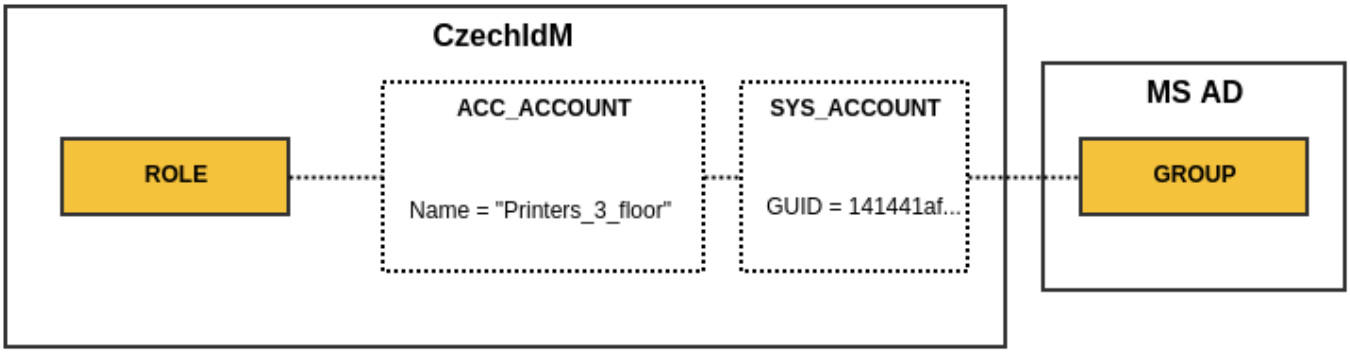
Accounts - working with objects on connected systems

Types of Accounts

Accounts are entities in CzechIdM that link the data in CzechIdM (Role, Identity, etc.) with the data in a connected system such as Group and User Accounts. In fact, there are 2 types of accounts:

- **AccAccount** - Stores ID of an entity in CzechIdM that is linked to a connected system Object.
- **SysAccount** - Stores ID of a connector object (representation of a real connected system Object).

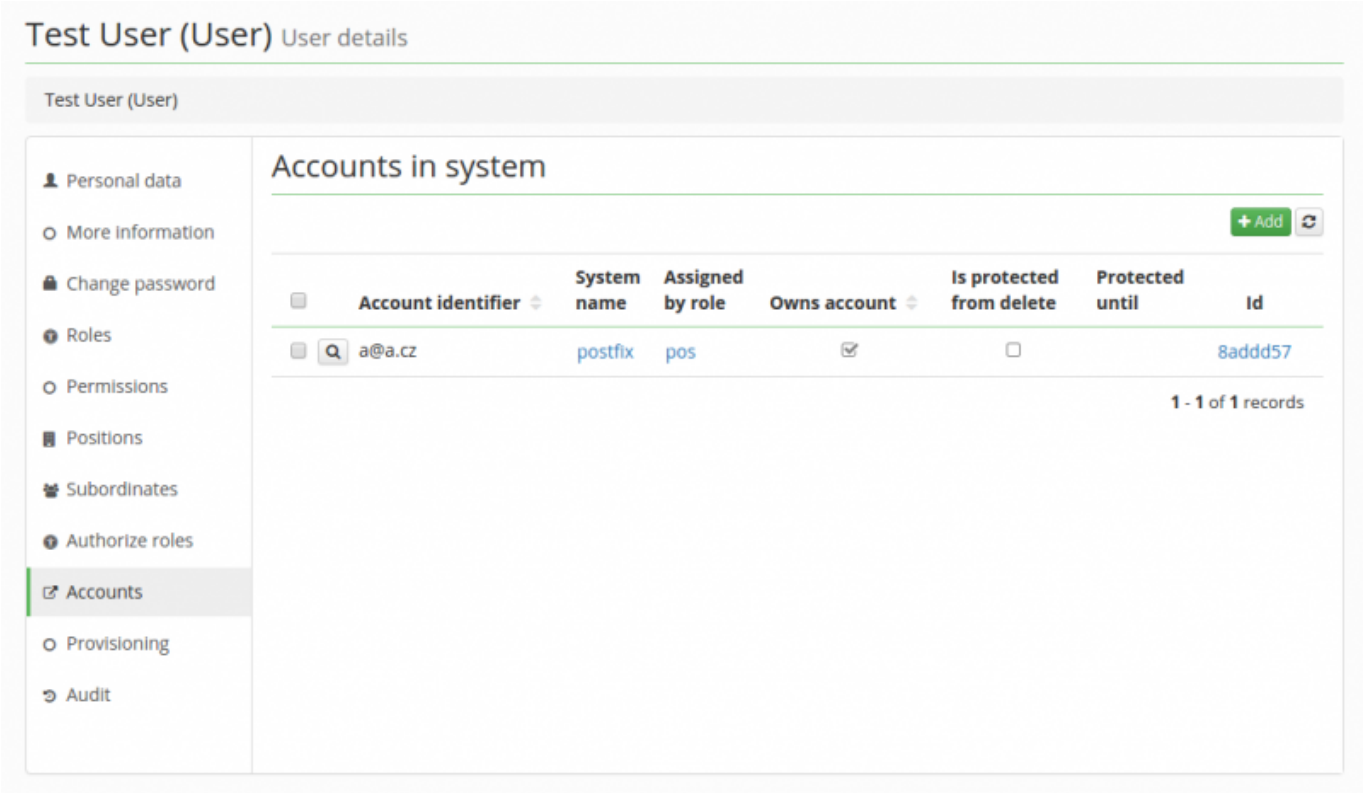
Provided we have a MS Active directory connected to CzechIdM, SysAccount might store a GUID of GROUP. AccAccount can store a role name.



SysAccount IDs are returned by a connector. So it depends on the connector we have chosen for connecting a system. Some connectors allow choosing an ID attribute, some do not. AccAccount IDs are chosen in CzechIdM Provisioning and Synchronization configuration for the connected system.

Listing Accounts for Identity, Role and TreeNode

On a user detail tab panel, there is a tab called **Accounts** as you can see in the screenshot below. When you access this page, it will show all accounts on a connected system that CzechIdM has in its evidence.



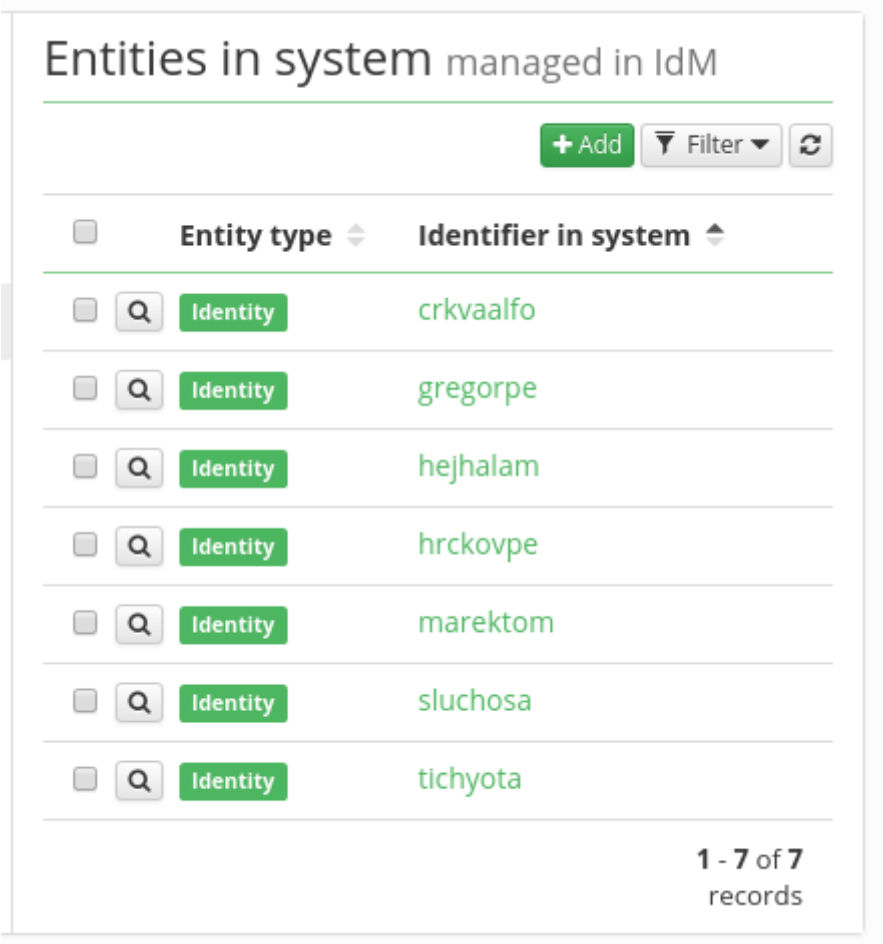
The same principle applies to the rest of the entities that the Account management supports. An identity account is specific in several ways:

- Supports the so called protected state of accounts
- Can be assigned by a role.
- Can be manually linked to objects in a connected system.

Linking object to CzechIdM entity manually

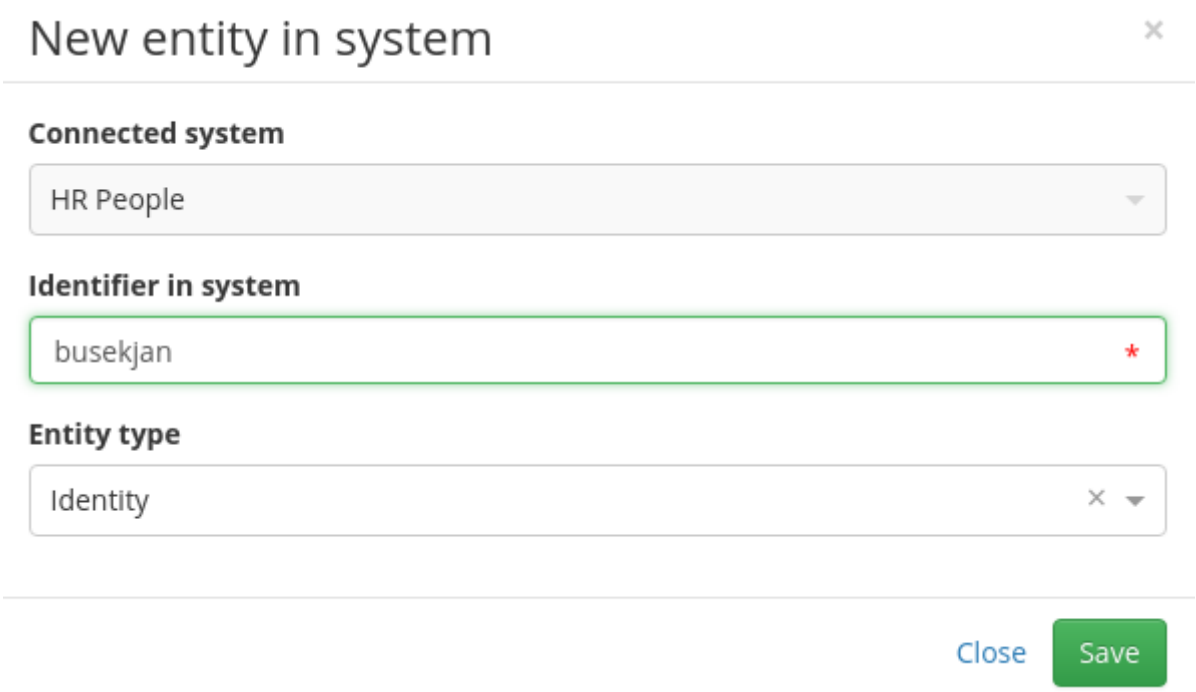
Usually, linking objects to CzechIdM entities takes place during a data Synchronization or Provisioning when the CzechIdM system is deployed in the production environment. But it is a common situation that some data have to be corrected in an end system as well, e.g. LDAP. It may well be that the algorithm for object linking during synchronization does not work for all entities on the end system, or the individuals who entered some data manually before CzechIdM had been implemented may have made some mistakes. In either one of those cases, having the option in CzechIdM to link an object to an entity manually comes in handy.

To do so, open the detail of the system on which you want to link an identity to some object: **Systems → System detail**. Next, the first thing to do is to create a SysAccount and define its ID. In the example below, a manually created identity is being connected to its mirrored object in the HR system. Go to the **Entities** tab, there is a list of all entities on the system, that CzechIdM knows of.

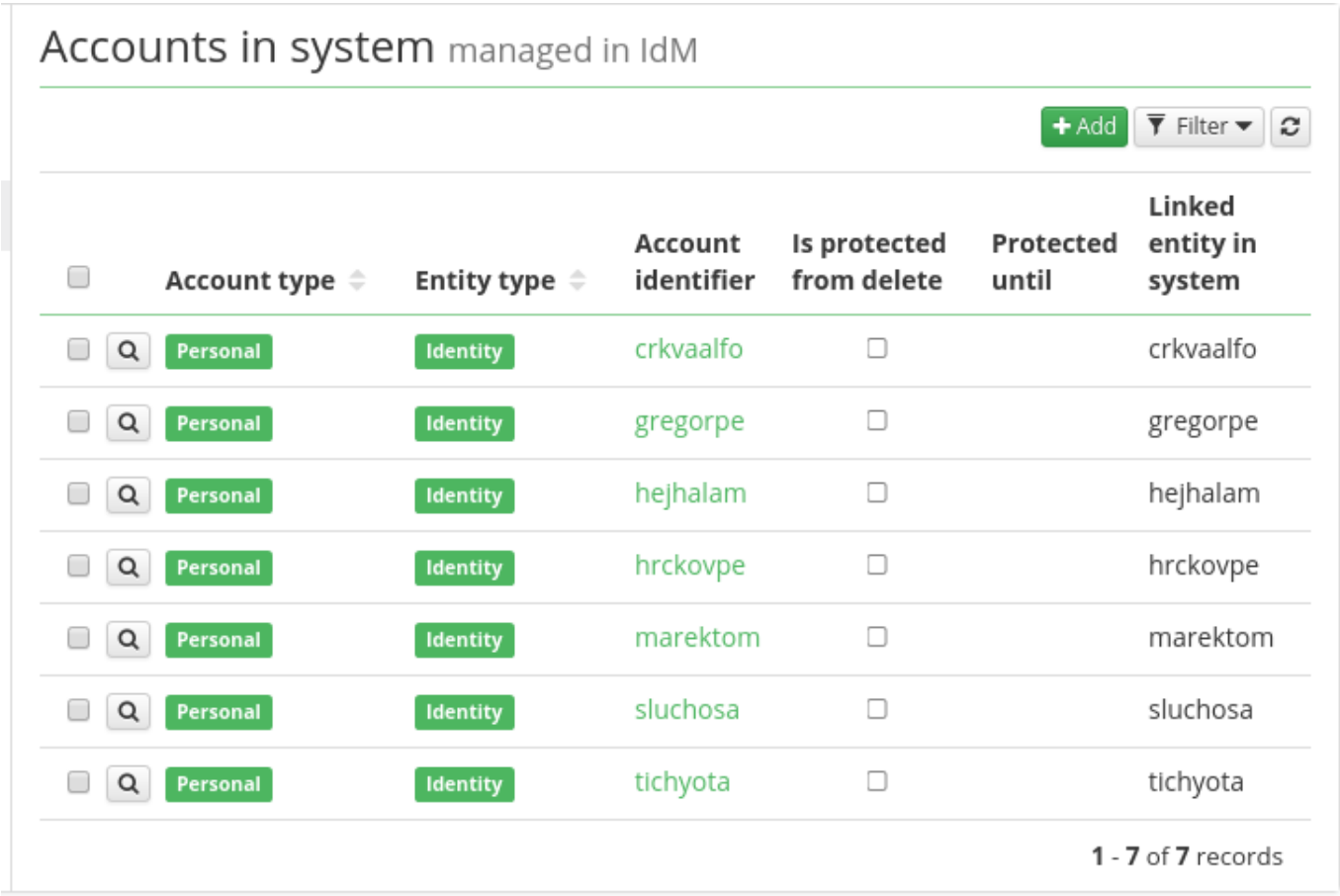


In the next step, we create a new system Entity (make sure the entity with the desired identifier is not yet present in the table):

- Connected system - Read-only
- Identifier in the system - here, the ID (e.g. login) of the object on the end system is to be typed in.
- Entity type - Type of entity in CzechdIdM



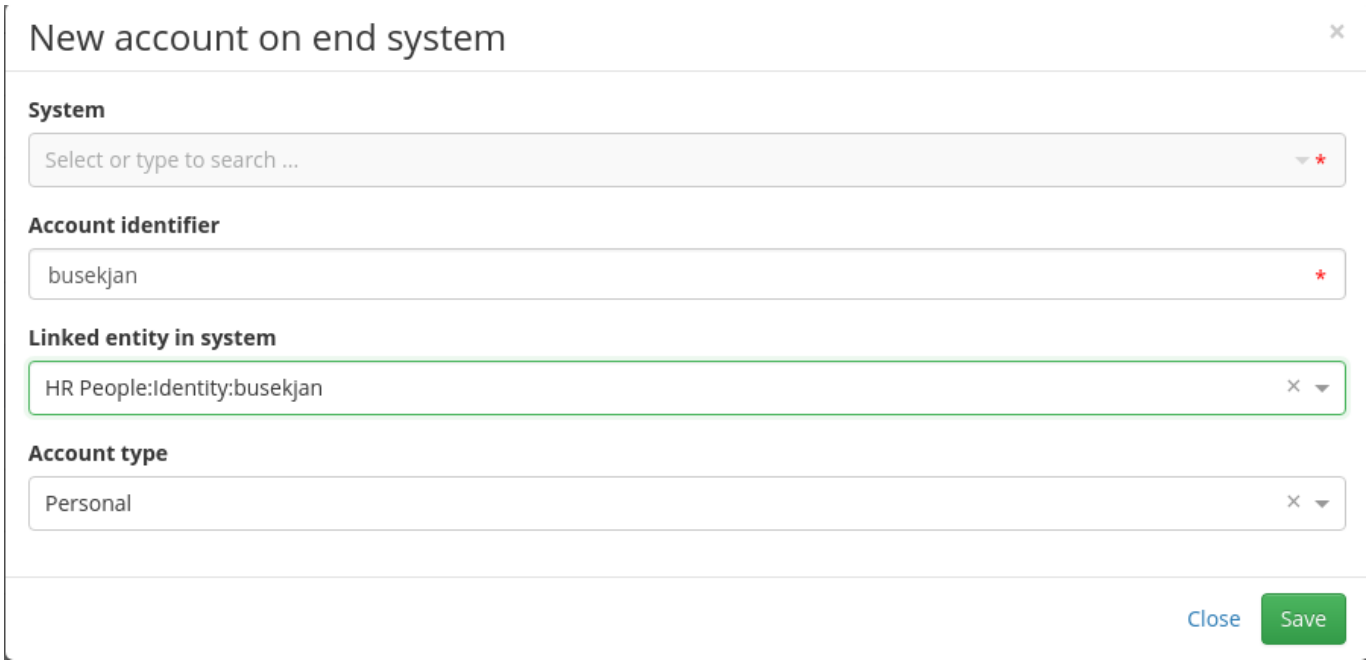
Once a system entity is created, we proceed to create an AccAccount. Go to the tab **Accounts** and click on the Add button.



An AccAccount has the following options:

- **System** - Read only - name of the system for which we want to create an AccAcount
- **Account identifier** - ID of the CzechIdM entity (e.g. login or employee number)
- **Linked entity in system** - the linked SysAccount

- **Account type** - usually personal (only a descriptive attribute now)



Fix Me! To link the account to the entity in IdM (typically an identity), an additional step is needed - add a link to the account (for source systems), or assign some role to the identity (for managed systems).

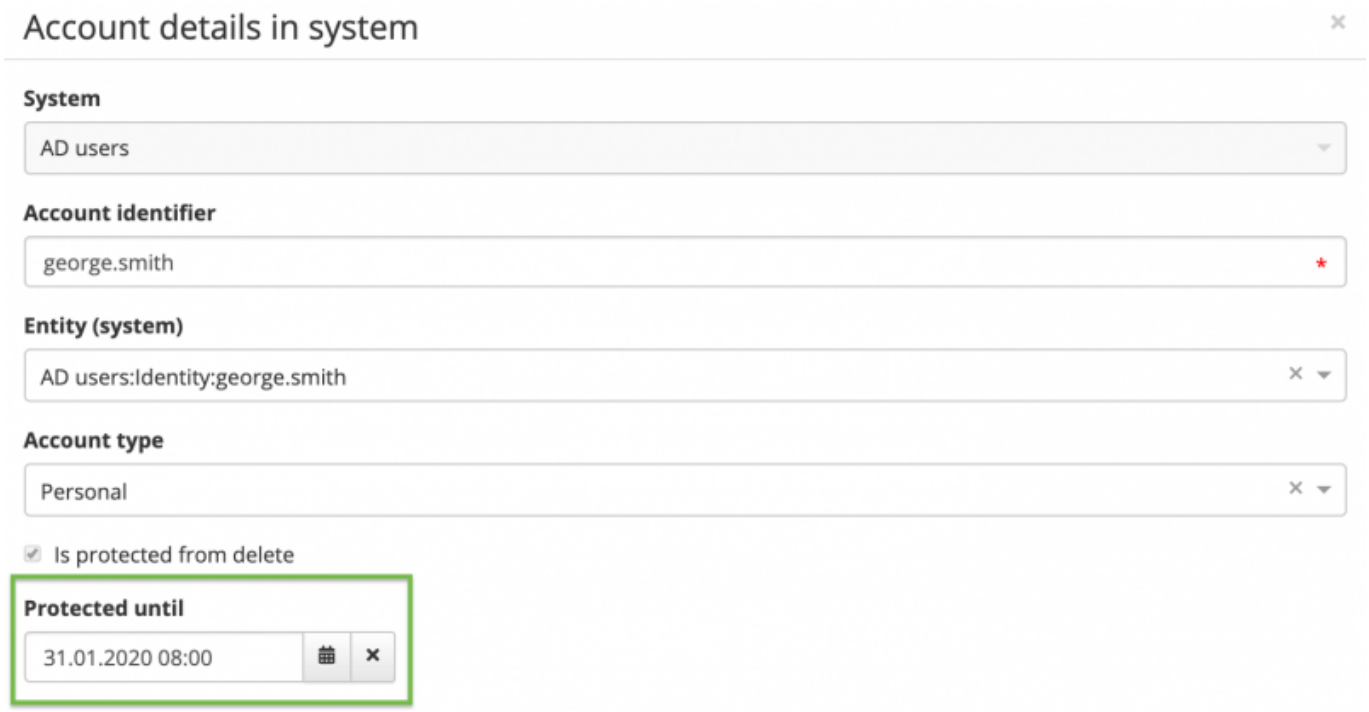
Manually delete accounts on system with account protection

If you need to immediately remove account on connected system, where account protection is on, or if you want to force delete user with all accounts:

1) Go to user contracts a set it's validity to past.

This will remove **all accounts** of the user. If you want to remove only one selected account of the user from some system (e.g. AD), then remove all roles that are assigned to the user for this system (e.g. all AD groups and the main AD role) instead of inactivating the whole contract of the user.

2) Go to user profile → Accounts, and there you will see account in protection, so edit account and set protection validity to past



3) Go to Settings → Task scheduler → Scheduled task and run AccountProtectionExpirationTaskExecutor

- The account on system will be deleted when the task is over.

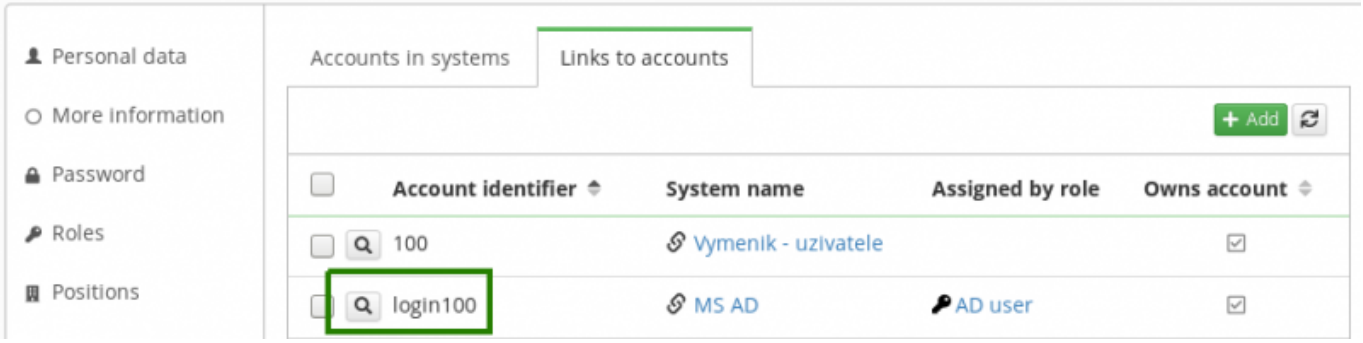
Manually unlink account from the identity and IdM without deleting it

Starting with IdM 13.0, you can you the bulk action Stop managing accounts. Learn more

You can use this tutorial e.g. in the following situations:

- an account is linked to a wrong identity, so you want to unlink it (so it can be managed by IdM without any specific identity owner, or linked to some different identity)
- an account is linked to an identity, but you don't want to manage this account by IdM at all. At the same time, you don't want to delete it from the connected system (e.g. some technical account on MS AD)

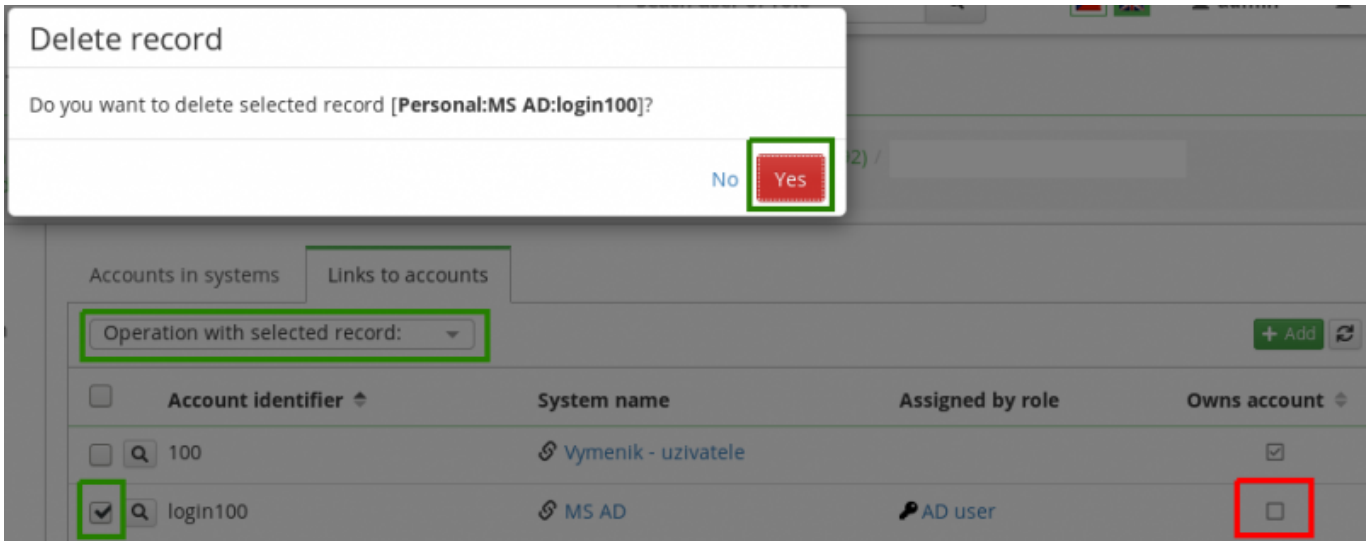
1) Go to user profile → Accounts → Links to accounts. Select the account that you want to unlink and click on the magnifying glass.



2) Uncheck the checkbox "Owns account" and click "Save".

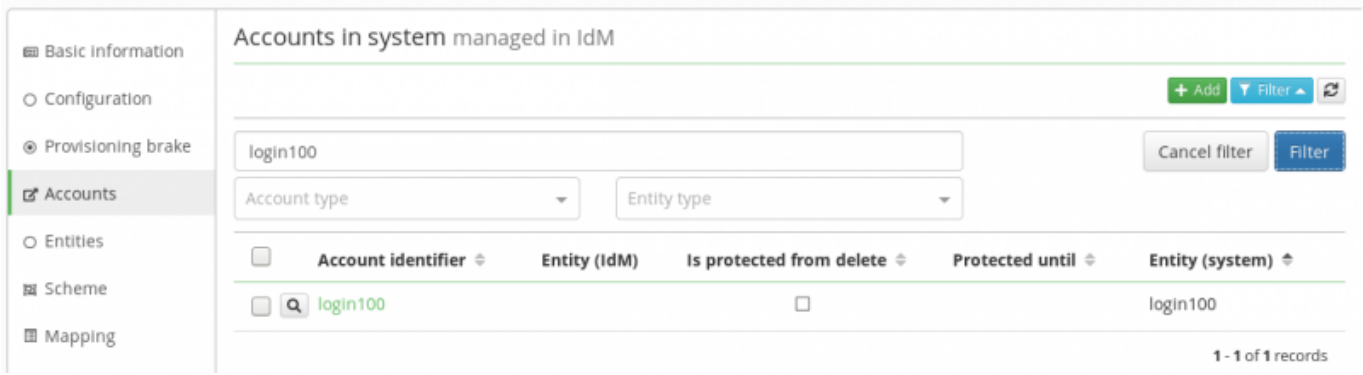
3) Remove the link to the account from the identity.

Before that, make sure that the checkbox "Owns account" is really not checked (you did this in the previous step). Otherwise this action would delete the object from the connected system.

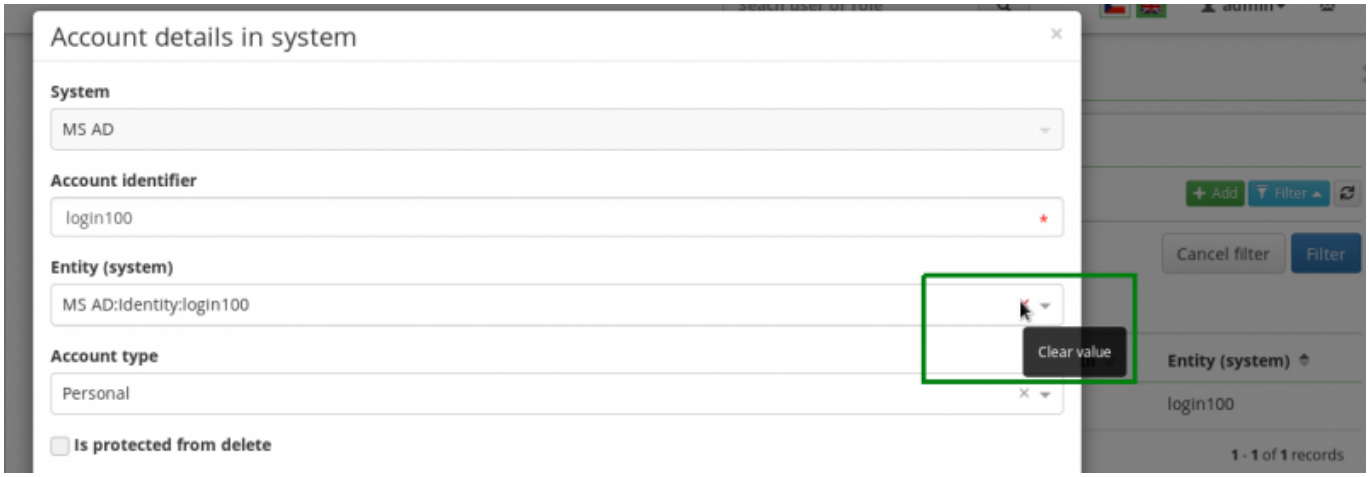


STOP here, if you still want to manage this account by IdM. This depends on the type of the account. Usually, it's recommended to manage accounts of all common users by IdM. Depending on your IdM implementation strategy, technical, privileged or testing accounts may not be in the scope of IdM. If you don't want to manage the account by IdM, continue with the next step.

4) List accounts managed in IdM on the connected system (Systems → e.g. MS AD → Accounts) and filter the account by its identifier.

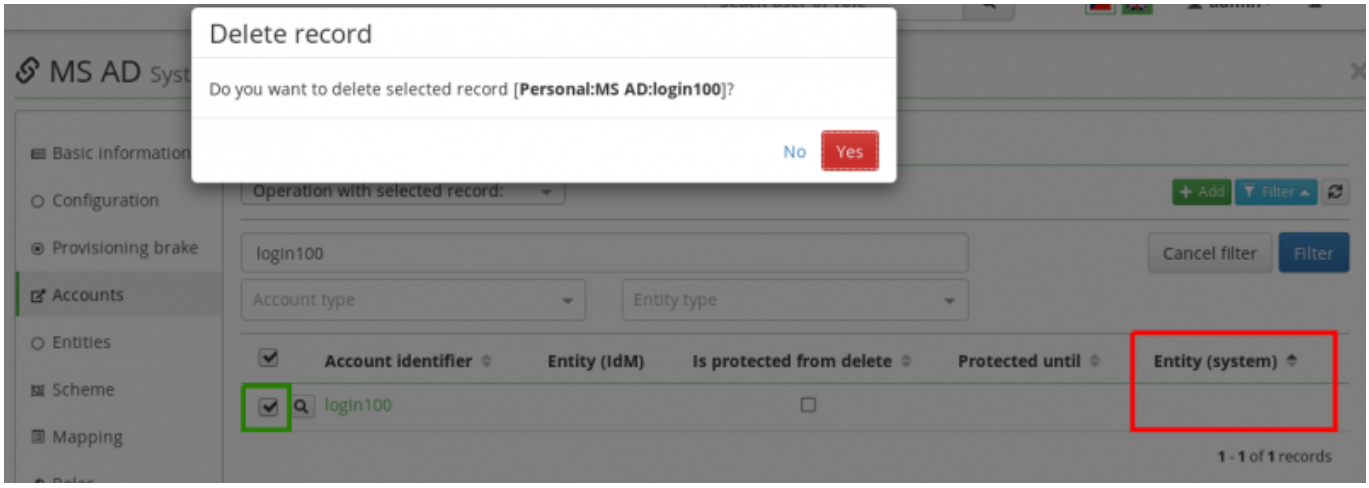


5) Remove the link to the system account - open the account and clear the value in the select box for Entity (system). Then scroll down and click "Save".



6) Remove the account object from IdM.

Before that, make sure that the value in "Entity (system)" is really empty (you did this in the previous step). Otherwise, this action would delete the object from the connected system.

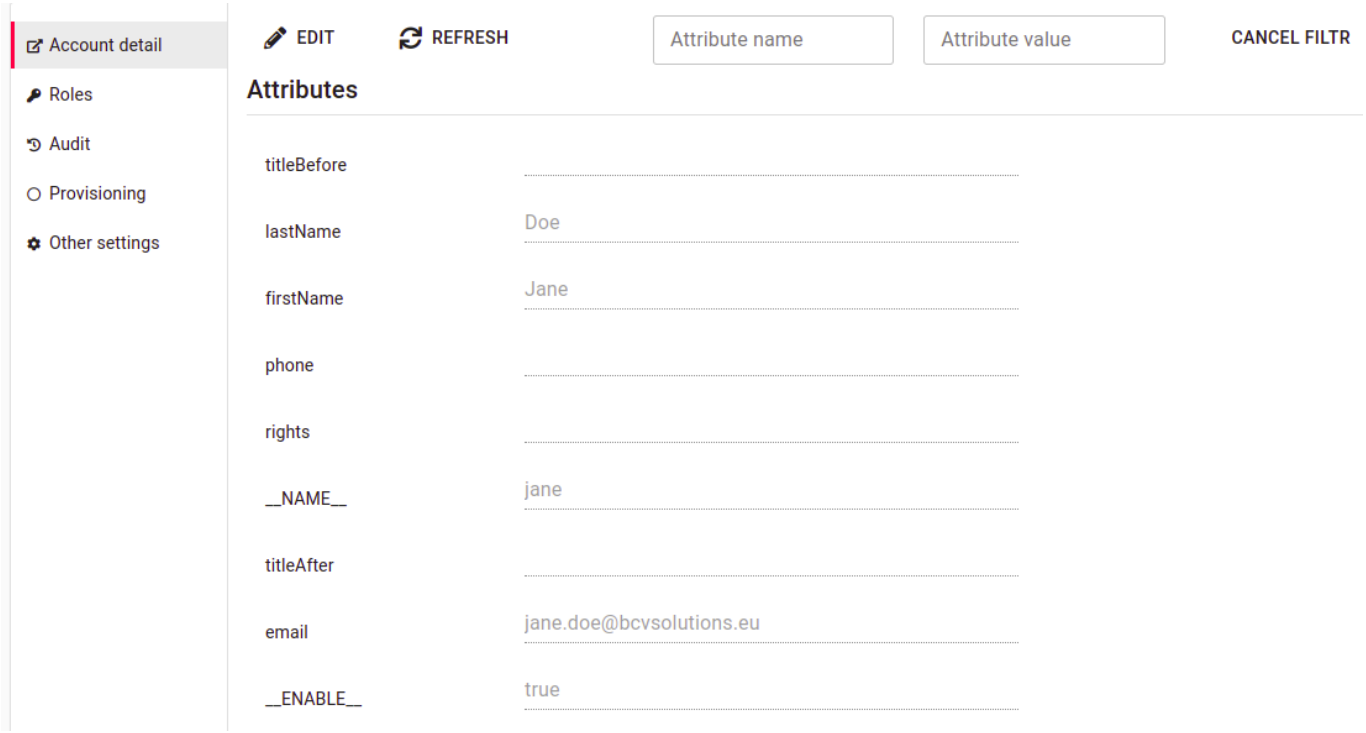


Finally, you can make sure that the object still exists on the connected system. You can find it on the tab **Entities** of the connected system and open its detail. You could delete this entity ("SysAccount") from this tab, it will make no change on the real connected system. But you usually don't have any reason to do this, because the object really exists on the system and the Entities are mostly an evidence about really existing objects on the connected system.

Manually change the value of an attribute for an account

This feature was introduced in IdM 13.0.

Once you open an account (either from the account agenda or from the detail of its owner, you can manually manage values of attributes for a specific account.

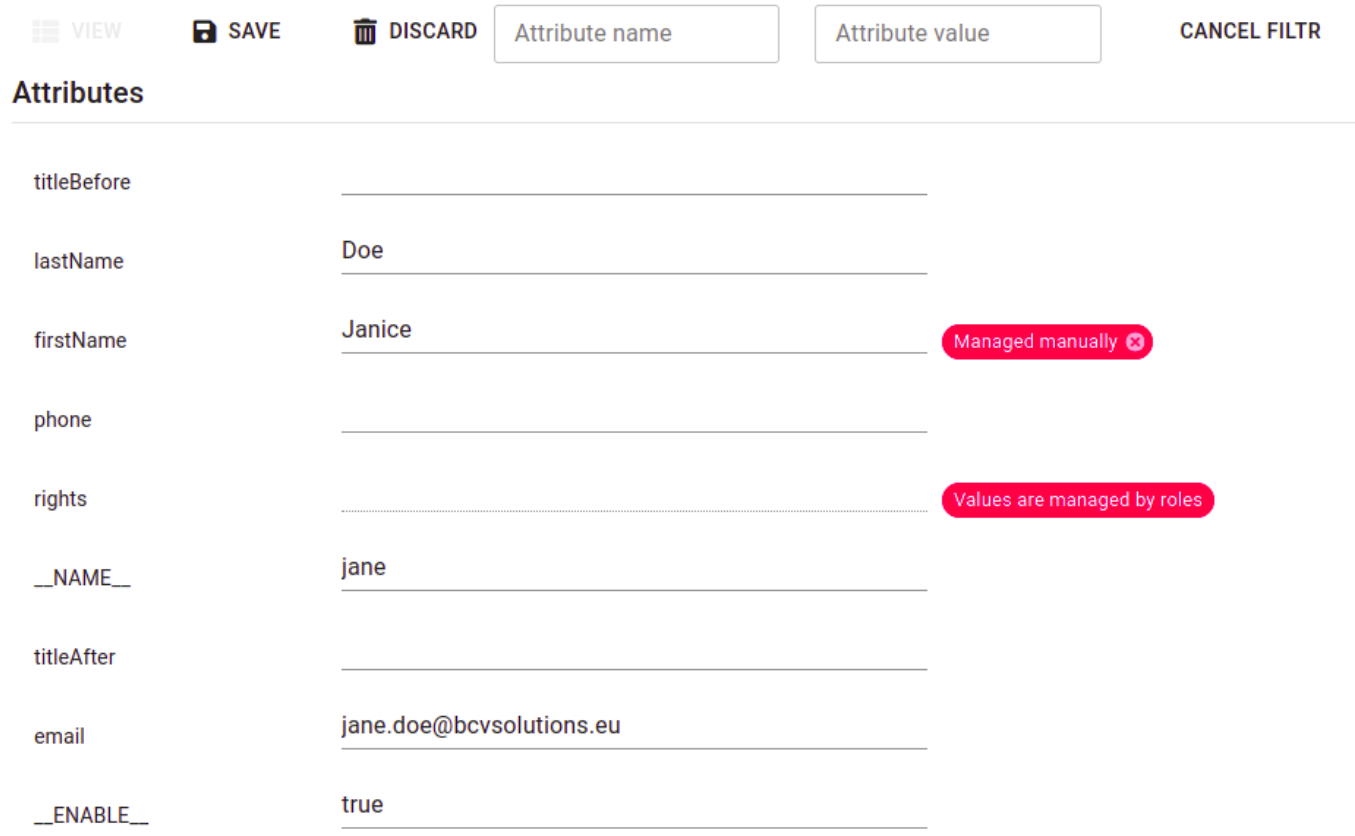


Once you start managing the value of an attribute, the value will be sent to the system directly. There is no way to modify it with a script. Standard mapping configuration will not be used.

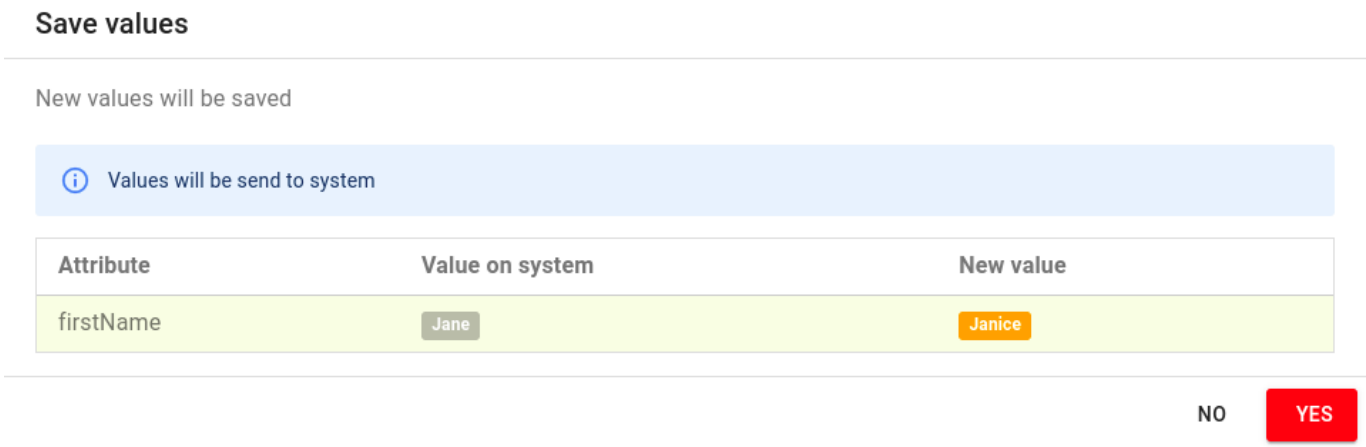
You can modify even values for attributes which are not present in a mapping. You will be able to see and modify all attribute values from the schema.

Currently, this is not supported for virtual systems. You can manually change only the values which are present in the mapping of the system.

To edit the value of an attribute, click Edit, change the value. You will notice that the value will now show that it is manually managed.



Then, click the Save button. You will be presented with a differential view of the modified attribute values.



Confirm it and the value will be provisioned to the system.

Admin tutorials

- Supported bulk actions for account