Improved Password Security for RMS

Introduced 2017

In response to requests for improved password security we have added an optional layer of requirements for passwords. Currently you can set the number of days between resets, the minimum length, the number of changes before a password can be repeated, the number of invalid attempts before an account is suspended, and the number of times in a day that passwords can be changed by any employee. To this we are giving you the option of requiring upper/lowercase letters, numbers, and symbols.

Be sure to read all the way through the instructions and then alert employees to the policies your facility has chosen to follow. If you have any questions, please give the office a call, 585-637-3240.

Table of Contents

Set-up

Step 1: Make sure that everyone can change his/her own password. If you are going to enforce the rules, then you don't want a line outside your office asking you to reset passwords!

Modules – Passwords. If you have *not* routinely set employees so they have the right to change their own passwords, then you will need to review all current employees and make sure they have a rights level of 1-4 (able to change their own password). This field is in the bottom left area of the window. Do NOT simply give everyone a level 5. That would be counterproductive.

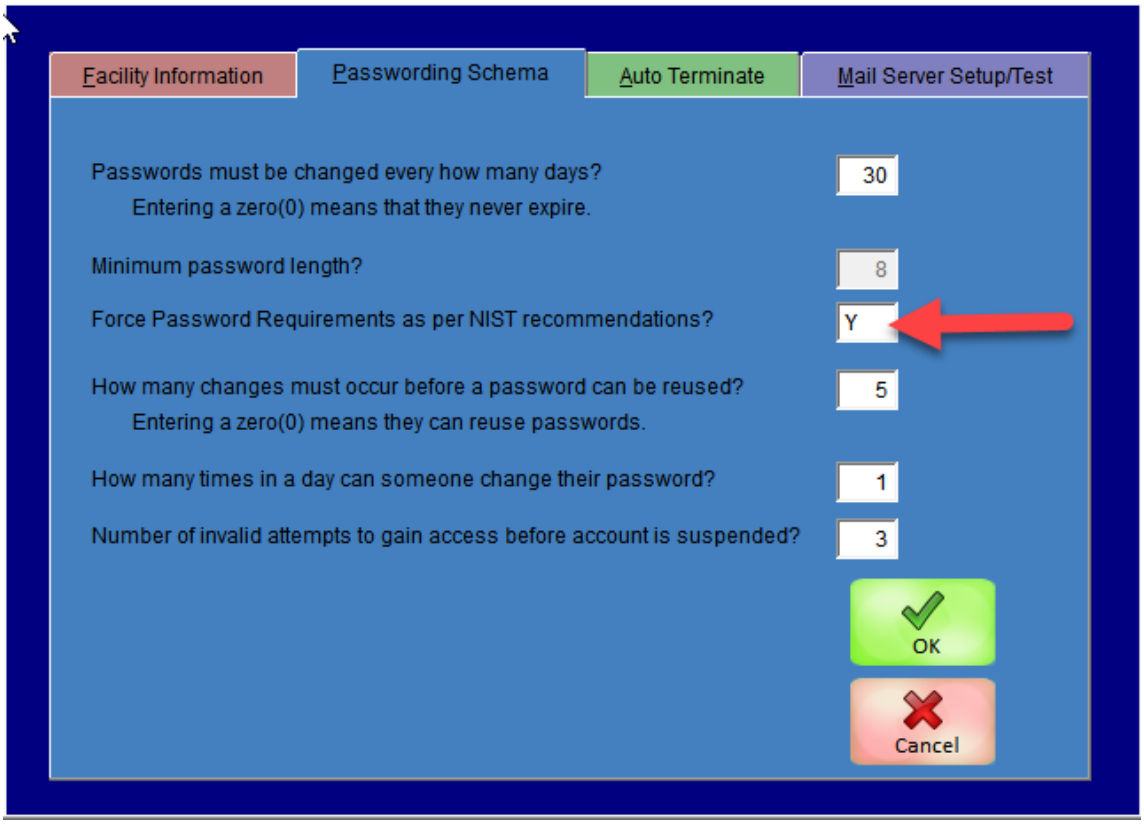
Step 2: ADT – Utilities – System Configuration – Passwording Schema tab (second tab, blue)
For those facilities who have been using the older enhanced password requirements, all of your settings should remain intact. However, realize that there is an additional question now, third bullet below. For those of you who are investigating this for the first time, we will review all of the options:

- *Passwords must be changed every how many days?* How often do you want to require employees to change passwords? If your policy requires changes every month, then you will

want to set this to 30. If you are never requiring changes to passwords then a 0 (zero) means they will never expire.

- *Minimum password length.* If you will be using the NIST requirements below, then you can leave this 0. If you will not, then you may want to establish a minimum length. Length needs to be between 0 and 10.
- *Force Password Requirements as per NIST* (National Institute of Standards and Technology, a branch of the US Department of Commerce) *recommendations?* This means that requirements of a minimum length of 8 along with 3 of the following – uppercase letters, lowercase letters, symbols, numbers – must be in your password before you will be allowed to save.
- *How many changes must occur before a password can be reused?* A zero means that they can reuse passwords. The number must be between 0 and 5.
- *How many times in a day can someone change their password?* How many resets are you going to allow your employees to make in a day. A zero here means they are unlimited in the number of changes they can make in any single day. The number must be between 0 and 3.
- *Number of invalid attempts to gain access before account is suspended?* How many times can an employee type in their password incorrectly before their account will need to be reset? You don't want to make this too short, i.e. 1 or 2 if you are going to use NIST. Passwords will be cap sensitive so you want to allow for someone forgetting and having the cap lock on. Number must be between 0 and 5.

Below is an illustration of the Passwording Schema. Set values according to YOUR facility's policies.



First Login After Setup

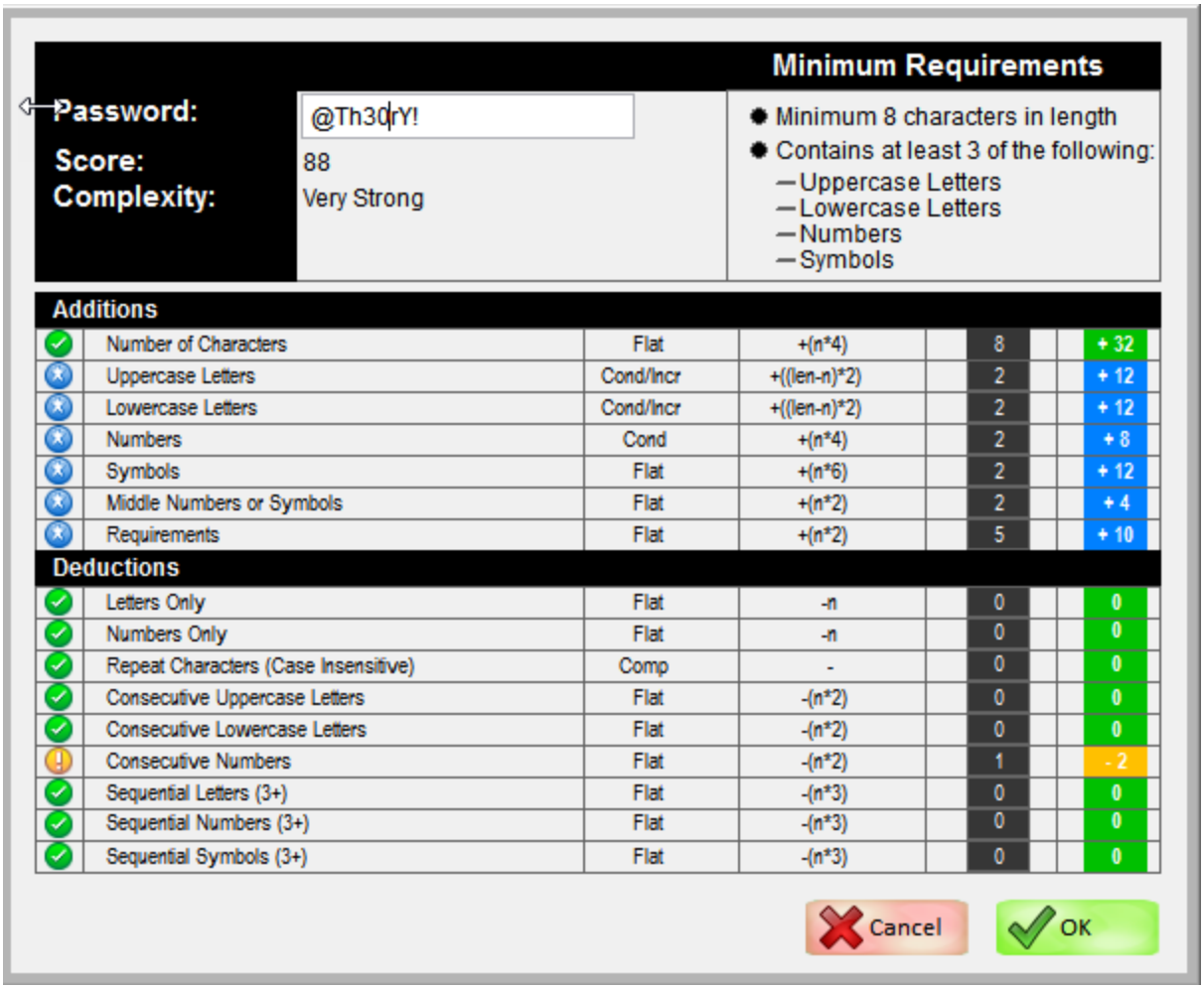
If you have elected to use NIST, keep in mind that now passwords are letter case sensitive. Employees need to know that when using their "old" passwords, ***they must enter it with all caps***. Passwords are not CASE sensitive. Whatever number of days you chose for the first question, will be the number of days employees have until they are required to create a new password.

How Do Employees Reset Passwords?

Modules – Passwords

Employees with Password Rights Level of 1 through 4

These employees have the right to set their own password but not to the full password module. When they click on Passwords in the Modules menu, they will see the screen below. As they enter a password, it will calculate a score and give them feedback. It will enforce a minimum of 8 characters and at least three of the following – uppercase letters, lowercase letters, numbers, and symbols.

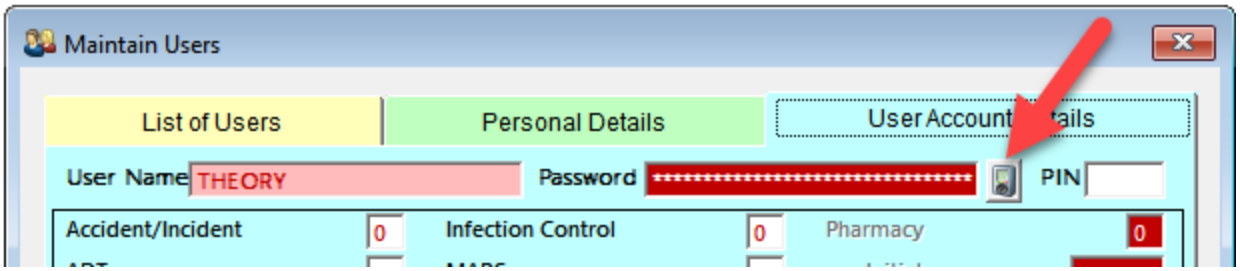


In the illustration above you can see that each position and character type gives you "points". Green boxes mean that you have met the minimum requirement (exactly 8 characters). Blue indicates that you have exceeded the minimum (2 symbols, 2 numbers and they are in the middle, etc.). The area at the bottom of the screen shows where you can make improvements, yellow areas. In our example, two "Consecutive Numbers" is shown as a weakness and would suggest that you could make the password stronger if you separated them.

As long as you meet the minimum requirements, you will be allowed to save.

Employees with Password Rights Level of 5

Whether setting up a new employee or resetting a password, they will see a new button located to the right of the Password field on the User Account Details tab in the Password module.

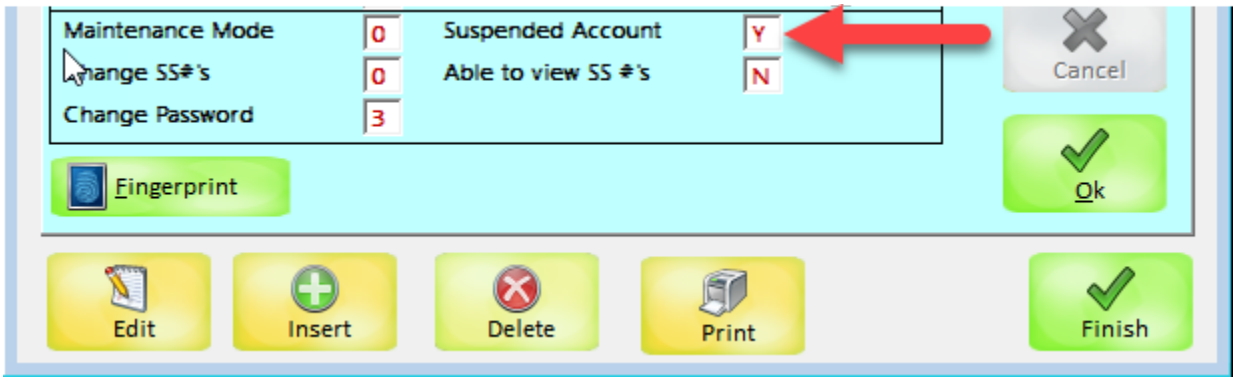


Clicking this button will display the same screen as above for users with rights 1-4. The same rules will apply as previously discussed.

Suspended Accounts

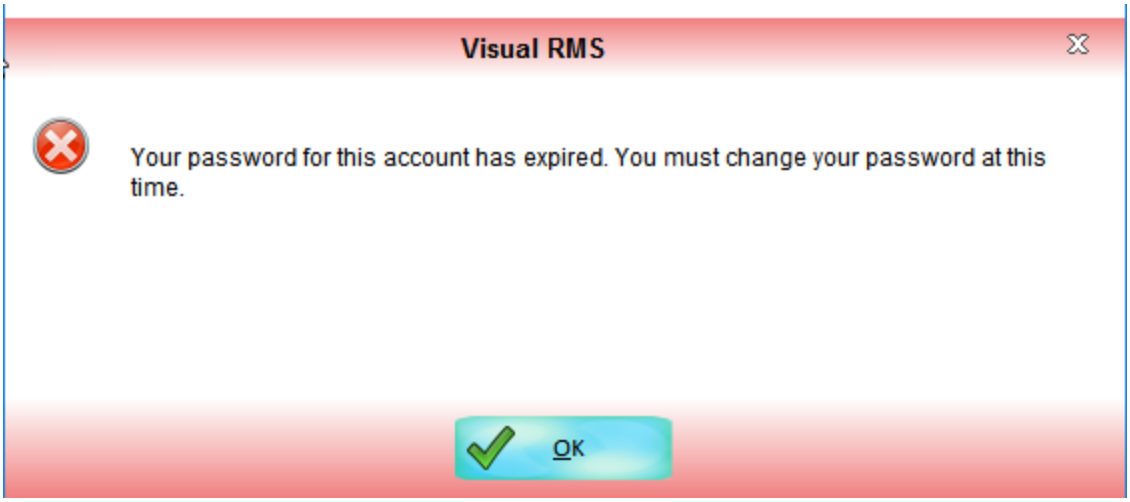
If an employee exceeds the number of invalid attempts, their account will be suspended and they will *not* be able to log into the system. They will need someone with a rights level of 5 to reset it for them (may also need assistance in resetting the password if they have forgotten it).

On the User Account Details tab in the Password module, at the bottom you will see a field called Suspended Account. If suspended, this will show Y(es). To reset, replace the Y with N(o). The account will then be active once again. The illustration below shows a suspended account.



When the Password Expires

If you set the requirement that the password needs to be changed every x days, then after that time period elapses, employees will be prompted to reset. Upon login with their old password, they will see this message,



When they click OK, they will be asked to enter their old password. Then they will click the button next to "New Password" in order to open the password screen. They will have all of the same prompts as illustrated under "Employees with Password Rights Level of 1 through 4" (see page 3).