

Password provisioning

Attribute mapping details

☐ Disabled

Mapping name
provisioning identity (Identity - Provisioning)

Attribute in schema
__PASSWORD__(__ACCOUNT__)

Name
__PASSWORD__
User-defined name of the attribute

Strategy
Set value as it is

☐ Send always
☐ Send IdM value only if its not null
☐ Identifier
☐ Entity attr.
☐ Extended attr.
Main form definition is supported only.
☐ Confidential attr.
☐ Authentication attr.
Attribute used for authentication on connected system.
☐ Include on password change
Send this attribute into provisioning, when password is changed.
☒ Attribute with password
Attribute will contain value of password. The attribute can't be override by role mapping. Into transformation will be add password in object GuardedString. Script must return null, or GuardedString.
☒ The value is cached
The attribute value will be saved and read from the cache. At this moment, it is used only in sync. The key is this attribute and attributes from the end system (icAttribute). The value is the transformed value from the end system.

For connector that allow password change (table, ad, ldap, ...) is possible provisioning password. Every of these connectors has special settings for password attribute. Eq.:

After you choose the password attribute and generate schema for system. It is possible **create** mapping for password. Main password attribute can be mapped as `_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 second 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 for password change. When CzechIdM creates new one account in end system. Is password sent together with another attributes (some connectors may reimplement the behavior with own - AD).

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



Remember all password attributes must have checked 'Password attribute'. Including main password attribute `_PASSWORD_`



In older versions (<9.3.0) exists attribute `_PASSWORD_` the attribute still exists but for proper functioning must the attribute have checked checkbox 'Password attribute', otherwise behavior with password change through system will not work



correctly. In existing mapping is password attribute checked for all `__PASSWORD__` attributes by flyway script.

Passwords and transformation

Transformations on password will be applied in these situations:

Password change

User change his password for accounts (doesn't matter if account include CzechIdM account) - classic password change form. After will be password check by password policy it will be started provisioning operation to system with `__PASSWORD__`, all another attributes marked as password and all another password that must be included in password change.

If script for transformation password/s contains errors it will be throw exception:

the exception **is not stored** in provisioning operation queue.

Create new account and password generate

When administrator/automatic process add to user role with mapped system (mapping for system must contains password attributes. At least one attribute must be marked as password attribute) will be generated new password and this password will be transformed by each script in password attributes. To all script will be sent same password.



Please check all transformation script for password and remove all debug, info, error logs that the script contains. Into script will be sent user password and password is very sensitive information.

Password is generated by password policy for generating that has assigned system. If system doesn't contains password policy for generate password will be generated by CzechIdM default password policy. If even default password policy doesn't exist **no password will be generated**. Into script will be sent null. **Please check attributeValue in script for null!**

Attribute Password in schema (`__PASSWORD__`)



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

☰ Attribute details

Attribute belongs to object

__ACCOUNT__

Name

__PASSWORD__

Data type

eu.bcvolutions.idm.core.security.api.domain.GuardedString

☐ Required

☒ Able to read

☐ Multivalued

☒ Able to create

☒ Able to edit

☐ Returned by default

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

From:
<https://wiki.czechidm.com/> - IdStory Identity Manager

Permanent link:
https://wiki.czechidm.com/tutorial/adm/password_provisioning?rev=1560316378

Last update: **2019/06/12 05:12**

