

Account Policies

This page explains how to manage all kinds of policies related to the account, especially those related to passwords, audit results, privacy, and user accounts.

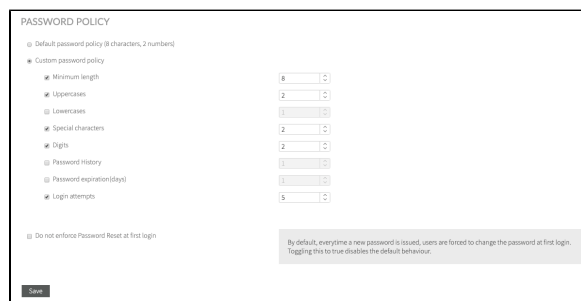
Contents:

- [Account Policies](#)
 - [Password strength](#)
 - [Password History](#)
 - [Password expiration \(days\)](#)
 - [Login attempts](#)
 - [Do not enforce Password Reset at first login](#)

Account Policies

Go to **Account Management > Account Policies** to set a password policy for your account.

There is a default policy (8 characters, 2 numbers), but this policy is customizable.



The screenshot shows the 'PASSWORD POLICY' configuration page. It features a sidebar on the left with a tree view containing 'Default password policy (8 characters, 2 numbers)' and 'Custom password policy'. The 'Custom password policy' is selected and expanded, showing several settings: 'Minimum length' (8), 'Uppercases' (2), 'Lowercases' (1), 'Special characters' (2), 'Digits' (2), 'Password History' (1), 'Password expiration(days)' (1), and 'Login attempts' (5). Each setting has a numeric input field with a dropdown arrow. At the bottom of the sidebar is a checkbox for 'Do not enforce Password Reset at first login'. A 'Save' button is located at the bottom left. A grey informational box on the right states: 'By default, everytime a new password is issued, users are forced to change the password at first login. Tagging this to true disables the default behavior.'

Password strength

You can configure the strength (complexity) of the passwords by specifying the following rules:

- The minimum password length.
- The number of uppercase and lowercase letters, digits, and special characters that a password should contain.

Password History

Enforcing the Password History policy sets how often an old password can be reused. You can define the number of previous passwords remembered, discouraging users from reusing previous passwords and preventing them from alternating between several common passwords.

Password expiration (days)

Apply this policy to determine how long users can keep a password before they are required to change it, thus forcing users to periodically change it. Once the password expiration date is reached, the user redirects to a "change your password" page.

Login attempts

Setting the maximum number of allowed login attempts protects against "brute-force" or dictionary-based attempts to guess passwords. You can specify a maximum number of consecutive login attempts allowed after the account is automatically locked.

Only the Kiuwan owner (or a Kiuwan user with **Users Management** privilege) can enable the locked account.

Do not enforce Password Reset at first login

By default, whenever Kiuwan generates a new password, the user has to change the password for the first time. When the option "Do not enforce Password Reset at first login" is set up, this behavior is disabled.

You can create a new password in the following situations:

- Creation of a new user.
- Resetting a password (by the administrator).
- Following the "Forgot my password" process on the main login page.