# Table of Contents

Privacy/Security Features in Kroll™ ................................................................. 2
  User Groups .................................................................................................. 2
  User Group Permissions ................................................................................ 3
  Associating/Disassociating a Pharmacist ...................................................... 4
  Setting up a Temporary User ......................................................................... 5
  Kroll User Information Report ...................................................................... 6
  Store Configuration ....................................................................................... 9
  Passwords ...................................................................................................... 9
  Logging .......................................................................................................... 10
  Reports .......................................................................................................... 11
    Local Profile Access .................................................................................... 11
    Network DIS Access .................................................................................... 14
Privacy/Security Features in Kroll™

User Groups

1. From the Start Screen, select 'Edit / Users and Groups'.

2. Click on the 'User Groups' Tab.

3. Insert or edit a user group and assign a Privilege Level. A user that has the Change Users permission (see below) can only edit or create a user with an equal or more restricted (higher numbered) privilege number.

4. Users can then be assigned to this User Group. A user may belong to more than one group. If so, they will be granted any permission if that permission is enabled in any one of the groups they belong to.

A user can also be added to a user group when creating or editing an individual user record.
User Group Permissions

1. From the Start Screen, select ‘File/Configuration/Permissions’.

2. Select the appropriate User Group.

The following permissions are related to Privacy/Security and when checked, users belonging to that group will be able to perform the action:

- View Patient
- Allow Patient changes
- Allow Running Reports for All Patients
- View Credit Card Numbers
- Allow Credit Card Password Management
- Allow Viewing History Records
- Allow Unlocking user accounts of lower privilege level
- Change Users
- Change Store Config
- Change User Permissions
Associating/Disassociating a Pharmacist

In order for a technician or an assistant to perform functions on behalf of a pharmacist, the pharmacist must associate those users to his/her account. If a user has not already been associated and a function being performed requires the association, the ‘Pharmacist Association Form’ will automatically appear. Alternatively, the association can be set proactively by choosing File > Users > Associate Pharmacist.

When associating assistants/technicians to a pharmacist, set a specific time in the ‘Association Expires today at’ field. A suggestion might be to enter the time when the pharmacist’s shift is ending. When the time is set, the association will automatically expire at that time, forcing a new association to be required for this assistant/technician if they are still using the system.

A pharmacist user can also disassociate all users currently associated with their account at any time by selecting File > Users > Disassociate Pharmacist. This immediately terminates any associations regardless as to the expiry time previously configured.
Setting up a Temporary User

If an individual will only be working at this pharmacy for a temporary period, create a temporary user account.

Ensure that a date is recorded in the ‘Expires on’ field. When this date is achieved, the user account becomes inactive automatically.
Kroll User Information Report

This report is useful in identifying user accounts of former employees that you want to inactivate.

1. From the Start Screen, select Reports > Administration > User Information Report.
2. When set up as noted, the report generated looks as shown in the image below. The first few pages will provide details of the **User Group Permissions** set up in your system.

The last page will note all user accounts currently within the system.
Any user account for an individual listed on the report that is no longer employed can then be easily disabled. Navigate to the ‘User Information’ screen and check the Disabled box.
Store Configuration

1. From the Start Screen, navigate to File > Configuration > Store > Security.

The following sections within security are applicable to Privacy and Security.

Passwords

1. **Min password length** – defines the minimum password length (minimum number of characters).

2. **Min password age** – defines the minimum number of days a password must be used until it can be changed.

3. **Force password change** – defines how often a user must change their passwords.

4. **Prevent usage of X previously used passwords** – defines how often a password can be reused.

5. **Disable user after X failed attempts** – X represents the number of unsuccessful log in attempts that can be made by a user before the user’s account is locked out.

6. **Force password change for new users** – when checked any new user will be prompted to enter in a new password upon first log in.
7. **Enforce complex passwords** – when checked opens up the other 2 options and requires a minimum password length of at least 8 characters.
   - **Force the use of X numbers in password** – X = the minimum number of numeric characters in the password.
   - **For the use of X symbols in the password** – X = the minimum number of symbols, such as !, @, $, etc., in the password.

8. **Blank screen** – defines the number of minutes of inactivity on a workstation before the screen blanks out

9. **Require User ID for every Rx** – when checked, the user is prompted to enter in their user ID for each Rx which will then be saved against the Rx record. When unchecked, the user ID of the person logged into the workstation will be saved against each Rx processed.

10. **Require password After no Rx Activity in X minutes** – X = the number of minutes of inactivity that need to elapse before a user is forced to login.

11. **Allow Password Recovery With App** – when checked allows users with the appropriate permissions to reset their passwords using the Google Authenticator App.

**Logging**

1. **Log Rx Reprints, Log Rx Modifies, Log AR modifications, Log AR Deletions, Log Credit Card Access and changes, Log User information access and changes**: When checked, the user is required to enter a reason for the change. This reason, along with the user who made the change, will be recorded and made available in the ‘Security Audit Report’.

2. **Restrict and Log running of reports for all patients** – when checked will force the user to enter in their user name and password. If they do not have permission to run reports for all patients, the system will not let them continue.

3. **Log On Hand changes** – when checked, forces extra information to be entered when making a manual on hand change in a drug card
   - **Require User Log in** – when checked, will force the user to enter their user name and password for each on hand change
   - **Only Log for drug schedules** – can refine the logging of on hand changes to selected drug schedules. Leaving the field blank will apply logging to on hand changes to any drug in any schedule.
Reports

Local Profile Access

1. When accessing the ‘Security Audit Report’, the screen below displays. Under the ‘Selection’ Tab – you can define what you want to include on the report.

2. **Patient Tab** – define which patients you want to include on the report.
3. **Options tab** – provides more opportunity to fine tune the report content.

4. To see accesses to patient records, place a check beside **Print patient accesses**.
Based on the above criteria, the first page of the report would look as shown below.
Network DIS Access

1. When accessing the ‘Patient Network Audit Report’, the following screen displays. The ‘Selection’ Tab – provides you with the ability to define the date range and for which patients you want to generate the report.

2. Options Tab – can force the report to page break on patient
The report looks as shown below:

NOTE: This report can be quite lengthy, it is suggested that you Preview the report first.