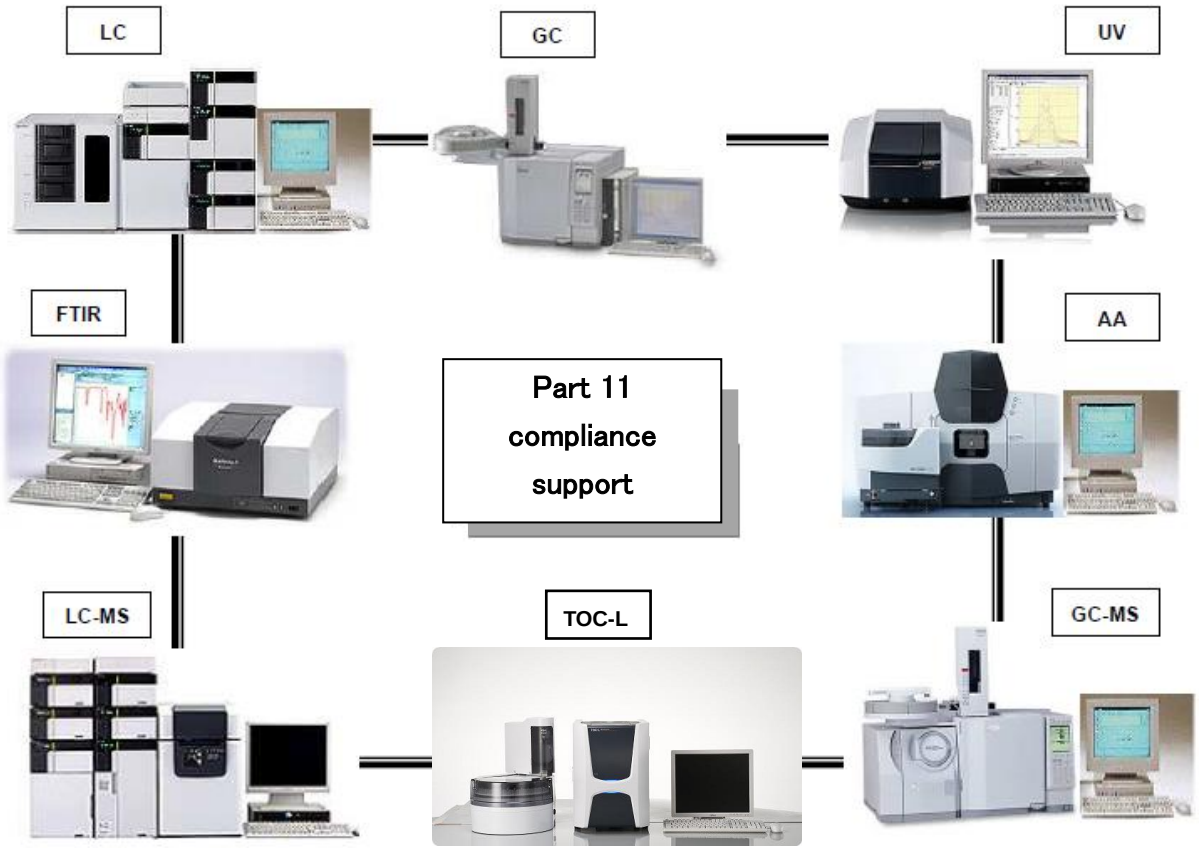
Compliance of Shimadzu Total Organic Carbon (TOC) Analyzer with FDA 21 CFR Part 11 Regulations on Electronic Records and Electronic Signatures
TOC-Control L Ver.1 / LabSolutions DB/CS Ver.6



SHIMADZU

Solutions for Science
since 1875

Analytical & Measuring Instruments Division
Shimadzu Corporation

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.shimadzu.com

Contents

1. Introduction

In August 20, 1997 a new regulation from the U.S. FDA (Food and Drug Administration) was introduced, 21 CFR Part 11 entitled “Electronic Records; Electronic Signatures”. This regulation provided requirements to ensure that electronic records and electronic signatures are trustworthy, reliable and identical to paper records and handwritten signatures. It also provided guidelines for submission of electronic records to the FDA.

This paper describes how to comply with the 21 CFR Part 11 by using Shimadzu analytical instruments data management software TOC-Control L Ver.1 and later/ LabSolutions DB/CS Ver.6 and later developed for compliance with the above mentioned FDA 21 CFR Part 11.

2. Outline and Structure of FDA 21 CFR Part 11

The structure of FDR 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.

2.1 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.

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

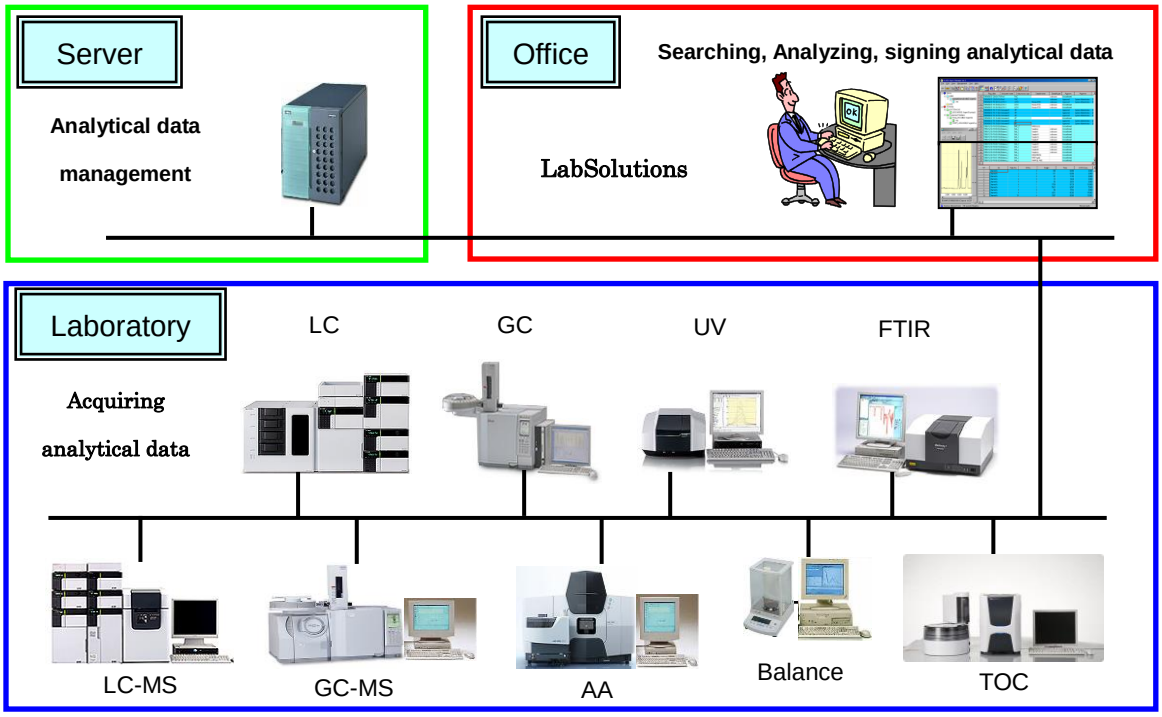
An environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

3. Equivalence between FDA 21 CFR Part 11 Requirements and Shimadzu TOC-Control L Ver.1/LabSolutions Ver.6

3.1 Basic Policy for FDA 21 CFR Part 11 Compliance

Shimadzu achieves FDA 21 CFR Part 11 compliance through integrated control of data for TOC, chromatographs (LC, GC, LC-MS, GC-MS, etc.), spectrophotometers (UV, FT-IR, AA, etc.), balances, and other common laboratory instruments.

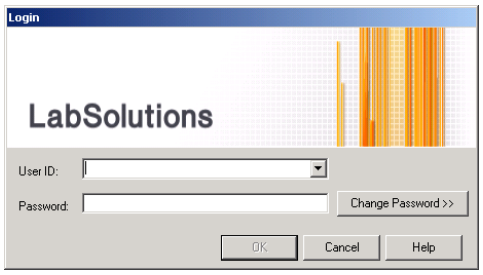
Shimadzu supplies products and technologies based on LabSolutions Ver.6 and later to assist with FDA 21 CFR Part 11 compliance for analytical data from laboratory instruments, such as chromatographs and balances.



TOC-Control L software was designed to run. A pre-registered user name (login ID) and password must be entered before using TOC-Control L software.

Similarly, LabSolutionsDB/CS software runs and requires input of a pre-registered user name (login ID) and password before it can be used.

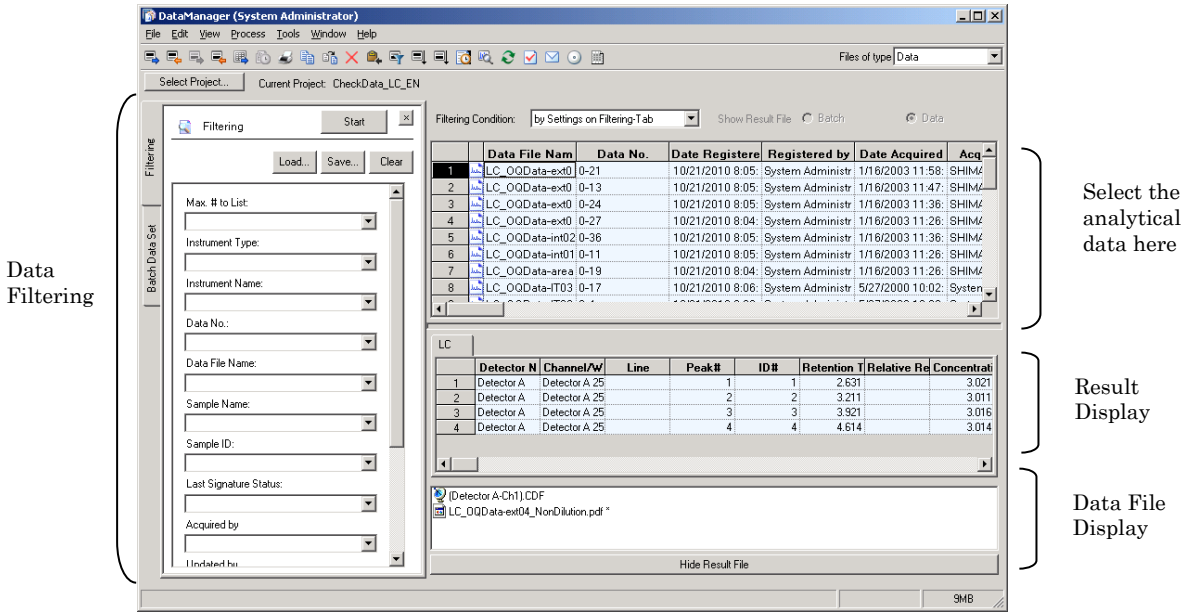
Consequently, a system comprising TOC-Control L and LabSolutionsDB/CS can be configured as a closed system, as it allows system access to be controlled according to the authority for electronic records in the system.



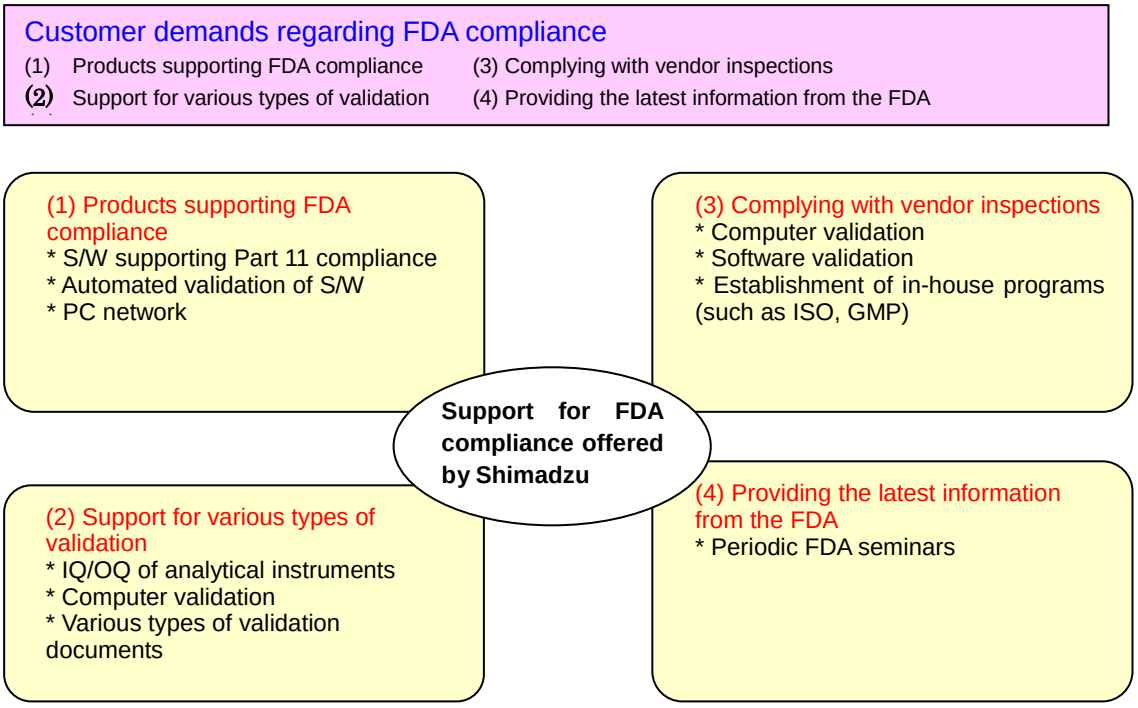
LabSolutions Login Screen

TOC-Control L 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.



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.



3.2 FDA 21 CFR Part 11-compatible Software for Total Organic Carbon (TOC) Analyzer

A combination of TOC-Control L Ver.1 and later TOC-L control software and the LabSolutionsDB/CS and later data control software is used to achieve FDA 21 CFR Part 11 compatibility for Total Organic Carbon (TOC) Analyzer.

3.2.1 Software configuration

- TOC-Control L software controls Shimadzu TOC-L instruments for the measurement of TOC data, data processing, and printing.
- LabSolutionsDB/CS saves data measured or processed by TOC-Control L in a database. The saved data can be searched or browsed using the LabSolutions DataManager software, and can be restored if required. Electronic signatures are applied using the LabSolutions DataManager software.
- The LabSolutions DB/CS database is a secure, access-controlled SQL Server, or Oracle database.
- TOC-Control L and LabSolutions DB/CS incorporate security and user management functions that are independent of the OS features. A user name (login ID) and password must be entered before using these programs.

3.3 Subpart B Electronic Records

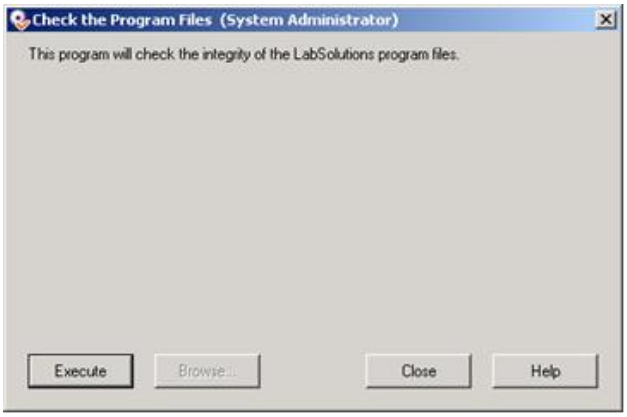
3.3.1 Sec. 11.10 Controls for closed systems

Sec. 11.10 Controls for closed systems

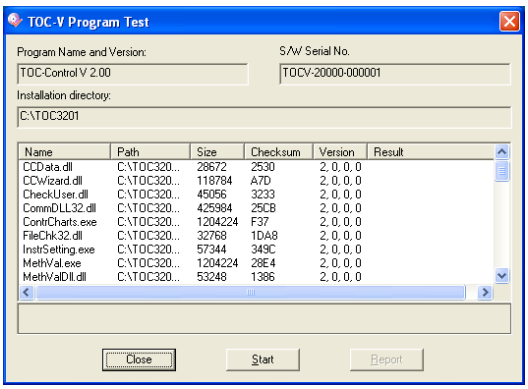
Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the 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.



LabSolutions Program Check Screen



TOC-Control L Program Check Screen

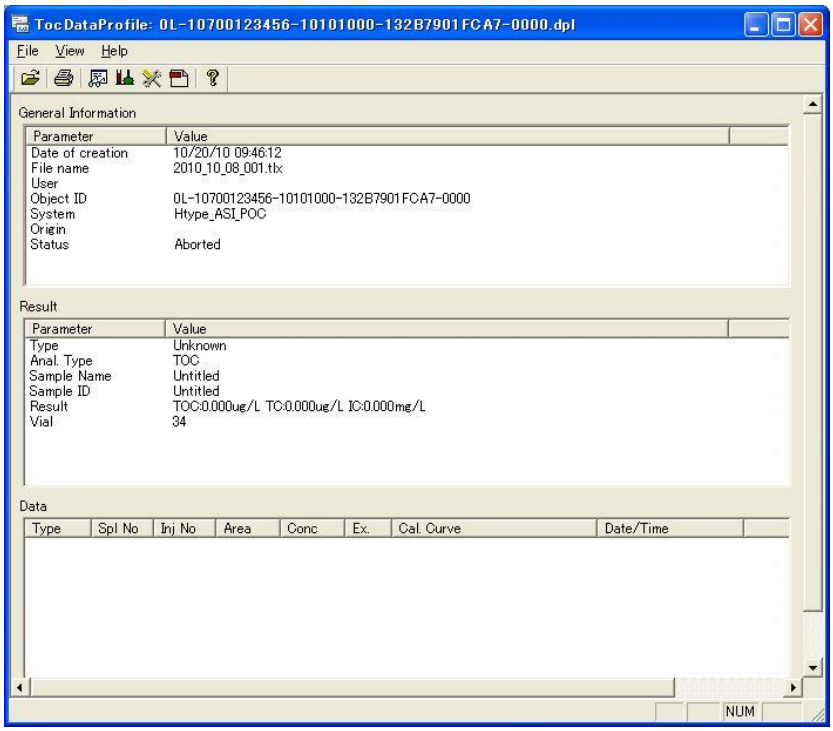
(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying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

TOC-Control L Data Profile

Data Profile	**Measurement Results**
	Cal.Curve Parameters
	Method Parameters
	Instrument Settings



TOC-Control L Data Profile Screen

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

・Protection of records

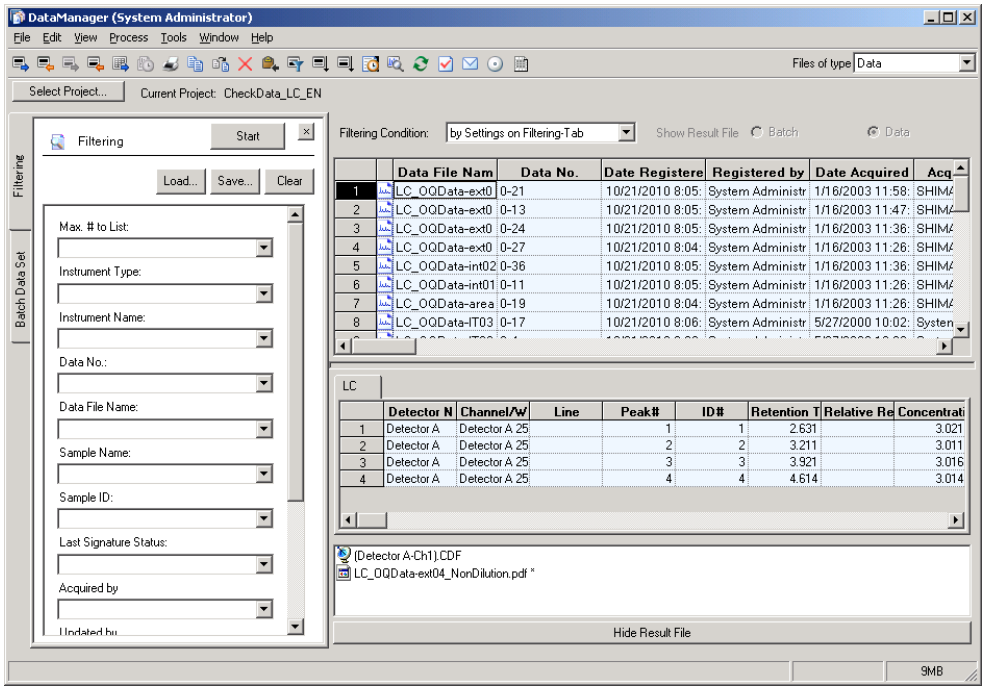
Data files are stored in a safe, access-controlled database, such as SQL Server or Oracle.

・Rapid searching

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

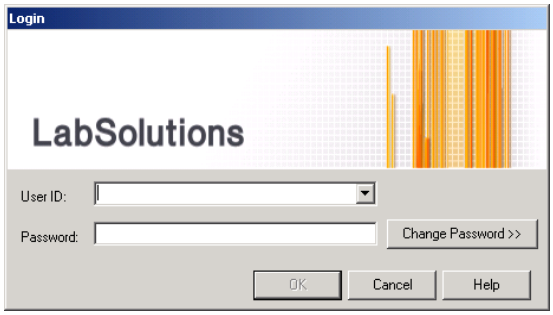
・Recovering records

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



(d) Limiting system access to authorized individuals.

Access to the system can be limited, as the system requires input of a user ID or login ID and password before the system can be used.



LabSolutions Login Screen

TOC-Control L Login Screen

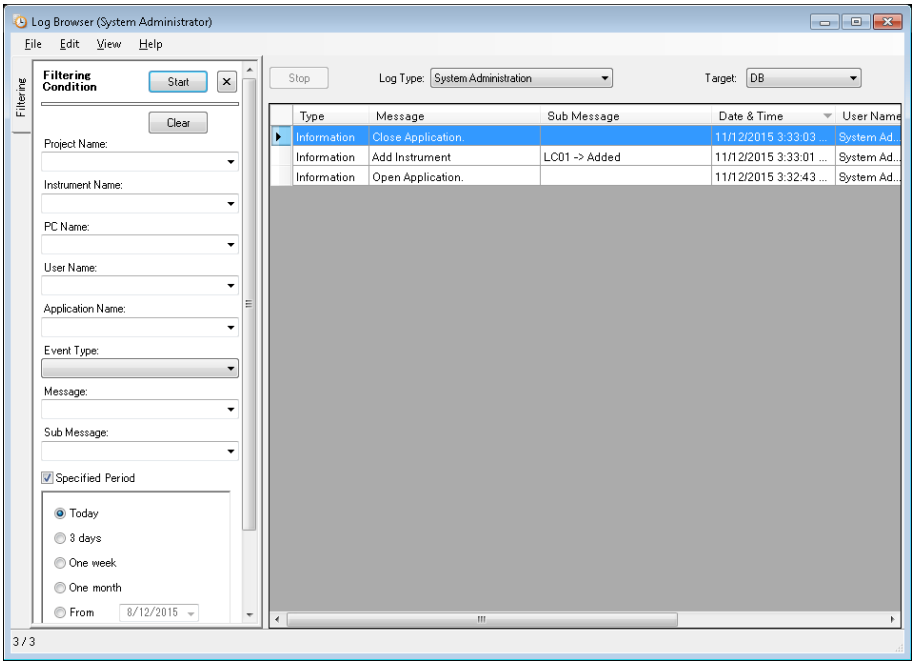
(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained 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 maintain 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 a computer and kept in database formats.

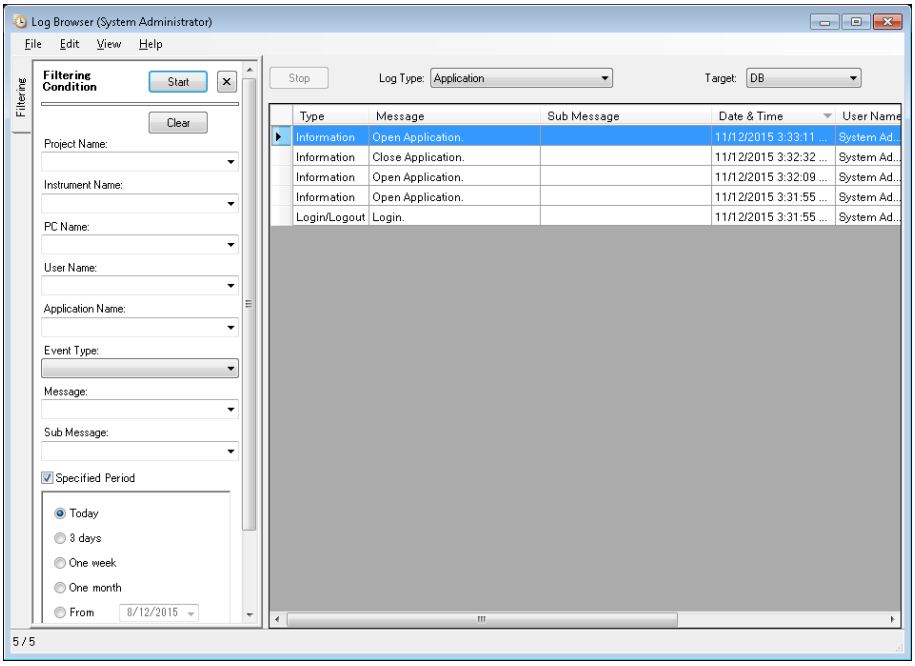
TOC-Control L incorporates six different kinds of Logs, including "Administration" (System Administration), "Create/Edit Data", "Maintenance", etc. These logs are generated automatically by a computer. The data log is saved in a data file.

Each time a new analysis or data reprocessing is performed, measurement results are automatically saved in a database. This data is protected from being overwritten or

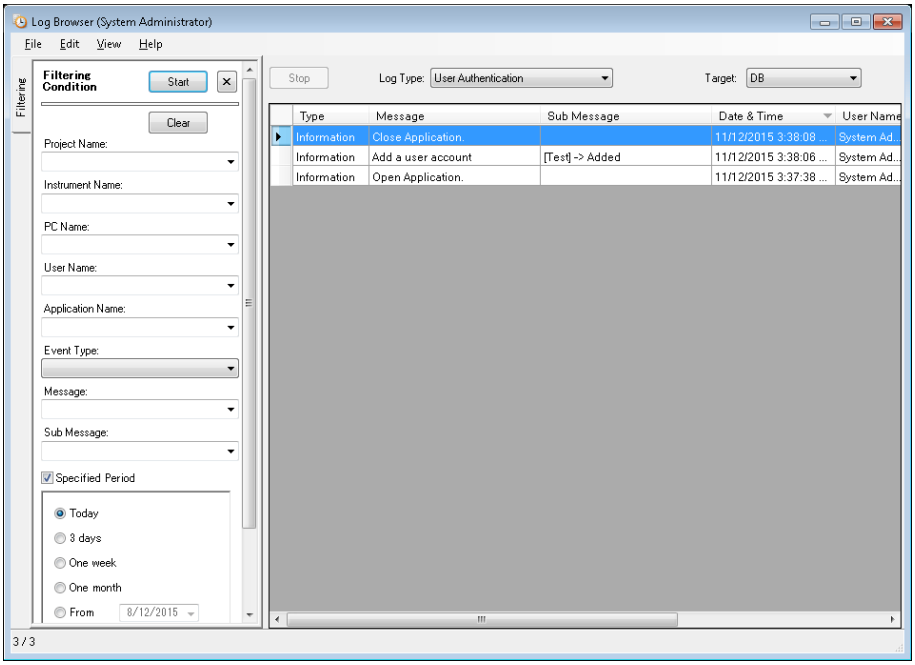
deleted, thereby ensuring an adequate audit trail capability.



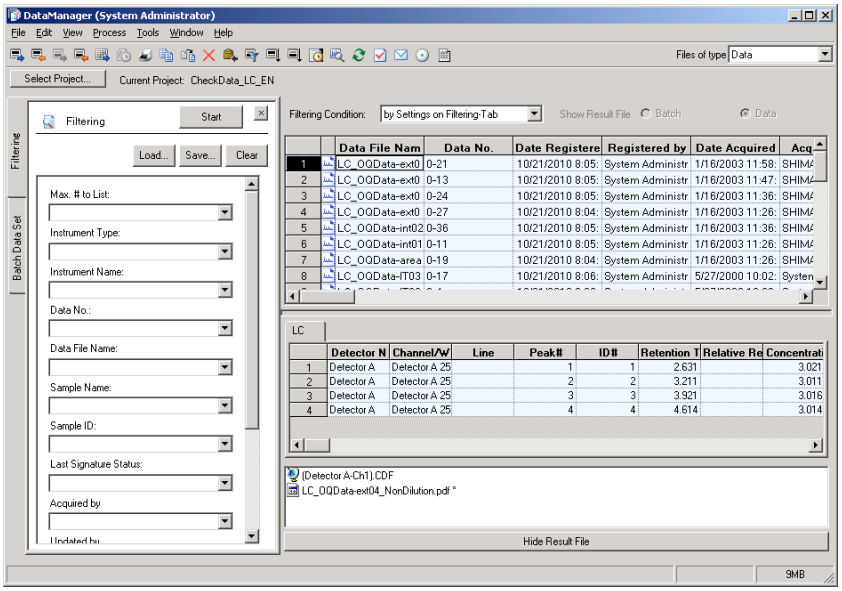
LabSolutions System Administration Log



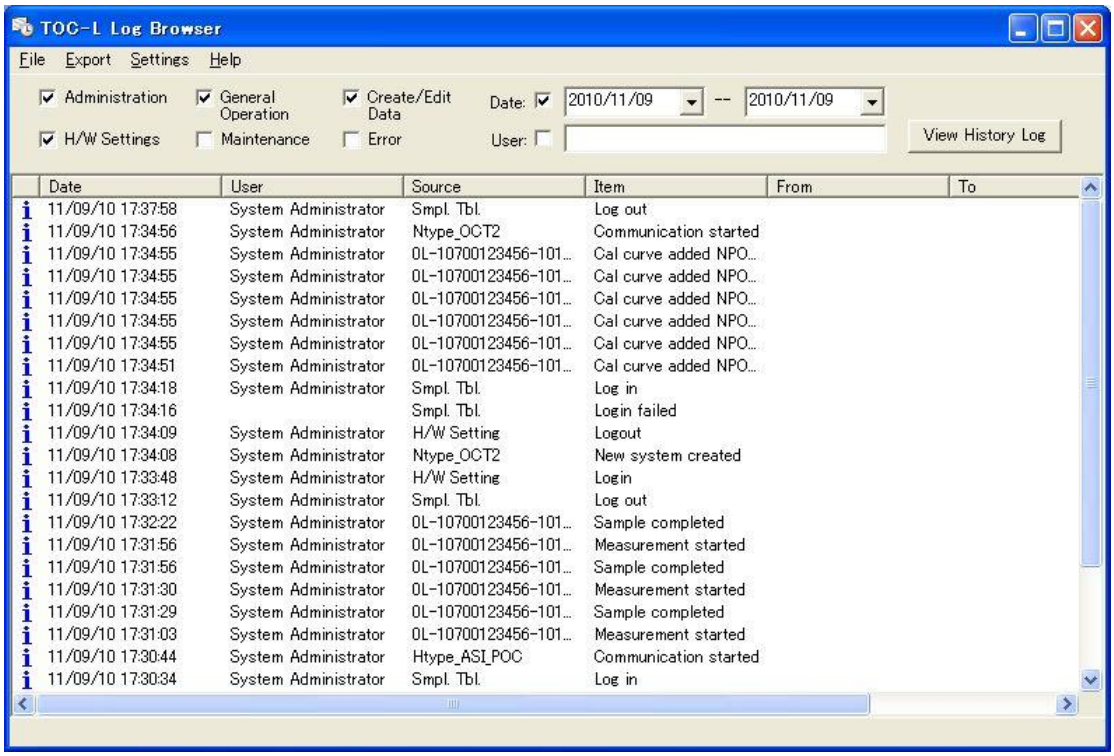
LabSolutions System Application Log



LabSolutions User Authentication Log



Data Stored in the Database



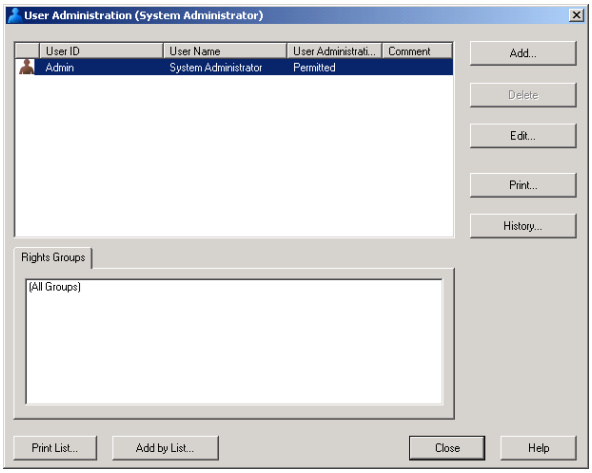
TOC-Control L System Log

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

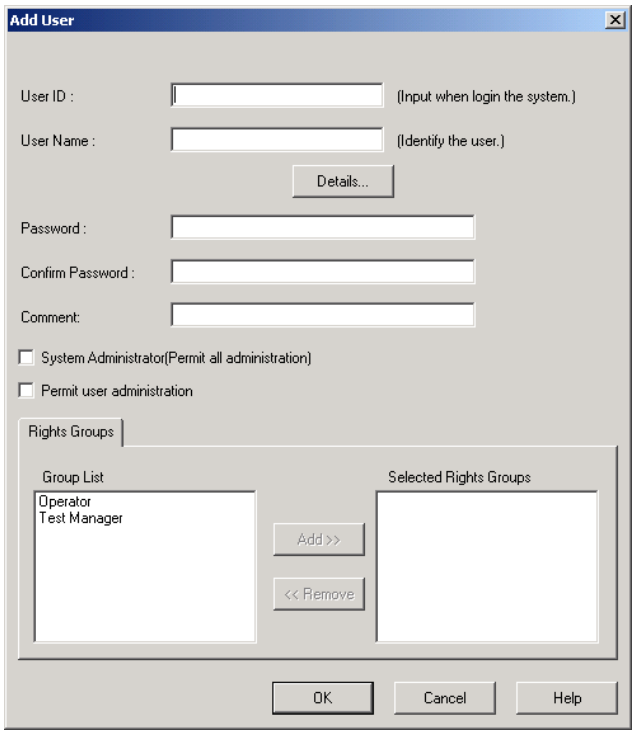
As it is not possible to predict a fixed procedure in advance for general TOC measurements, this system incorporates no function to directly support this provision.

(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.

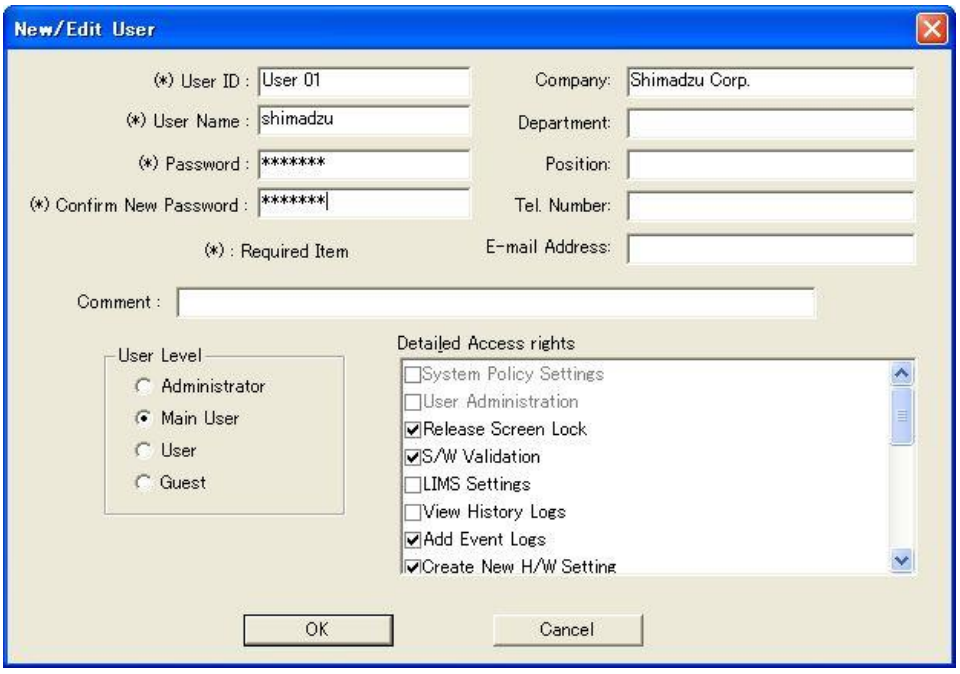
This system offers authority check functions that set the authority each user has for each instrument and function. Unauthorized people can be prevented from accessing an instrument or function. TOC-Control L permits the access authority of each user to be set in four levels for each instrument and function by default. LabSolutions permits the access authority of each user to be set for each function.



LabSolutions User Management



LabSolutions User information Entry



TOC-Control L User Management

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

When the PC is connected to the instrument, the serial number of the connected instrument can be checked in TOC-Control L. Moreover, the measurement data also includes the serial number of the instrument and the serial number of the software. The serial number can be checked to verify that the designated instrument was used for the measurements.

(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. Authentication system is 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.

3.3.2 Sec. 11.30 Controls for open systems

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.)

3.3.3 Sec. 11.50 Signature manifestations

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;

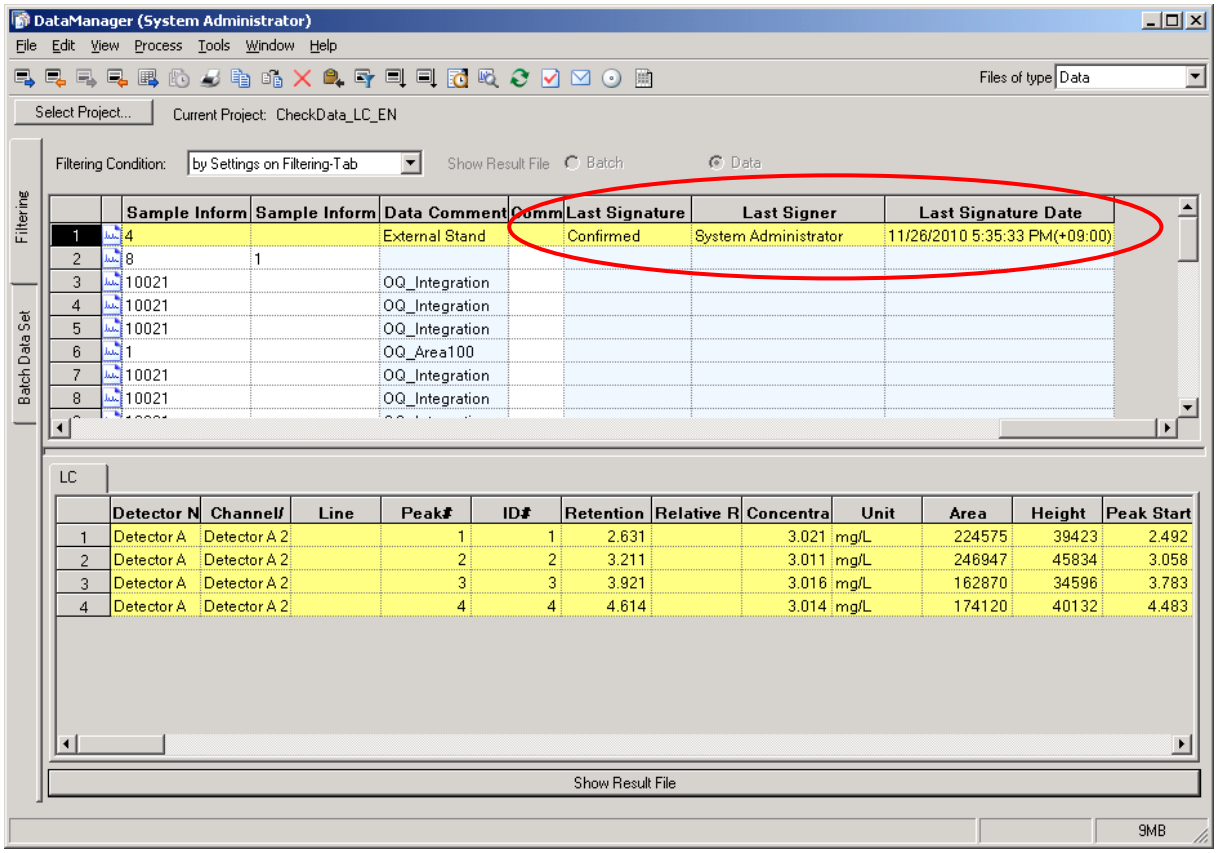
(2) The date and time when the signature was executed; and

(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).

In this system, electronic signatures are applied using the LabSolutions Manager software.

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.



3.3.4 Sec. 11.70 Signature/record linking

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.

3.4 Subpart C Electronic Signatures

3.4.1 Sec. 11.100 General requirements

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.

In this system, electronic signatures are applied using the LabSolutions software. This system does not permit the same login ID or user name to be assigned to different individuals. Once assigned, the login ID cannot be deleted, although it can be invalidated. 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 practical operating procedures. The details above must be incorporated in the SOP created by the customer.

3.4.2 Sec. 11.200 Electronic signature components and controls

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 login 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 login 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 login 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.

Compliance with fingerprint authentication is available as an option.

3.4.3 Sec. 11.300 Controls for identification codes/passwords

Sec 11.300 Controls for identification codes/passwords

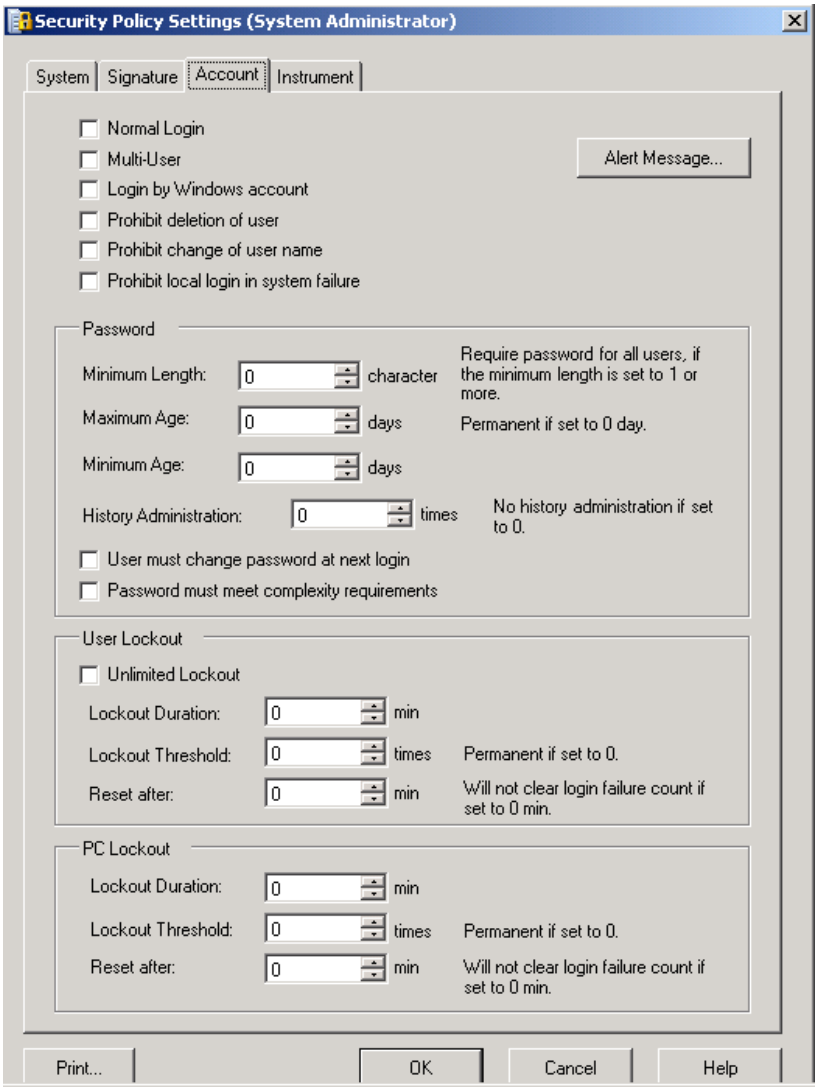
Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

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

(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 login IDs can be invalidated.



LabSolutions Manager Password Administration Settings

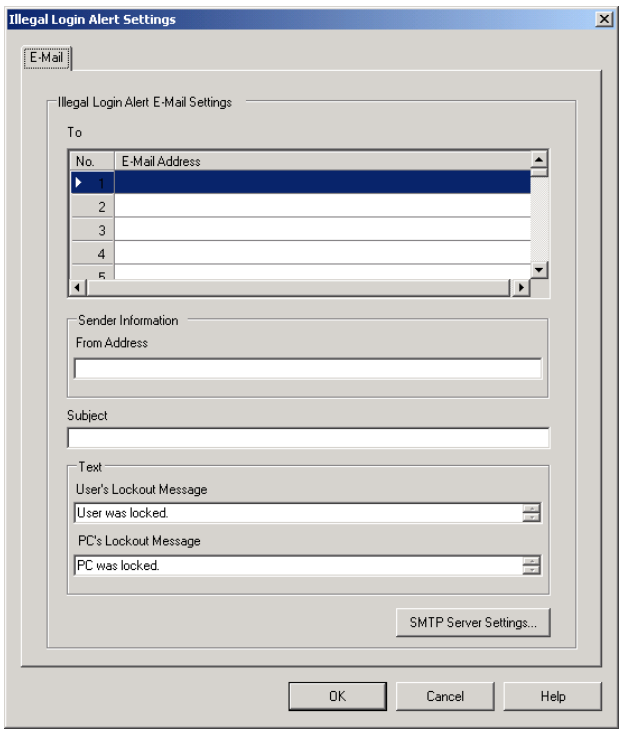
(c) Following loss management procedures to electronically reauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous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

The system administrator of this system can invalidate accounts and issue new login ID's and passwords. The system administrator can also set a new password to 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 allows to preset maximum number of unsuccessful login attempts after which the user ID is deactivated for a time period that can also be preset. An electronic mail can automatically be sent to a designated address, as shown below



(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 TOC-Control L/LabSolutions Documents are also available for other models. Contact your Shimadzu representative if you require these documents.

4. Compatibility of Shimadzu TOC-Control L Ver.1/LabSolutions DB/CS with FDA 21 CFR Part 11 Requirements

The tables below list the compatibility of Shimadzu TOC-Control L Ver.1 and later and LabSolutions DB/CS Ver.6 and later 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?	Not Supported

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. Enquiries

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 enquiries, contact your Shimadzu representative.

Web http://www.shimadzu.com