User Security Settings

Last Modified on 09/22/2023 9:51 am PDT

This feature is applicable to GiveSmart customers who ONLY own the Fundraise module. If you own 2 or more GiveSmart modules, our Single Sign-On feature would override this functionality.

If you would like these controls for security settings, contact your Customer Success Manager or GiveSmart Fundraise Support to enable this feature for you.

Security Settings are an optional, granular approach to user account security. By clicking the Security Settings button you can change the complexity required for a user's password, have the passwords expire and more.

Mark users for password reset

Reset all users passwords so everyone needs to create a new one.

Password Strength

Set the level of complexity for passwords by requiring different types of characters: Upper case letters, Lower case letters, numbers and/or special symbols.

You can also set the minimum password length. By default a password cannot be less than 6 characters, and no password can ever be less than six characters. The maximum length of a password is 32 characters.

Failed Logins

When you enable Failed Logins, you can set the **Allowed failed login attempts** from 1-10. This setting will trigger the how may times the user can incorrectly guess their password before being locked out for a set amount of hours.

When the user has entered their password correctly and has reached the Allowed failed login attempts, they can be locked out of their account for 1-24 hours when you set the **Suspend user's account for** setting.

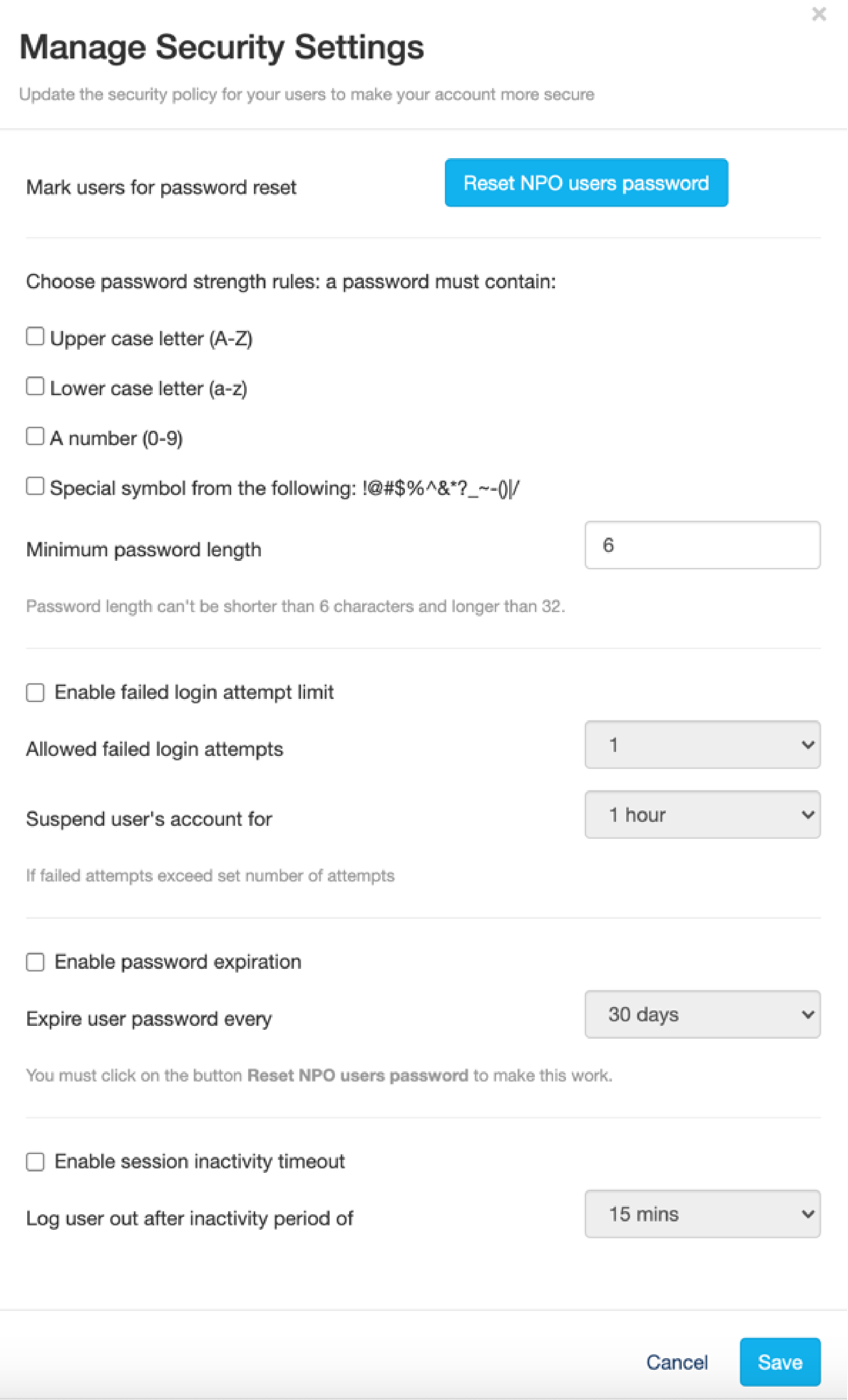
Password Expiration

If you Enable password expiration, you can set when a user's password will expire: every 30 days, 45 days, 90 days, or 180 days.

Session Timeout

With Enable session inactivity timeout checked, you can automatically log your users out of GiveSmart Fundraise if they have not touched it for a certain length of time, The Log user out after inactivity period of choices are: 15 mins, 30 mins, 45 mins, 60 mins, or 90 mins.

Make sure to save your settings once you've made changes.



Manage Security Settings

Update the security policy for your users to make your account more secure

Mark users for password reset

Choose password strength rules: a password must contain:

□ Upper case letter (A-Z)

□ Lower case letter (a-z)

□ A number (0-9)

□ Special symbol from the following: !@#$%^&*?_~-()|/

Minimum password length: 6

Password length can't be shorter than 6 characters and longer than 32.

□ Enable failed login attempt limit

Allowed failed login attempts: 1

Suspend user's account for: 1 hour

If failed attempts exceed set number of attempts

□ Enable password expiration

Expire user password every: 30 days

You must click on the button **Reset NPO users password** to make this work.

□ Enable session inactivity timeout

Log user out after inactivity period of: 15 mins