The system can be configured to use a password policy, which means that new passwords entered by users will be validated according to a certain set of requirements. Passwords that do not meet the specified conditions will be rejected.

Configuring a password policy

To enforce a password policy on your website, enable the **Use password policy** setting in **Settings -> Security & Membership -> Passwords**. The specific rules of the policy can be configured through the remaining settings in the category:

- **Minimal length** - sets the minimum number of total characters required for user passwords.
- **Number of non alphanumeric characters** - sets the minimum number of non alphanumeric characters (i.e. any character except for numbers and letters) that must be present in a password in order for it to be accepted.
- **Regular expression** - can be used to enter a regular expression that will be used to validate user passwords.
  - For example: *^(?=.*\d)(?=.*[a-z])(?=.*[A-Z]).*$*
  - This sample expression would require passwords to contain at least one lower case letter, upper case letter and number. The minimum amount of characters would be determined by the other policy settings.

The requirements defined by all three settings are combined together to form the final password policy.

How is password policy applied

The policy is applied in all sections of the website where a new password can be entered. This includes:

- Web parts that display forms on the live site (**My account** or the **Registration form**).
- Administration interface (**Users** application).

The requirements of the policy, except for the regular expression, are additionally observed when the system automatically generates new passwords. This is also the case if the **Use password policy** setting is disabled, so you can affect how passwords should be generated even if you do not wish to set a policy for your website's users.

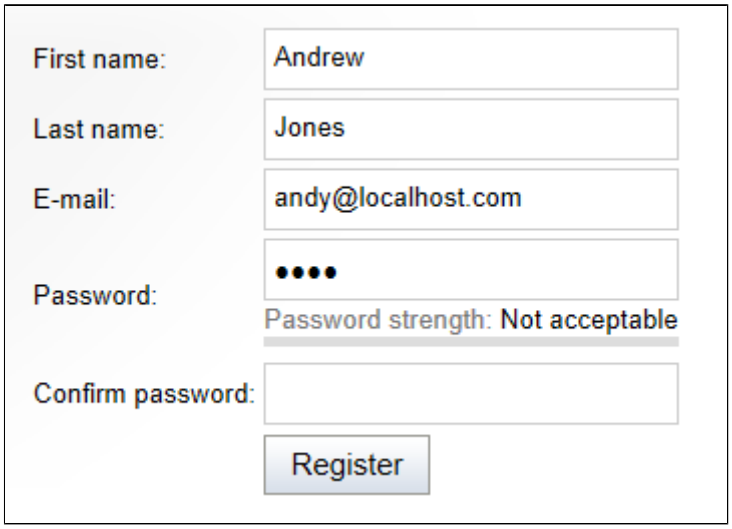
Enforcing password policy on existing users

When you introduce a password strength policy, existing users are by default allowed to keep their passwords unchanged.

To force existing users to observe the policy, enable the **Force password policy on logon** setting. With this setting enabled, the system will check whether a user's password meets the policy requirements every time a user logs in. When the password doesn't meet the requirements, the user is presented with a form, which requires the user to changes the existing password.

Password strength indicator

When a user types in a password, it is validated in real time and its status is reflected by an indicator below the field. If a policy is set, passwords that do not fulfill the requirements will be rejected with the *Not acceptable* status.



Valid passwords will have a different status displayed according to their relative strength, which is calculated based on the recommended values for the total password length (*12* by default) and number of non alphanumeric characters (*2* by default). If a password policy is not enabled for the website, the current strength status of passwords will still be shown, but only as a recommendation and all passwords will be accepted.

To help users come up with an appropriate password, you can use the **Policy violation message** setting to specify a text message that will be displayed to users who attempt to enter a password that does not fulfill the requirements of the password policy. If left empty, a default message will be shown, informing about the minimum password length and number of non alphanumeric characters. If you wish to use a regular expression, it is recommended to describe its requirements in a custom message.

Customizing the password strength indicator

You can change the recommended values that are used to calculate the password strength by editing the code of the appropriate controls:

- To set different values globally for the entire application, edit the code behind of the **~/CMSModules/Membership/FormControls/Passwords/PasswordStrength.ascx** control and enter different numbers for the mPreferedLength and mPreferedNonAlphaNumChars variables.
- You can also override the values for specific instances where this control is used through its **PreferedLength** and **PreferedNonAlphaNumChars** properties (e.g. in the code of the *Registration form* web part).
- The appearance of individual password strength status labels may be customized through CSS styles. Each one has a different class assigned, e.g. *PasswordStrengthNotAcceptable.*

Password policy and strength in custom forms

When creating custom forms, you can add password fields that validate according to the specified policy and display password strength. Use the **Password strength** or **Password with confirmation** form control for the given field, which automatically ensure this functionality.