

Password Security Settings

We know that often the data our customers collect is highly sensitive and requires the utmost security. While for others, super-stringent security is not only unnecessary but also a nuisance. To accommodate our range of users, our password security settings allow [administrative users](#) to determine the precise level of security necessary to protect your Alchemer account.

Available Settings

Before we talk about settings available, let's get on the same page with some definitions:

- **Password Expiration:** This is an account level setting, selected by a Alchemer account administrator, that will automatically expire passwords after a certain time interval
- **Password Reset:** A password reset is a manual action taken by either the account administrator or the user to change the user's password

Password Security Setting Options

Password Expiration

- **Expiration Interval:** Set a time interval for password expiration (e.g. 3 days to 12 months)

Password Reuse Limitations

- **Password Reuse Rules:** Disallow password reuse either by password history or interval of time elapsed (e.g. every X passwords or every X months/years)

Password Complexity Rules

Basic:

- **Minimum/Maximum Length:** Specify a minimum and/or maximum password length
- **Require at least one upper and one lowercase letter:** Choosing this option requires all users' passwords to contain at least one uppercase and one lowercase letter
- **Require at least one number:** Choosing this option requires all users' passwords to contain at least one number
- **Require at least one special character:** Choosing this option requires all users' passwords to contain at least one special character

Complex:

- **Set up a complex rule (using Regex):** You can specify your own password pattern using Regex - Regular Expressions

Additional Protection

- Password cannot contain Alchemer user information (e.g. username, email address, user id)

Setup

1. Go to **Security > Settings** from the Left Hand Navigation Menu
2. **Expiration Interval** - Choose an expiration interval from the menu (optional)
3. **Password Complexity Rules - Basic**
 - a. Choose a min or max length (if you wish)
 - b. Choose from 3 basic settings (you know, if you want)
 - Require at least one upper and one lowercase letter
 - Require at least one number
 - Require at least one special character
 - c. Finally, indicate whether you want to restrict the use of Alchemer user information

Security > Settings

Password Settings

Expiration Interval: 6 Months

Reuse Limitations: every 10 passwords

Password Complexity Rules:
 No restrictions on passwords
 Create basic set of rules
 Create complex set of rules using regex

Minimum Length: 8
At least 8 characters

Maximum Length: 100
No more than 100 characters

Require at least one upper and one lower case letter
 Require at least one number
 Require at least one special character

Additional Protection: Password cannot contain application user information

4. **Password Complexity Description** - This is what displays to your users when creating a new password so they know what the password requirements are. You are responsible for this content, so make sure the rules are properly conveyed.

Description

Password Requires:
8 Characters
1 Capitalization
1 Special Character
Cannot Contain Alchemer user information

5. **Password Complexity Rules - Complex**

Using Regex overrides all Basic Password Complexity Settings (min/max length, require upper

and lowercase letters, numbers and special characters)

- a. Specify a Regex (Regular Expression) Rule
- b. Indicate whether you want to restrict the use of Alchemer user information
- c. Remember to provide a **Password Complexity Description** otherwise, your users will not know what the password requirements are!

How will new settings be applied to existing user passwords?

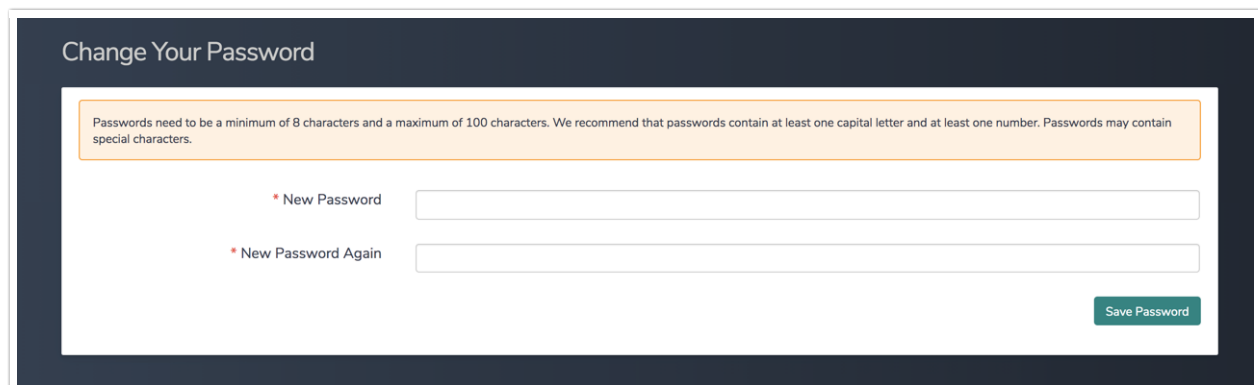
Should you choose to customize your users' password security settings, their existing passwords will be grandfathered until they are reset either by the account administrator or the user.

If you'd like for the settings to take effect right away, you have two options:

1. You'll need to manually reset all passwords (to do so go to your **Account > User Management > Users**. Select a user to edit and click **Reset Password**).
2. You can select the 3-day Expiration Interval to force a reset for all users in 3 days (if you're OK with waiting that long).

What will it look like for users?

The Password Complexity Description will display to the user when creating or resetting a new password:



The screenshot shows a 'Change Your Password' form. At the top, there is a title 'Change Your Password'. Below the title is a light orange box containing the following text: 'Passwords need to be a minimum of 8 characters and a maximum of 100 characters. We recommend that passwords contain at least one capital letter and at least one number. Passwords may contain special characters.' Below this box are two input fields. The first is labeled '* New Password' and the second is labeled '* New Password Again'. To the right of the second input field is a green button labeled 'Save Password'.

Related Articles