Password policies

Definition

Password domain

> Is a logical way of grouping managed systems that are sharing the same password for each account. If the administrator chooses to have the same password for every system, only one password domain should exist. If the administrator chooses to assign a different password for each system, then a password domain should be created for each managed system.

Password policies

> Password policies allow you to define custom rules that passwords must comply with to enhance system security. For each password domain, Soffid allows you to create different password policies related to user type. It is only possible to define a single password policy for one password domain and one user type.

There are two kinds of password policies.

- The first one is for user selected passwords. That is the default behavior.
- The second one is system generated passwords. These policies are useful for shared accounts when using Enterprise Single Sign-on.

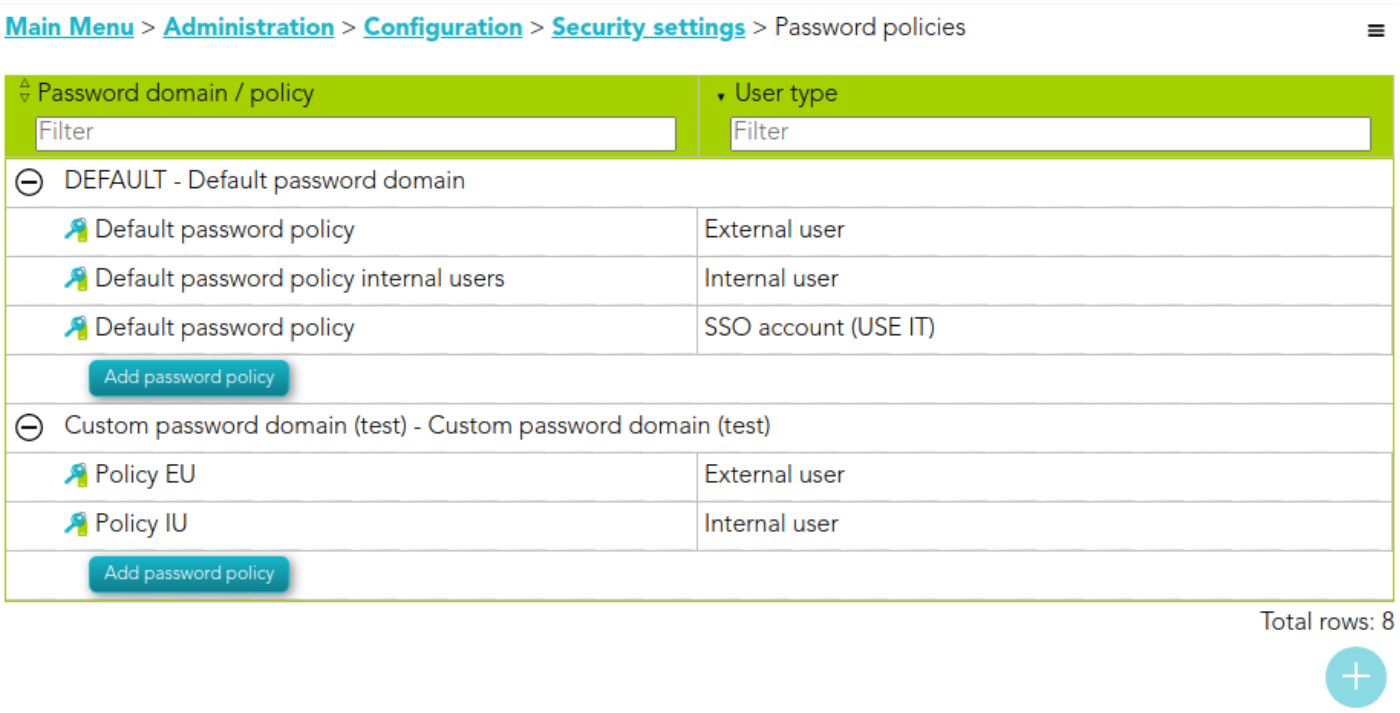
A password policy will also define how often the password needs to be changed and how many days are allowed to change it.

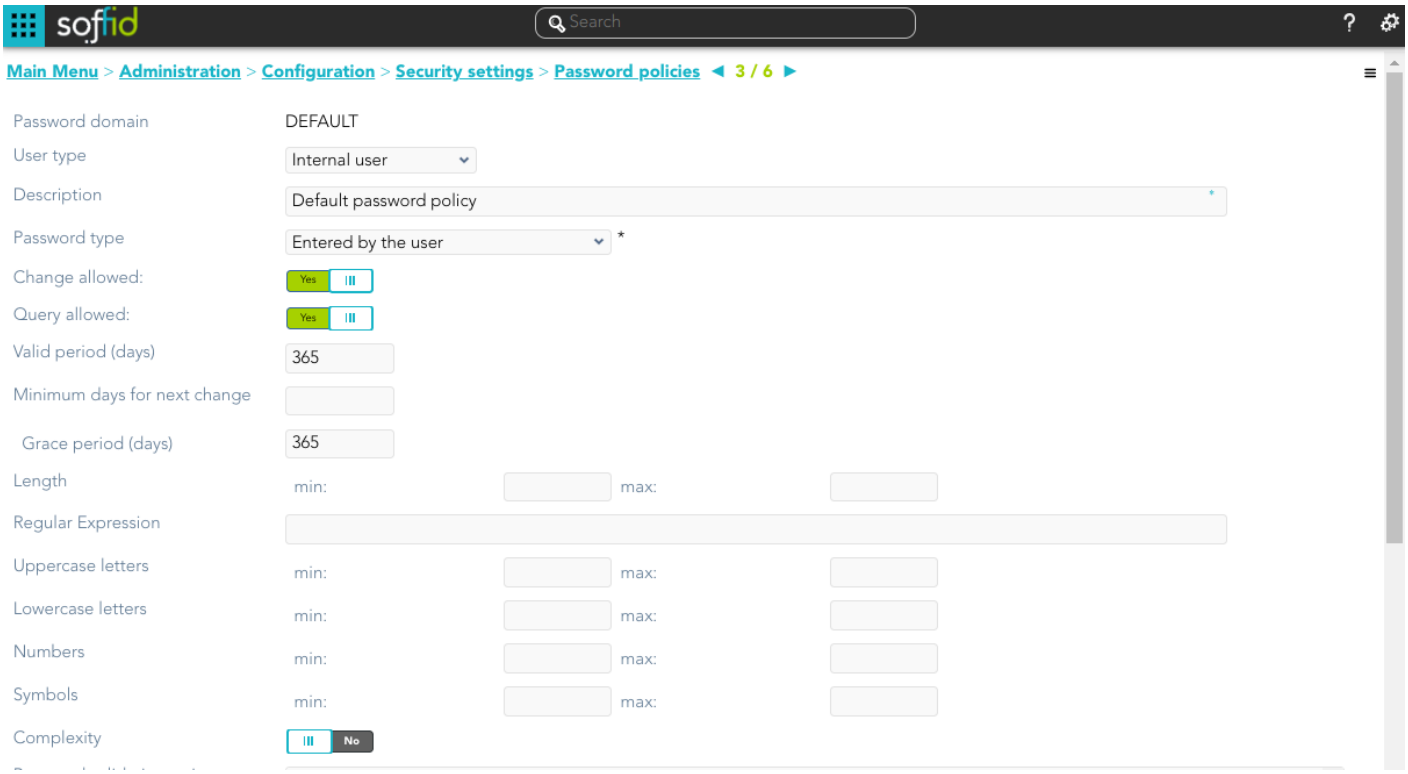
Regarding password complexity, you can specify the minimum and the maximum number of lowercase letters, uppercase letters, numbers, and symbols, as well as password length.

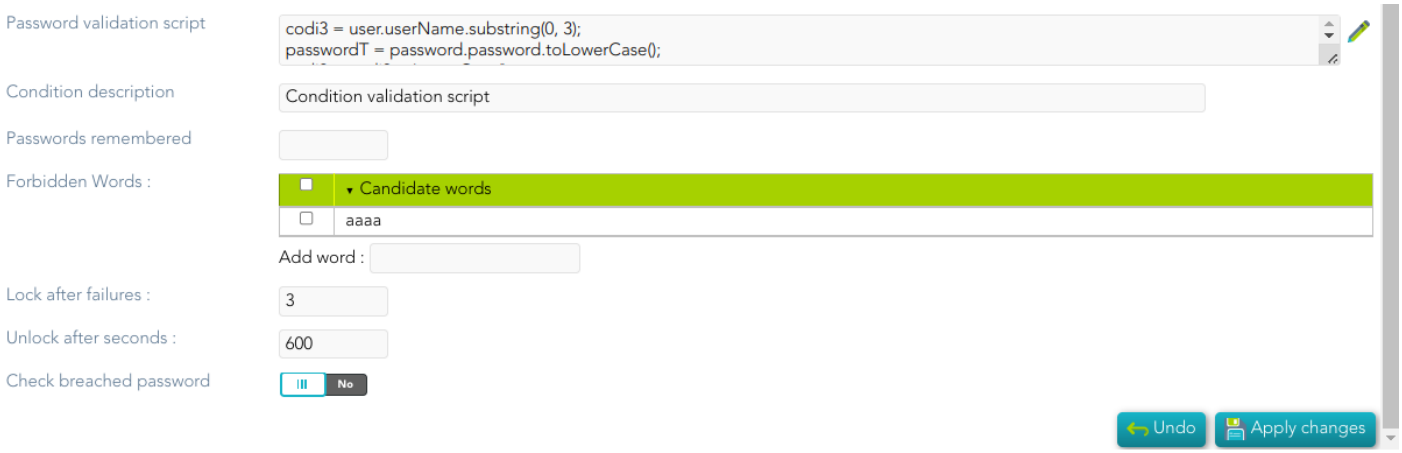
The administrator users can define a regular expression that must match each password. This can be used, for instance, to ensure that the first password is not numeric.

It is allowed to create a list of forbidden words that cannot be used as passwords.

Screen overview







Related objects

1. **Password domain**
2. **User Type**

Standard attributes

Password Domain

- **Code**: password domain identifier code.
- **Description**: a brief description of the password domain.

Password policies

- **Password domain**: the password policy belongs to that password domain.
- **User type**: specific user type for which the password policy is created.
- **Description**: a brief description of the password policy.
- **Password type**: the king of policies password:
  - **Entered by the user**: that is the default behavior.
  - **Automatically generated**: these policies are useful for shared accounts when using Enterprise Single Sign-on.
- **Change allowed**: if it is checked, the user could change automatically generated passwords.
- **Query allowed**: if is checked, the user can view the current password.
- **Valid period (days)**: the change of the password will be asked in that number of days. That option is available when you select the "Entered by the user" option.
- **Minimum days for next change**
- **Grace period (days)**: additional days allowed to the valid period, for changing the password. That option is available when you select the "Entered by the user" option.

- **Renewal Time**: added number of days to change the password. That option is available when you select the "Automatically generated" option.
- **Length (min & max)**: added the number of days to change the password.
- **Regular expression**: the password must comply with that regular expression.
- **Uppercase letters (min & max)**: min and max number of uppercase letters that be included on the password.
- **Lowercase letters (min & max)**: min and max number of lowercase letters that be included on the password.
- **Numbers (min & max)**: min and max number of numbers that be included on the password.
- **Symbols (min & max)**: min and max number of symbols that are included on the password.
- **Complexity**: Similar operation to the same option in Active Directory. It is mandatory to use three different types of characters (uppercase, lowercase, numbers, and symbols), it is not allowed to use the user code, name, or surname.
- **Password validation script**: script to validate additional password conditions. The result must be true or false.
- **Condition description**: description of the validation script. This condition will be displayed in the Password policy field when the user try to change the password from My Profile.
- **Passwords remembered**: the number of passwords the system will remember.
- **Forbidden words**: list of forbidden words that may not be used to create a password if they are selected. It will be case insensitive. For instance, there will be no distinction between "Soffid", "SOFFID", or "soffid".
- **Lock after failures**: the number of login attempts before blocking an account.
- **Unlock after seconds**: the number of seconds an account is blocked.
- **Check breached password**

Password validation script example:

```
codi3 = user.userName.substring(0, 3);
codi3 = codi3.toLowerCase();
if(codi3.equals(passwordT.substring(0,3)))
  return false;
return true;
```

Actions

Password policies query actions

Add new domain	Allows you to create a new **password domain**. You can choose that option on the hamburger menu or click the add button (+).To add a new password domain it will be mandatory to fill in the required fields
Add new password policy	Allows you to create a new **password policy** on a specific password domain. Below the father password domain, you can find the button to perform that action. To add a new password policy it will be mandatory to fill in the required fields.

Password domain detail actions

Apply changes	Allows you to save a new password domain or to update the password domain changes. To save the data it will be mandatory to fill in the required fields.
Delete	Allows you to delete a password domain. To delete a password domain you can click on the hamburger icon and then click the delete button (trash icon). Soffid will ask you for confirmation to perform that action, you could confirm or cancel the operation.
Undo	Allows you to quit without applying any changes.

Password policies detail actions

Apply changes	Allows you to create a new password policy or to update password policy changes. To save the data it will be mandatory to fill in the required fields.
Delete	Allows you to delete a password policy. To delete a password policy you can click on the hamburger icon and then click the delete button (trash icon). Soffid will ask you for confirmation to perform that action, you could confirm or cancel the operation.
Undo	Allows you to quit without applying any changes.
Add word	Allows you to create a new forbidden word. Those forbidden words may not be used to create a password if they are selected.

Revision #31
Created 6 April 2021 14:27:24 by pgarcia@soffid.com
Updated 17 July 2024 11:40:38 by pgarcia@soffid.com