

## 6.2.5 Configure Access to OpenClinica

To enhance system security, you can configure OpenClinica so that authorized users are only allowed a specified number of failed login attempts, and after that, they are locked out. By default, the feature is disabled. After a user has been locked out, you unlock them so they can successfully log in again.

This page is not approved for publication.

### 6.2.5.1 Set Lockout Feature

To set the lockout feature:

1. From the Tasks menu, in the Administration module, select Users.  
The Administer Users page opens.
2. Click the Lockout Configuration link.  
The Lockout Configuration page opens:




The screenshot shows a form titled "Lockout Configuration". It has two input fields: "Lockout Enabled:" with a dropdown menu set to "FALSE", and "# of Failed Attempts:" with a text input field containing the number "3". Below the form are two buttons: "Submit" and "Cancel".

3. To activate the lockout feature, set the Lockout Enabled value to TRUE.
4. For the # of Failed Attempts, enter a value between 1 and 25.
5. Click Submit.  
The system displays a confirmation message.

OpenClinica tracks the number of consecutive failed login attempts. After that number equals the value specified for the # of Failed Attempts, the user cannot log in to OpenClinica. For the user to regain access to OpenClinica, an administrator must unlock the user's account in the Administer Users interface.

### 6.2.5.2 Unlock a Locked-Out User

If a user fails to log in successfully more than the allowed number of times as specified via the lockout feature, you must unlock the user account using the Administration module. To unlock a user account:

1. From the Tasks menu, in the Administration module, select Users.  
The Administer Users page opens.
2. Click the Unlock icon  in the Actions column for the user whose account you want to

unlock.

The user account is unlocked. The unlock icon no longer appears in the Administer Users table.

3. The user can log in to OpenClinica again using the new, temporary password sent to the user's email account.

## 6.2.5.3 Additional Password Configuration Options

You can also specify these configuration options for managing user passwords in the `datainfo.properties` file:

- The default method for how a user receives their password, either via email or from the business administrator.
- If a user must change their password on the first log in.
- If a user's password should expire, and if so, the length of time until it expires.

For details, see [Configuring the OpenClinica Application](#).

## 6.2.5.4 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.

### Configure Password Requirements

Minimum length:	<input type="text" value="8"/>	(Minimum length will not be verified if set to zero or less)
Maximum length:	<input type="text" value="-1"/>	(Maximum length will not be verified if set to zero or less)
Passwords must contain:	<input type="checkbox"/> Lower case characters <input type="checkbox"/> Upper case characters <input type="checkbox"/> Digits <input type="checkbox"/> Special characters	
User is required to change password (after first login)?	<input checked="" type="radio"/> Yes <input type="radio"/> No	(Changes in this configuration are applied after a server restart.)
Password expiration time (in days):	<input type="text" value="360"/>	(Password expiration will not be verified if set to zero or less. Changes in this configuration are applied after a server restart.)

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:** Specify 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.