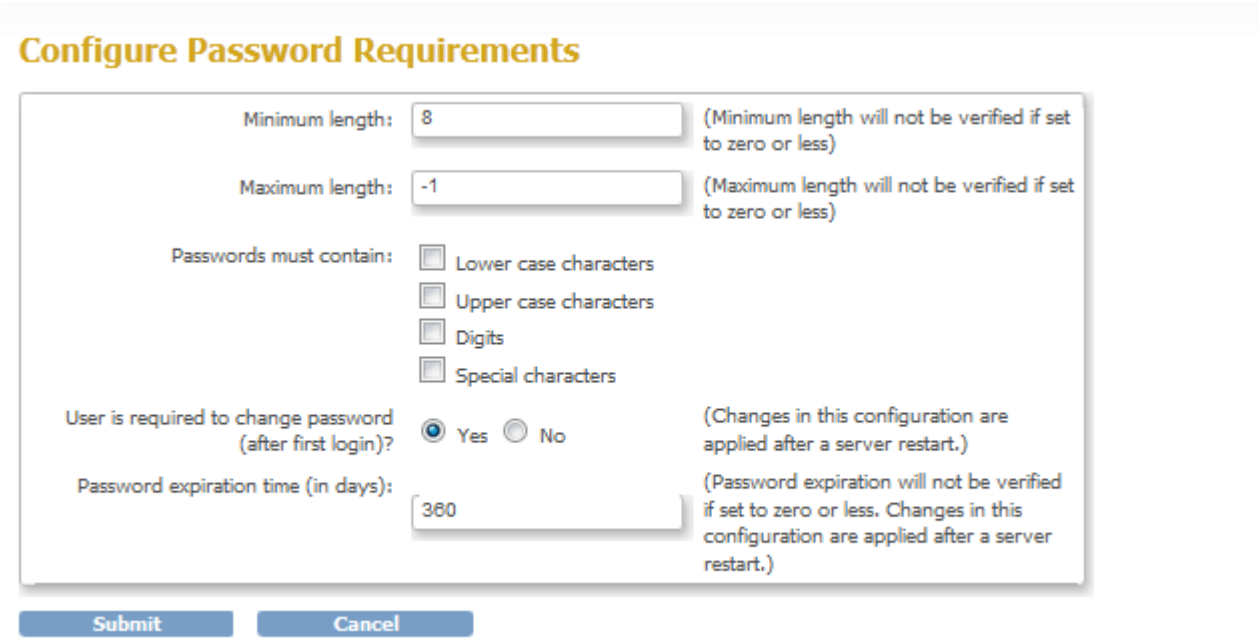
8.2.5.4 Configure Password Requirements

Starting with OpenClinica 3.1.3, in the Administration module, the Configure Password Requirements page allows an administrator to configure the password policy for your OpenClinica system. A password policy that forces users to use strong passwords makes your system less vulnerable to bruteforce attacks that try to guess a user's password.

To access the Configure Password Requirements page, from the Tasks menu, in the Administration module, select Users, then Configure Password Requirements.



In the Configure Password Requirements, you can define the values for the following options:

- **Minimum length**: minimum number of characters a password may contain. If this value is set to zero or any negative number, OpenClinica will not check the minimum length of the user's password. However, disabling the minimum password length does not allow an user account to have no password - in this case valid password consists of at least one character.
- **Maximum length**: maximum number of characters a password may contain. If this value is set to zero or any negative number, OpenClinica will not check the maximum length of the user's password.
- **Passwords must contain**: Specifiy types of characters that must be present in a password. The character types groups are Lower Case Characters, Upper Case Characters, Digits and Special Characters. The following characters are considered special characters: ! @ # $ % & * ( )
- **User is required to change password (after first login)**: Should the user be forced to change his password upon first login to OpenClinica. When OpenClinica creates a user account, a password is generated and sent via email to the email address configured in the user's account or shown to the administrative user who created the account. This setting is used to ensure the user won't be able to use the system-generated password after the first login. A change in this configuration will be effective only after restarting the OpenClinica application server.

- **Password expiration time (in days)**: Number of days after a password is set to be considered expired. Once a user authenticates to OpenClinica and their password is expired, the system will prompt the user to change their password. If this value is set to zero or any negative number, OpenClinica never consider a user's password expired. A change in this configuration will be effective only after restarting the OpenClinica application server.

This page is not approved for publication.