



Version 4.0

User Management

The routine provides the way to add, edit or delete the user records in the system. It also includes the mechanism to grant or revoke the permissions to the users, to access the system resources. This routine is available to only users who have the appropriate permission to access this routine. A user with a permission to access this routine, is able to create or edit the other users but in order to delete any user, a separate permission is required. Any user with all the permissions won't be able to delete him/her self, though.

Procedure – How to Add a new User

When this routine is accessed, by default, it is in the 'SEARCH' mode. Change its mode to the 'ADD' mode by clicking the Button labeled 'New'. The background color of the User Name, Name, Password and Confirm Password will change slightly. Type in a unique 8 to 20 characters long, the required User Name. The uniqueness is verified by the system. Type in the required user's full Name (up to 60 characters long). Type in the user's Email address (optional). Following the Procedure – How to grant or revoke Permissions, assign the appropriate permissions. Type in the required Password following the guideline 'Password Characteristics' given below. Type in the Password again in the Confirm Password field.

Procedure – How to grant or revoke permissions

The procedure is the same for a new user being created or an existing user being edited. A permission button displaying 'No' means the user does not have this permission and the button displaying 'Yes' means the user has the permission to this access. A permission button can be toggled between 'No' and 'Yes' by clicking it or by pressing the <SPACE BAR> when the button has the focus. A recommendation on granting and revoking permissions according to the designation of the user, may be accessed by

choosing the user type in the 'User Type' choice list. For example choosing an Administrator in the 'User Type' will grant all the permissions at once, a typical administrator would require. Of course, this permission selection is further customizable. You don't have to follow the PROLIS recommendations on granting and revoking permissions according to the user designation. The tool is available as an initial guideline. Always use your Organization's policy and the employee structure you have, as a guideline to control security.

Permissions Listing

01. Customer Service:

A user needs to have this permission granted, to access the 'Customer Service' routine. Typically, users of non-technical nature, responsible to correspond with physicians, patients and other clients inquiring about routine business and services, require this permission granted. Some times the Lab Director and the supervisor (if capable of Result Interpretation) is also granted this permission.

02. Accession:

A user needs to have this permission granted, to access the routine 'Accessioning'. Depending upon the individual organization's setup, these users could be of technical or non-technical nature. In smaller reference labs and Physician Office Labs (POL), technologists perform this function and should have this permission granted.

03. Result Entry:

Typically a Technologist or a result entry Clerk needs to have this permission granted, to access the routine 'Result Entry'. The user responsible to review and release results, would also require this permission granted. The user with this permission only, is not able to release results.

04. Result Release:

A user responsible to review and release results, requires this permission granted, typically along with 'Result Entry' permission. For example a Technologist (if allowed to release results, Technical Supervisor, General Supervisor, Lab Director and the Lab Manager (if possesses technical capabilities). One should not get confused between the Result Interpretation requirements and those of Result Release and Review. The Result Review and Release process should be used to capture the typographical errors and any unacceptable data sent by the Lab Equipment Interface.

05. Quality Control Layout:

This permission handles the Quality Control Layout routine. The Quality Control result entry is not under this permission control, rather it is under Result Entry permission.

06. Test Management:

A dictionary routine to manage Analytes, Groups, Profiles and Worksheets, can only be accessed by the user if this permission is granted.

07. Billing

This permission controls all kind of billing.

08. Report Build:

This permission controls the routine to register the Crystal Report files in the system and the report specific user permissions to process reports.

09. Report Process

This permission enables the user, to access the report processing area in the PROLIS.

10. Hard Deletion:

It is a special permission without which the user is not able to delete any Dictionary Item, even with the

granted permission to manage the Dictionary Item.

11. Soft Deletion:

Some items in the system, can not be hard deleted. This permission is required to handle those items.

12. System Config:

System wide settings are controlled by this permission.

13. User Management:

The access of the routine being described, is controlled by the User Management permission.

14. Dictionary

Most of the dictionary building routines in general, are controlled with this permission. A couple of dictionary building routines like Component building and the QC Layout, have their own dedicated permissions.

15. Dictionary on the Fly:

A permission to handle all the supplementary routines to major Dictionary routines. These supplementary routines are used within the Accessioning routine. Supplementary routines include 'Supplementary Provider Management', 'Supplementary Insurance Management', 'Supplementary Client Management' and 'Supplementary Patient Management'.

16. Account Receivable:

This permission controls all the routines of Accounts Receivables except Accounts Receivables report processing.

17. Custom1:

18. Custom2:

Sample Users

Name	User Name	Designation	Manager	Password	Permissions granted
Greg Salvadore	gsalvadore	Administrator	Tech Support	regvad304	All, All reports
Dr. Jonathan Meyer	jmeyer01	Director	Administrator	shirly001	1,2,3,4,5,6,9,11,15 and all reports
Christin Ompipur	comnipur	Supervisor, Tech	Director	nycpolice8	1,2,3,4,5,6,8,9,10,11,12, 14,15 and all reports
Sumen Shivdasani	shivdasani	Technologist	Supervisor	inasadvihs	2,3,4,5,9,11,15 and all reports
Michael Moore	michaelm	Accessioner	Supervisor	mleahcim	2,9,15 and no report