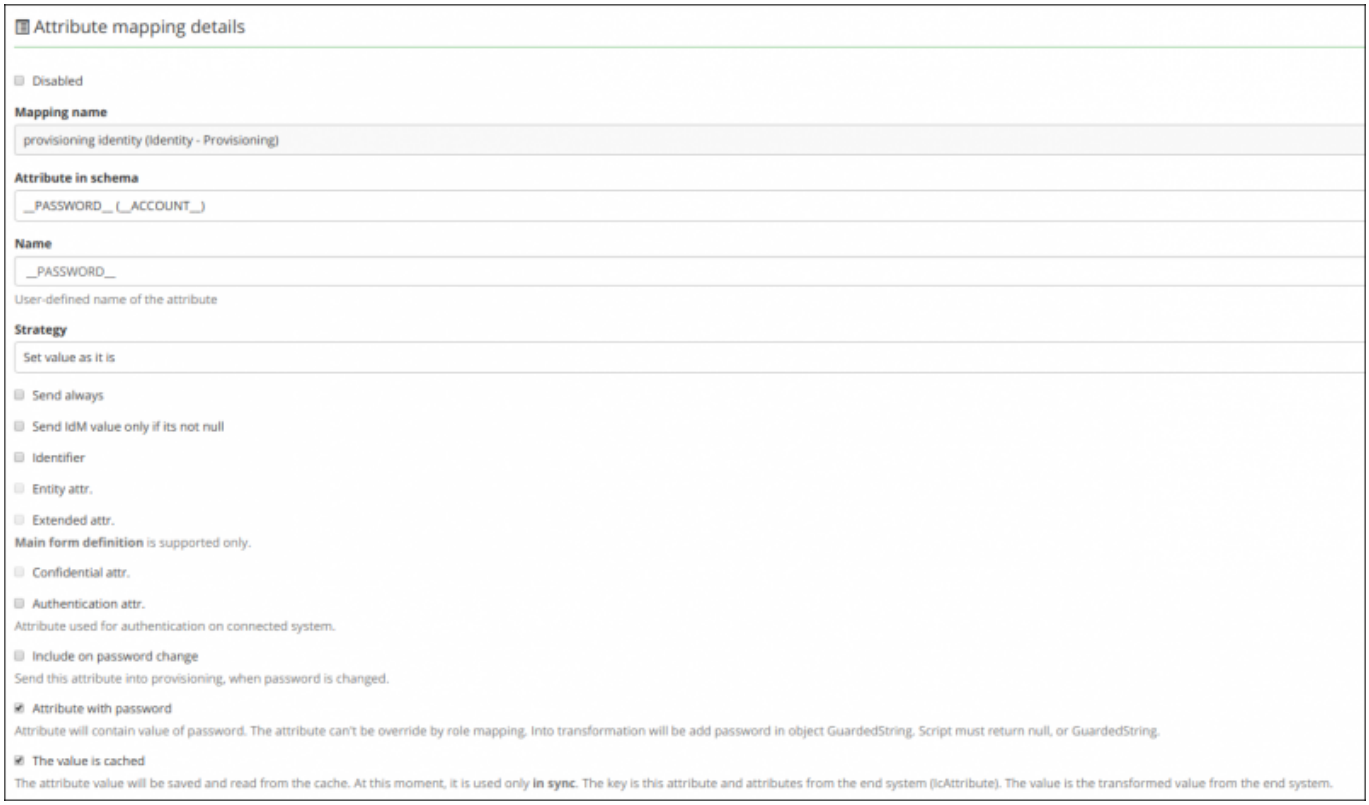
Password provisioning



Connects which support changing user's password (table, ad, ldap, ...) it is possible to provision passwords. Each of these connectors has special settings for password attribute. Eq.:

After you choose the password attribute and generate the schema for the system, it is possible to **create** mapping for password. Main password attribute can be mapped as the **__PASSWORD__** attribute.

Main password attribute (__PASSWORD__) is sent to end system only with uid, all attributes including another attributes marked as password will be sent in a separate provisioning operation. If application property (*idm.sec.acc.provisioning.sendPasswordAttributesTogether*) is set to true, only one provisioning operation will be created. This behavior is only active when changing the password. When CzechIdM creates a new account on the end system, the password is sent together with other attributes (some connectors may reimplement the behavior with their own - AD).

All password attributes will be transformed using transformation scripts before provisioning to the end system. The transformation scripts must return **GuardedString** or **null**, all another object throw exception. All transformation scripts obtain password in **attributeValue**. For transformation script, the classic rules for check security etc. will be applied .

Remeber all password attributes must have checked 'Password attribute'. Including main password attribute __PASSWORD__

In older versions (before 9.3.0) there is an attribute __PASSWORD__. The attribute still exists but for proper functioning the attribute must have the checkbox 'Password

attribute' checked, otherwise the password change will not work correctly. In existing mappings, the password attribute is checked for all __PASSWORD__ attributes by the flyway script.

Passwords and transformation

The transformations of password will be applied in these situations:

Password change

User changes his password for accounts (doesn't matter if the account includes his CzechIdM account) - classic password change form. After that, the password will be checked by the password policy and provisioning operation to system with __PASSWORD__ will be started.

If the script for transforming password/s contains errors it will throw an exception which **is not stored** in the provisioning operation queue.

Creating a new account and generating password

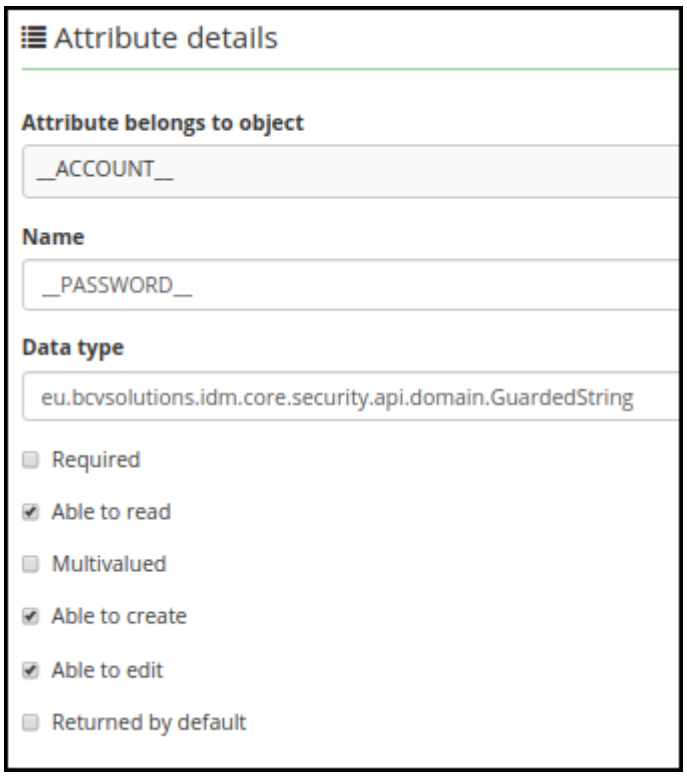
When the administrator or an automated process adds a role with a mapped system to the user and the mapping for the system contains password attributes, new password will be generated and this password will be transformed by each script in password attributes. The same password will be sent to all scripts.

Please check all the transformation script for password and remove all debug, info, error logs that the script contains. The user password and will be sent into the script and the password is very sensitive so we should never log it.

The password is generated by a password policy for generating password that is selected for the system. If system contains no password policy for generating passwords, the password will be generated by the CzechIdM default password policy. If even default password policy doesn't exist **no password will be generated**. Null value will be sent into the script. **Please check attributeValue in script for null!**

Attribute Password in schema (__PASSWORD__)

If the attribute PASSWORD is missing, you must create this attribute manually.



- **Name:** __PASSWORD__
- **Data type:** eu.bcvsolutions.idm.core.security.api.domain.GuardedString
- **Able to create:** true
- **Able to edit:** true
- **Able to read:** true