User Administration

17/04/2025 12:35 pm BST

Summary

This sheet provides information on user administration and password policies.

Password Complexity Requirements

Passwords must meet the following complexity requirements:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
- Be at least 12 characters in length. Contain characters from 3 of the following 4 categories:

1. Uppercase characters (A through Z).
2. Lowercase characters (a through z).
3. Number/s (0 through 9).
4. Non-alphabetic characters (for example, !, $, #, %).

How long until a password expires?

Passwords will expire 42 days after they have been created/reset. This is to enhance the security and protect data

Why do passwords expire?

The reason password expiration policies exist, is to mitigate the problems that would occur if an attacker acquired the password to your system. These policies also help minimise some of the risk associated with other users accessing your login.

Why should you create individual users rather than one practice login?

All financial and clinical transactions performed in Merlin are audited by user login. This allows practices to analyse data entry. Auditing serves business purposes as varied as lost transaction recovery, fraud detection, disaster recovery and regulatory compliance.

In addition, if individual logins are used, practices can benefit from the system's user roles functionality.

Warning
If shared logins are used, passwords can be changed on expiration by any user. If the password change is not communicated around the practice, users will not be able to login.
It is not recommended to send passwords via email, or to store passwords in plain text on computers. Our recommendation is to setup individual logins for each individual within the business.

Renewing an expired Password

1. Select 'Ok' when presented with this message.
2. Enter a new password (Password must meet complexity requirements).
3. Confirm your new password.
4. Select 'Change'.
5. A notification will display 'Your password has been changed. Login with your new password to continue'.
6. Login with your new credentials.

Resetting a user's password

To perform this task, your user will require the user roles: 'Security - Edit User' and 'Security - Change User Password'.

If you do not have these user roles assigned, you will not be able to reset a password.

To reset your user or another user's password

1. Select Administration from the top menu.
2. Navigate to System > Security.
3. Select the relevant username from the list.
4. Select the 'Edit' button
5. Tick the 'Password' checkbox.
6. The password field will become active. Enter your new password.
7. Re-enter a new password.
8. Select the checkbox 'Change at Login' if you want the user to be prompted to change to a new password of their choice following first log in.
9. If you know the user's old password, enter it into the 'Enter old password to confirm'.
10. If you do not know the user's old password, tick 'Admin User Override'.
11. Select 'OK' and enter your username and password.
12. Select 'OK'.
13. A notification should display stating 'User successfully updated'.