



LabSys LIMS v3.00

What's New

Version 1.0

LabSys Ltd.

Purpose of this Manual

The purpose of this manual is to list the new and revised functions of LabSys LIMS for v3.00

LabSys Limited.
140 Slaney Close,
Dublin Industrial Estate,
Glasnevin, Dublin 11,
IRELAND

Tel: + 353 1 660 7744

Fax: + 353 1 668 1329

Internet: www.labsys.ie

labsys lims v3.00 whats new.doc

© 2002 LabSys Ltd., All Rights Reserved.

LabSys and LabSys LIMS are trademarks of LabSys Ltd., other Patents Pending. Other product, company and services names mentioned herein may be trademarks, registered trademarks or service marks of their respective holders.

Contents

| | |
|--|----------|
| LabSys LIMS v3.x | 4 |
| Changes in Functionality in v3.00 | 5 |
| FDA 21 CFR Part 11 - Main Functions and Interfaces | 5 |
| Assumptions/Prerequisites | 6 |
| Out of Scope | 6 |
| Audit Trails | 6 |
| Electronic Signatures | 6 |
| Application Security | 7 |
| Windows Username and Password Authentication | 7 |
| Database Username and Password Authentication | 7 |
| Application Timeout | 7 |
| What's New in LabSys LIMS v3.00 | 8 |
| QC LIMS | 8 |
| Sample Groups | 8 |
| Specification Instructions | 8 |

LabSys LIMS v3.x

The development of LabSys LIMS 3.x is focussed on the requirements of the regulated industries, primarily the Pharmaceutical industries. In this respect the majority of the enhancements and functionality changes are in providing a system that can be used to provide full compliance with FDA 21CFR Part 11. This is a wide-ranging and complex rule that affects many parts of LIMS and other systems.

Changes in Functionality in v3.00

The FDA regulation 21 CFR Part 11 final rule provides criteria under which FDA will consider electronic records to be equivalent to paper records, and electronic signatures equivalent to traditional handwritten signatures. The key objective in developing LabSys LIMS v3.00 was to ensure that it enables and supports compliance with 21 CFR 11.

Section 11.10 of the rule describes controls for closed systems, systems to which access is controlled by persons responsible for the content of electronic records on that system. These controls include measures designed to ensure the integrity of system operations and information stored in the system. Such measures include:

- (1) Validation;
- (2) the ability to generate accurate and complete copies of records;
- (3) archival protection of records;
- (4) use of computer-generated, time-stamped audit trails;
- (5) use of appropriate controls over systems documentation; and
- (6) a determination that persons who develop, maintain, or use electronic records and signature systems have the education, training, and experience to perform their assigned tasks.

Section 11.10 also addresses the security of closed systems and requires that:

- (1) System access be limited to authorised individuals;
- (2) operational system checks be used to enforce permitted sequencing of steps and events as appropriate;
- (3) authority checks be used to ensure that only authorised individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform operations;
- (4) device (e.g., terminal) checks be used to determine the validity of the source of data input or operation instruction; and
- (5) written policies be established and adhered to holding individuals accountable and responsible for actions initiated under their electronic signatures, so as to deter record and signature falsification.

FDA 21 CFR Part 11 - Main Functions and Interfaces

The main functional requirements are:

- †† Provide a system that allows records to have an audit trail associated with them.
- †† Provide a system that allows users to configure LabSys LIMS for Electronic Signatures, so that user ID and password must be entered to confirm the signing of each record.
- †† Distinguish between "continuous" and "non-continuous" sessions for the purposes of Electronic Signatures.
- †† Provide an integrated security approach using the underlying policies and functions of the Operating System.

These are further described in the following sections.

Note:

It is important to note that these functions are configurable and can be switched on and off. This ensures that those sectors that do not require such rigorous auditing and security are not forced to do so.

Assumptions/Prerequisites

There are a number of assumptions and prerequisites

- †† In order for Electronic Signatures to function as specified by the FDA guidelines, LabSys LIMS maximises the Windows security features that operate around system passwords, therefore NT is a prerequisite in order for Electronic Signatures to function as specified by the FDA guidelines.

- †† There are a certain amount of files contained within LIMS that are used to store information that do not have a maintenance function attached to them or a program that directly updates them. These files will not be audited.

- †† The user has the option of selecting a product by product class for auto approval. This will continue to function as it does currently and will not require an electronic signature at either the sample or test validation stage.

Out of Scope

- †† LabSys LIMS is considered to be closed systems under the definitions of the rule.

Audit Trails

A new Audit database has been created with equivalent sets of files for each in the LIMS database. This Audit database holds a direct copy of all the fields from the file being audited. These files will contain the existing fields for the files and the following additional fields:

- †† USERA = User Id who committed the transaction,
- †† TIMEA = System Time of Change,
- †† DATEA = System Date of the Change,
- †† TRNID = UPDATE, DELETE, BEORA = 1 character field for "Before" and "After" B/A record.

A new Audit Trail Inquiry has been provided to search and display the audit files for the LabSys LIMS tables. The program is designed to be as generic as possible, i.e. the user is allowed to specify the database, table and fields they wish to display.

Electronic Signatures

Part of the requirement for Electronic Signatures is that the signed record shall contain information associated with the signing that clearly indicates the following:

- †† The name of the signer,
- †† Date,
- †† Time,
- †† Meaning of the signing (Modified, Created, Approved).

Each relevant LIMS file has been changed to contain each of these fields, these fields being updated as part of the Signature process. A generic Electronic Signature dialog has

been added throughout the system and , if in use, the user will be forced to enter a valid password before a LIMS record is updated.

For example in Sample Validation, when a verdict is chosen for a sample the dialog will be presented, the user must enter their password, if the password is valid the sample is given a verdict, otherwise the sample remains unchanged. This ensures that the person performing the update is who they purport to be and not an impostor.

Application Security

The principal function of this change is to provide integrated application security. In previous versions of LIMS a user name and password were stored within the LIMS database for each LIMS user. From this version the system can be configured to use the underlying Operating System and Database security functions.

Windows Username and Password Authentication

The system has been changed to authenticate the entered username and password using the configured Windows security provider. If the authentication fails then the user is not allowed to connect to LIMS.

Database Username and Password Authentication

Following a successful authentication on Windows the entered username and password is authenticated against the LIMS database. This database could be:

- †† Progress
- †† MS SQL Server
- †† Oracle
- †† DB2/400

In order for the security functions to be fully implemented it will be necessary to have each user set up as both a Windows user and as a database user.

Application Timeout

Following a period of inactivity within the LIMS application the application will be “locked”, requiring the user to enter their password in order to access the application. The user is not logged off during this process, the application is merely locked in order to prevent unauthorised use while the system is unattended.

What's New in LabSys LIMS v3.00

QC LIMS

Sample Groups

The principal function of this procedure is to login/schedule either single or multiple sets of samples in to the system manually or through a scheduler. It should be possible to either maintain or Inquire into these Sample Groups.

This functionality makes it possible to set up repetitive sets of samples once and to have these scheduled automatically on a regular basis. For example Environmental samples may be required weekly, monthly and annually, It is now possible to set up this set of samples on a schedule and the system will automatically schedule the samples at the required time.

Specification Instructions

This new function provides a facility whereby users can enter and edit large amounts of Specification Instructions and comments for a product specification that can then be viewed and/or printed by the users. These instructions are not revision controlled within the document but will be revision controlled in the Specification context as they will be linked to a specific Specification.

These Specification Instructions are preferable to comments because comments do not allow the user to edit comments already entered and when a new version of a specification is created the comments may need to be rewritten entirely.

Editing Specification Instructions Document/Specification Maintenance.

Specification Maintenance allows linking of the Specification to a list of Specification Instructions based on Lab and Specification/Version. Instructions inserted are stamped with the entry date , time and user-id. Instructions that are updated are stamped with the modification date, time and user-id

Viewing Specification Document.

Various inquiries have been modified to allow for viewing of the Specification Instructions.

