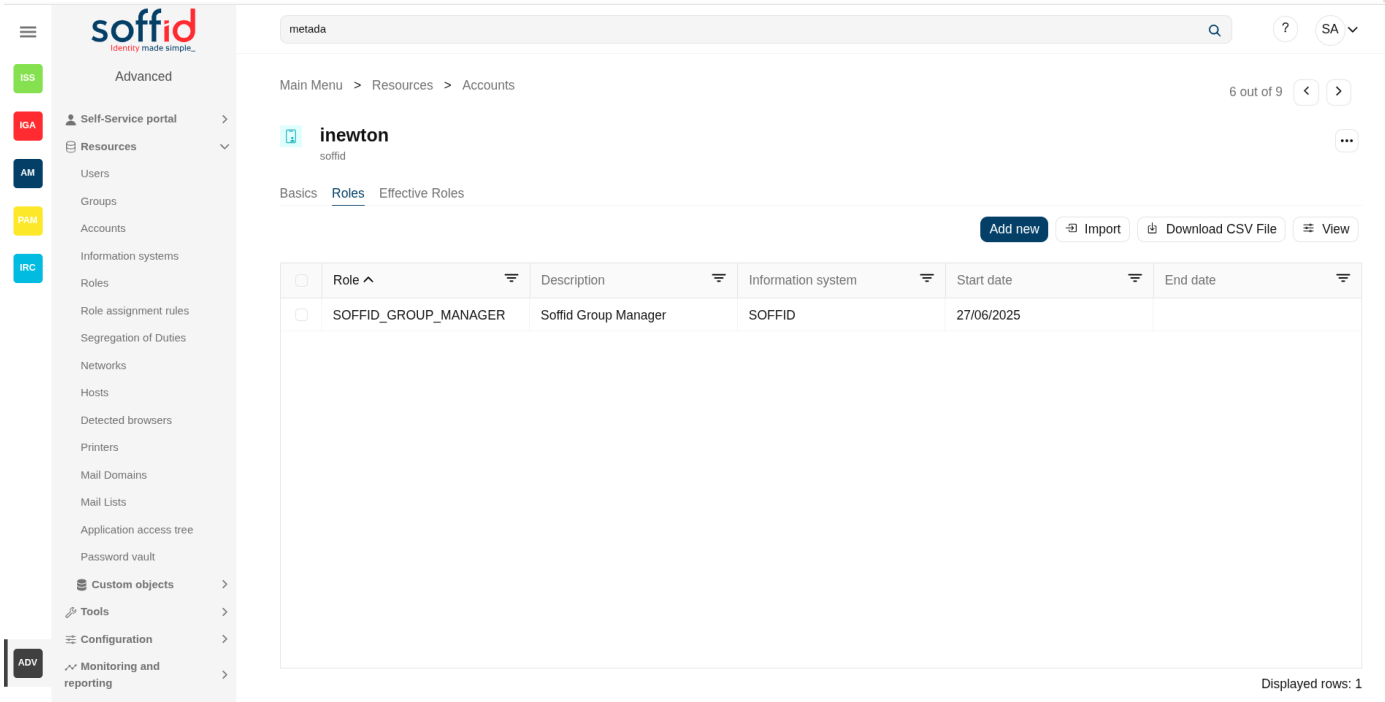
By clicking on a record, it is shown the detail role assignment information.

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

The attributes:

- **Role**: name used to identify the role.
- **Description**: detailed role description.
- **Information system**: asset or application, from a functional point of view, on which the permissions are granted or revoked.
- **Start date**: at this date, Soffid will connect to the system and will assign the role. If there is no approval start, it will be assigned at the moment.
- **End date**: at this date, Soffid will connect to the system and will revoke the role.
- **Risk**: risk related with SoD rules
- **Category**: category value of the role
- **Domain value**: you can set a limitation of the role scope by selecting the domain. Initially, there are two domains defined, Groups and Information Systems. Soffid allows you to add more domains.
- **Domain description**: domian description

Image



Effective roles

Hierarchy of permissions assigned to or inherited.

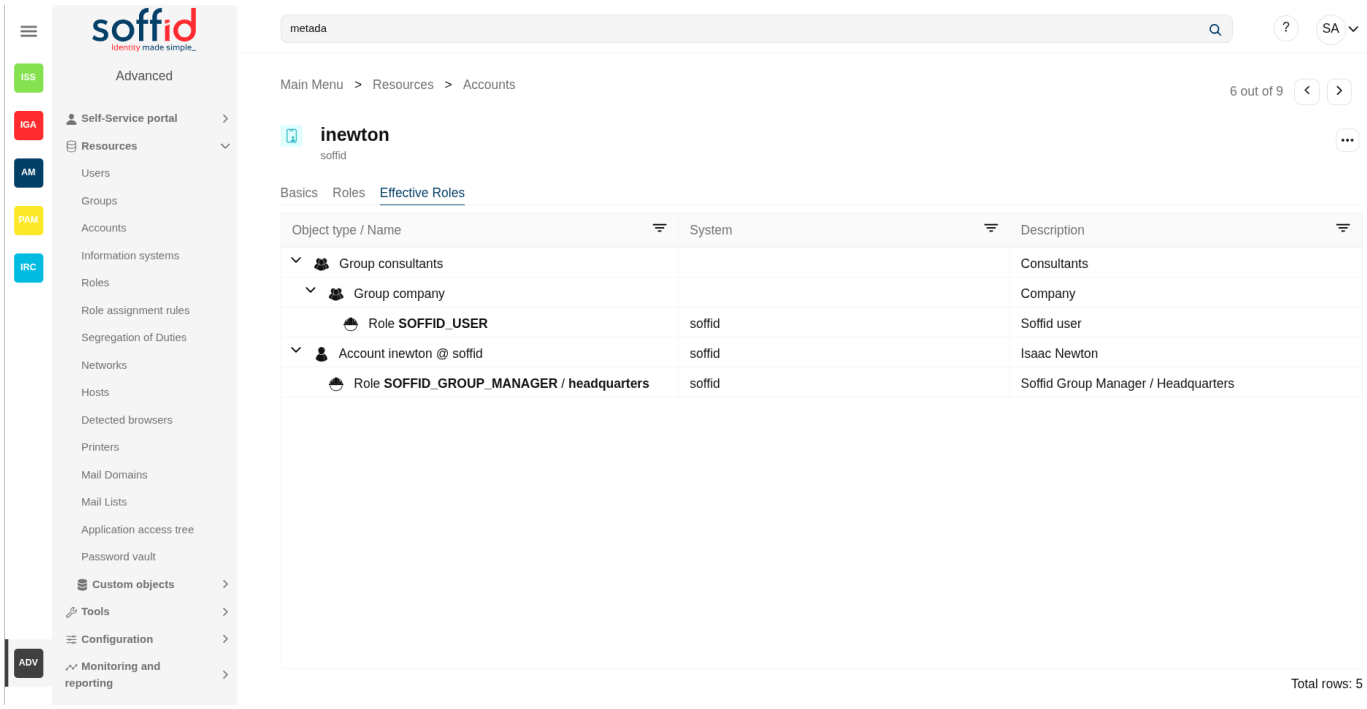
This screen details the effective roles for the selected account.

- 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.

The attributes:

- **Object type / name**: object type owner of the role / name used to identify the role.
- **System**: target system owner of the role.
- **Description**: detailed role description.

Image



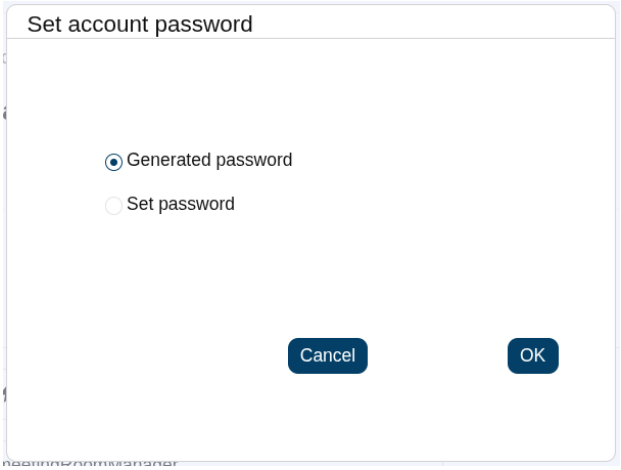
Actions

Account query actions

"Query buttons"	Allows you to query accounts through different search systems, Quick, Basic and Advanced.
"Table filter"	It allows you to filter a column in the table based on the results loaded in it.
Add new	Allows you to add a new account in the system. 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 this button. 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.
View	Allows you to add or remove columns to the table. It is also possible to change the order of the columns.

Account detail actions

Apply changes (dick button)	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. **Kubernetes key**: • Allows you to add a YAML descriptor
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.
Expand all	Displays all the attributes of the different blocks.
Collapse all	Hide all attributes of the different blocks.
"Types of views"	Change the view type: Classic view, Modern view, Compact design.

Roles

Add new	Allows you to assign a new role to the account. 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.
Delete	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 clicking this button. 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.
View	Allows you to add or remove columns to the table. It is also possible to change the order of the columns.

Revision #11
Created 26 June 2025 13:26:04 by Sion Vives
Updated 13 March 2026 15:28:59 by Sion Vives