# Enabling Strong Passwords

Last Modified on 01/09/2024 2:46 pm EST

Version 21.3

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

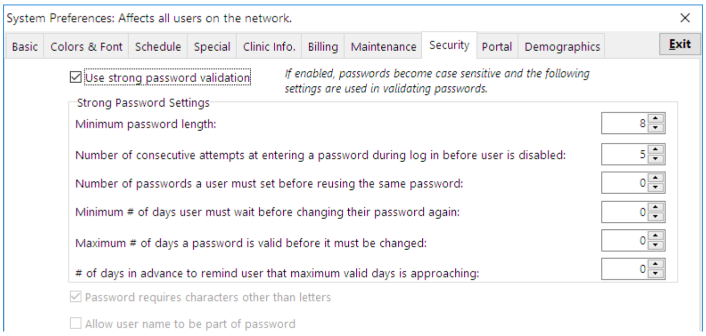
## About

Enabling strong passwords is a way to apply a defined list of password settings for all users. Click**here** to review OP's recommendations for creating and maintaining Strong Passwords.

> **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.

## Enable Strong Passwords

1. Navigate to the Security tab of the System Preferences window by following the path above.
2. Select the **Use strong password validation** checkbox.
3. Complete the password rules. Once rules are saved, if any of the rules are not followed during password creation, the password will be denied. These rules do not operate independently. Meaning, you must enable strong passwords in order to set all of the rules. The image below is followed by a description of what each setting means as it relates to what is entered in each field:



☑ 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

- **Minimum Password Length**: Users must enter a password of **8** or more characters.
- **Number of consecutive attempts at entering a password during login before user is disabled**If a user enters an incorrect password **5** times in a row, their login will be disabled.
  - Min/Max Value for this field: 0-15
  - Default value for this field: 5
  - A pop-up will appear if a non-admin user attempts to exceed the “number of consecutive attempts” and fail to login. Admin users get an infinite number of tries.
- If a user resets their password, and it is one of the last**6** passwords used, they will be prompted to enter another password.
- User must wait at least**7** days before changing their password again. This prevents the quick recycling of passwords to get back to a previously used password.
- Users must change their passwords every **30** days.

> **Note**: The value entered in the Minimum # of days setting must always be less than the value entered in the Maximum # of days setting.

- The user will be reminded **5** days before the 90-day maximum (set in the rule above) that their password is about to expire.
- The following two options are not editable:
  - Password requires characters other than letters
  - Allow user name to be part of the password

## Re-enable Disabled Users

Users are automatically disabled when they have exceeded the number of consecutive login attempts (per the set rules) or when a user's Login ID is changed. In the latter scenario, OP will also remove that user from all Membership categories in the Security Administration window. Users can be re-enabled by a Practice Administrator. To re-enable a user:

1. Navigate to the Security Settings window: **Admin tab > Security Administration**.
2. Select the user from the Users column in the left panel of the window.
3. Right-click the user's name and select **Edit User**.
4. Select the **Enabled** checkbox.

Version 21.2

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

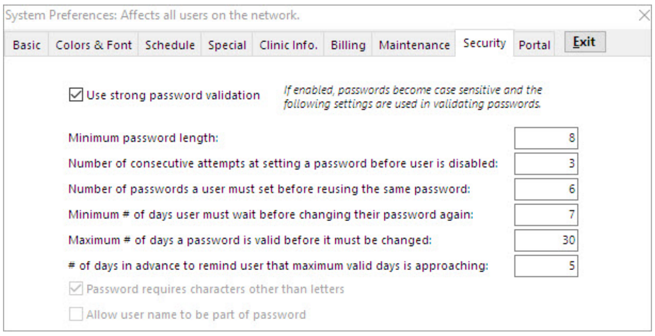
# About

Enabling strong passwords is a way to apply a defined list of password settings for all users. Click **here** to review OP's recommendations for creating and maintaining Strong Passwords.

> **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.

## Enable Strong Passwords

1. Navigate to the Security tab of the System Preferences window by following the path above.
2. Select the **Use strong password validation** checkbox.
3. Complete the password rules. Once rules are saved, if any of the rules are not followed during password creation, the password will be denied. These rules do not operate independently. Meaning, you must enable strong passwords in order to set all of the rules. The image below is followed by a description of what each setting means as it relates to what is entered in each field:



☑ Use strong password validation

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

| | |
|---|---|
| Minimum password length: | 8 |
| Number of consecutive attempts at setting a password before user is disabled: | 3 |
| Number of passwords a user must set before reusing the same password: | 6 |
| Minimum # of days user must wait before changing their password again: | 7 |
| Maximum # of days a password is valid before it must be changed: | 30 |
| # of days in advance to remind user that maximum valid days is approaching: | 5 |

☑ Password requires characters other than letters

☐ Allow user name to be part of password

- Users must enter a password of **8** or more characters.
- If a user enters an incorrect password **3** times in a row, their login will be disabled.
- If a user resets their password, and it is one of the last **6** passwords used, they will be prompted to enter another

password.
- User must wait at least **7** days before changing their password again. This prevents the quick recycling of passwords to get back to a previously used password.
- Users must change their passwords every **30** days.

**Note**: The value entered in the Minimum # of days setting must always be less than the value entered in the Maximum # of days setting.

- The user will be reminded **5** days before the 90-day maximum (set in the rule above) that their password is about to expire.
- The following two options are not editable:
  - Password requires characters other than letters
  - Allow user name to be part of the password

## Re-enable Disabled Users

Users are automatically disabled when they have exceeded the number of consecutive login attempts (per the set rules) or when a user's Login ID is changed. In the latter scenario, OP will also remove that user from all Membership categories in the Security Administration window. Users can be re-enabled by a Practice Administrator. To re-enable a user:

1. Navigate to the Security Settings window: **Admin tab > Security Administration**.
2. Select the user from the Users column in the left panel of the window.
3. Right-click the user's name and select **Edit User**.
4. Select the **Enabled** checkbox.