

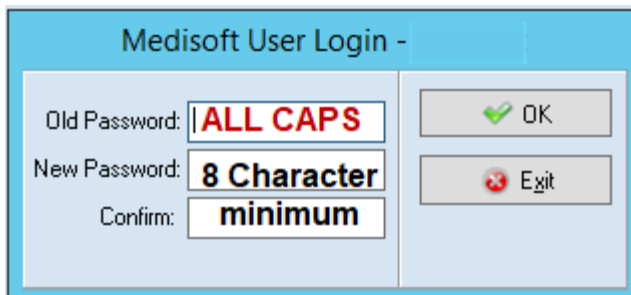
## CGM MEDISOFT Password Guide for version 26 and higher

Passwords are now case sensitive and have a minimum password length of 8 characters. It can contain numbers or alpha characters and IS now case-sensitive. If you try to save a password that doesn't meet the requirements, you will receive a warning.

- For customers upgrading from v25 or older; when you log in the first time, you must enter your existing password in **ALL CAPITAL LETTERS** to log into the program.
- If your existing password is 8 characters or longer, you will not be prompted to update it.
- If your existing password is fewer than 8 characters you will be prompted to create a new password. FIRST log in with your existing password **IN ALL CAPITAL LETTERS**, then you will see this message, select OK:



Then, follow the prompts to create a new password



## New practices

When you create a new practice, a system/administrator user with a password with access level of 1 (all access) is automatically created for you. The username for this password is **SYSTEM** and the password is **MEDISOFT1** (all capital letters). This new login has been added to the Tutorial database and will be added to any practice upon upgrade that has no active Users with an Access Level of 1 or has no Users created at all.

## Medisoft Mobile

CGM MEDISOFT Mobile app will remain case **Insensitive** for passwords. Mobile will still allow you to log into a device with your passwords, which were set in a pre-26 Medisoft version that is shorter than the new required 8 minimum after Medisoft has been upgraded to 26+ UNTIL that user's password is changed in CGM MEDISOFT.

## Login/Password Management

Use Login/Password Management to set the requirements and application of login rights and password usage. For example, you can set the length of valid passwords (minimum of 8 characters), the valid time frame in which a password can be used before it has to be changed, how long a user has to wait before reusing a password, and so on.

Go to File, Login/Password Management screen. Login user with Access Level 1 can set additional Password rules. The following are the default Version 26+ rules. Change the Maximum allowed attempts to 10 temporarily as users get accustomed to new pw requirements:

The screenshot shows a configuration window for 'Login/Password Management'. It is divided into two main sections: 'Password' and 'Login'.  
In the 'Password' section, there are five settings:

- Renewal Interval: 1 days
- Reuse Period: 0 days
- Minimum Characters: 8 (minimum 8) - This field is highlighted with a red border.
- Maximum Characters: 75
- Require Alphanumeric:

In the 'Login' section, there is one setting:

- Maximum allowed attempts: 10 - This field is highlighted with a yellow background.

On the right side of the window, there are four buttons: 'Save', 'Cancel', 'Help', and 'Reset to Defaults'.

For New User Setup training please contact CompuHealth Northwest at [support@chnwmd.com](mailto:support@chnwmd.com) or (360) 592-0926.