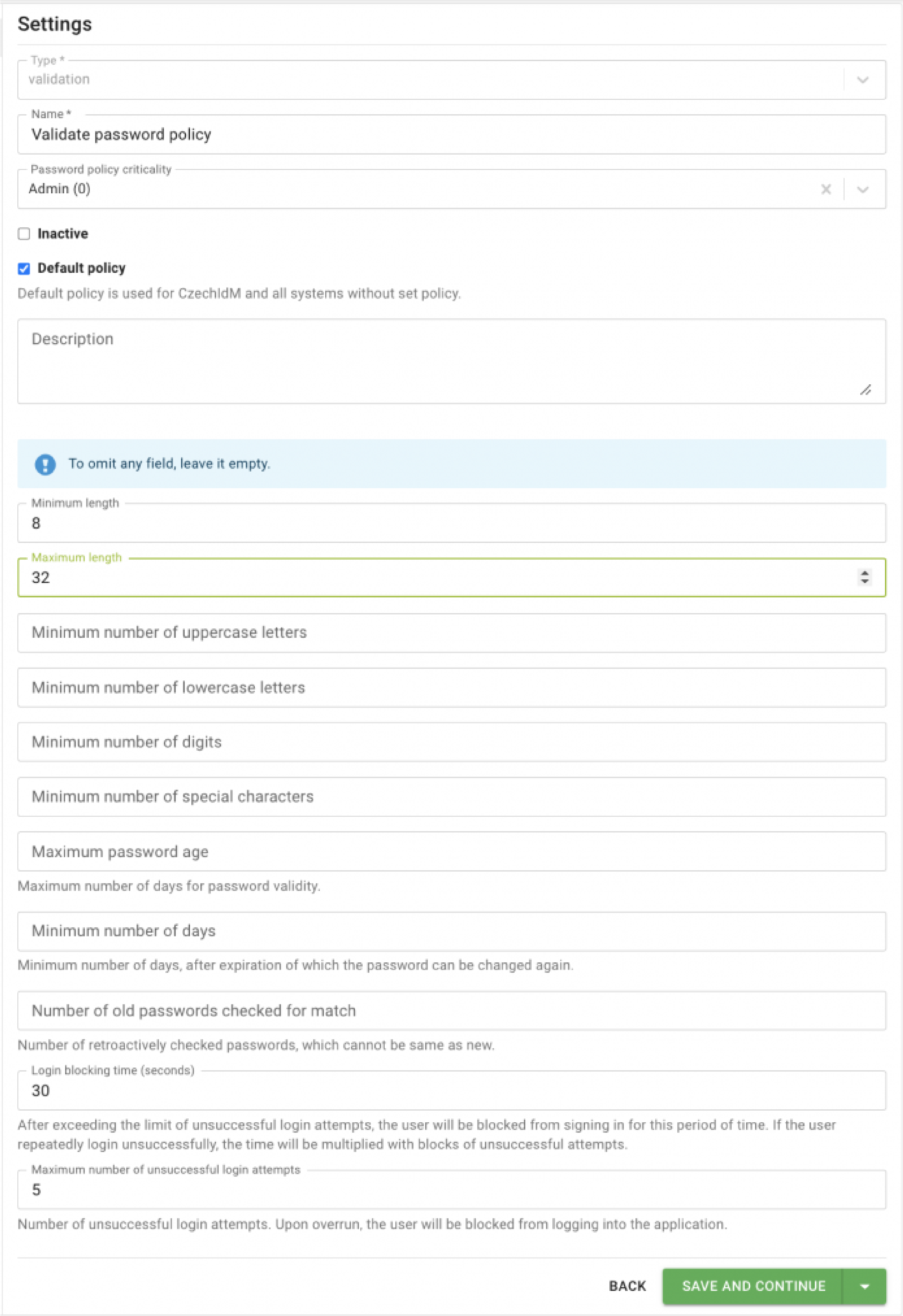
Passwords - policies and their configuration

A password policy determine, which rules must be met by new passwords either changed by users or generated by CzechIdM itself.

A new password policy

A new password policy can be created in the tab **Settings → Password policies**. In the table, you’ll find a list of existing policies, and you can create a new policy by clicking the green **Add** button.



Settings

Type *
validation

Name *
Validate password policy

Password policy criticality
Admin (0)

□ **Inactive**

☑ **Default policy**

Default policy is used for CzechIdM and all systems without set policy.

Description

To omit any field, leave it empty.

Minimum length
8

Maximum length
32

Minimum number of uppercase letters

Minimum number of lowercase letters

Minimum number of digits

Minimum number of special characters

Maximum password age

Maximum number of days for password validity.

Minimum number of days

Minimum number of days, after expiration of which the password can be changed again.

Number of old passwords checked for match

Number of retroactively checked passwords, which cannot be same as new.

Login blocking time (seconds)
30

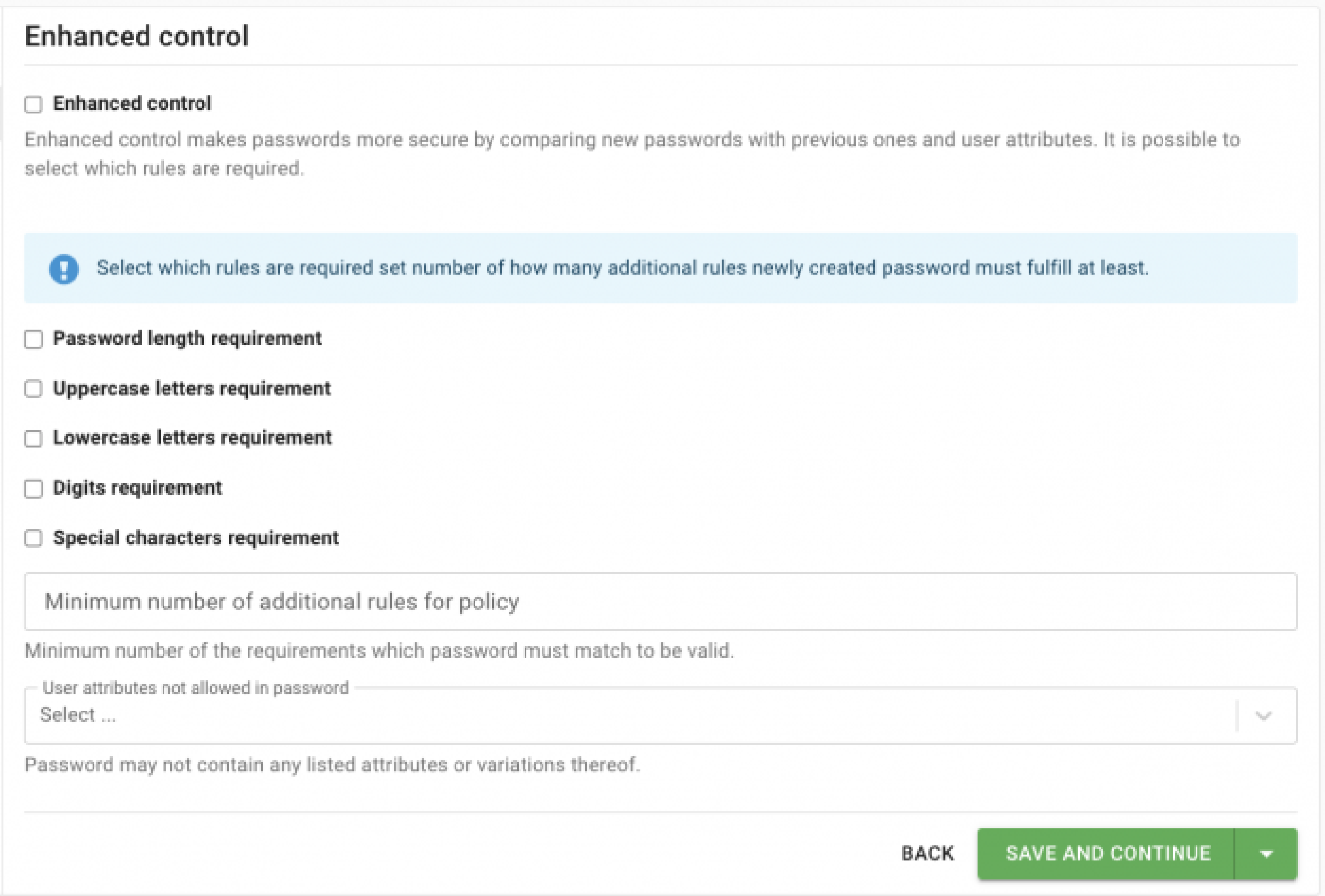
After exceeding the limit of unsuccessful login attempts, the user will be blocked from signing in for this period of time. If the user repeatedly login unsuccessfully, the time will be multiplied with blocks of unsuccessful attempts.

Maximum number of unsuccessful login attempts
5

Number of unsuccessful login attempts. Upon overrun, the user will be blocked from logging into the application.

The following basic attributes of a password policy can be filled in:

- **Type** – CzechIdM allows defining 2 policy types for passwords used by users in CzechIdM and connected systems.
    - Validation – This policy is used when a password (in CzechIdM or a password to an administered system supporting the setting of password) is set or changed, e.g., when a user performs a password change in the GUI of CzechIdM.
    - Generation – This policy is applied when the user sets or changes the password using the password generator in CzechIdM, i.e. the user lets CzechIdM to generate the password according to this policy.
- **Name** – the desired name of the policy. This name is displayed in the settings of the systems where the policy is to be applied.
- **Inactive** – An inactive policy is not offered in the system configuration.
- **Default policy** – The standard policy is used for password validation against the CzechIdM system and it also validates all passwords on systems where no other policy is defined.
- **Description** – optional description of the policy. It is convenient to summarize the basic policy rules in it.
- **Generation type** - can be chosen from these types: random, passphrase and prefix/suffix - it is visible if you set **Type → Generation**
    - Random - random generated password,
    - Passphrase - random generated words by internal dictionary.
- **Password policy criticality** - this filed defines what criticality have this policy
    - Admin - For administrative accounts and users.
    - Technical account - For technical accounts.
    - User - For regular User accounts or users.
- **Minimum length** – determines the minimum number of characters in a password
- **Maximum length** – determines the maximum number of characters in a password
- **Prefix** - prefix is a string that will be added at the beginning of a newly generated password. Beware that final length and another settings may be not passed with password policy settings. - it is visible if you set **Type → Generation**
- **Suffix** - suffix is a string that will be added at the end of a newly generated password. Beware that final length and another settings may be not passed with password policy settings. - it is visible if you set **Type → Generation**
- **Minimum number of uppercase letters** – determines the number of upper-case characters which the password must contain. The set of characters is defined in the tab Characters.
- **Minimum number of lowercase letters** – determines the number of lower-case characters which the password must contain. The set of characters is defined in the tab Characters.
- **Minimum number of digits** - determines the number of numerals which the password must contain. The set of characters is defined in the tab Characters.
- **Minimum of special characters** - The set of characters is defined in the tab Characters.
- **Number of old passwords for match** – The number of days of password validity. This attribute is important mainly in the Standard policy, which is applied for CzechIdM
- **Maximum time for password change** – This setting specifies how many of the user's previous passwords must be checked to ensure that the new password is not the same as any of those old passwords. For example, if the setting is set to 5, the new password must be different from the last 5 passwords used by the user.
- **Minimum number of days for password validity**. The number of days when the password cannot be changed. Sparsely used option.



Enhanced control

□ Enhanced control

Enhanced control makes passwords more secure by comparing new passwords with previous ones and user attributes. It is possible to select which rules are required.

Select which rules are required set number of how many additional rules newly created password must fulfill at least.

□ Password length requirement

□ Uppercase letters requirement

□ Lowercase letters requirement

□ Digits requirement

□ Special characters requirement

Minimum number of additional rules for policy

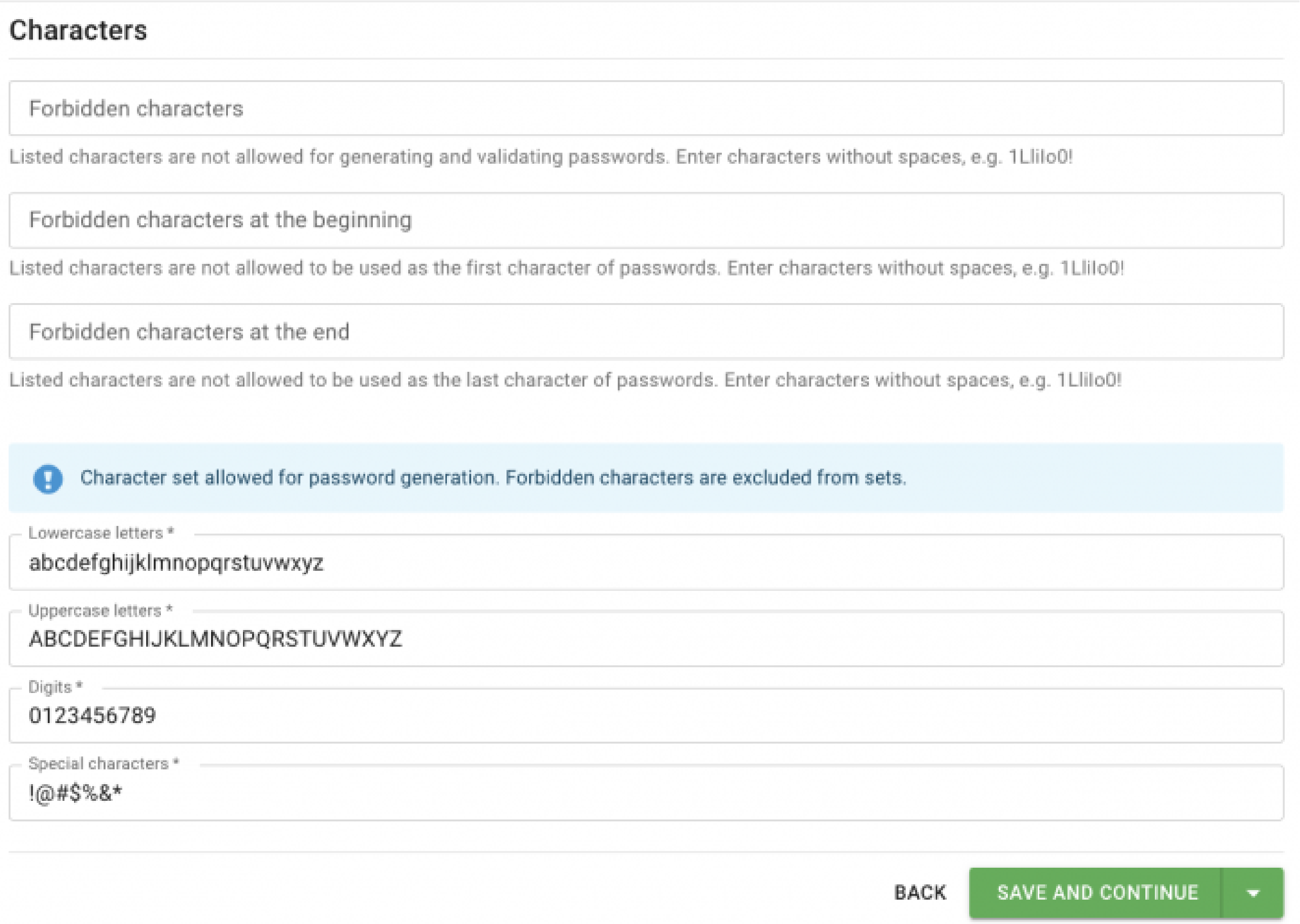
Minimum number of the requirements which password must match to be valid.

User attributes not allowed in password: Select ...

Password may not contain any listed attributes or variations thereof.

The policy can be saved by clicking *Save and continue*, or advanced options can be set in the form menu Enhanced control, where the following options can be set:

- **Enabled** – enables the whole form for extended checking
- **Requirement checkboxes** – contains a set of 5 checkboxes. Every checked checkbox must be always fulfilled. If an option is not checked, then the item is counted in the next point.
- **Minimum number of additional rules for policy** – If a number is defined, then the minimum number of rules fulfilled must be the same as the number of those which were not marked as required in the previous point. For example, if all the 5 checkboxed required are checked and the value of 4 is filled in this box, then the password must fulfill at least 4 out of the 5 rules.
- **User attributes not allowed in password** – In this box, you can select user's attributes which will be checked for similarity with the password. For example, if the attribute user name is set, then the user's password must not contain his login.



Characters

Forbidden characters

Listed characters are not allowed for generating and validating passwords. Enter characters without spaces, e.g. 1LlIlo0!

Forbidden characters at the beginning

Listed characters are not allowed to be used as the first character of passwords. Enter characters without spaces, e.g. 1LlIlo0!

Forbidden characters at the end

Listed characters are not allowed to be used as the last character of passwords. Enter characters without spaces, e.g. 1LlIlo0!

Character set allowed for password generation. Forbidden characters are excluded from sets.

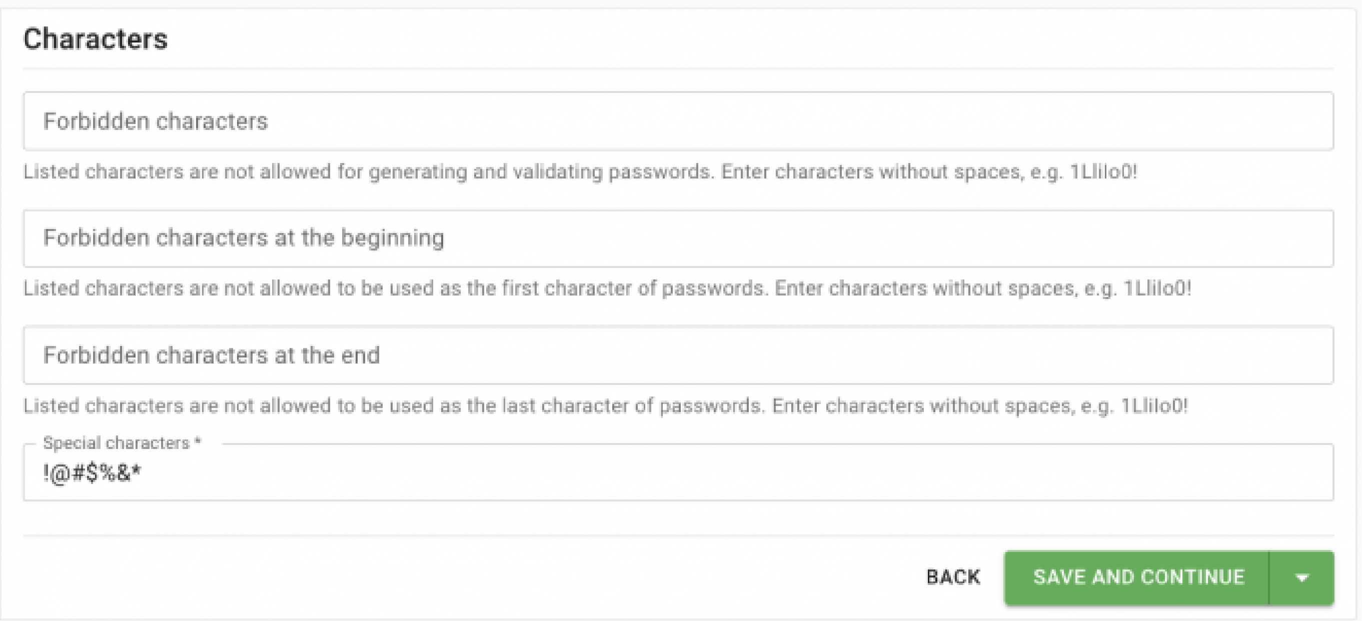
Lowercase letters *: abcdefghijklmnopqrstuvwxyz

Uppercase letters *: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Digits *: 0123456789

Special characters *: !@#$%&*

In the tab **Characters for password generate**, there are sets of characters for individual groups – lower-case characters, upper-case characters, numerals, special characters.



Characters

Forbidden characters

Listed characters are not allowed for generating and validating passwords. Enter characters without spaces, e.g. 1LlIlo0!

Forbidden characters at the beginning

Listed characters are not allowed to be used as the first character of passwords. Enter characters without spaces, e.g. 1LlIlo0!

Forbidden characters at the end

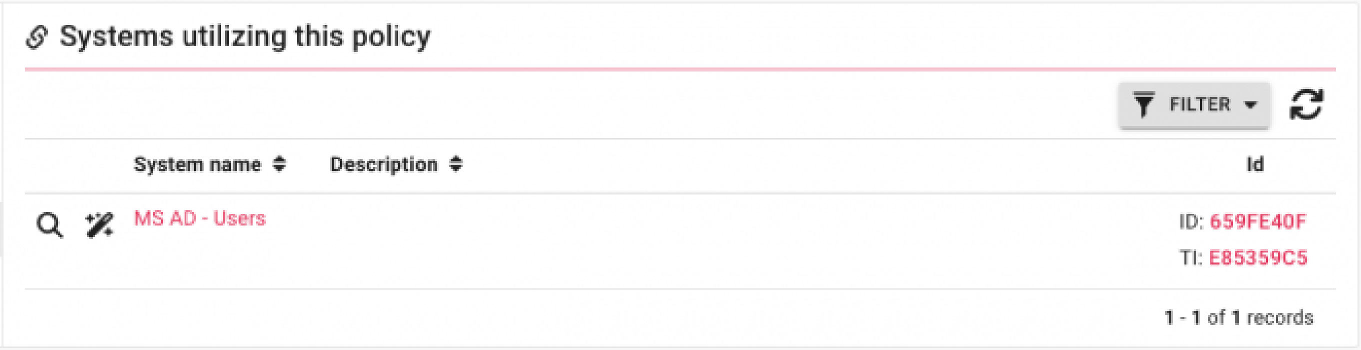
Listed characters are not allowed to be used as the last character of passwords. Enter characters without spaces, e.g. 1LlIlo0!

Special characters *: !@#$%&*

In the **Characters for password validate** tab, you can find rules regarding forbidden characters, restrictions on characters at the beginning or end of the password, and guidelines for using specific special characters.

In addition, it can be set here which characters will be forbidden in the policy. This is important mainly for policies of password generation. Also, automatically generated passwords are usually sent by SMS or mails and the way some characters are displayed can confuse the user, e.g., similarities of ‘I’ and ‘l’ or ‘,’ and ‘.’. Sometimes it is convenient to prohibit also characters ‘y’ and ‘z’ for generating due to different layouts of users’ keyboards.

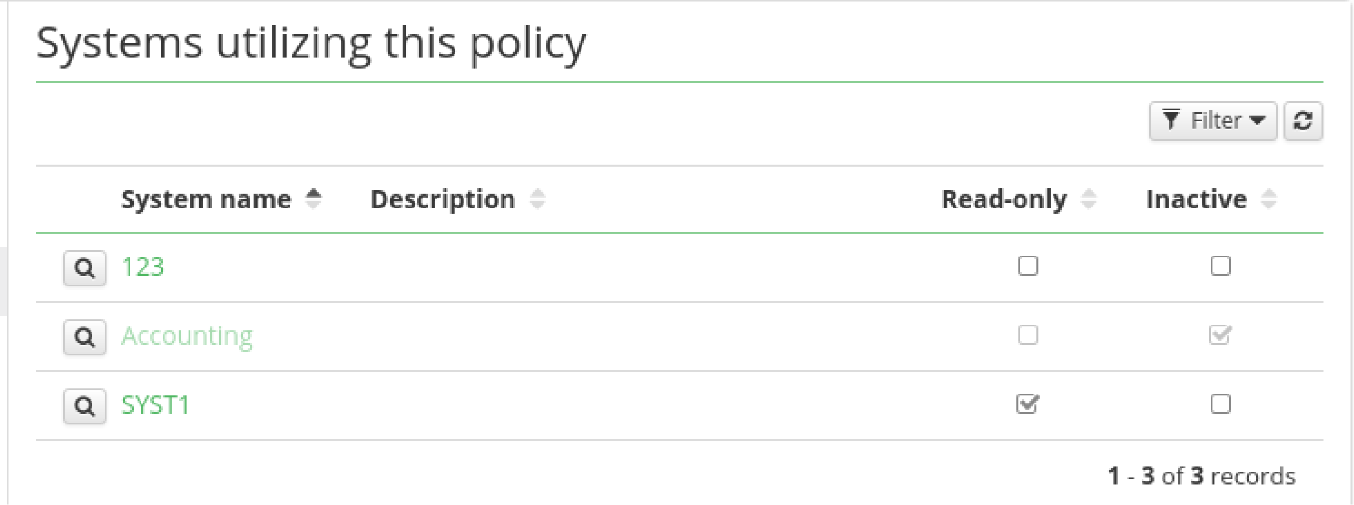
In the last tab **Connected systems**, you can see a list of systems where the policy is currently set.



Systems utilizing this policy

System name	Description	Id
MS AD - Users		ID: 659FE40F TI: E85359C5

1 - 1 of 1 records



Systems utilizing this policy

System name	Description	Read-only	Inactive
123		☐	☐
Accounting		☐	☑
SYST1		☑	☐

1 - 3 of 3 records

Be careful if the policy is set to be a **Standard policy**, it is then applied in all locations where there is no other policy, i.e. **this list can be empty yet the policy is still applied on some systems**.

Setting policy to administered system

The preparation of a password policy was introduced in the previous section. If a policy has been marked as a **Standard policy**, then this policy is now active for both CzechIdM and all administered systems where a policy has not been chosen yet.

Otherwise, a policy needs to be set for the system. This is done in the system detail. The detail can be accessed via the menu **Connected systems → system detail (magnifying glass) → Basic information** where password policies can be selected.

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

Permanent link:
https://wiki.czechidm.com/tutorial/adm/password_policy

Last update: **2024/08/06 10:05**