Password encryption in database

There are multiple different formats that can be used to store passwords in the database. They may be saved either in plain text or as the result of a security hash function.

You can choose which option should be used in **Site Manager -> Settings -> Security & Membership -> Passwords** via the **Password format** setting:

- The default and recommended option is **SHA2 with salt**.

The Password format setting is stored in a database table *Users*.

Password salt

Passwords are usually stored using the SHA2 hash format with the additional application of a **salt**. Salt is a string that is appended to passwords before they are encrypted, which helps protect the passwords against dictionary or other types of brute force attacks. It also ensures that every user has a different password hash, even if multiple users have the same password.

In Kentico, we add two types of salt to the password:

- **Custom salt** - by default, the UserGuid column is used to append the GUID of each user to the passwords. You can customize this setting to use a different table column as a password salt. Add the following key into the **<appSettings>** section of the web.config file and type the column name as a value:

  ```
  <add key="CMSUserSaltColumn" value="UserCreated" />
  ```

- **Password salt** - to increase the length of the salt (to further improve the security of hashed passwords), you can define a custom string, which will be appended to every password. You only need to include the following key into the **<appSettings>** section of your web.config file:

  ```
  <add key="CMSPasswordSalt" value="SaltText" />
  ```

Password and salt are composed in this way:

Password	Custom salt	Password salt

Please keep in mind that, if you change the password format, it only affects how future passwords will be stored. Existing passwords will remain unchanged. You will need to reset all passwords, so that they are stored in the new format.

For this reason, it is recommended to set the appropriate format directly after installation, before you create user accounts or allow users to start registering.