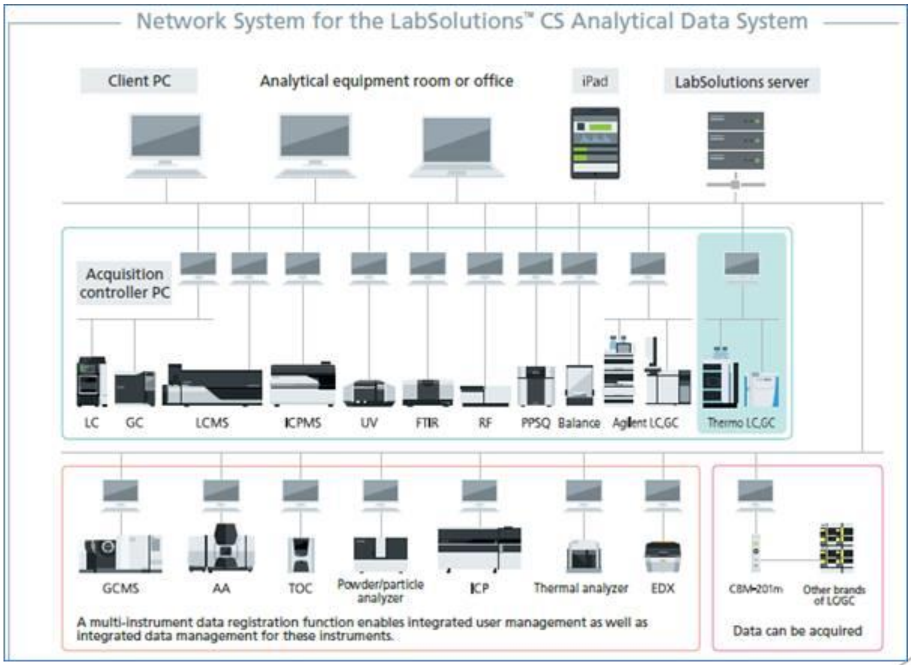
SHIMADZU
Excellence in Science

Shimadzu LabSolutions Software

Databases & Client\Server Version

Technical Controls built-in LabSolutions for 21 CFR Part 11 Compliance



Network System for the LabSolutions™ CS Analytical Data System

A multi-instrument data registration function enables integrated user management as well as integrated data management for these instruments.

Disclaimer

(1) Shimadzu Corporation retains the copyright over this document. The contents of this document must not be reproduced or copied in total or in part without the express permission of Shimadzu Corporation.

(2) The contents of this document may be changed without notice.

(3) Great care was taken when preparing this document. However, any errors or omissions contained may not be corrected immediately.

For technical enquiries, contact your Shimadzu representative.

Web http://www.ssi.shimadzu.com/

Phone Number: 1-800-477-1227

Table of Contents

Introduction

On August 20, 1997 the United States FDA (Food and Drug Administration) issued the regulations pursuant to 21 CFR Part 11. These regulations provide guidelines on using electronic records and electronic signatures (ER/ES) by defining the criteria under which electronic records and electronic signatures are considered to be trustworthy, reliable, and equivalent to paper records with handwritten signatures. It also provides guidelines for submission of electronic records to the FDA.

This paper describes the tools provided by the LabSolutions Database and Client/Server software to assist Shimadzu customers with 21 CFR Part 11 regulatory compliance.

Outline and Structure of FDA 21 CFR Part 11

The structure of 21 CFR Part 11 document is shown below:

Subpart A – General Provisions
11.1 Scope.
11.2 Implementation.
11.3 Definitions.

Subpart B – Electronic Records
11.10 Controls for closed systems.
11.30 Controls for open systems.
11.50 Signature manifestations.
11.70 Signature/record linking.

Subpart C – Electronic Signatures
11.100 General requirements.
11.200 Electronic signature components and controls.
11.300 Controls for identification codes/passwords.

Subpart A relates to general provisions, including definitions of terminology.

Subpart B and Subpart C cover the requirements for the software and data system. The equivalence between the requirements of Subpart B and Subpart C and the Shimadzu software is described below.

Definitions

Section 11.3 defines the terminology related to FDA 21 CFR Part 11.

11.3(b)-(3) Biometrics

The identification of an individual from physical characteristics, such as fingerprints.

11.3(b)-(4) Closed system

An environment in which system access is controlled by persons who are responsible for the content of all electronic records that are on the system.

11.3(b)-(5) Digital signature

Electronic signatures based on cryptographic methods for author identification and data protection.

11.3(b)-(6) Electronic record

Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

11.3(b)-(7) Electronic signature

A means of identifying an individual in a computer system that is the legal equivalent of a handwritten signature.

11.3(b)-(9) Open system

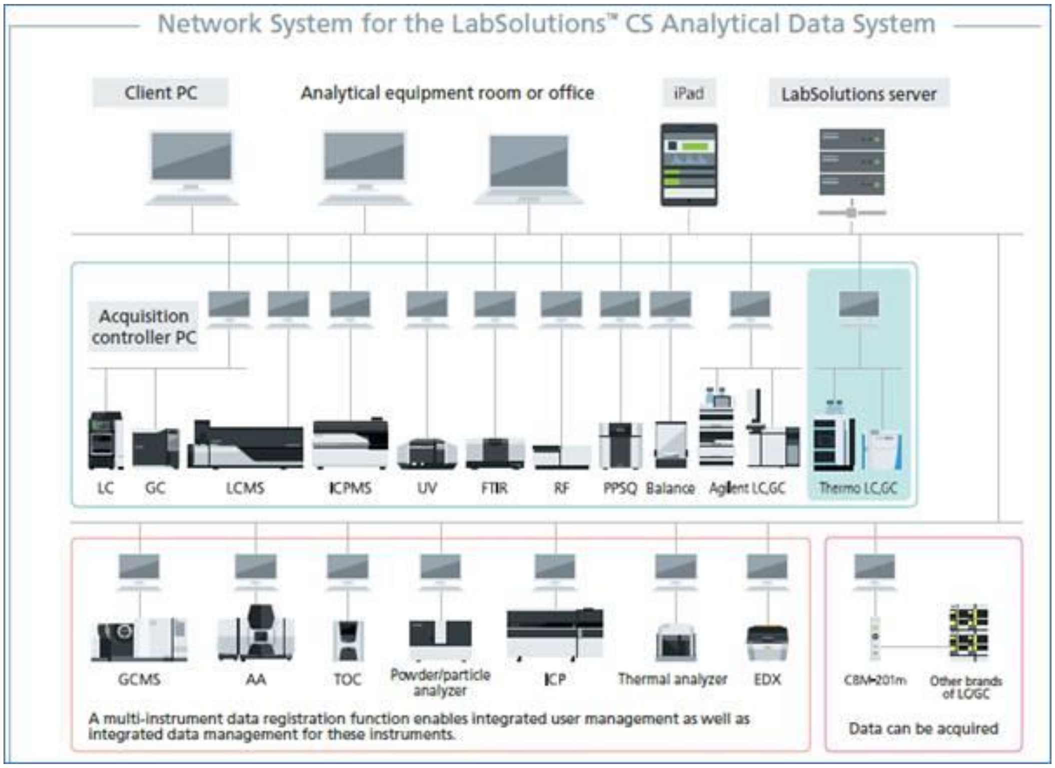
An environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Equivalence Between FDA 21 CFR Part 11 Requirements and Shimadzu LabSolutions Database and Shimadzu LabSolutions Client/Server Software

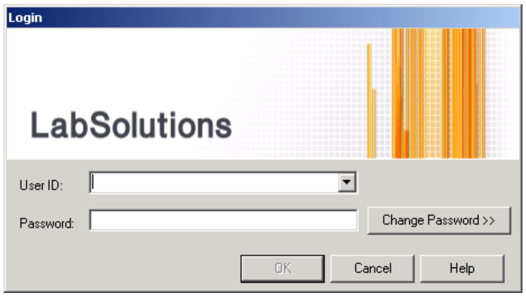
Basic Policy for FDA 21 CFR Part 11 Compliance

Shimadzu achieves FDA 21 CFR Part 11 compliance through integrated control of data for HPLC, GC, LCMS, ICPMS, UV, FTIR, RF, PPSQ, Balance, GCMS, AA, TOC, Particle Analyzers, Thermal Analyzer, and EDX instruments.

Shimadzu supplies products and technologies based on LabSolutions Database and LabSolutions Client/Server to assist with FDA 21 CFR Part 11 compliance for analytical data from laboratory instruments, such as chromatographs and balances.

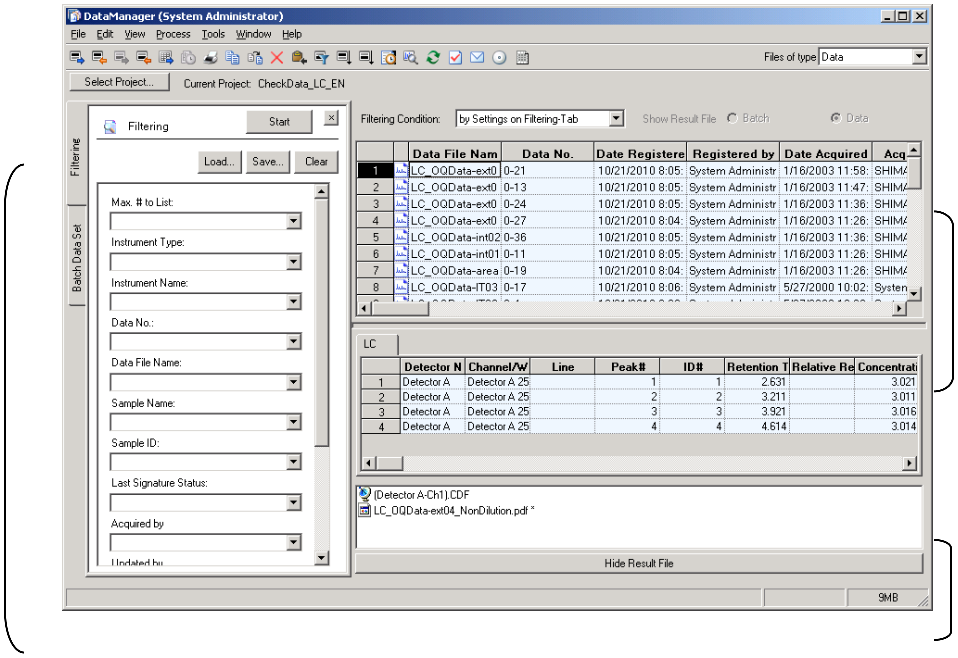

Network System for the LabSolutions™ CS Analytical Data System
Client PC
Analytical equipment room or office
iPad
LabSolutions server
Acquisition controller PC
LC
GC
LCMS
ICPMS
UV
FTIR
RF
PPSQ
Balance
Agilent LC,GC
Thermo LC,GC
GCMS
AA
TOC
Powder/particle analyzer
ICP
Thermal analyzer
EDX
CBM-201m
Other brands of LC/GC
A multi-instrument data registration function enables integrated user management as well as integrated data management for these instruments.
Data can be acquired

Access to LabSolutions Database and LabSolutions Client/Server software is controlled by User IDs and passwords. Linking to Windows XP / Windows 7 / Windows 10 and database management software (SQL Server) security functions achieves reliable data protection. Introduction of LabSolutions software can create a closed system as defined in provision § 11.3 of the Part 11 document.



LabSolutions Login Screen

To permit easy checking of data, the LabSolutions screen is divided into multiple areas as shown below. The interface is compatible with electronic signatures.



Files of type: Data

Current Project: CheckData_LC_EN

Filtering Condition: by Settings on Filtering-Tab

	Data File Nam	Data No.	Date Registere	Registered by	Date Acquired	Acq
1	LC_OQData-ext0	0-21	10/21/2010 8:05:	System Administr	1/16/2003 11:58:	SHIMA
2	LC_OQData-ext0	0-13	10/21/2010 8:05:	System Administr	1/16/2003 11:47:	SHIMA
3	LC_OQData-ext0	0-24	10/21/2010 8:05:	System Administr	1/16/2003 11:36:	SHIMA
4	LC_OQData-ext0	0-27	10/21/2010 8:04:	System Administr	1/16/2003 11:26:	SHIMA
5	LC_OQData-int02	0-36	10/21/2010 8:05:	System Administr	1/16/2003 11:36:	SHIMA
6	LC_OQData-int01	0-11	10/21/2010 8:05:	System Administr	1/16/2003 11:26:	SHIMA
7	LC_OQData-area	0-19	10/21/2010 8:04:	System Administr	1/16/2003 11:26:	SHIMA
8	LC_OQData-IT03	0-17	10/21/2010 8:06:	System Administr	5/27/2000 10:02:	Systen

	Detector N	Channel/W	Line	Peak#	ID#	Retention T	Relative Re	Concentrati
1	Detector A	Detector A 25		1	1	2.631		3.021
2	Detector A	Detector A 25		2	2	3.211		3.011
3	Detector A	Detector A 25		3	3	3.921		3.016
4	Detector A	Detector A 25		4	4	4.614		3.014

(Detector A-Ch1).CDF
LC_OQData-ext04_NonDilution.pdf *

Data
Filtering

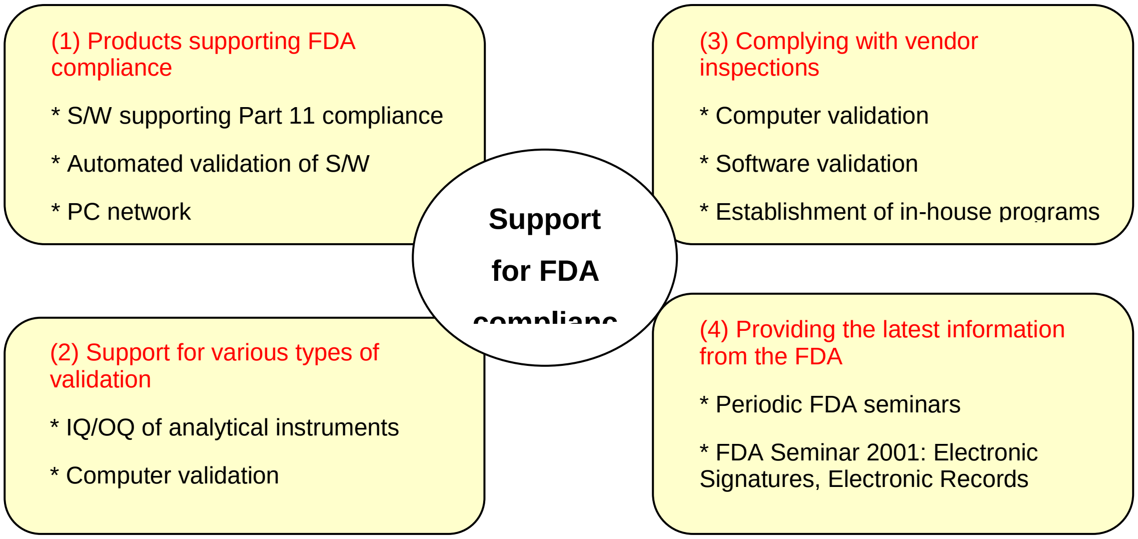
Select the
analytical
data here

Peak report
display

To support customer compliance with FDA regulations, Shimadzu compiles the latest information on FDA regulations, develops products based on this information, promotes customer education on compliance issues via seminars and other means, provides customer assistance and offers support for FDA inspections.

Customer demands regarding FDA compliance

(1) Products supporting FDA compliance (3) Complying with vendor inspections



(1) Products supporting FDA compliance

* S/W supporting Part 11 compliance

* Automated validation of S/W

* PC network

(3) Complying with vendor inspections

* Computer validation

* Software validation

* Establishment of in-house programs

Support for FDA complianc

(2) Support for various types of validation

* IQ/OQ of analytical instruments

* Computer validation

(4) Providing the latest information from the FDA

* Periodic FDA seminars

* FDA Seminar 2001: Electronic Signatures, Electronic Records

LabSolutions Database and Client\Server Software can be used to achieve FDA 21 CFR Part 11 compliance compatible with the following Shimadzu Hardware.

Shimadzu LC Systems

Shimadzu GC Systems

LabSolutions LCMS Systems

LabSolutions GCMS Systems

Shimadzu ICPMS Systems

Shimadzu UV Systems

Shimadzu FTIR System

Shimadzu RF Systems

Shimadzu PPSQ Systems

Shimadzu AA Systems

Shimadzu TOC Systems

Shimadzu Particle Analyzers

Shimadzu Thermal Analyzers

Shimadzu EDX Instruments

Shimadzu Balances

LabSolutions Database and LabSolutions Client/Server software can be used to help achieve FDA 21 CFR Part 11 compatibility for the listed Shimadzu programs.

Software configuration

LabSolutions Database and LabSolutions Client/Server software can used to maintain data and assist with 21CFR Part 11 compliance.

All data collected by the LabSolutions Database and LabSolutions Client/Server software is stored in a Secure, access-controlled SQL database.

Electronic Signatures can be added to any and all data within the LabSolutions Database and LabSolutions Client/Server software. The signatures are then stored with the data in the database.

Electronic records (Audit Trails) are kept for all data that is stored within the database.

All data in the LabSolutions Database and LabSolutions Client/Server software can be processed at will and then used to generate reports that can be printed on any printer that the computer hosting LabSolutions Database and LabSolutions Client/Server software has access to.

Data that is saved in the secure database can be browsed or searched using the LabSolutions Database and LabSolutions Client/Server software but only by people who have the proper permissions within LabSolutions Database and LabSolutions Client/Server software to access the data.

LabSolutions Database and LabSolutions Client/Server software keeps all old versions of data and reports and they can be recalled as needed.

LabSolutions incorporates security and user management functions that are independent of the hosts operating system features. A user name (User ID) and password must be entered before using these programs.

Software operating environment

LabSolutions Software runs under Windows XP professional 32 bit, or Windows 7 professional 32 and 64 bit, and Windows 10 professional 64bit.

The hard disk drive where LabSolutions is installed and the LabSolutions database is configured must be formatted as an NTFS (New Technology Filing System) drive.

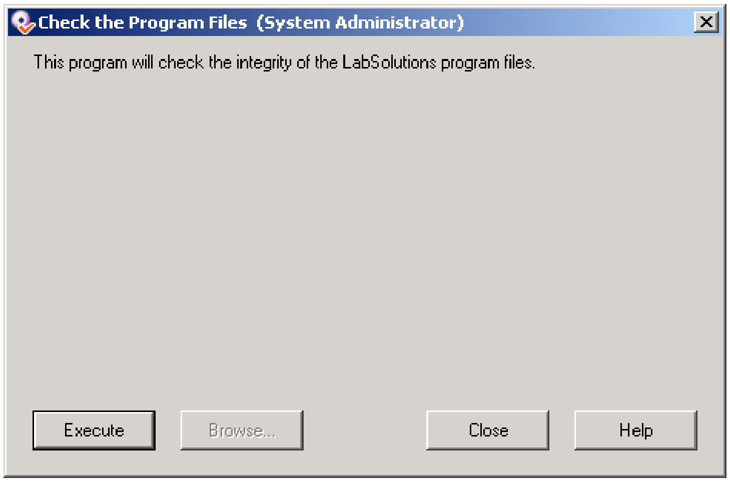
Subpart B Electronic Records

Sec. 11.10 Controls for closed systems

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records are incorporated as software functions and are verified to operate according to the specifications at the development stage. Therefore, when a customer conducts software validation, it is necessary to ensure that no alteration of the installed software has occurred. Shimadzu supports validation operations by issuing an IQ (Installation Qualification) Protocol to confirm that installation was conducted correctly and OQ (Operational Qualification) Protocol that defines periodic system checks.



Check the Program Files (System Administrator)

This program will check the integrity of the LabSolutions program files.

(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

Data generated by this system contains all the required information provided in the table below. This information is stored in a single file and cannot be separated, allowing for a complete record to be retained in a machine-readable format. An accurate report can also be produced in a human-readable form.

This capability to generate accurate and complete copies of data in both human readable and electronic form supports submission of reports for inspections.

LabSolutions Data File

Properties Information
Sample information (Sample Name, Sample ID, Vial No. etc.)
Names of files used for analysis and re-analysis
Names of users who created or edited data
Date and time when data was created or edited
Comments
Data Acquisition Information
Chromatograms
System configuration and instrument control methods

Data processing methods (original data; including peak integration programs)
Status information (analyzer operation log during data acquisition)
Batch table (for analysis batch processing data)
Data Analysis Information (including first analysis at the time of data acquisition)
Analysis results
Data processing methods (the latest data; including peak integration programs)
Data processing methods (audit trail log for analysis records)
Report format (for data outputted as a report)
Batch table (for re-analysis batch processing data)

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

- **Protection of records**

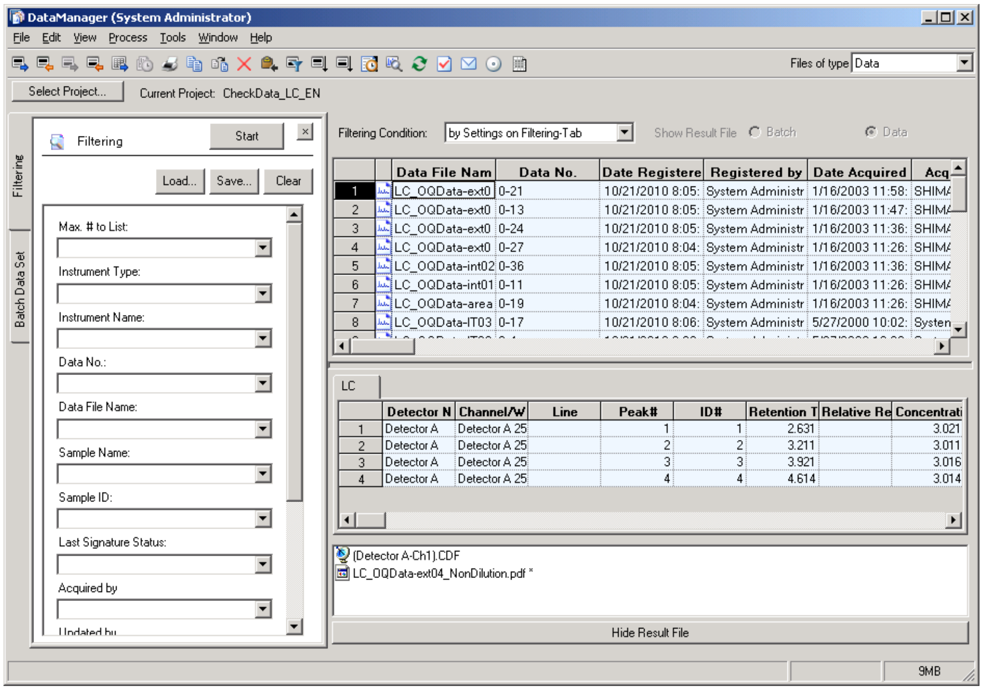
  Data files are stored together with meta data (methods, schedules, etc.) in a safe, access-controlled SQL Server database.

- **Rapid searching**

  LabSolutions search function allows for a ready record retrieval as data files are stored in a database.

- **Recovering records**

  Data can be archived to removable media, such as CD-R for long-term storage. This data can be referenced directly from the CD, without copying it back to the hard disk, and can be fully recovered to its original state from the database, when required.



Files of type: Data

Current Project: CheckData_LC_EN

Filtering Condition: by Settings on Filtering-Tab

Show Result File ○ Batch ● Data

Max. # to List:

Instrument Type:

Instrument Name:

Data No.:

Data File Name:

Sample Name:

Sample ID:

Last Signature Status:

Acquired by

Updated by

	Data File Nam	Data No.	Date Registere	Registered by	Date Acquired	Acq
1	LC_OQData-ext0	0-21	10/21/2010 8:05:	System Administr	1/16/2003 11:58:	SHIMA
2	LC_OQData-ext0	0-13	10/21/2010 8:05:	System Administr	1/16/2003 11:47:	SHIMA
3	LC_OQData-ext0	0-24	10/21/2010 8:05:	System Administr	1/16/2003 11:36:	SHIMA
4	LC_OQData-ext0	0-27	10/21/2010 8:04:	System Administr	1/16/2003 11:26:	SHIMA
5	LC_OQData-int02	0-36	10/21/2010 8:05:	System Administr	1/16/2003 11:36:	SHIMA
6	LC_OQData-int01	0-11	10/21/2010 8:05:	System Administr	1/16/2003 11:26:	SHIMA
7	LC_OQData-area	0-19	10/21/2010 8:04:	System Administr	1/16/2003 11:26:	SHIMA
8	LC_OQData-IT03	0-17	10/21/2010 8:06:	System Administr	5/27/2000 10:02:	Systen

LC

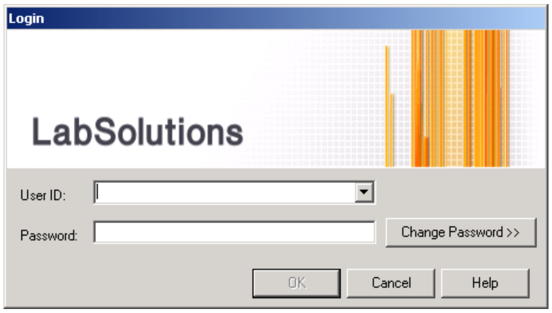
	Detector N	Channel/W	Line	Peak#	ID#	Retention T	Relative Re	Concentrati
1	Detector A	Detector A 25		1	1	2.631		3.021
2	Detector A	Detector A 25		2	2	3.211		3.011
3	Detector A	Detector A 25		3	3	3.921		3.016
4	Detector A	Detector A 25		4	4	4.614		3.014

(Detector A-Ch1).CDF

LC_OQData-ext04_NonDilution.pdf *

(d) Limiting system access to authorized individuals.

Access to the system is limited, as the system requires input of a User ID and password before the system can be used. LabSolutions allows access to each function to be set separately for each user.



User ID:

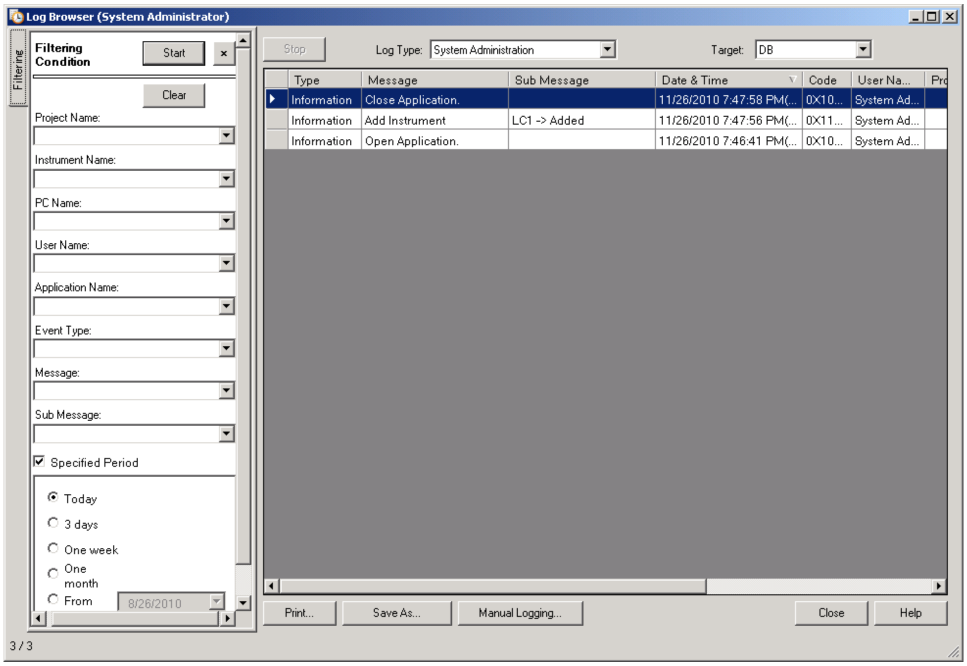
Password:

(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

LabSolutions software maintains three different logs: the data log that records operations conducted on the analytical data; the system log that records system logins, logouts and changes to the environment settings; and the user authentication log that records changes to user registration details. These logs are generated automatically by the software and kept in database.

These logs are mutually independent as the method of control is different for each one: the data log is controlled along with the data it relates to and the system log is saved separately from specific data.

Each time a new analysis or data reprocessing is performed, calculated results, method, schedule and raw data is automatically saved in a database along with the audit trail. This data is protected from being overwritten or deleted, thereby ensuring an adequate audit trail capability.



☑ Specified Period

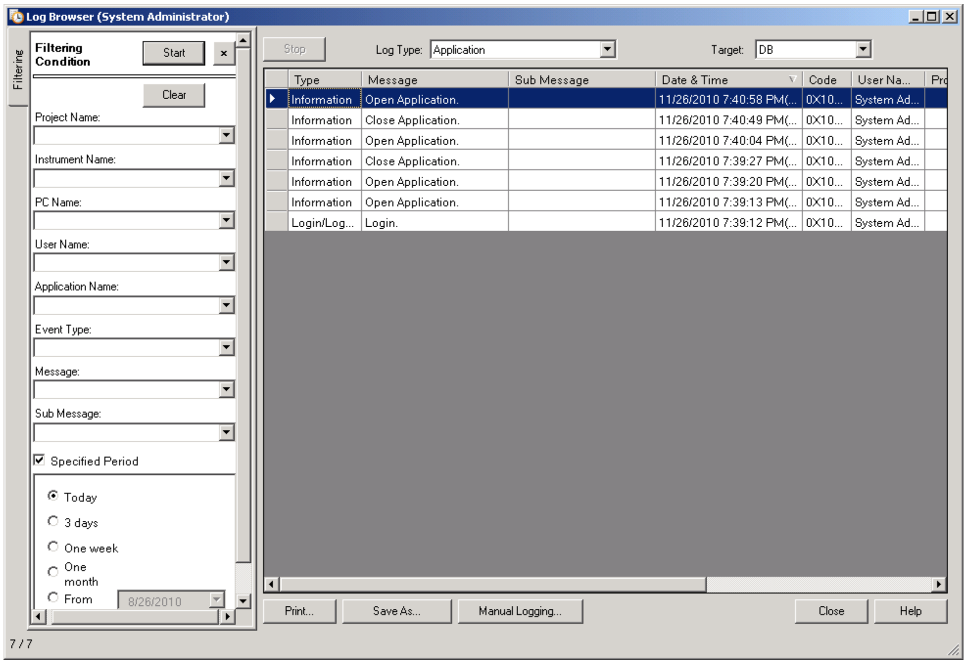
● Today
○ 3 days
○ One week
○ One month
○ From 8/26/2010

Log Type: System Administration

Target: DB

	Type	Message	Sub Message	Date & Time	Code	User Na...	Pro
▶	Information	Close Application.		11/26/2010 7:47:58 PM(...	0X10...	System Ad...	
	Information	Add Instrument	LC1 -> Added	11/26/2010 7:47:56 PM(...	0X11...	System Ad...	
	Information	Open Application.		11/26/2010 7:46:41 PM(...	0X10...	System Ad...	

System Administration Log



Project Name:

Instrument Name:

PC Name:

User Name:

Application Name:

Event Type:

Message:

Sub Message:

☑ Specified Period

● Today
○ 3 days
○ One week
○ One month
○ From 8/26/2010

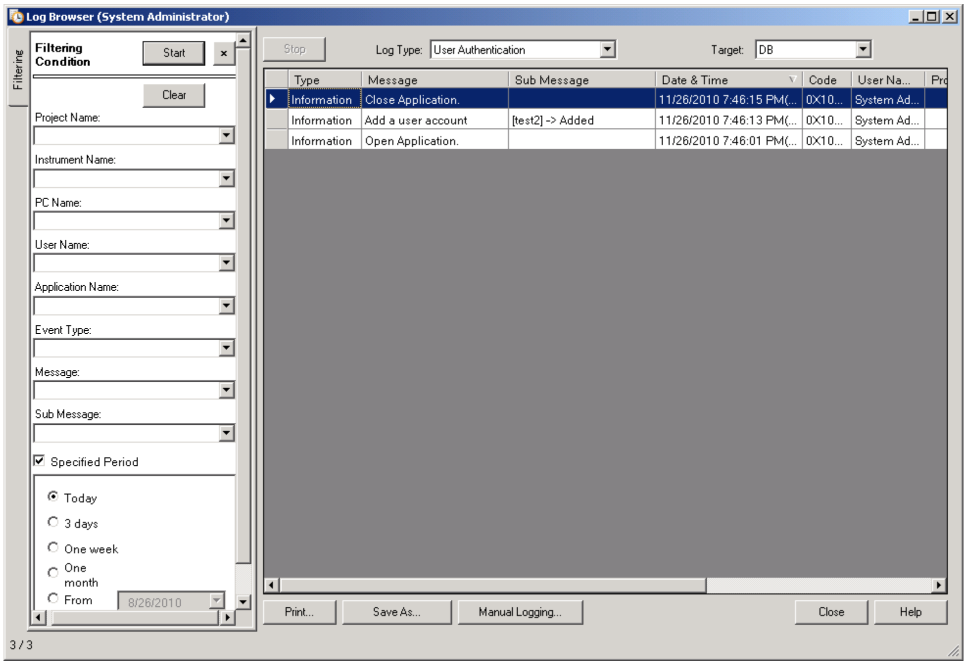
Log Type: Application

Target: DB

Type	Message	Sub Message	Date & Time	Code	User Na...	Pro
Information	Open Application.		11/26/2010 7:40:58 PM(...	0X10...	System Ad...	
Information	Close Application.		11/26/2010 7:40:49 PM(...	0X10...	System Ad...	
Information	Open Application.		11/26/2010 7:40:04 PM(...	0X10...	System Ad...	
Information	Close Application.		11/26/2010 7:39:27 PM(...	0X10...	System Ad...	
Information	Open Application.		11/26/2010 7:39:20 PM(...	0X10...	System Ad...	
Information	Open Application.		11/26/2010 7:39:13 PM(...	0X10...	System Ad...	
Login/Log...	Login.		11/26/2010 7:39:12 PM(...	0X10...	System Ad...	

7 / 7

Application Log



Project Name:

Instrument Name:

PC Name:

User Name:

Application Name:

Event Type:

Message:

Sub Message:

☑ Specified Period

● Today
○ 3 days
○ One week
○ One month
○ From 8/26/2010

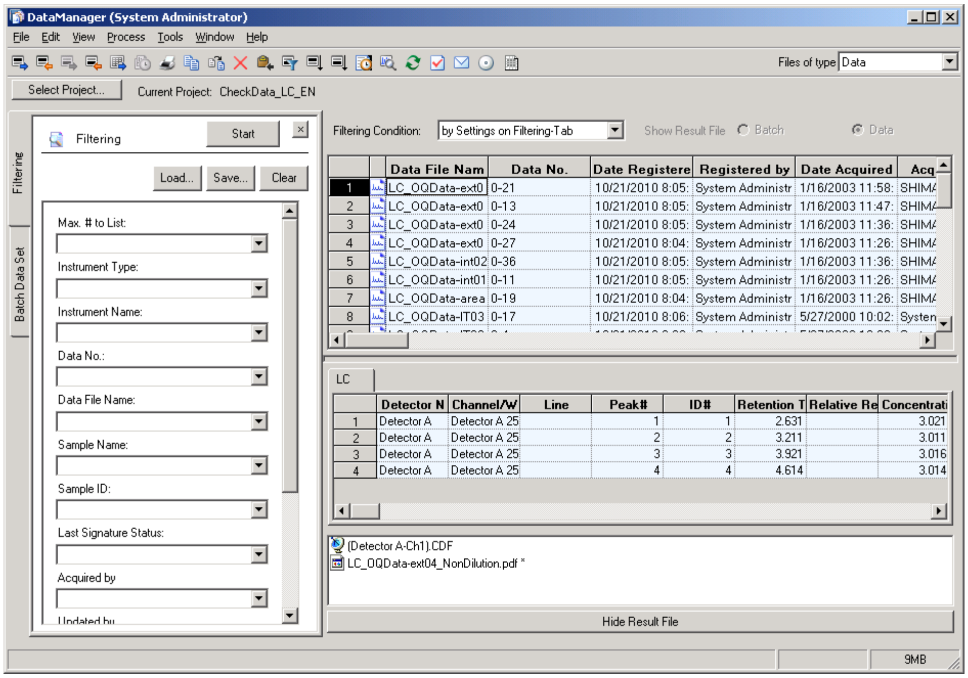
Log Type: User Authentication

Target: DB

Type	Message	Sub Message	Date & Time	Code	User Na...	Pro
Information	Close Application.		11/26/2010 7:46:15 PM(...	0X10...	System Ad...	
Information	Add a user account	[test2] -> Added	11/26/2010 7:46:13 PM(...	0X10...	System Ad...	
Information	Open Application.		11/26/2010 7:46:01 PM(...	0X10...	System Ad...	

3 / 3

User Authentication Log



Files of type: Data

Current Project: CheckData_LC_EN

Filtering Condition: by Settings on Filtering-Tab

	Data File Nam	Data No.	Date Registere	Registered by	Date Acquired	Acq
1	LC_OQData-ext0	0-21	10/21/2010 8:05:	System Administr	1/16/2003 11:58:	SHIMA
2	LC_OQData-ext0	0-13	10/21/2010 8:05:	System Administr	1/16/2003 11:47:	SHIMA
3	LC_OQData-ext0	0-24	10/21/2010 8:05:	System Administr	1/16/2003 11:36:	SHIMA
4	LC_OQData-ext0	0-27	10/21/2010 8:04:	System Administr	1/16/2003 11:26:	SHIMA
5	LC_OQData-int02	0-36	10/21/2010 8:05:	System Administr	1/16/2003 11:36:	SHIMA
6	LC_OQData-int01	0-11	10/21/2010 8:05:	System Administr	1/16/2003 11:26:	SHIMA
7	LC_OQData-area	0-19	10/21/2010 8:04:	System Administr	1/16/2003 11:26:	SHIMA
8	LC_OQData-IT03	0-17	10/21/2010 8:06:	System Administr	5/27/2000 10:02:	Systen

	Detector N	Channel/W	Line	Peak#	ID#	Retention T	Relative Re	Concentrati
1	Detector A	Detector A 25		1	1	2.631		3.021
2	Detector A	Detector A 25		2	2	3.211		3.011
3	Detector A	Detector A 25		3	3	3.921		3.016
4	Detector A	Detector A 25		4	4	4.614		3.014

(Detector A-Ch1).CDF
LC_OQData-ext04_NonDilution.pdf *

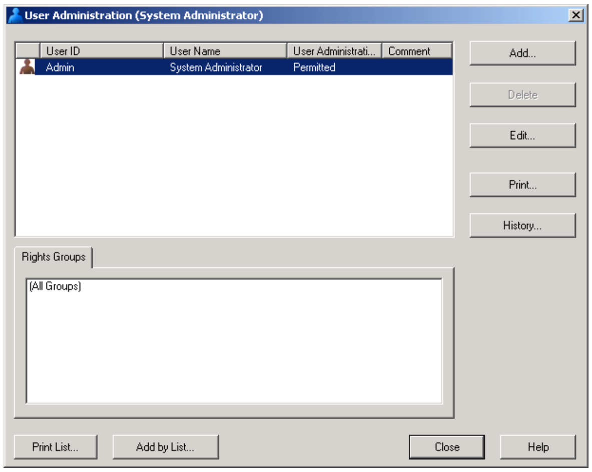
Data Stored in the Database

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

This system offers schedule and method (including time programs) functions that permit customer to preset sequences. The schedules and methods are stored in the database with analysis results when an analysis is run, allowing confirmation that the analysis has been run according to the sequence.

(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

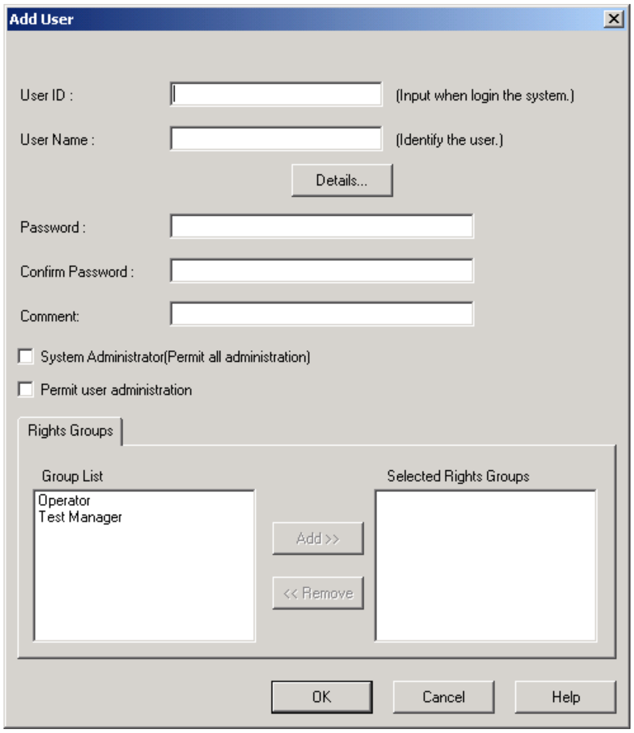
This system offers authority check functions that set the authority each user has for each instrument and function. Unauthorized people are prevented from accessing an instrument or function.



User ID	User Name	User Administrati...	Comment
Admin	System Administrator	Permitted	

(All Groups)

User Control



User ID : (Input when login the system.)

User Name : (Identify the user.)

Password :

Confirm Password :

Comment:

□ System Administrator(Permit all administration)

□ Permit user administration

Group List:
Operator
Test Manager

User Information Entry

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

The unit configuration is stored for each method at the time the method is created. When measurement is commenced an error is generated if the actual unit configuration differs from the unit configuration stored for the method. Another function is provided to read and display the instrument serial number.

(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

When creating or reviewing specification requirements during development of a FDA 21 CFR Part 11-compliant system, Shimadzu verifies that the FDA 21 CFR Part 11 requirements are satisfied. Also, Shimadzu contracts a specialist consultant to evaluate and provide feedback for the required specifications.

Education and training is provided to maintenance and service engineers. An authentication system has been implemented for staff involved with the maintenance and servicing of FDA 21 CFR Part 11-compliant systems.

Shimadzu provides training courses for customers using FDA 21 CFR Part 11-compliant systems.

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

This item shall be declared and implemented in the "SOP for FDA 21 CFR Part 11 Compliance" created by the customer.

(k) Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

Instruction Manuals are supplied with Shimadzu products or they can be purchased separately.

Development documents and Instruction Manuals shall be handled throughout the software lifecycle using a quality control system conforming to ISO9001.

This quality control system shall define procedures for document revision and change control. A record of revisions made to documents shall be kept.

Sec. 11.30 Controls for open systems

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in Sec. 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

This item is not applicable as this system is designed for configuration as a closed system.

(If electronic mail functions are used in a system connected to the Internet, appropriate control measures must be undertaken or the system will be considered an open system. In this situation, disable the electronic mail functions.)

Sec. 11.50 Signature manifestations

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

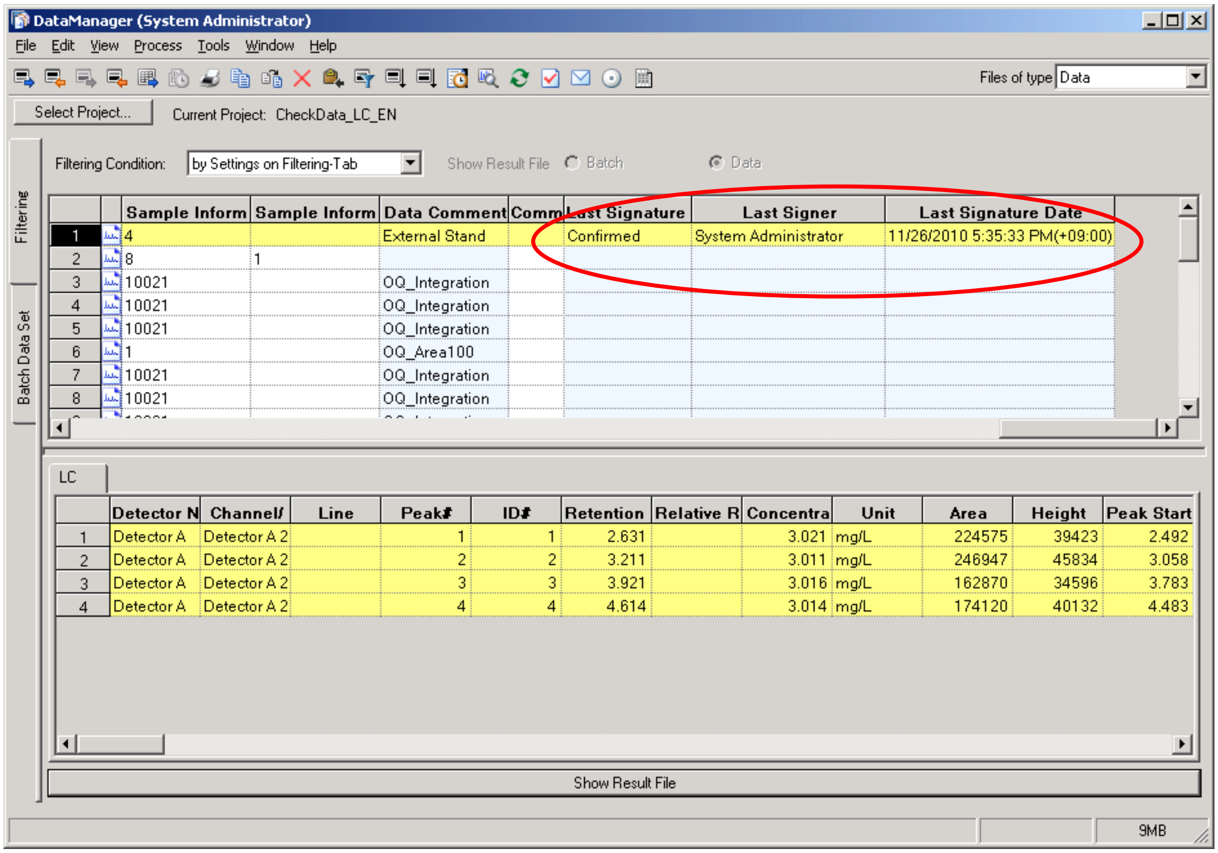
(1) The printed name of the signer;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

The electronic signatures function of this system incorporates the printed name of the signer, date and time when the signature was executed and the meaning associated with the signature (such as approval). The signatures are displayed with these elements in the electronic records list.


DataManager (System Administrator)
File Edit View Process Tools Window Help
Select Project...
Filtering
Batch Data Set
LC
Show Result File
9MB

Files of type: Data

Current Project: CheckData_LC_EN

Filtering Condition: by Settings on Filtering-Tab

Show Result File ○ Batch ● Data

	Sample Inform	Sample Inform	Data Comment	Comm	Last Signature	Last Signer	Last Signature Date
1	4		External Stand		Confirmed	System Administrator	11/26/2010 5:35:33 PM(+09:00)
2	8	1					
3	10021		OQ_Integration				
4	10021		OQ_Integration				
5	10021		OQ_Integration				
6	1		OQ_Area100				
7	10021		OQ_Integration				
8	10021		OQ_Integration				

	Detector N	Channel/	Line	Peak#	ID#	Retention	Relative R	Concentra	Unit	Area	Height	Peak Start
1	Detector A	Detector A 2		1	1	2.631		3.021	mg/L	224575	39423	2.492
2	Detector A	Detector A 2		2	2	3.211		3.011	mg/L	246947	45834	3.058
3	Detector A	Detector A 2		3	3	3.921		3.016	mg/L	162870	34596	3.783
4	Detector A	Detector A 2		4	4	4.614		3.014	mg/L	174120	40132	4.483

Sec. 11.70 Signature/record linking

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

Signature information is stored in the same field as the database record and is controlled in the same way as the record. The signature information is simultaneously retained in the operation log. The operation log is linked to the database where the corresponding record is stored. The contents of the operation log cannot be copied or moved and the operation log can be deleted only after it is archived.

Subpart C Electronic Signatures

Sec. 11.100 General requirements.

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

This system does not permit the same User ID or user name to be assigned to different individuals. It is possible to prohibit user account deletion. Although users can be disabled. Consequently, each electronic signature is unique to one individual.

(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional
certification or testimony that a specific electronic signature is the legally binding
equivalent of the signer's handwritten signature.

This item relates to standard operating procedures. The details above must be incorporated in the SOP created by the customer.

Sec. 11.200 Electronic signature components and controls

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinctive identification components such as an identification code and Password.

Electronic signatures used by this system employ two distinctive identification components: a User ID and a password.

(i). When an individual executes a series of signings during a single continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by the individual.

(ii). When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

This system requires a User ID and password to initially log into the system. Subsequently, the user selects and checks the contents of the data to be signed and must then re-input his/her password for each subsequent signing. After logging off the system, the user must subsequently repeat all the operations above.

Consequently, to make a series of signings, the User ID and password are required for the first signing. Input of the password alone is sufficient for subsequent signings.

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

Even the system administrator is unable to obtain the password of another person. Because only the genuine owner knows the correct combination of User ID and password, no other single person can falsify the signature of the genuine owner.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

The current version is does not support signatures based on biometrics.

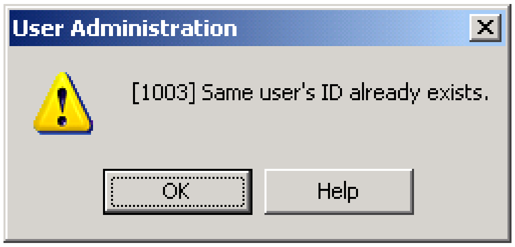
Sec. 11.300 Controls for identification codes/passwords

Sec 11.300 Controls for identification codes/passwords

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

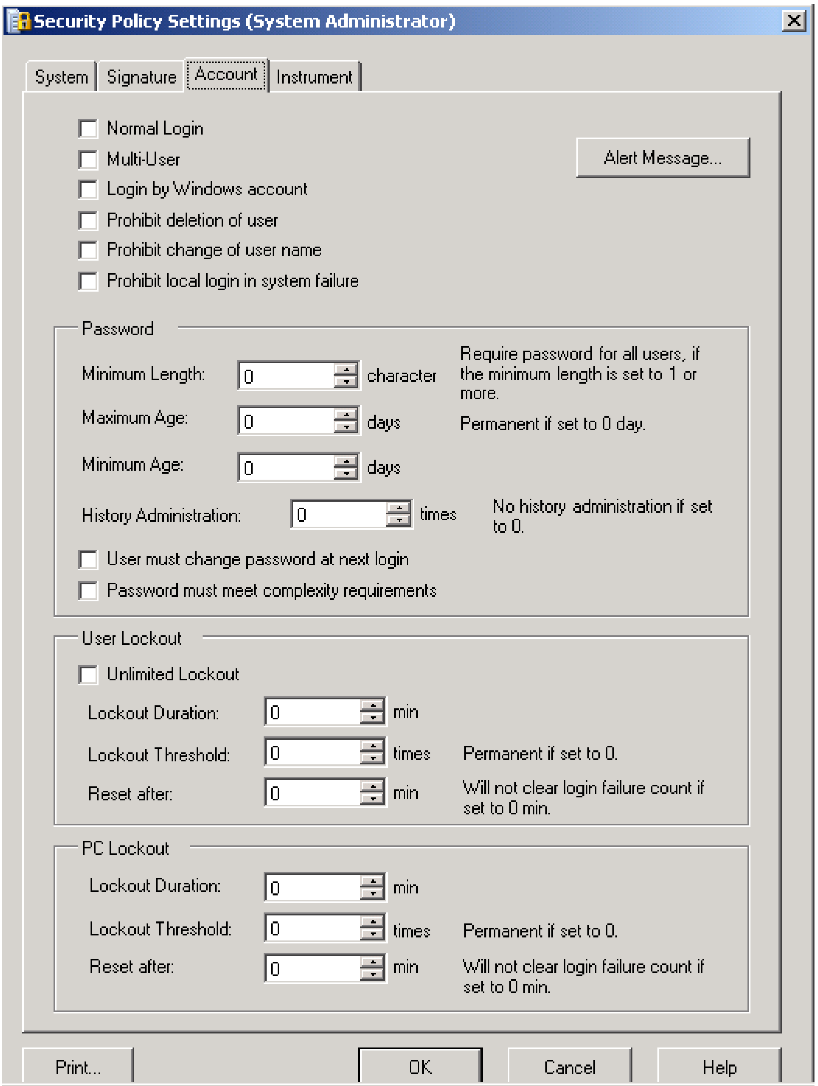
This system does not permit a User ID to be deleted once it has been registered. (Although it can be disabled.) It is not possible to register a User ID that was registered previously. Consequently, it is impossible to assign an identical combination of User ID and password to more than one person.


User Administration

[1003] Same user's ID already exists.

(b) Ensuring that identification code and password issuance is periodically checked, recalled, or revised (e.g. to cover such events as password aging).

The minimum password length and period of validity can be set to prevent password obsolescence. Unwanted User IDs can be disabled.



☐ Normal Login
☐ Multi-User
☐ Login by Windows account
☐ Prohibit deletion of user
☐ Prohibit change of user name
☐ Prohibit local login in system failure

Password

Minimum Length: 0 character — Require password for all users, if the minimum length is set to 1 or more.

Maximum Age: 0 days — Permanent if set to 0 day.

Minimum Age: 0 days

History Administration: 0 times — No history administration if set to 0.

☐ User must change password at next login
☐ Password must meet complexity requirements

User Lockout

☐ Unlimited Lockout

Lockout Duration: 0 min

Lockout Threshold: 0 times — Permanent if set to 0.

Reset after: 0 min — Will not clear login failure count if set to 0 min.

PC Lockout

Lockout Duration: 0 min

Lockout Threshold: 0 times — Permanent if set to 0.

Reset after: 0 min — Will not clear login failure count if set to 0 min.

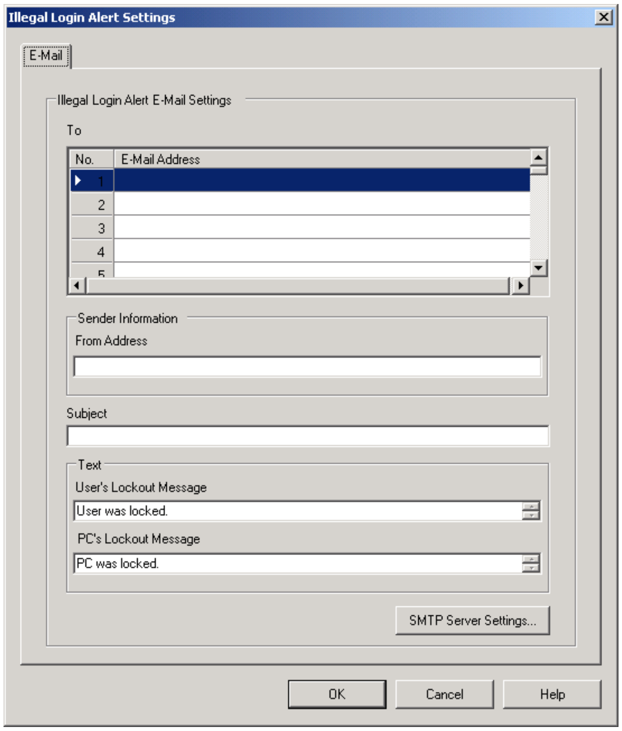
(c) Following loss management procedures to electronically reauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

The system administrator of this system can disable accounts and issue new User ID’s and passwords. The system administrator can also reset a password for a person who forgot his/her password.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

This system administrator can preset maximum number of unsuccessful login attempts after which the user ID is deactivated for a time period that can also be preset by the system administrator. An electronic mail can automatically be sent to designated addresses, as shown below.

The system is therefore able to detect and notify attempts at unauthorized access.



No.	E-Mail Address
1	
2	
3	
4	
5	

User's Lockout Message: User was locked.

PC's Lockout Message: PC was locked.

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

This item does not apply to this system; as such devices are not used.

This completes the outline of the FDA 21 CFR Part 11-compliance of Shimadzu analytical instruments using LabSolutions Database and LabSolutions Client/Server software.

Contact your Shimadzu representative if you require these documents.

4. Compatibility of Shimadzu LabSolutions Database and LabSolutions Client/Server software with FDA 21 CFR Part 11 Requirements

The tables below list the compatibility of Shimadzu LabSolutions Database and LabSolutions Client/Server software with items of FDA 21 CFR Part 11.

The tables relate to a closed system configuration, with the Windows environment and databases recommended by Shimadzu installed.

Subpart B Electronic Records

11.10 Procedures and Management for a Closed System

	Question	Compatibility
11.10(a)	Is the system validated?	Yes
11.10(a)	Can invalid records and altered records be identified?	Yes
11.10(b)	Can the system print an accurate and complete hardcopy of electronic records to paper?	Yes
11.10(b)	Does the system offer functions to create an accurate and complete copy in electronic format for FDA audits, inspections and copies?	Yes
11.10(c)	Is rapid restoration of electronic records possible throughout the storage period?	Yes
11.10(d)	Is system access restricted to people with access authority?	Yes
11.10(e)	Is a computer-generated audit trail available that records the date and time? The audit trail must record the date and time of operator inputs, electronic report generation, and modifications and deletions.	Yes
11.10(e)	Is previous information retained after an electronic record is modified? (Record does not become vague.)	Yes
11.10(e)	Is restoration of the electronic-record audit trail possible throughout the storage period?	Yes
11.10(e)	Is the audit trail compatible with FDA inspections and copies?	Yes
11.10(f)	When system operation and operation sequence are critical, can the system control the operation procedure? (For a process control system, for example.)	Yes

11.10(g)	Does the system ensure the following? Electronic signatures to electronic records? Access to I/O devices for operation or computer system? Record editing and other operations possible by approved personnel only?	Yes
11.10(h)	If the system allows input of data and work instructions only from an input device (a terminal, for example), is a validity check conducted on all data and work instructions received by the system? (Note: This applies to systems in which data or work instructions can be generated by multiple input devices. In this case, the system must conduct integrity verification of network-linked data sources, such as balances and wireless remote-controlled terminals.)	Yes
11.10(i)	Are OJT and other training documents available to for system users, developers, and IT support?	Yes
11.10(j)	Does a policy exist that declares the individual's responsibility for actions started based on electronic signatures?	Applies to customer's system management
11.10(k)	Are controls applied to the distribution and reading of documents related to system operation and maintenance?	Applies to customer's system management
11.10(k)	Is a formal change management procedure in place for audit trails and system documents related to changes organized in time sequence?	Yes

11.30 Additional Procedures and Management for an Open System

	Question	Compatibility
11.30	Is the data encrypted? Are digital signatures used?	This system was designed to operate as a closed system.

11.50 Signed Electronic Records

	Question	Compatibility
11.50	Do the signed electronic records contain the following information? （1） Name of the signer (print) （2） Date signed （3） Significance (Approval, Review, Responsibility, etc.)	Yes
11.50	Does this electronic signature information above appear on the display and in printouts?	Yes
11.70	Are signatures and electronic records linked to prevent illegal cutting, copying, or moving to avoid falsification?	Yes

Subpart C Electronic Signatures

11.100 Electronic Signatures (General)

	Question	Compatibility
11.100(a)	Is each electronic signature unique to an individual?	Yes
11.100(a)	Electronic signatures cannot be re-used or re-assigned to other people?	Yes
11.100(b)	Is each individual's ID verified before an electronic signature is assigned?	Yes

11.200 Electronic Signatures (Non-biometric)

	Question	Compatibility
11.200(a)(1)(i)	Does the signature comprise at least two elements, such as ID code and password or ID card and password?	Yes
11.200(a)(1)(ii)	If multiple signatures are made during one consecutive login, is password entry required for each signature? (Note: The first signature after login must be made using all of the (at least two) elements of the signature.)	Yes

11.200(a)(1)(iii)	If signatures are not made during one consecutive access, are all of the (at least two) elements of the signature required for each signature made?	Yes
11.200(a)(2)	Can a non-biometric signature be used by the correct person only?	Yes
11.200(a)(3)	Must at least two people cooperate to falsify an electronic signature?	Yes

11.200 Electronic Signatures (Biometric)

	Question	Compatibility
11.200(b)	Can a biometric signature be used by the correct person only?	Yes

11.300 ID Code and Password Management

	Question	Compatibility
11.300(a)	Is appropriate management conducted to maintain the uniqueness of the ID code and password combinations? That is, is it impossible for more than one person to have the same ID code and password combination?	Yes
11.300(b)	Are procedures in place to ensure that the ID code validity is checked periodically?	Applies to customer's system management
11.300(b)	Do passwords periodically expire and require changing?	Yes
11.300(b)	Are procedures in place to delete the ID code and password of a retired or transferred worker?	Yes
11.300(c)	Are procedures in place to electronically invalidate an ID code or password that was forgotten?	Yes
11.300(d)	Are procedures in place to detect attempts at illegal operation and notify security?	Yes
11.300(d)	Are procedures in place to notify the administrator of repeated attempts at access or attempts at access by a person with inadequate authority?	Yes

11.300 Tokens, Cards and Devices to Generate ID and Password Information

	Question	Compatibility
11.300(c)	Are procedures in place to manage the loss or theft of devices?	Not used by this system
11.300(c)	Are procedures in place to electronically disable a device that was lost or stolen?	
11.300(c)	Are procedures in place to manage the supply of temporarily or permanent replacement devices?	
11.300(e)	Are tokens or cards periodically inspected?	
11.300(e)	Do these inspections check for unauthorized modifications?	

5. Inquiries

Refer to the FDA home page (www.fda.gov) or the Shimadzu web site for more detailed information on FDA 21 CFR Part 11.

For technical inquiries, contact your Shimadzu representative.

Web http://www.ssi.shimadzu.com/

6. Revision Information

Version Number	Author	Changes	Date
1.0	Robert Karro	Original Document	1/1/18
2.0	Robert Karro	Formatting and grammatical updates	9/13/18