Enabling Strong Passwords 21.3.34

Last Modified on 11/17/2023 4:33 pm EST

Version 21.3

> **Path: Admin tab > Global Preferences > Security tab**

About

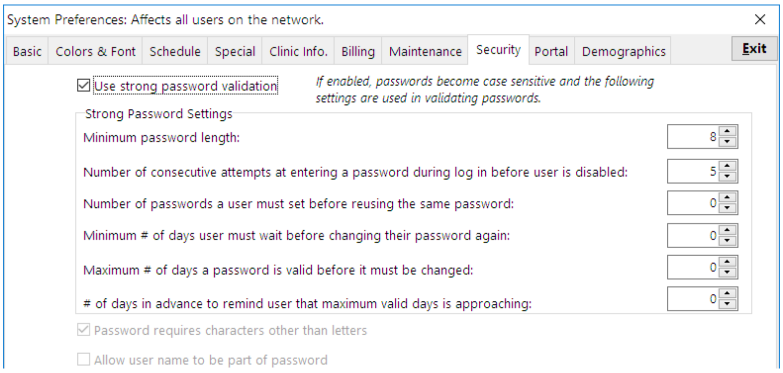
This article will go over the changes to the Strong Passwords enabled section in Global Preferences. Seethis article for the original.

> **Warning**: If an Administrator changes the password requirements for users by either disabling or enabling Strong Passwords, all user passwords will need to be reset.

Overview of Updates

- Resetting Passwords can be done by Admin users - no need to call Support.
- Users are given a default of 5 attempts to log in before they are locked out. See section below for more details.
- A new pop-up will appear if you attempt to exceed your “number of consecutive attempts” and fail to login (if you are a nonadmin user). Admin users get an infinite number of tries.

Enable Strong Passwords - Consecutive Attempts Updates



System Preferences: Affects all users on the network.

☑ Use strong password validation

If enabled, passwords become case sensitive and the following settings are used in validating passwords.

Strong Password Settings

Minimum password length:	8
Number of consecutive attempts at entering a password during log in before user is disabled:	5
Number of passwords a user must set before reusing the same password:	0
Minimum # of days user must wait before changing their password again:	0
Maximum # of days a password is valid before it must be changed:	0
# of days in advance to remind user that maximum valid days is approaching:	0

☑ Password requires characters other than letters

□ Allow user name to be part of password

Previously, when a practice had Strong Passwords enabled, the setting for**Number of consecutive attempts at setting a password before user is disabled** if left blank would assume the value of 2 and disabled users after 2 failed login attempts. This value of 2 never displayed in the field informing the user that this was occurring.

To improve this workflow we have done the following:

- Renamed the field to **Number of consecutive attempts at entering a password during login before user is disabled**to ensure it's clear to the user that after x attempts they will be disabled.
- Established a new **min/max** value for this field: 0-15
- Established a new **default** value for this field: 5
- If a practice has a value already set, the following will take place upon update:
  - If a practice has a value already set**between 0-15** we will respect that value and make**no changes to the system**.
  - If a practice has a value **greater than 15**, upon editing we will**change to 15**.

- If a practice **enables strong passwords for the first time**, we will **default in a value of 5** and it will display in the field.
- If a practice has a **NULL value**, we will **change to 5** and it will display in the field.

Note: This will only apply to NON ADMIN users. ADMIN users will NOT be disabled after x attempts and that is by design.