223-60092D
Mar. 2012

LabSolutions

System Users Guide

Read the instruction manual thoroughly before you use the product.
Keep this instruction manual for future reference.

Introduction

Read this Instruction Manual thoroughly before using the product.

Thank you for purchasing Shimadzu analytical instrument workstation “LabSolutions” (hereafter referred to as “the software” or “LabSolutions”).

This manual describes the procedures for operating this product. Read this manual thoroughly before using the product and operate the product in accordance with the instructions in this manual.

Also, keep this manual for future reference.

This manual assumes that the reader is knowledgeable of basic operations of Windows. For the operation of Windows, refer to the instruction manual that comes with that product.

Important

- If the user or installation location changes, ensure that this Instruction Manual is transferred with the product.
- If this manual is lost or damaged, immediately contact your Shimadzu representative to request a replacement.
- To ensure safe operation, contact your Shimadzu representative for product installation, adjustment, or re-installation (after the product is moved).

Original version is approved in English.

Notice

- LabSolutions software expands/limits its functions and controllable instruments according to the LabSolutions license. Please note that, depending on your license, some functions or instruments in this manual are not shown, or some windows styles in this manual may differ from those in the software.
- Information in this manual is subject to change without notice and does not represent a commitment on the part of the vendor.
- Any errors or omissions which may have occurred in this manual despite the utmost care taken in its production will be corrected as soon as possible, although not necessarily immediately after detection.
-
- Microsoft, Windows, Windows 7, Windows Vista and Windows XP are registered trademarks of Microsoft Corporation in the United States and/or other countries.
  Adobe, Adobe logo and Adobe Reader are trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.
  Other company names and product names mentioned in this manual are trademarks or registered trademarks of their respective companies. The TM and ® symbols are omitted in this manual.
- Microsoft® Windows® 7 Operating System is referred to as “Windows 7”.
  Microsoft® Windows Vista® Operating System is referred to as “Windows Vista”.
  Microsoft® Windows® XP Professional Edition is referred to as “Windows XP”.
- Replacement parts for this product will be available for a period of seven (7) years after the product is discontinued. Thereafter, such parts may cease to be available. Note, however, that the availability of parts not manufactured by Shimadzu shall be determined by the relevant manufacturers.

Instruction Manuals

■ List of Instruction Manuals

Name	Content
Getting Started Guide	This manual follows an actual data acquisition procedure to describe basic methods of operation for first-time users. Read this manual to learn basic operations of the software.
Operators Guide	This manual describes overall operations and handy functions in more details, such as the software's system configuration, data analysis, batch processing, confirmation of data acquisition results, and report functions.
System Users Guide	This manual describes system administration and data management of the software. Refer to this manual as necessary.
Installation & Maintenance Guide	This manual describes installation and maintenance of the software.
Data Acquisition & Processing Theory Guide	This manual describes peak detection and quantitation of sample components. Refer to this manual as necessary.
Help	Clicking the on-screen [Help] button or pressing the [F1] key displays a description of on-screen parameters, answers to specific questions or solutions to various problems. Also, clicking the [Help] button on the error message window displays the details of the error or solutions to the error. Refer to Help before contacting us.

■ Indications Used in Instruction Manuals

Cautions and Notes are indicated using the following conventions, and the following symbols are used in this manual:

Indication	Meaning
⚠ CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor to moderate injury or equipment damage.
NOTE	Emphasizes additional information that is provided to ensure the proper use of this product.
☞ Reference	Indicates the location of related reference information.
[ ]	Indicates the names of buttons, menu options, setting options, windows/sub-windows, and icons that are displayed in a window. Example: Click [OK].

Warranty

Shimadzu provides the following warranty for this product.

1. Period:

Please contact your Shimadzu representative for information about the period of this warranty.

2. Description:

If a product/part failure occurs for reasons attributable to Shimadzu during the warranty period, Shimadzu will repair or replace the product/part free of charge (including USB dongles). However, in the case of products which are usually available on the market only for a short time, such as personal computers and their peripherals/parts, Shimadzu may not be able to provide identical replacement products.

3. Limitation of Liability:

(1) In no event will Shimadzu be liable for any lost revenue, profit or data, or for special, indirect, consequential, incidental or punitive damages, however caused regardless of the theory of liability, arising out of or related to the use of or inability to use the product, even if Shimadzu has been advised of the possibility of such damage.

(2) In no event will Shimadzu's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount you paid for the product.

4. Exceptions:

Failures caused by the following are excluded from the warranty, even if they occur during the warranty period.

1) Improper product handling
2) Repairs or modifications performed by parties other than Shimadzu or Shimadzu designated companies
3) Product use in combination with hardware or software other than that designated by Shimadzu
4) Computer viruses leading to device failures and damage to data and software, including the product's basic software
5) Power failures, including power outages and sudden voltage drops, leading to device failures and damage to data and software, including the product's basic software
6) Turning OFF the product without following the proper shutdown procedure leading to device failures and damage to data and software, including the product's basic software
7) Reasons unrelated to the product itself
8) Product use in harsh environments, such as those subject to high temperatures or humidity levels, corrosive gases, or strong vibrations
9) Fires, earthquakes, or any other act of nature, contamination by radioactive or hazardous substances, or any other force majeure event, including wars, riots, and crimes
10) Product movement or transportation after installation
11) Consumable items
    Note: Recording media such as floppy disks and CD/DVD-ROMs are considered consumable items.

* If there is a document such as a warranty provided with the product, or there is a separate contract agreed upon that includes warranty conditions, the provisions of those documents shall apply.
* Warranty periods for products with special specifications and systems are provided separately.
* **The license cannot be reissued if you lose the USB dongle provided with the product.**

Contents

1 System Administration

The various system administration functions in this software include system security, user administration, rounding of numerical values, and setting the number of significant digits. The system operation history can be searched and checked in the [Log Browser]. The operating status of the system is checked in the [Output Window].

This section describes the procedures for setting the various system administration functions.

1.1 System Administration Functions

The software contains functions that meet the reliability requirements mandated in various regulations.

Account policies that prevent illegal access such as the minimum number of characters in passwords, password update interval, and the permitted number of entry attempts are set in Security Policy section of this software. The audit trail function records the history of all changes to instrument parameters and data processing parameters. The log browser allows you to quickly search the system operation history.

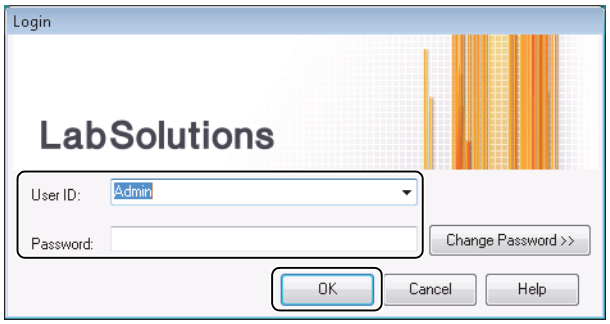
This section describes the system administration functions of the software.

1.1.1 Open System Administrator Window

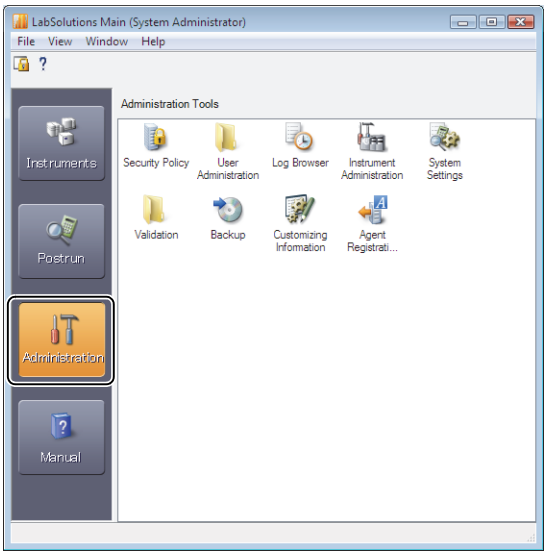
Access each of the system administration functions from the [System Administrator] sub-window of the [LabSolutions Main] window.

1 **Double-click the**  **icon on the Desktop.**

2 **Enter a [User ID] and [Password], and click [OK].**



3 **Click the (Administration) icon.**



The [System Administrator] sub-window opens.

1.1.2 System Administration Functions

The following functions are accessed in the system administration section.

These functions can only be accessed by users that have been assigned the appropriate rights.

Function	Contents
Security Policy Settings	
System Policies	The audit trail parameters for system administration functions and the time for automatic screen lock are set on this tab.
Account Policies	The password policy parameters, number of login retries, and illegal access notification are set on this tab.
Instrument Policies	The audit trail parameters and data access limitations are set on this tab.
User Administration	
User Administration	Register new users, change users, and set/change passwords in the User Administration window.
Rights Groups Administration	The rights for groups of users are assigned in this window.
Forced Logout	Use this window to forcibly logout users that are currently logged into the software.
Release PC Lockout	Use this window to release PCs that were locked out of the software system as a result of an illegal access.
Release User Lockout	Use this window to release users that were locked out of the software system as a result of an illegal access.
Log Browser	System-related operation logs can be filtered, displayed and printed from this window.
Instrument Administration	Use this window to administer the PCs and instruments that are connected to the system.
System Settings	Use this function to set the rounding procedure, number of significant digits and number of decimal places.
Validation	
PC Information	Displays information about the PC where the software was installed.
Check the Program Files	Determines whether the software program files installed on the PC have been altered.
System Administration Information Printing	Prints the Security Policy, System Connection Information, User List and Rights Group List.
Backup	Use this function to backup the system administration and application logs.
Customization Information	Use this function to initialize or copy customization information (e.g. the software's sub-window layouts, color settings, and assistant bars) from one user to another.
Agent Registration Settings	Use this function to set registration method of CLASS-Agent.

NOTE

- Users that are assigned system administrator rights possess the rights to all functions.
- Refer to Help for information on the rights required for each function.

1.2 Before System Operation

The software can be used in its default status. However, to fully utilize the software's data administration functions, set the system administration policy, register system users, set user rights, set the number of digits for data display, and make other settings before starting system operation.

The system administration policy (security policy) prevents illegal operation by creating a history of who performs specific operations.

1.2.1 System Administration Policy (Security Policy)

Set the password policy and the login method, response to illegal access, audit trail function, and file access limitations in the security policy.

This section describes the procedure for setting security policies according to various regulations.

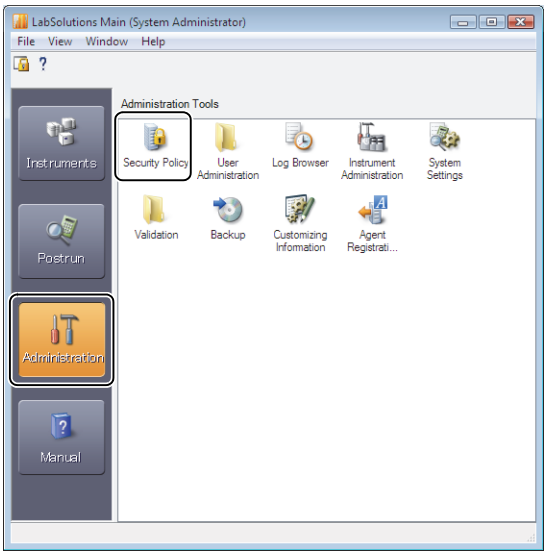
NOTE

- Log in with a user ID having the [System Administration] rights to set security policies.
- Settings made in the [Security Policy Settings] sub-window are enabled when the next user logs into the software.

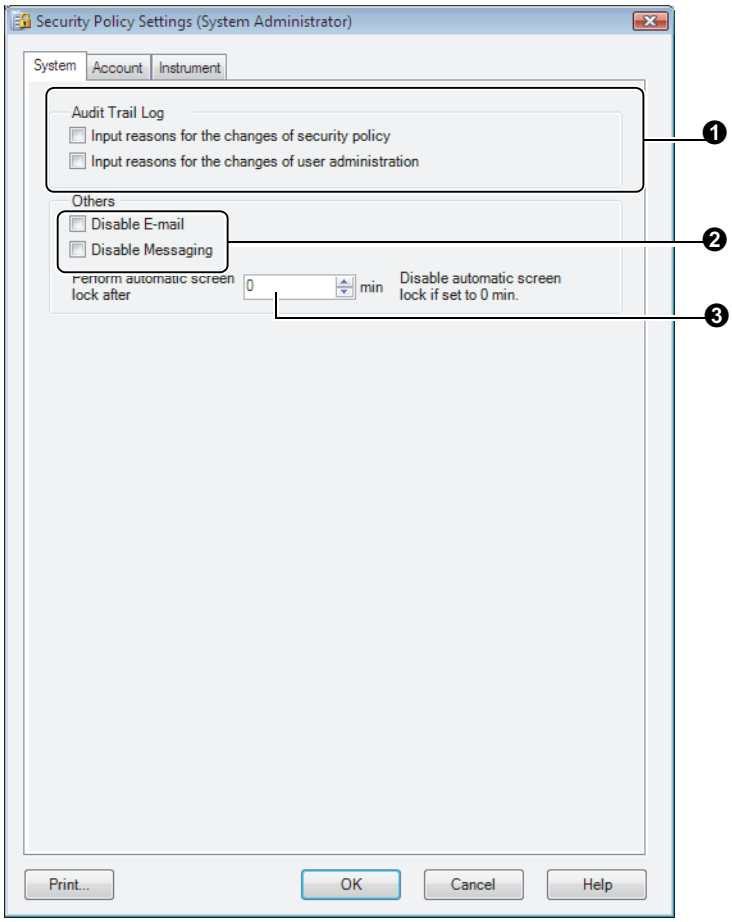
■ System Policies

Determine whether to prompt input of a reason for the changes of system security policy or user administration, whether to prohibit use of the e-mail function, and the wait time for automatically locking the screens to protect the system.

1 **Double-click the (Security Policy) icon in the [Administration Tools] sub-window of the [LabSolutions Main] window.**



2 Set each item on the [System] tab, and click [OK].



No.	Explanation
❶	Select these items to cause the [Audit Trail Log - Input Reason] sub-window to open and require entry of a reason for the security policy change or when a change is made in user administration such as the addition of a user account or a change to user rights. **NOTE** Once the audit trail log setting is selected it cannot be deselected to assure the integrity of logs. **Reference** The change reasons are recorded with the corresponding events in each of the audit trail logs, and can be checked by opening the audit trail log in [Log Browser] *(P.24)* then double-clicking the respective event row.
❷	Select these to disable the e-mail delivery or messaging function for security reasons. **Reference** When the e-mail delivery or messaging function is used, a message can be sent when an error or warning occurs on the software, when batch processing starts or ends, and when startup or shutdown ends. This allows the other PCs on the network to know how data acquisition is progressing. Refer to Help for details.
❸	Use this item to set a screen lock wait time. The screen is automatically locked if no operations are performed on screen within the preset time. **Reference** *"1.3.2 Screen Lock to Protect System" P.20*

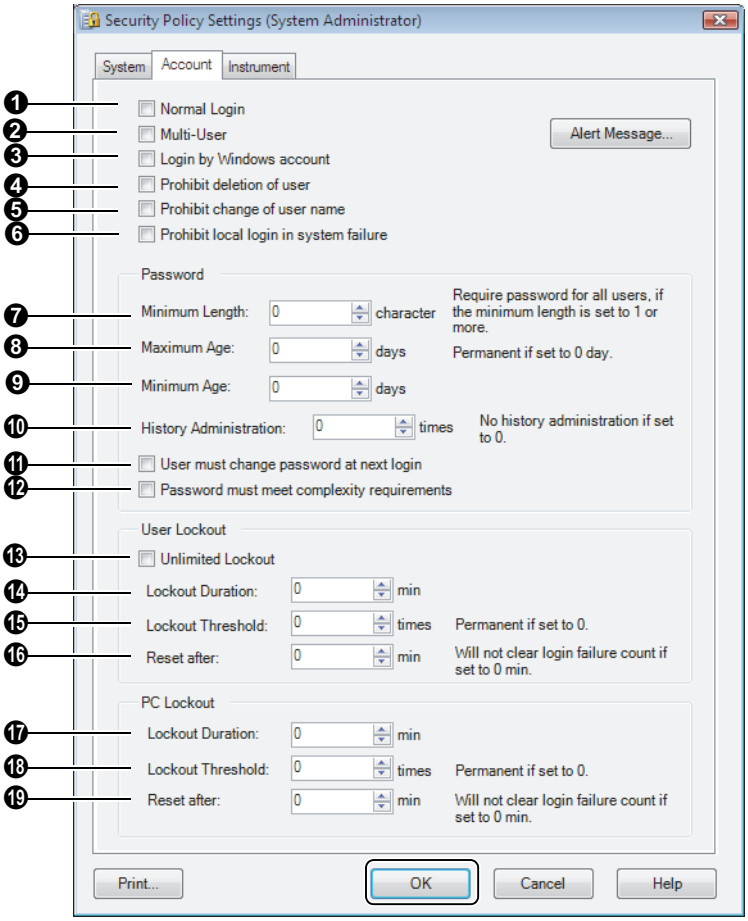
■ Account Policies

Determine how the user logs into the software, the minimum number of characters in passwords, password expiration date, and lockout operations to prevent illegal access.

1 **Double-click the (Security Policy) icon in the [Administration Tools] sub-window of the [LabSolutions Main] window.**

2 **Click the [Account] tab.**

3 **Set each item, and click [OK].**



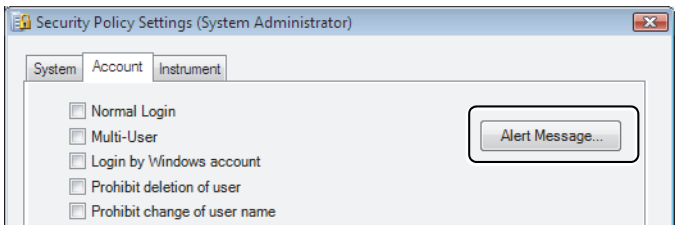
No.	Explanation
❶	Disables the list function for selecting registered user IDs in the [Login] window. When normal login is enabled, the ID of the previous user is displayed for the next software login.
❷	Enables multiple users to login on a single PC. The [LabSolutions Main] window matched to the rights of the logged in users is displayed. If this item is not selected, only one [LabSolutions Main] window can be opened on a single PC.
❸	If this item is selected, users can access the software directly and skip the [Login] sub-window as long as the user ID logged into the OS of the PC is registered in the software.

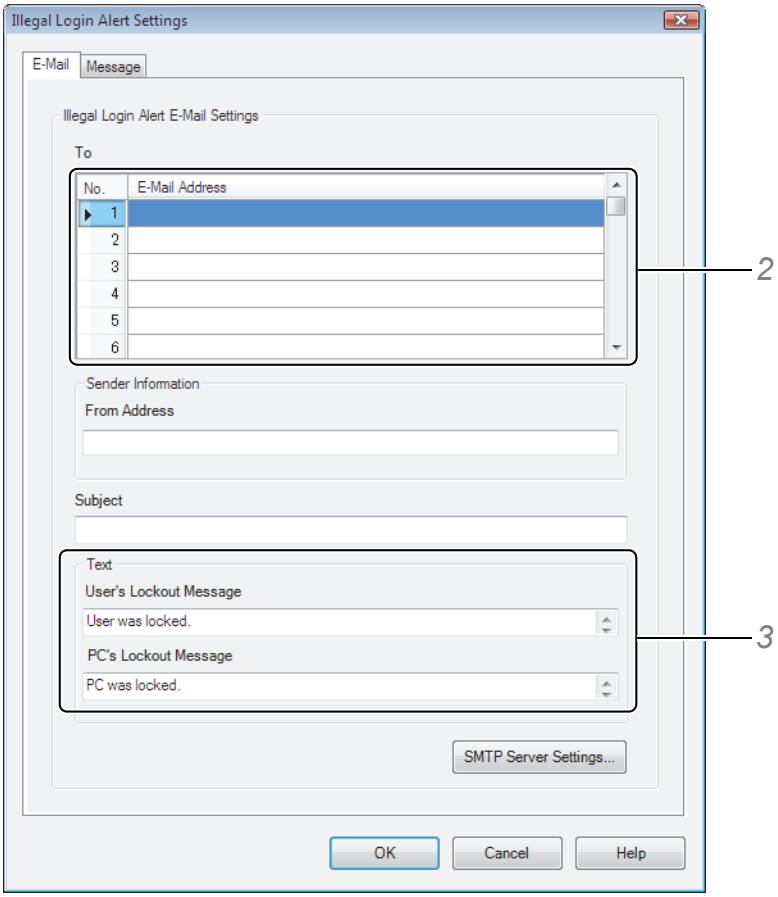
No.	Explanation
❹	Prohibits deletion of user information registered to the software. Deleted user administration information remains in the system but cannot be restored. If a user with the same name as a deleted user is registered, the newly registered user is regarded as a different user.
❺	Prohibits changes to registered user names. This item is automatically selected when user information is shared with CLASS-Agent.
❻	If this item is selected and there is a system failure, local login is prohibited.
❼	Sets the minimum number of characters in the password.
❽	Sets the expiration date of the password from the time it was first set or changed. If this item is set to 0, the password can be used indefinitely.
❾	Sets the number of days in which a new password may not be changed. If this item is set to 0, the password can be changed immediately after it is created.
❿	Sets the number of old passwords that are recorded to stop duplication when passwords are changed.
⓫	Select this item to force new users to change their password from the password that was distributed by the administrator.
⓬	If this item is selected, passwords must contain at least 6 characters with 3 of those characters being uppercase, lowercase, numbers, or symbols. Passwords comprised of only alpha-numeric characters will no longer be accepted.
⓭	If this item is selected and a user fails to login in the set number of attempts, said user is locked out of the system until a user with [Permit User Administration] privileges releases the user in the [Release User Lockout] sub-window.
⓮	If a user fails to login in the set number of attempts, this setting determines that amount of time that must pass until that user can login again. If this item is set to 0, user lockout is disabled.
⓯	Sets the maximum number of user login attempts. If this item is set to 0, users have an indefinite numbers of login attempts.
⓰	Sets the time that must pass before the login failure count is reset to 0 (zero). If this item is set to 0, login failure count reset is disabled.
⓱	If a the set number of PC login attempts is reached, this setting determines that amount of time that must pass until that PC can be used again. If this item is set to 0, PC lockout is disabled.
⓲	Sets the maximum number of login attempts that are permitted on a PC. If this item is set to 0, PCs have an indefinite numbers of login attempts.
⓳	Sets the time that must pass before the login failure count is reset to 0 (zero). If this item is set to 0, login failure count reset is disabled.

NOTE

- The lockout parameters protect PCs from illegal access.
  For example, if the attempt limit is 3 and the lockout time is 5, a user must wait 5 minutes if the wrong password is entered 4 times. If the correct password is input on the 4th attempt, the login failure count of 3 returns to 0 after 5 minutes pass.
- The administrator PC or other PCs can be notified that users and PCs have been locked out due to a wrongly entered password or an illegal access. Use the following procedure to enable illegal access notification. The messaging function is not used on Windows 7/Windows Vista. The message cannot be sent and received using the messaging function on Windows 7/Windows Vista.

1 Click [Alert Message].



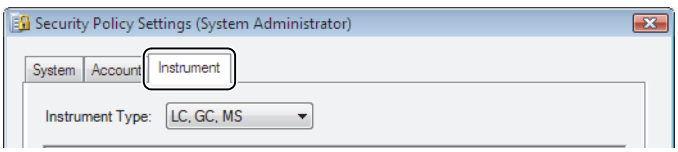


2 Enter the E-Mail Address or PC name where the notification is to be sent.
3 Enter the content of the message to send when a user or PC is locked out.

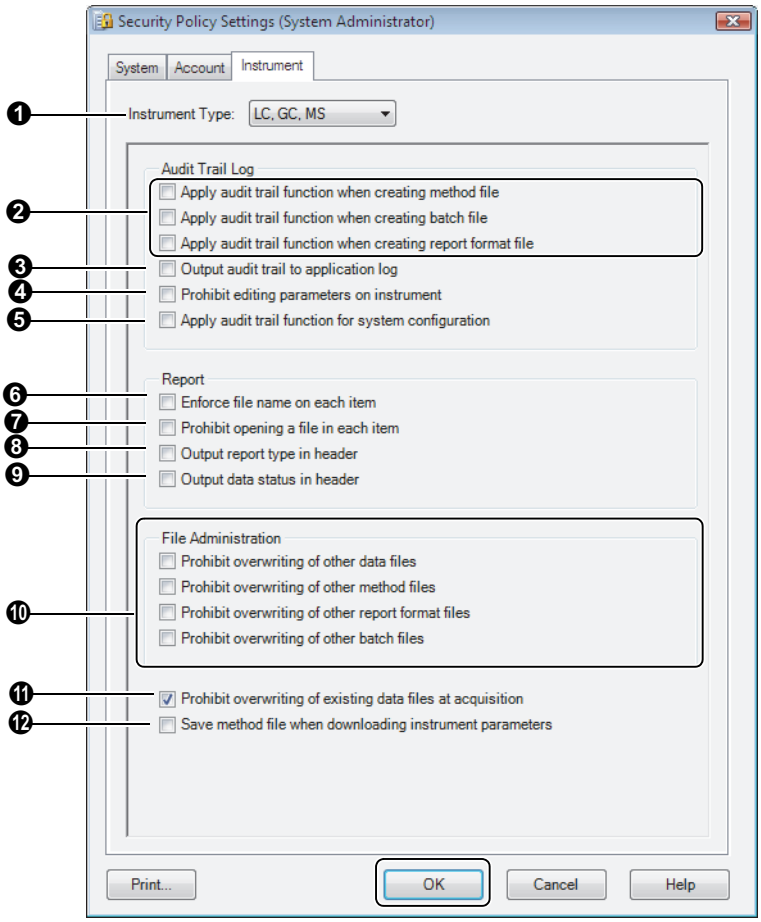
■ Instrument Policies

1 **Double-click the (Security Policy) icon in the [Administration Tools] sub-window of the [LabSolutions Main] window.**

2 **Click the [Instrument] tab.**



3 Set each item, and click [OK].



No.	Description
❶	The type of the instrument is displayed.
❷	Creates an audit trail log entry when new method, batch or report format files are created. **Reference** *"3.1.3 Audit Trail Log in Method Files, Batch Files and Report Format Files" P.58*
❸	Records audit trail entries to the log database so they can be viewed in [Log Browser] *(P.24)*.
❹	Prohibits editing of instrument parameters on the analytical instrument to prevent unauthorized manipulation of parameters.
❺	Creates an audit trail log entry when the system configuration is edited. **Reference** *"3.1.2 Audit Trail Log in System Configuration Files" P.57*
❻	Prints the name of the data file (method or batch) loaded to each report item in the header of the report item. If multiple report items have been added to a report, compare the file names to determine whether the report is for all of the items in a single file or from multiple files. If this is selected, the data file name is printed in all of the report item titles.
❼	Prohibits multiple files from being added to a single report item.
❽	Prints the report source in the report header (Single Run, Real Time Batch, Post Run Batch, Report Editor).
❾	Prints the status of the postrun data in the report header. [Temporary] indicates data that has been changed but not saved. [Manual Integration] indicates data that has undergone manual peak integration.
❿	Prohibits the overwriting of files with the same name and file type.
⓫	Prohibits overwriting of data files with the same name during single run and realtime batch analyses.
⓬	Overwrites method file when instrument parameters are downloaded.

1.2.2 Rights Groups

Make groups of operation rights that bundle multiple system operation rights according to the operation requirements for the software users.

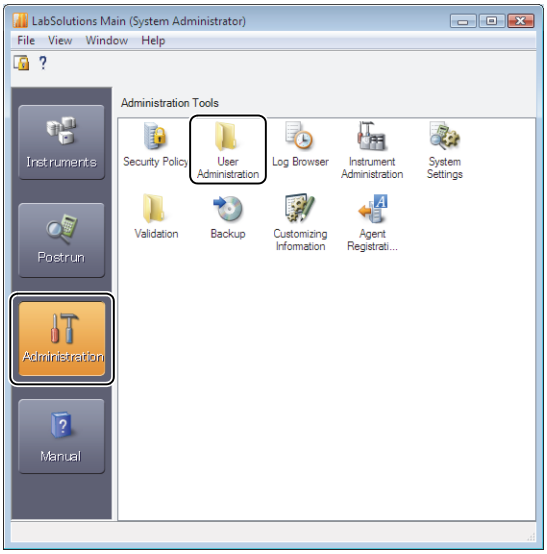
This section describes how to create new rights groups and edit the rights in each group.

NOTE

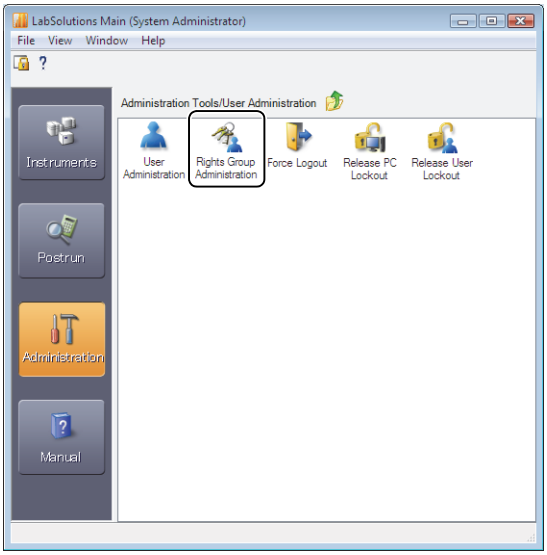
- Log in with a user ID having the [Permit User Administration] rights to register, change or delete rights groups.
- If [System Administrator] or [Permit User Administration] is selected, operations cannot be assigned in groups. The rights must be individually assigned in the [Add User] *(P.13)* or the [Edit User] sub-windows *(P.16)*.

■ New Rights Groups

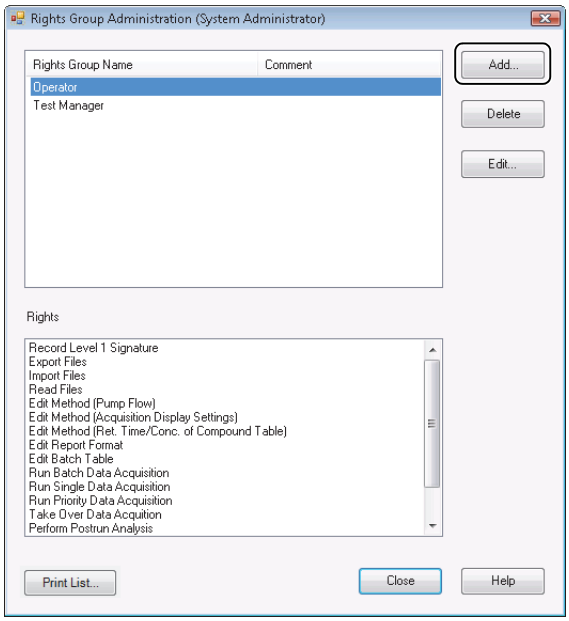
1 **Double-click the [User Administration] folder icon in the [Administration Tools] sub-window of the [LabSolutions Main] window.**



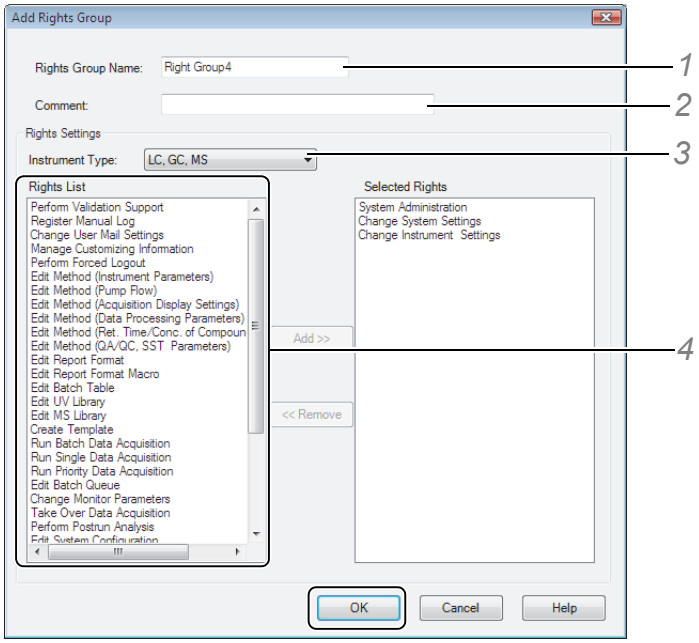
2 **Double click the (Rights Group Administration) icon.**



3 Click [Add].



4 Set each item to be added and move them to the [Selected Rights] box, then click [OK].

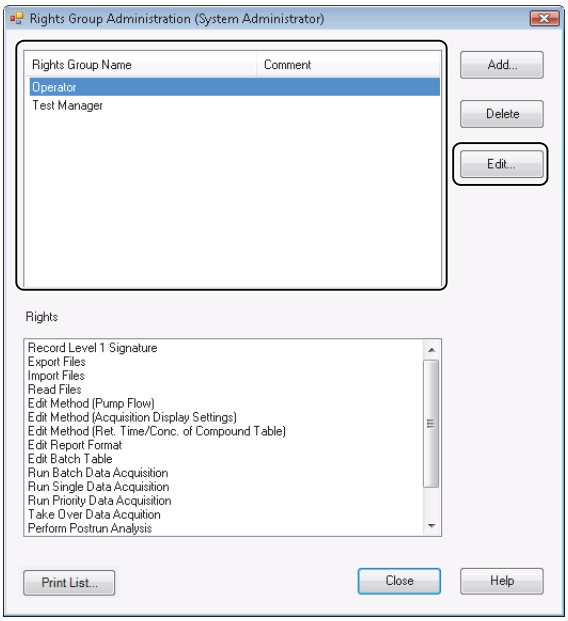


1 Enter the name for the rights group.
2 Enter a description for the rights group.
3 Specify the type of the instrument.
4 Either double-click the desired operation right one at a time in the [Rights List], or select multiple rights while holding down the [Ctrl] key and then click [Add].
The selected operation rights move to the [Selected Rights] list.
Rights can be returned to the [Rights List] with double-click or by clicking [Delete].

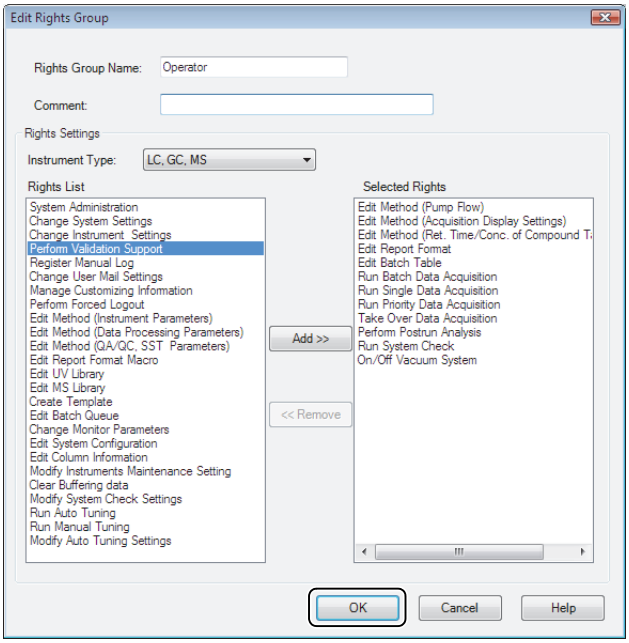
NOTE
There are two default rights groups, [Test Manager] and [Operator].

■ Edit the Operation Rights in a Group

1 **Double-click the name of the group to change in the [Rights Group Administration] sub-window, or select the rights group and click [Edit].**



2 **Add or remove the rights and click [OK].**



NOTE

- The edited operation rights for the users assigned to the selected group are enabled at the next login.
- Refer to Help for details on the operation rights.

1.2.3 User Registration

Users must be registered before they can use the software. When users are registered, the use of software operations can be monitored or restricted.

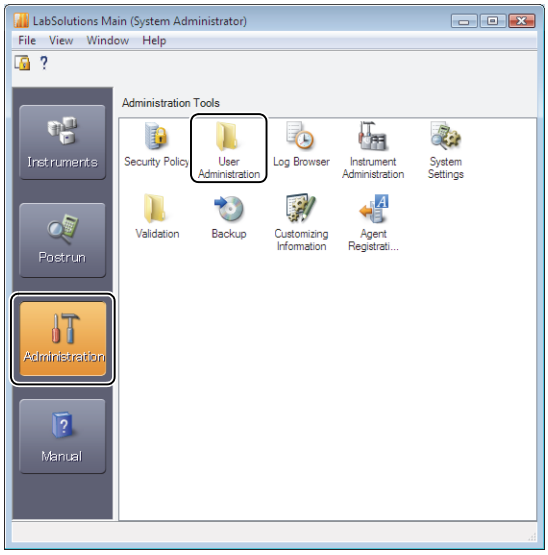
This section describes the procedures for registering new users and changing the rights of registered users.

NOTE

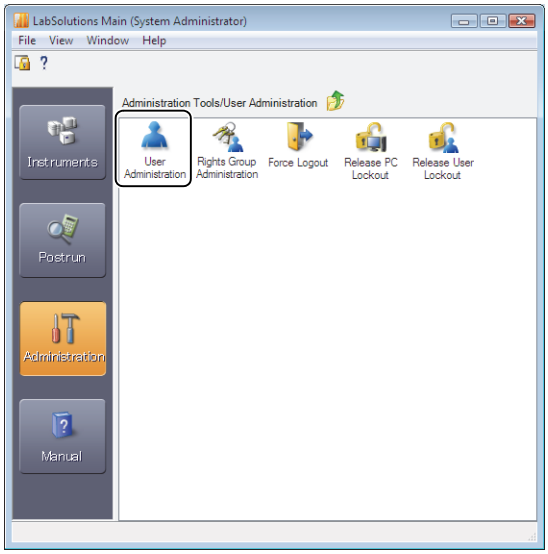
To register, change or delete users, log in by a user ID with [Permit User Administration] selected.

■ New Users

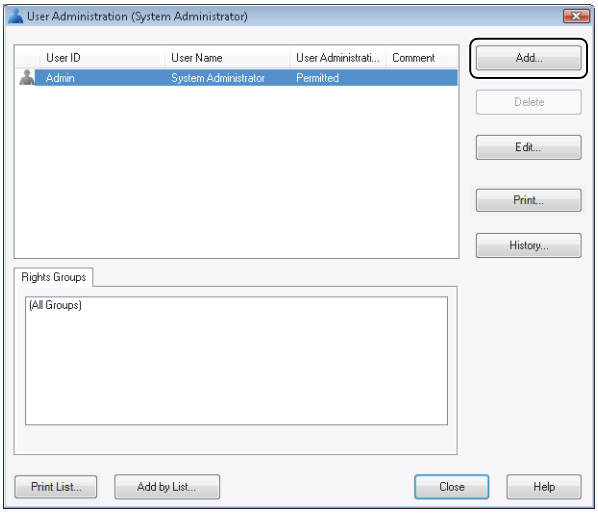
1 **Double-click the [User Administration] folder icon in the [Administration Tools] sub-window of the [LabSolutions Main] window.**



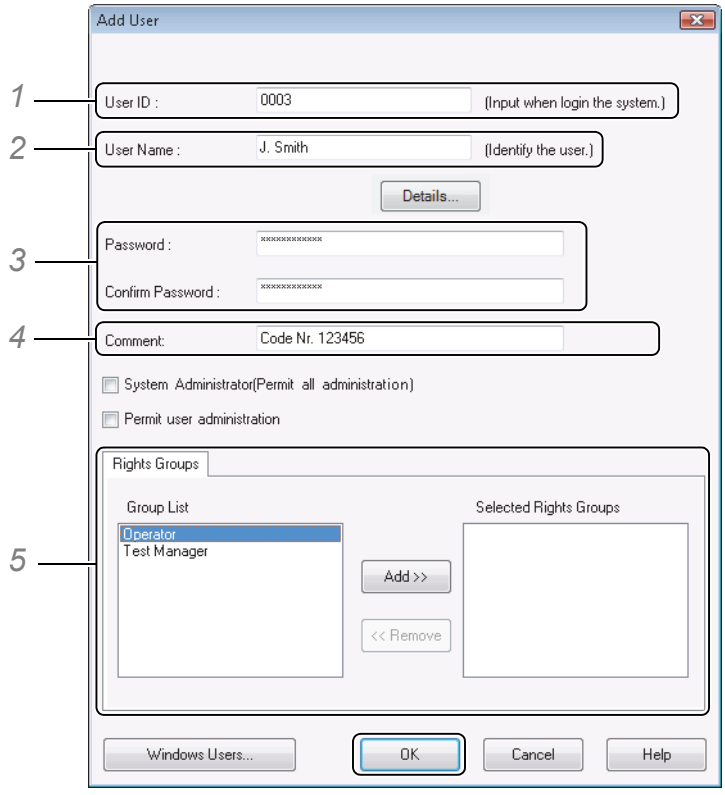
2 **Double click the (User Administration) icon.**



3 Click [Add].



4 Enter each of the following items, and click [OK].



1 Enter the user ID that will be used to log into the software.

NOTE

The User ID can be up to 31 characters in length. The User ID is not case-sensitive. All spaces entered before or after text strings are ignored.

Identical User IDs cannot be registered.

2 Enter the name of the user that will be displayed in the system.

3 If the [Minimum Length] of the password is set to 1 or more on the [Account] tab of the [Security Policy Settings] sub-window, enter the password that will be used at user login. Enter the same password in the [Confirm Password] box.

NOTE

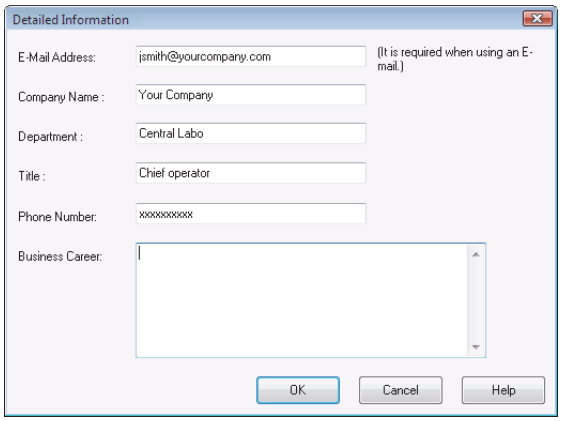
- The [Minimum Length] can include up to 14 alphanumeric characters and symbols. If [Password must meet complexity] is selected, passwords must contain at least 6 characters with 3 of those characters being uppercase, lowercase, numbers, or symbols and passwords comprised of only alpha-numeric characters will no longer be accepted.
- By using a combination of a user ID and password, the system can be operated by specific users at the operation level matched to their rights. Passwords are mandatory to securely manage data since use of both the user ID and password satisfies the electronic signature requirements.

4 Enter a user description as necessary.

5 Either double-click the user groups to individually move them to the [Selected Rights Groups] list, or select multiple groups with the [Ctrl] key held down, and then click [Add]. The selected groups move to the [Selected Rights Groups] list.
To return groups from the [Selected Rights Groups] list to the [Group List], either double-click a group in the [Selected Rights Groups] list, or select a group and click [Delete].

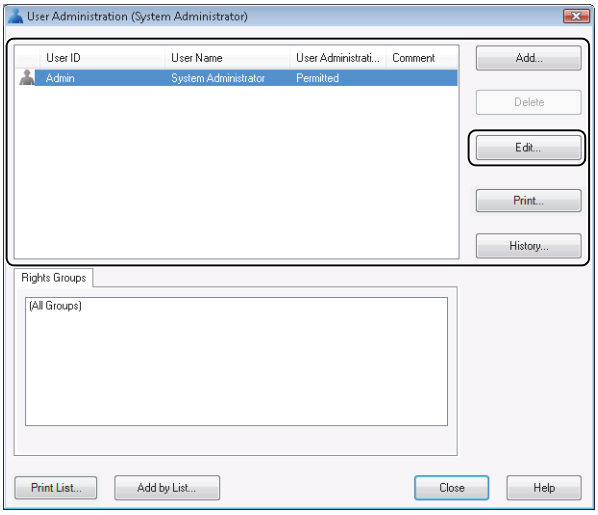
Other Operations

- If [System Administrator (Permit all administration)] is selected, [Permit User Administration] is automatically selected and that user becomes the system administrator.
- Click [Details] to enter the user's detailed information.

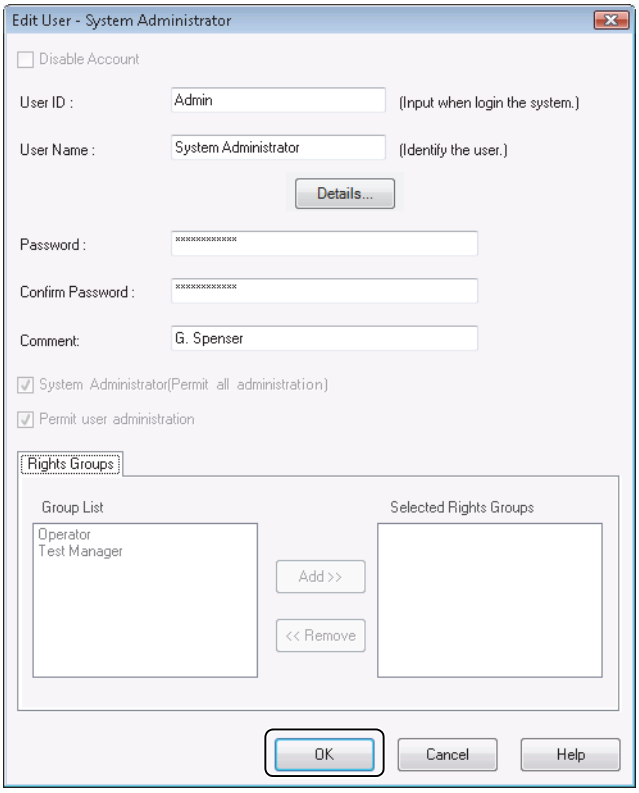


■ Change User Settings

1 **In the [User Administration] sub-window, double-click the user ID that needs to be changed, or select the user and click [Edit].**



2 **Make the desired changes, and click [OK].**



NOTE

- Select [Disable Account] to stop a user from logging into the software.
- If a user has been disabled, first deselect [Disable Account] to enable the user, and then change the desired settings.
- The system administrator (Admin) set at software installation cannot be deleted. Note that user IDs can be only be changed one time.
- If [Input reasons for the changes of user administration] is selected on the [System] tab *(P.4)* of the [Security Policy Settings] sub-window, a window opens to allow input of the reason for the change.

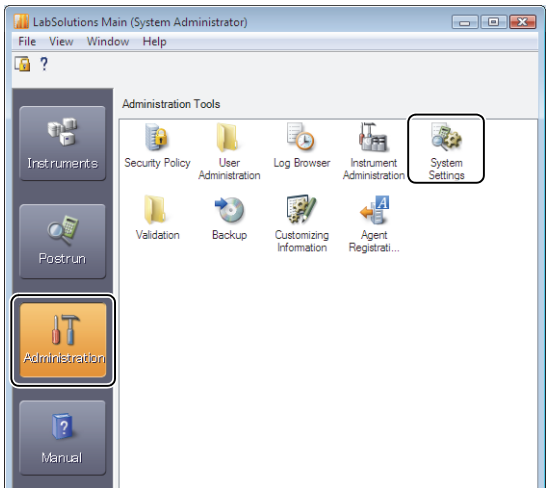
1.2.4 Numerical Rounding and Number of Displayed Digits

The rounding method and number of displayed digits can be batch-set in the [Data Proc. Settings] sub-window.

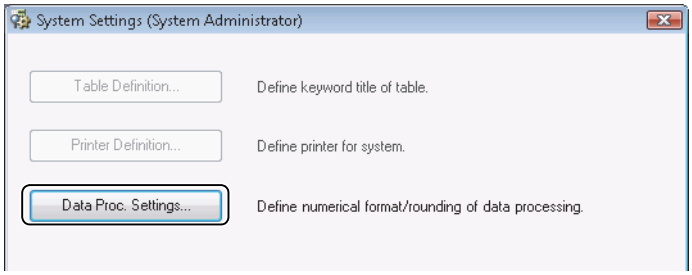
NOTE

Since system settings are changed in this sub-window, log in with a user ID having [Change System Settings] rights.

1 **Double-click the (System Settings) icon in the [Administration Tools] sub-window of the [LabSolutions Main] window.**

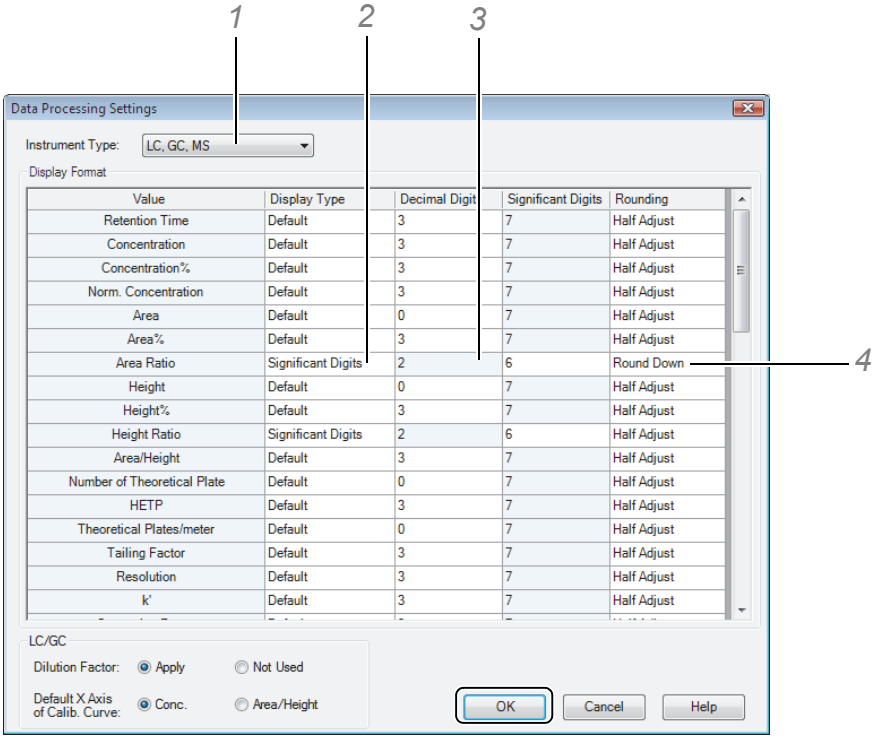


2 **Click [Data Proc. Settings...].**



3 Select the rounding method and number of displayed digits for specific calculation results, and click [OK].

In this example, the [Area Ratio] display format is set to 3 digits past the decimal point (i.e. the 4th digit past the decimal point is rounded down).



1 The type of the instrument is displayed.

2 Open the [Display Type] list for the [Area Ratio] row, and select [Default] from among [Default]/[Exponential]/[Significant Digits].

3 Enter 3 in the [Decimal Digits] column of the [Area Ratio] row.

4 Open the [Rounding] list for the [Area Ratio] row, and select [Round Down] from among [Half Adjust]/[Round Up]/[Round Down].

NOTE

If [Default] or [Exponential] is selected as the [Display Type], enter the number of decimal places in the [Decimal Digits] column, and if [Significant Digits] is selected, enter the number of digits in the [Significant Digits] column.

Other Operations (bottom of sub-window)

If [Apply] is selected for [Dilution Factor] the dilution factor is always calculated. If the dilution factor is not used for the sample, click [Not Used] and the dilution factor is ignored even if it is set in the MS data.

1.3 System Operation

Log into the system using the User Ids and Passwords to achieve secure system operation reliable data management. This process allows the system to be operated according to the assigned user rights.

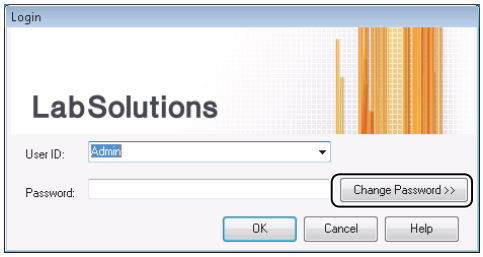
This section describes how to change user passwords and the screen lock function that protects the system.

1.3.1 Change User Passwords

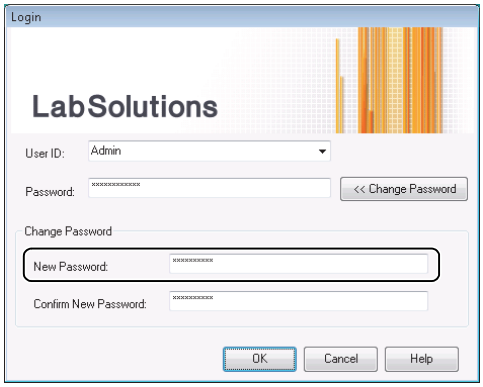
If the password expiration date has expired and a user attempts to log into the software, the password change sub-window opens. The user must change their password before they can enter the software.

This section describes the procedure for changing passwords. User passwords are only changed by the the user himself.

1 **Click [Change Password] in the [Login] sub-window.**



2 **Enter a [New Password].**



NOTE

- For security reasons, passwords are displayed as "*" on screen to make them unreadable to other people.
- Enter a password that is the [Minimum Length] or longer. The [Minimum Length] is set on the [Account] tab of the [Security Policy Settings] sub-window.

3 **Enter the same password again in the [Confirm New Password] box, and click [OK].**

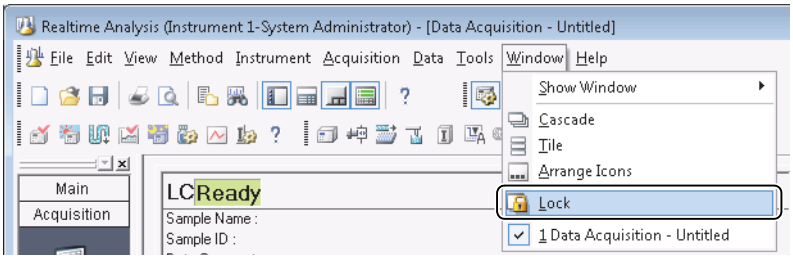
1.3.2 Screen Lock to Protect System

The [LabSolutions Main] window and sub-windows can be individually locked to protect the system from accidents or manipulation by other operators if the logged in operator temporarily leaves the PC.

When the lock function is enabled, the window is minimized and displayed as an icon on the taskbar. If the icon is clicked, the [User Authentication] sub-window opens to prompting the user to enter the user ID and password.

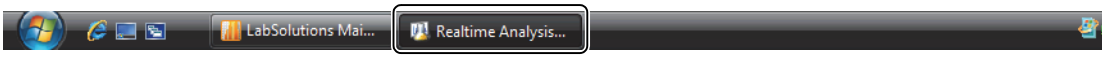
This section describes an example of how to lock screens in the [Data Acquisition] window.

1 **Click [Lock] on the [Window] menu.**

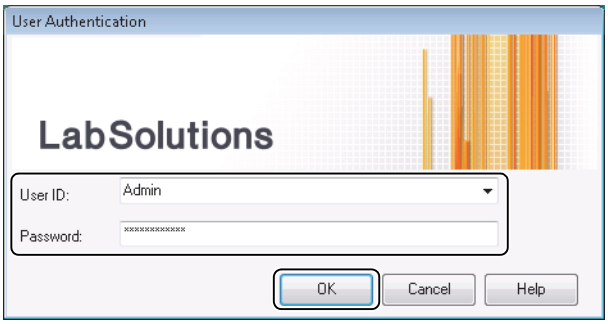


The [Data Acquisition] window is minimized and an icon is displayed on the taskbar.

2 **Click the [Realtime Analysis] icon on the taskbar to open the application.**



3 **Enter the [User ID] and [Password] for the user that locked the screen, and click [OK].**



NOTE

Only the user who locks the window can release the lock.

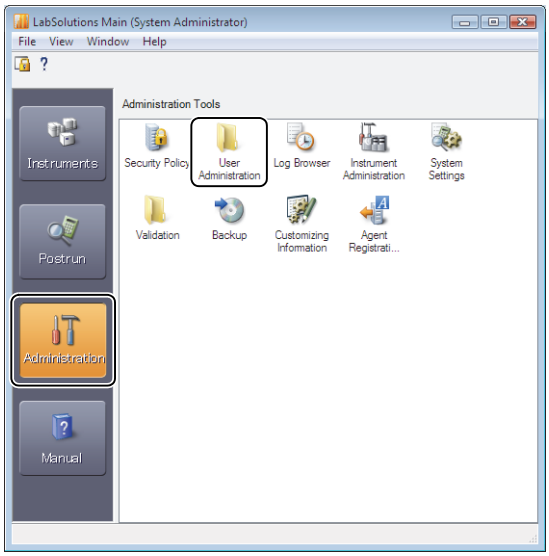
1.3.3 Release User or PC Lockout

Users and PCs that are locked because of an incorrect password or an illegal access to the software system can be released.

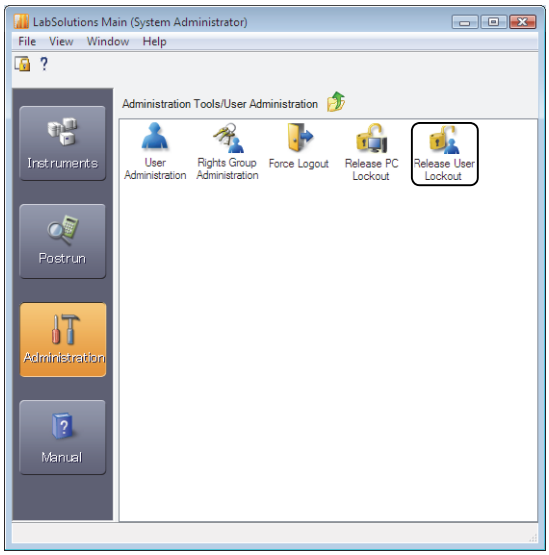
NOTE
To release a lockout, login with a user ID having [Permit User Administration] rights.

■ Release User Lockout

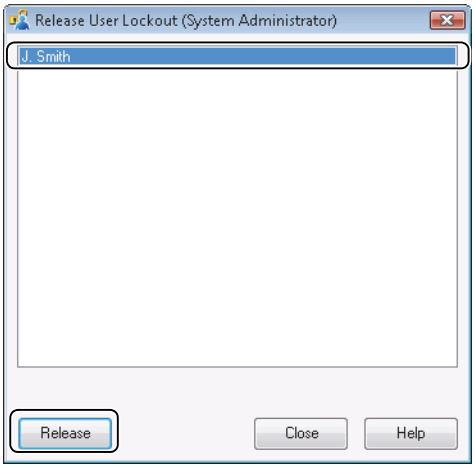
1 **Double-click the [User Administration] folder icon in the [Administration Tools] sub-window of the [LabSolutions Main] window.**



2 **Double click the (Release User Lockout) icon.**



3 **Select the user to be released, and click [Release].**



The selected locked out user is released, and can now re-enter the software.

4 **Click [Close].**

NOTE

- To release multiple locked out users, select the users, either with the [Ctrl] key held down or by selecting continuous users by dragging the mouse, and then click [Release].
- To release locked out PCs, click the (Release PC Lockout) icon in the [Administration Tools/ User Administration] window, and perform the same operation.
  Unlocked PCs can be used again by logging into the software from that PC.

1.3.4 Force Log Out Users

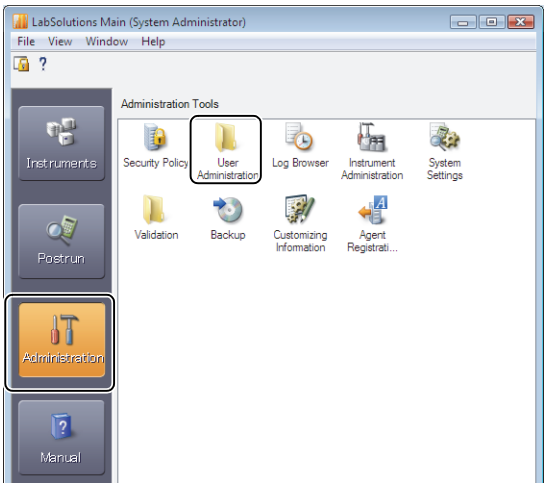
A user logged into the software can be forcibly logged out so that other users can use the analytical instrument that was being accessed by that user.

This section describes the procedure for forcibly logging out users logged into the software.

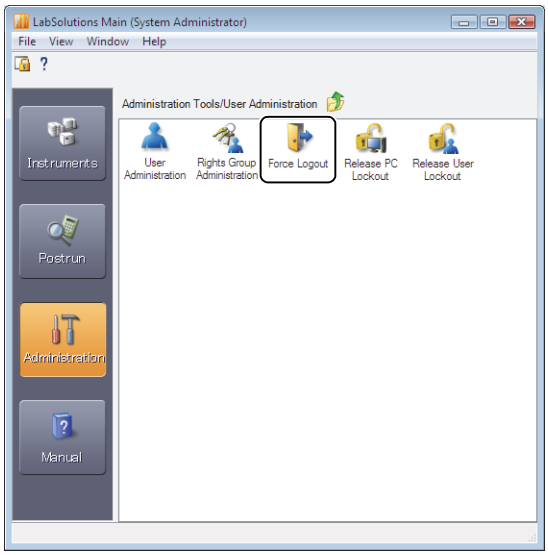
NOTE

To perform a force logout, log in by a user ID having the [Perform Forced Logout] rights.

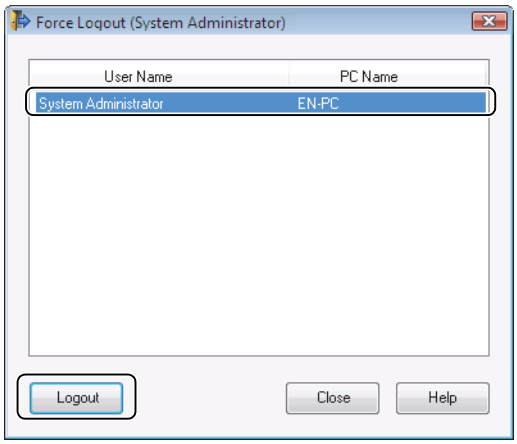
1 **Double-click the [User Administration] folder icon in the [Administration Tools] sub-window of the [LabSolutions Main] window.**



2 Double-click the (Force Logout) icon.



3 Select the user to be logged out, and click [Logout].



The selected user is forcibly logged out.

NOTE

- To forcibly log out multiple users, select the users, either with the [Ctrl] key held down or by selecting continuous multiple users by dragging the mouse, and then click [Logout].
- Files that are being edited at the time of a force logout are discarded.

1.4 System History Information

When changes are made to the system administration settings (user registration or passwords), a history of the changes is created.

View this history information in the [Log Browser]. The information can also be quickly filtered and displayed.

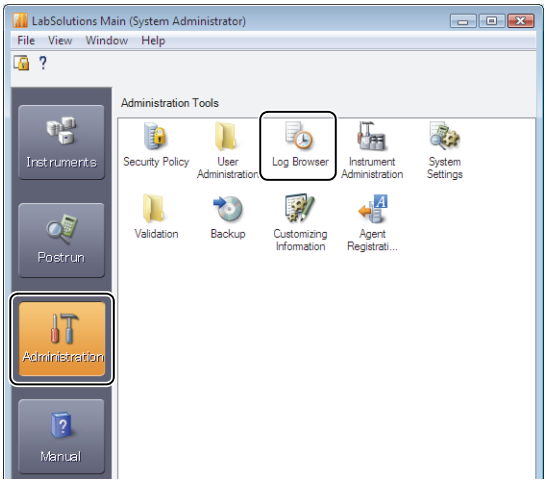
Check the history information of system administration to verify that preset security policies and user administration status are operating appropriately.

1.4.1 View History Information from the Log Browser

System administration change histories can be viewed from the [Log Browser]. histories for logins/logouts, data acquisition, addition of /disabling of users, can be searched and the results displayed on the screen.

Operation histories can be viewed from the [Log Browser]. Histories for logins/logouts, data acquisition, can be searched and the results displayed on the screen.

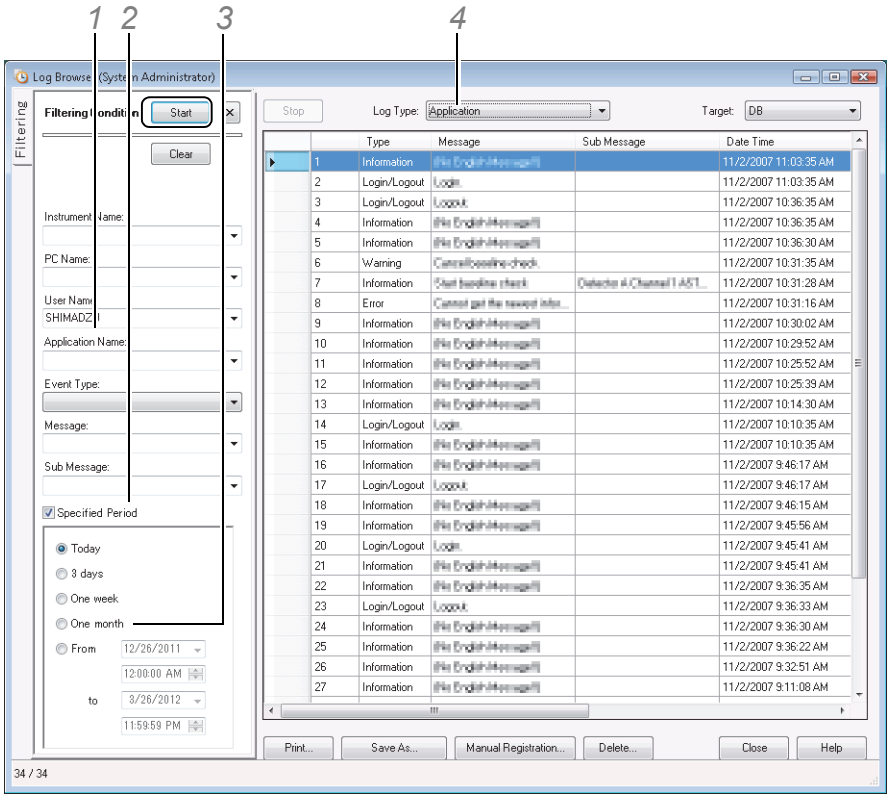
1 **Double-click the (Log Browser) icon in the [Administration Tools] sub-window of the [LabSolutions Main] window.**



The [Log Browser] opens with the latest log displayed.

2 Set the filtering conditions in the [Filtering Condition] section, and click [Start].

The following describes an example of how to display a history of changes made to the system by “User Name SHIMADZU” within the past month.



1 Enter “SHIMADZU” in the [User Name] box.

NOTE

If user name text strings exist from a previous filter operation, the history is displayed with user names that match the entered text strings.

2 Select [Specified Period].

3 Click [One month].

4 Click [Start].

5 Select [System Administration] from the [Log Type] list at the top of the [Log Browser] sub-window.

NOTE

[System Administration], [Application] and [User Authentication] are selectable from the [Log Type] list.

For example, when [Audit Trail] is selected from the [Event Type] list in the filtering conditions for a specific [Application Name], the audit trail log of data files or method files, can be viewed in [Log Browser].

A log matching the set filtering conditions is displayed.

Reference

For details on other filtering conditions, refer to Help.

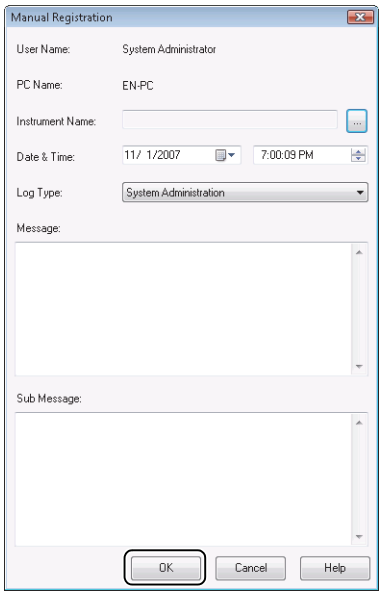
Other Operations (bottom of sub-window)

- Click [Print] to print a displayed log. Click [Save As] to save a displayed log to a CSV or text format file.
- Notes about events or users that are not automatically recorded by the system can be registered manually.
  Use the following procedure to manually enter logs entries.

NOTE

Log in with a user ID having the [Register Manual Log] rights to manually register log entries.

1 Click [Manual Registration].
2 Enter the necessary items, and click [OK].



The log entry is registered with the name of the user who manually created the log entry.

- Click [Delete] to delete the selected log. The currently displayed log must first be saved to a file before it can be deleted.

NOTE

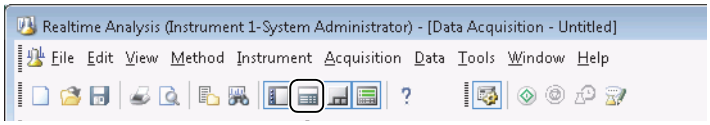
- Log in with a user ID having the [System Administration] rights to delete a log.
- Note that when a log is deleted, the entire log is deleted not just the range displayed on the screen.
- [User Authentication] cannot be deleted.

1.4.2 View History Information from the [Output Window]

A history of information about various operations and when an operator has logged into or out of the software can be viewed in the [Output Window] as well as in the [Log Browser]. The [Output Window] can be displayed in the [Realtime Analysis], [Postrun Analysis] and [Browser] programs.

This section describes an example of how to display [Output Window] in the [Data Acquisition] window.

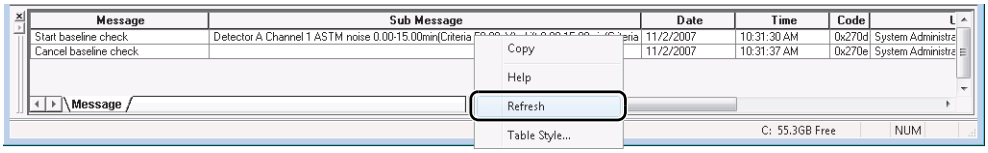
1 **Click (Toggle Output Window) on the toolbar in the [Data Acquisition] window.**



NOTE

The [Output Window] automatically opens when an error occurs during data acquisition (single run or realtime batch).

2 **Right-click on the [Output Window], and click [Refresh] in the displayed menu.**



The history information is refreshed.

Other Operations (bottom of sub-window)

- To hide [Output Window], click (Toggle Output Window) again.
- Double-click a row in the log to open the Help window for that particular message.

NOTE

Only logs from the current software session are displayed in the [Output Window]. To view previous histories, use the [Log Browser].

2 Data Management

The software contains various data management functions.

This chapter describes the operations of the [Data Explorer] sub-window and how to use files to efficiently manage acquired data and analysis results.

2.1 File Formats

The software uses the following file formats to handle acquired data and related information:

- Method files
- Data files
- Report format files
- Batch files
- UV spectrum files
- Other files

This section describes each of the file formats.

2.1.1 Method Files

Method files store information such as instrument parameters and data processing parameters.

The file extension of method files is ".lcm" for the LC, and is ".gcm" for the GC.

Method files store the following information.

Stored Information	Explanation
System Configuration Information	System configuration information is saved in the method files to allow for review of the instrument parameters.
Instrument Parameters	This information includes the instrument parameters for each instrument and also the baseline check settings.
Data Processing Parameters	Calibration curve information, column performance parameters, QA/QC parameters, peak integration parameters, identification parameters, quantitative parameters, and Compound/Group Tables are all saved in the method file.
Display Properties	The chromatogram XY range setting, whether the status bar is displayed or hidden, etc. are also saved in the method file.

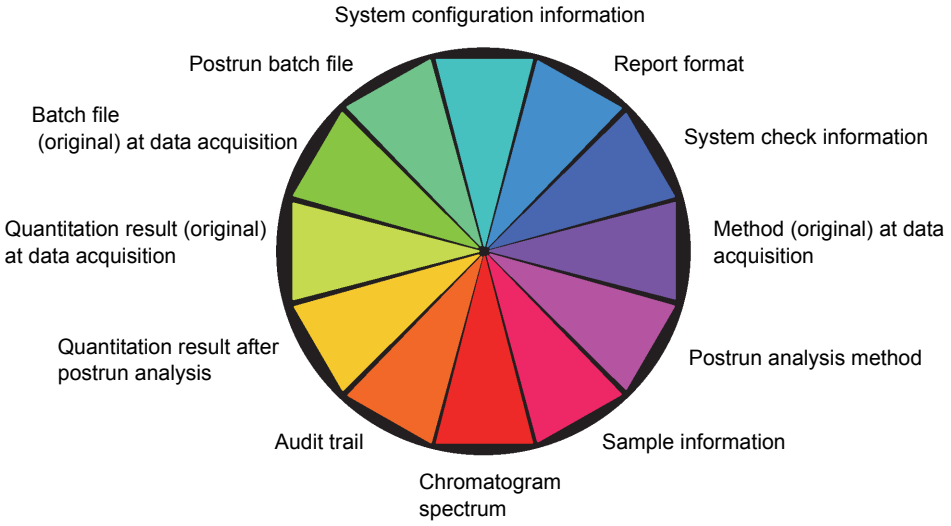
2.1.2 Data Files

The software stores the method files, batch files and report format files, chromatogram data, and quantitation results in a single data file. This structure is called an “All-In-One” structure and, since the data acquisition and analysis parameters are referenced from the same data file, it ensures the traceability of data.

If an MS detector is used, the tuning file is also saved in the data file.

The file extension of data files is ".lcd" for the LC or LCMS, and is ".gcd" for the GC.

■ Information Saved in Data Files



NOTE

- Edited data processing parameters are saved in the data file during postrun analysis. Click the 

(Apply to Method) icon on the [Data Analysis] assistant bar to save the edited data processing parameters as a method file for use in another data acquisition.
Refer to the Operators Guide or Help for more details.
- The report formats are also saved to the data file. Click [Data Report] on the [File] menu, then select [Print] to print the acquisition results of the currently loaded data file according to the report format stored with that data.
The report format can be edited by clicking the [Data Report] icon in the [Data Analysis] assistant bar to display the [Report] window. Click [Save Report Format File As] on the [File] menu to save the edited format for use with other data reports.

2.1.3 Report Format Files

Items such as pictures or logos and placeholders for chromatograms, results and etc., are pasted into the blank format and it is saved for future printing of data acquisition results.

The file extension for report format files is “.lsr”.

If a report format file is set at the time of data acquisition or postrun analysis, the results can be immediately printed according to that format.

Reference

Refer to the Operators Guide or Help for details on the report format files.

2.1.4 Batch Files

Data such as sample information and quantitative calculation conditions, are saved to a batch file during sequential measurement of multiple samples.

The item displayed in the Batch Table and the overall batch processing parameters are also saved to the batch files.

The file extension of batch files is ".lcb" for the LC, and is ".gcb" for the GC.

☞ Reference

Refer to the Operators Guide or Help for details on how to set batch files.

2.1.5 UV Spectrum Files

The software uses the JCAMP format with the file extension of ".jcm" for the UV spectrum file.

When peak identification using the similarity of UV spectra is performed, jcm files are included in the Compound Table as standard spectrum. The ".jcm" files can also be registered as spectra to the UV library files.

2.1.6 Other Files

The software uses the following files in addition to those described above.

File Name	Contents
Tuning Files	The conditions used to perform instrument adjustment (tuning) and the tuning results are saved. The file extension is ".lct".
UV Library Files	These files contain multiple UV spectrum data. They are used to perform library searches on the spectrum information for unknown samples. The file extension is ".llb".
MS Library Files	These files contain multiple MS spectrum data. They are used to perform library searches on the spectrum information for unknown samples. The file extension is ".lib".
Browsing Files	These files store information such as compound information displayed in [Quantitative Results View] and the names of method and data files loaded in the [Quant Browser] window. The file extension is ".lcq".
Layout Files	These files store information such as data file names and display layouts loaded in [Data Browser]. The file extension is ".lyt".
System Configuration Files	These files hold the link information for the PC and analytical instruments, names of the instruments that make up the system, and information on consumables. These file names are not used for regular operations.
PDF Files	These files contain electronic versions of printed reports. These files are a generic format that satisfies the requirement of human readable data, and are used when registering and managing the data acquisition result reports in a database.

2.2 [Data Explorer] Sub-Window

The [Data Explorer] sub-window has many features to efficiently manage method and data files. The contents of the files displayed in the [Data Explorer] sub-window can be loaded into a related window by double-clicking the desired file, or dragging-and-dropping the file onto the desired window.

This section describes operations in the [Data Explorer] sub-window.

■ Display the [Data Explorer] sub-window

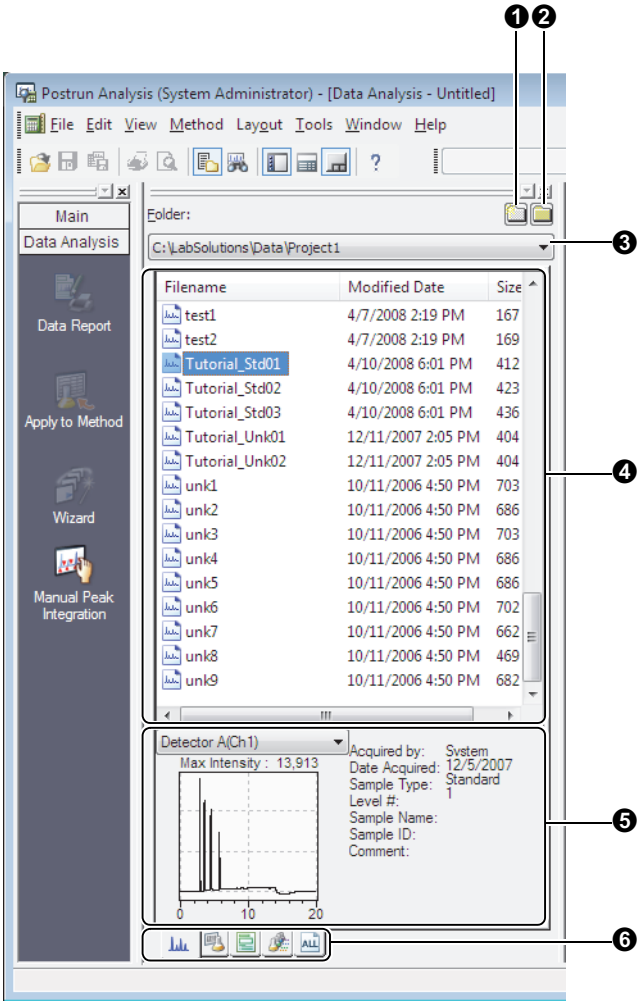
The [Data Explorer] sub-window can be displayed from the [Data Acquisition], [Data Analysis] and other windows.

If the [Data Explorer] sub-window is hidden, use the following procedure to display it.

1 **Click the (Toggle Data Explorer) icon on the toolbar.**

NOTE

To hide the [Data Explorer] sub-window, click the (Toggle Data Explorer) icon on the toolbar again.



No.	Explanation
❶	Creates a new folder, and copies the files in the currently displayed folder to this new folder.
❷	Click this icon to change the displayed folder. **Reference** For details, refer to *"2.2.1 Change the Displayed Folders" P.34*.
❸	The name of the current folder is displayed in this box. Up to 10 of the most recently displayed folders can be displayed by clicking . To display files in a different folder, select the folder name from the list and click the desired files.
❹	Displays a list of files in the currently displayed folder.
❺	Displays the chromatogram and file information for the selected file. If this information is hidden, use the right-click menu and select [Data Preview] to display the preview information. When a PDA detector is used, a Max Plot chromatogram is displayed. When an MS detector is used, the TIC of all segments and events is displayed. **NOTE** When multiple detectors are used, open the pull-down list at the top of the preview pane, and select the desired detector channel.
❻	Click the desired tab at the bottom of the [Data Explorer] to display only method files, data files, report format files, or batch files. Only the files with that specific file extension will be displayed.

Other Operations

- Information, such as, data acquisition date and sample name can be displayed in the list by right-clicking the [Data Explorer] sub-window, and selecting [File View] - [Detail] and then right-click again and select [Show File Information]. In the [Detail] display, the list can be sorted in ascending or descending order by clicking a column title such as [Acquired] or [Modified by].

  NOTE
  When [Show File Information] is selected, it may take time to display information depending on the number of files.

- The [Data Explorer] sub-window can be docked or displayed as a floating window. The docking position can be changed to the top, bottom, left or right of a window by dragging the title section of the [Data Explorer] sub-window to the desired location.
- The data preview position can be changed by clicking [Arrange Bottom] or [Arrange Right] from the data preview right-click menu.
  Change this data preview position depending on whether the [Data Explorer] docking position is horizontal or vertical.

2.2.1 Change the Displayed Folders

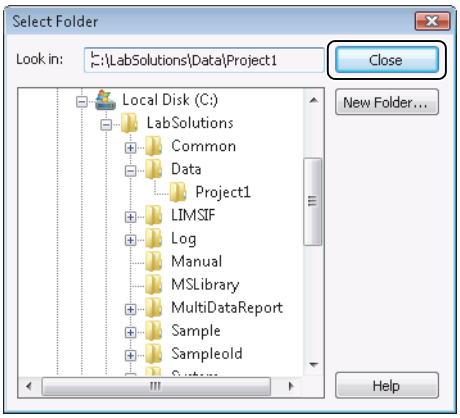
This section describes the procedure for changing the folders that are displayed in the [Data Explorer] sub-window.

1 **Click (Select Folder) in the [Data Explorer] sub-window.**

2 **Select the folder to display in the [Select Folder] sub-window, and click [Close].**

NOTE

Clicking a folder in the [Select Folder] sub-window displays that folder in the [Data Explorer] sub-window.



The [Select Folder] sub-window closes. The content of the selected folder is displayed in the [Data Explorer] sub-window.

2.2.2 Convert File Formats

Some files created in previous versions of this workstation can be updated in the [Data Explorer] sub-window.

■ Convertible File Types

The following file formats can be converted.

Original File Formats	File Formats After Conversion
LabSolutions data files	AIA files ASCII files PDF files JCAMP files (MS only)
LabSolutions batch files	ASCII files
CLASS-LC10 files (methods, raw data, calculation result, library)	LabSolutions files (extension: lcm, lcd or lib)
CLASS-LC10 spectrum files	JCAMP files
CLASS-VP files (methods, raw data, calculation result)	LabSolutions files (extension: lcm or lcd)
CLASS-VP spectrum files	JCAMP files
CLASS-GC10 files	LabSolutions files (extension: gcm or gcd)

Original File Formats	File Formats After Conversion
CLASS-VP4 files (methods, raw data, calculation result)	LabSolutions files (extension: gcm or gcd)
CHROMATOPAC files (analysis, raw data, calculation result)	LabSolutions files (extension: lcm, lcd, gcm or gcd)
AIA files	LabSolutions files (extension: lcd or gcd)
ASCII files	LabSolutions files (extension: lcd or gcd)
JCAMP files (LC, MS only)	LabSolutions files (extension: lcd)

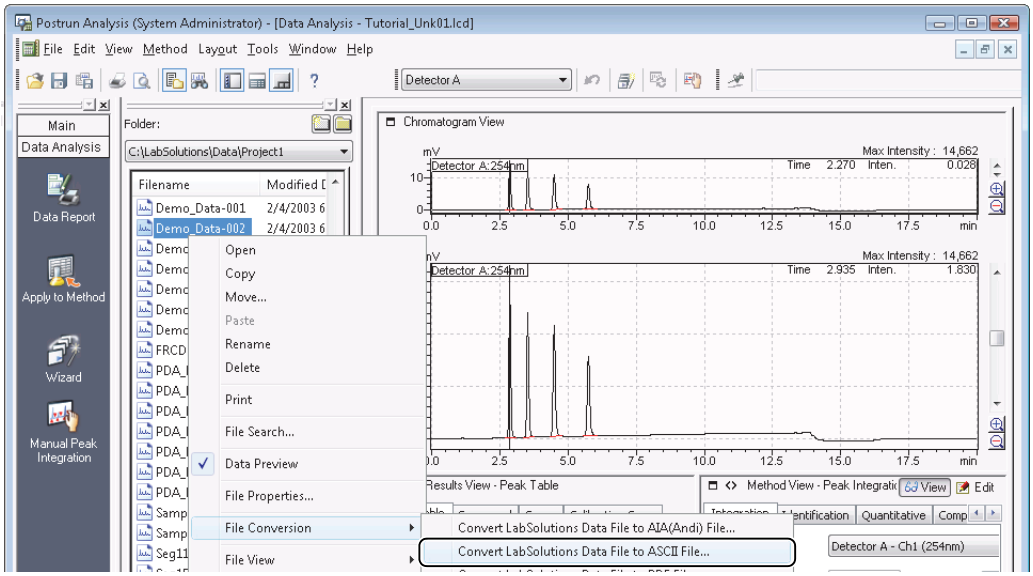
NOTE

Convertible file formats differ according to the installed license.

■ File Conversion

This section describes the procedure for converting data files to ASCII files.

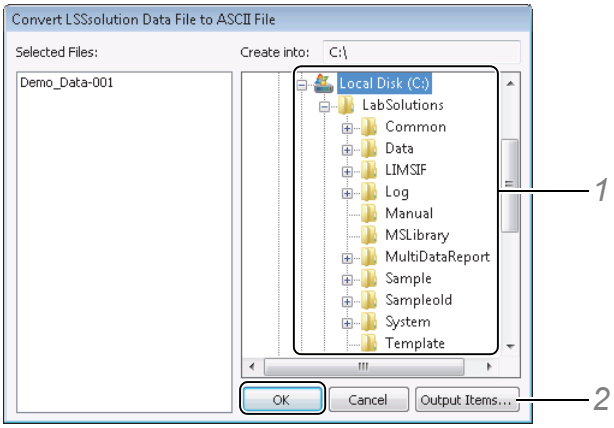
1 **Right-click the file to convert and select [File Conversion], and click [Convert LabSolutions Data File to ASCII File...].**



NOTE

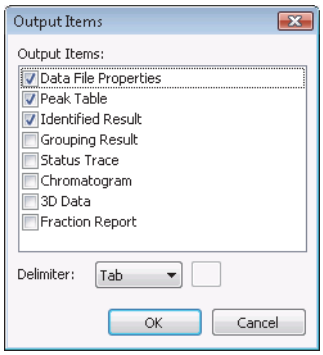
- To convert multiple files, either click the files with the [Ctrl] key held down, or drag the mouse to select files.
- The sub-menu displayed on the [File Conversion] menu differs according to the tab that is selected.
  Refer to Help for details.

2 Select the folder to save the converted file in and the items to output, then click [OK].



1 Select the folder where the converted file will be saved.

2 Select the items to be output in the [Output Items] sub-window.



The converted file is saved to the destination.

NOTE

Display items differ according to the instrument in use. Refer to Help for details.

2.3 File Search

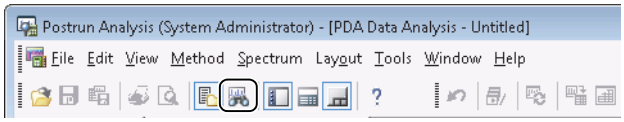
Use the file search function to easily search for data files, method files and other files using sample information as keywords. File information and chromatograms can be previewed in the search results sub-window.

Set the search conditions in the [LabSolutions File Search] sub-window.

This section describes how to set search conditions in the [Data Analysis] window.

2.3.1 Search Conditions

1 **Click (Search Files) on the toolbar.**

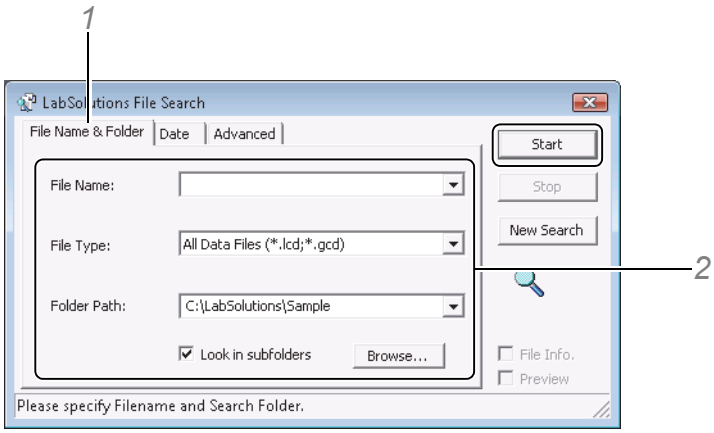


2 **Set the search conditions, and click [Start].**

The data file is searched according to the set conditions.

The search results are displayed at the bottom of the [LabSolutions File Search] sub-window.

[File Name & Folder] Tab



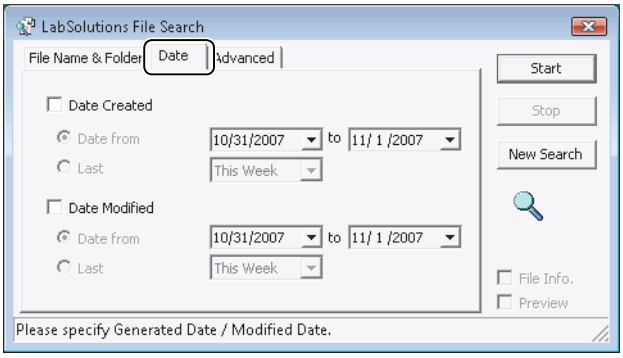
1 Click the [File Name & Folder] tab.
2 Enter the [File Name], [File Type], and [Folder Path] search items.

NOTE

- Select search conditions from a list of the 5 most recent conditions.
- Click [New Search] to clear the search conditions.

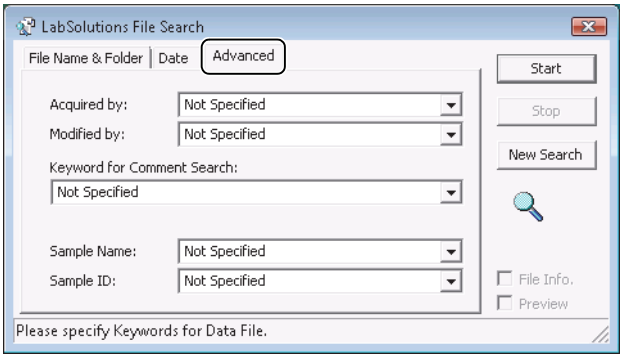
[Date] Tab

Specify a date on the [Date] tab to search by file creation date or modification date.



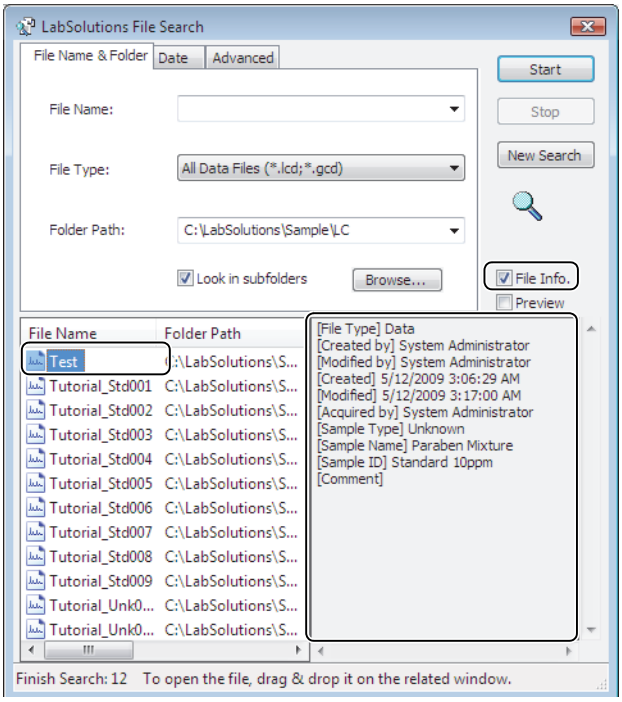
[Advanced] Tab

Use the [Advanced] tab to search by operator name, editor name, sample name, sample ID, and other filtering conditions.

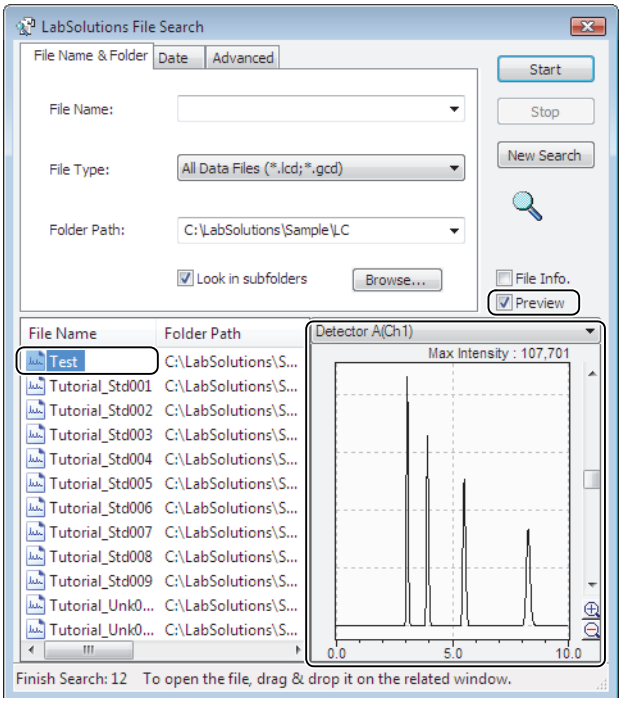


3 Check the search results.

To display the sample information of a specific file, select [File Info.] and click the file in the search results list.



To preview the chromatogram of a specific file, select [Preview], and click the file in the search results list.



NOTE

- Files displayed in the search results sub-window can be opened in other sub-windows by dragging-and-dropping them into the desired sub-window.
- Click (Close) to close the [LabSolutions File Search] sub-window.

2.4 Template Files

Prepare a template file containing preset parameters to ease the trouble of file setup and prevent setup errors when making new method files, report format files, and batch files.
This feature is useful for acquiring data by predetermined data acquisition settings.

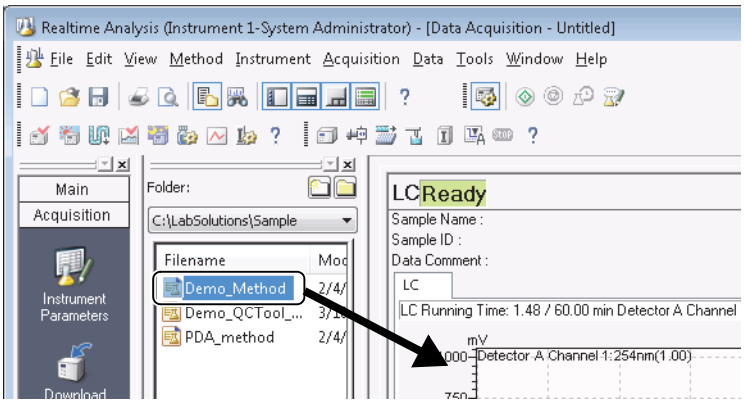
This section describes the procedure for saving method files, etc. as templates, and the procedure for using a template file to make new files.

2.4.1 Template Files Registration

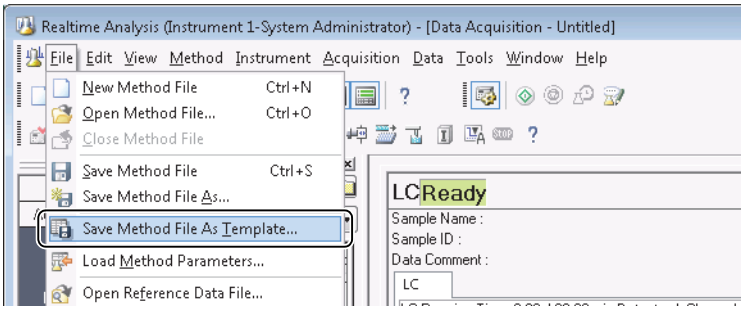
Registered (saved) template files are managed in an exclusive folder. This prevents the inadvertent overwriting of files.

This section describes how to register a method file loaded in the [Data Acquisition] window as a template file.

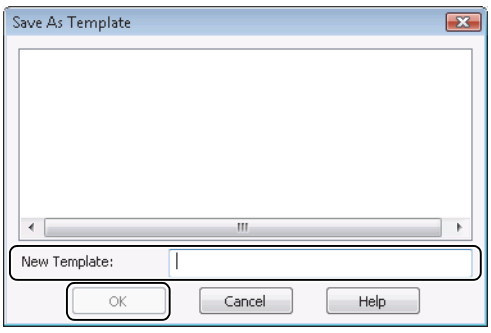
1 **Drag-and-drop the method file into the [Data Acquisition] window from the [Data Explorer] sub-window.**



2 **Click [Save Method File As Template] on the [File] menu.**



3 **Enter the template file name in the [New Template] box, and click [OK].**



The template is created.

NOTE

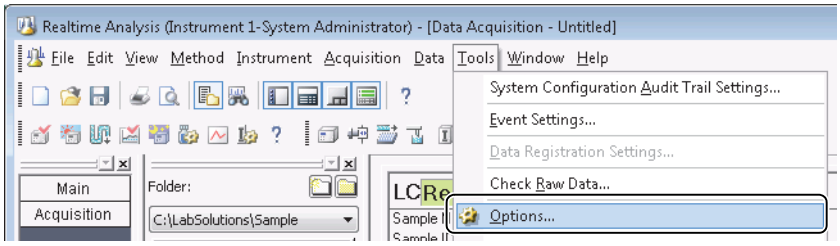
Batch Tables and report format files can be registered as template files from the following menus:

- Click [Save Batch As Template] on the [File] menu in the [Realtime Batch] window or the [Postrun Batch] window.
- Click [Save Report Format As Template] on the [File] menu in the [Report] window.

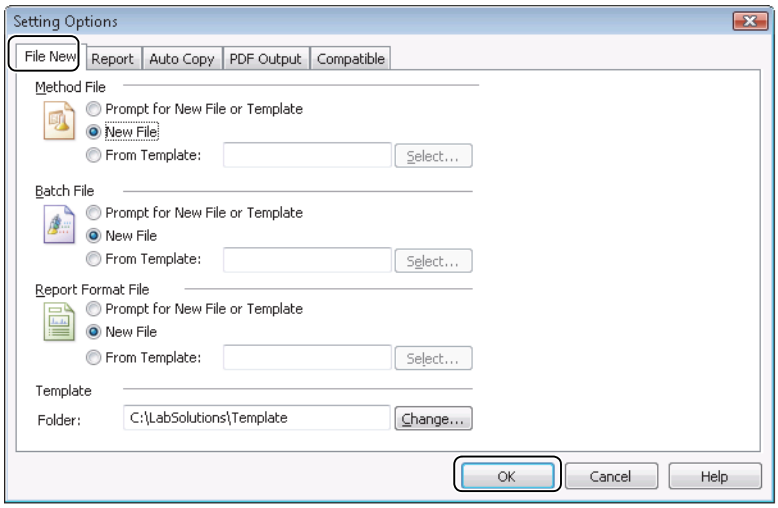
2.4.2 Create a New File from a Template File

The method for loading template files must be set before new files are made from template files.

1 **Click [Options] on the [Tools] menu.**



2 **Click the [File New] tab, set the operation for each file type, and click [OK].**



NOTE

- When [Prompt for New File or Template] is selected, the template selection sub-window opens when a new file is made.
- To always make new files from the same template file, select [From Template], and select the desired template file.

2.5 Link with CLASS-Agent

This section describes how to link LabSolutions users and result data with CLASS-Agent.

NOTE

The following information of LabSolutions shall be initialized in case that changing from the LabSolutions user authentication database to the CLASS-Agent user authentication database.

- Instrument System Configuration Settings
- Security Policy Settings
- Rights Groups Settings
- User ID, User Name, Password
- Data Proc. Settings
- Agent Registration Settings

Reference

Refer to the Instruction Manual to register the information again.

- For details Instrument System Configuration Settings, refer to “3 System Configuration in the Installation&MaintenanceGuide”.
- For details Security Policy Setting, refer to *"1.2.1 System Administration Policy (Security Policy)" P.4*.
- For details Rights Group Setting, refer to *"1.2.2 Rights Groups" P.10*.
- For details User ID, User Name, Password, refer to *"1.2.3 User Registration" P.13*.
- For details Data Proc. Settings, refer to *"1.2.4 Numerical Rounding and Number of Displayed Digits" P.17*.
- For details Agent Registration Settings, refer to *"2.5.3 Store Result Data on the CLASS-Agent Database" P.52*.

2.5.1 Preparations

■ Share Users

1 **Check the version of the Shimadzu CLASS-Agent User Authentication Tool.**

Open the Shimadzu User Authentication Tool from the [Control Panel].
Verify that the version in the title is 1.08 or later.

NOTE

If the version is earlier than 1.08, first upgrade the Shimadzu User Authentication Tool to the latest version.

2 **If CLASS-Agent uses an SQL server (MSDE) user authentication database, install LabSolutions on the server or client PC where the database is installed.**
If CLASS-Agent uses an Oracle user authentication database, install LabSolutions on the server where the database is installed.

NOTE

Oracle supports version 9j and 10g.

SQL server supports version 2000 and 2005.

3 **If the LabSolutions user and the Windows domain user are to be the same, setup the server installed with the existing authentication database so that it participates in the Windows domain. This process is common to both SQL server and Oracle databases.**

Add the following two users to the Windows domain:

- User name: SHIMADZU_USER
  Password: S#0758231443Da (Entry is case-sensitive. Enter the password accurately.)
  Rights: DomainUsers

- User name: Admin
  Password: Any
  Rights: DomainUsers

■ Store Result Data

1 **Check the version of the CLASS-Agent Manager.**

Open the CLASS-Agent Manager, click [About Agent Manager] on the [Help] menu, and verify that the version displayed in the sub-window is 2.32 or later.

NOTE

- If the version is earlier than 2.32, first upgrade the CLASS-Agent Manager to the latest version.
- The CLASS-Agent Manager must be installed on the LabSolutions client before result data can be stored.

2.5.2 Use an Existing CLASS-Agent User Authentication Database

The following procedure enables LabSolutions users and existing CLASS-Agent users to be administered in an integrated manner.

■ SQL Server (MSDE) CLASS-Agent User Authentication Database

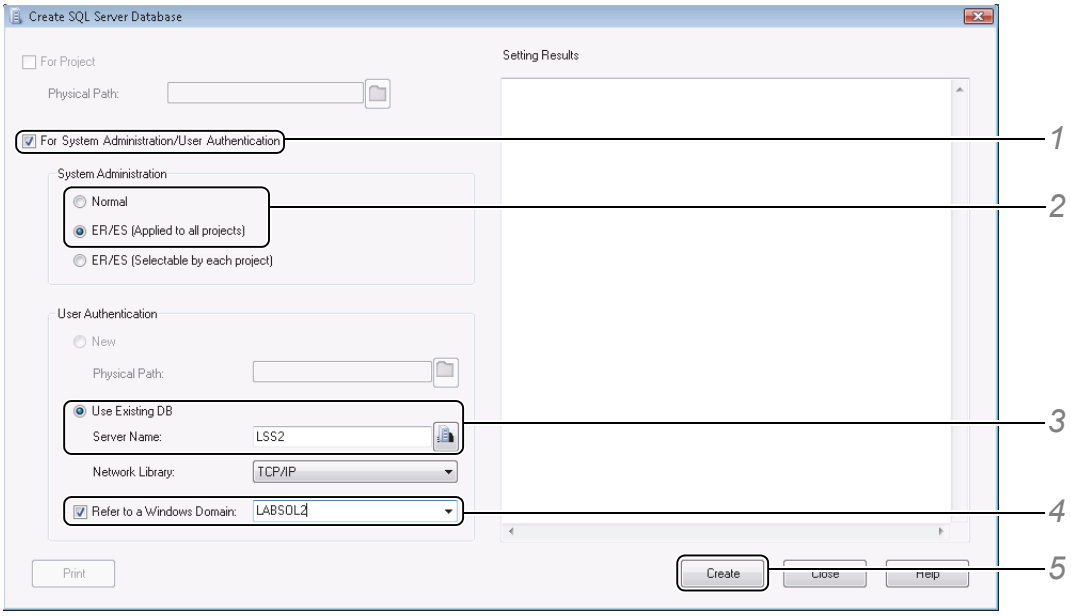
1 **Log into Windows as a user with administrator rights.**

When using a Windows domain, log into the target domain.

2 **Start up “C:\Program Files\LabSolutions\LSSCreateMsdeDb.exe”.**

NOTE

- “C:\Program Files\” is the default installation directory folder. Enter the installation directory folder if the installation directory folder is changes.
- Use [Run as administrator] to start up “LSSCreateMsdeDb.exe” on Windows 7/Windows Vista.



1 Select [For System Administration/User Authentication].

2 If the existing CLASS-Agent is set to the ER/ES mode, select [ER/ES (Applied to all projects)].
If the existing CLASS-Agent is set to the Normal mode, select [Normal].

3 Specify the [Server Name] where the existing authentication database is installed.

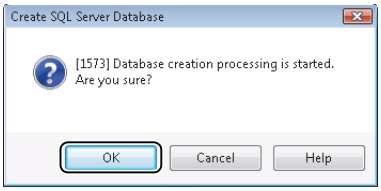
4 Select [Refer to a Windows Domain] to set the user to the same user as the Windows domain user. Specify the domain to link to.

NOTE

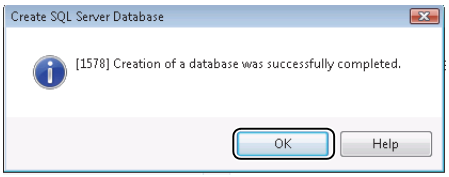
Once the [Refer to a Windows Domain] is selected, it cannot be deselected.

5 Click [Create].

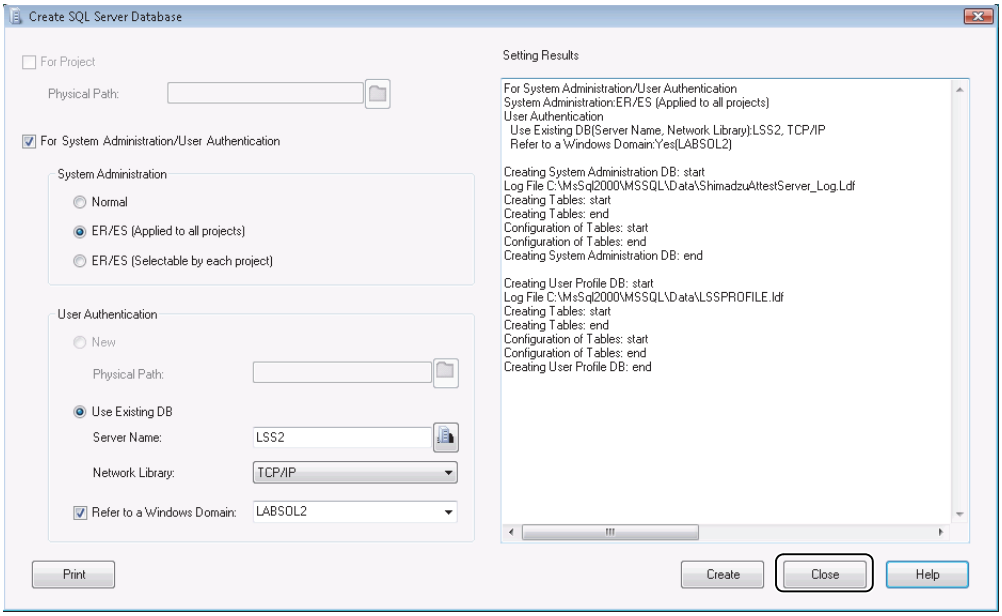
6 Click [OK].



7 Click [OK].



8 Click [Close].



This completes the database creation.

Link LabSolutions to the CLASS-Agent user authentication database.

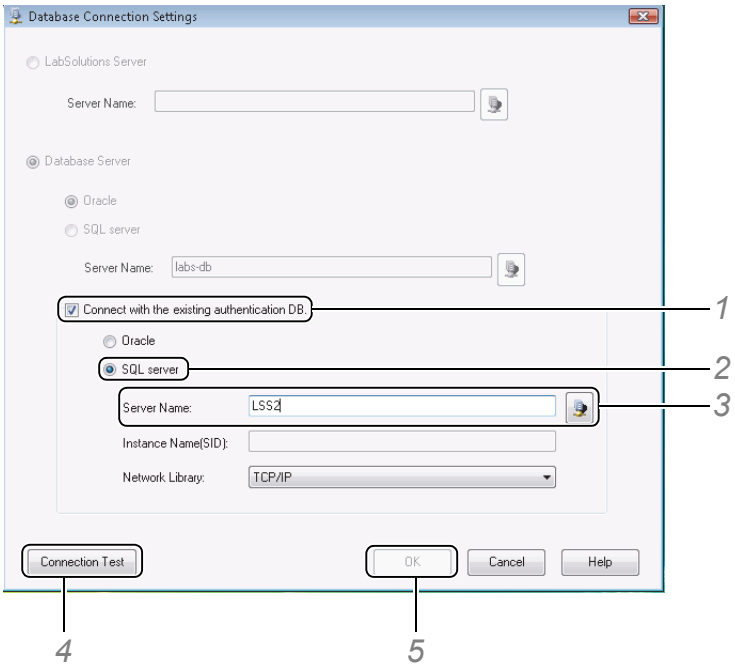
NOTE

Perform the following procedure on all LabSolutions clients.

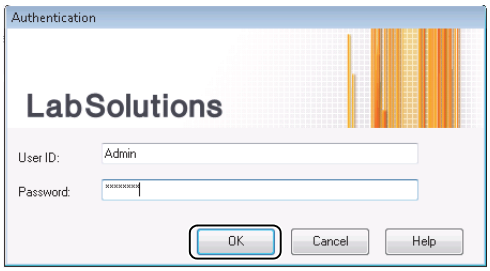
3 Start up “C:\Program Files\LabSolutions\LSSSetDbConnection.exe”.

NOTE

- “C:\Program Files\” is the default installation directory folder. Enter the installation directory folder if the installation directory folder is changes.
- Use [Run as administrator] to start up “LSSSetDbConnection.exe” on Windows 7/Windows Vista.



1 Select [Connect with the existing authentication DB].
2 Select [SQL server].
3 Specify the [Server Name] where the existing authentication database is installed.
4 Click [Connection Test].
5 If the test is successful, [OK] is enabled. Click [OK].
6 Wait for the LabSolutions [Authentication] sub-window to be displayed. Enter the [User ID] and [Password] of the user with administrator rights, and click [OK].



The sub-window closes when the authentication process ends.

This completes the process of linking LabSolutions to the user authentication database. Proceed to *"2.5.3 Store Result Data on the CLASS-Agent Database" P.52* to store the result data to the CLASS-Agent database.

■ Oracle CLASS-Agent User Authentication Database

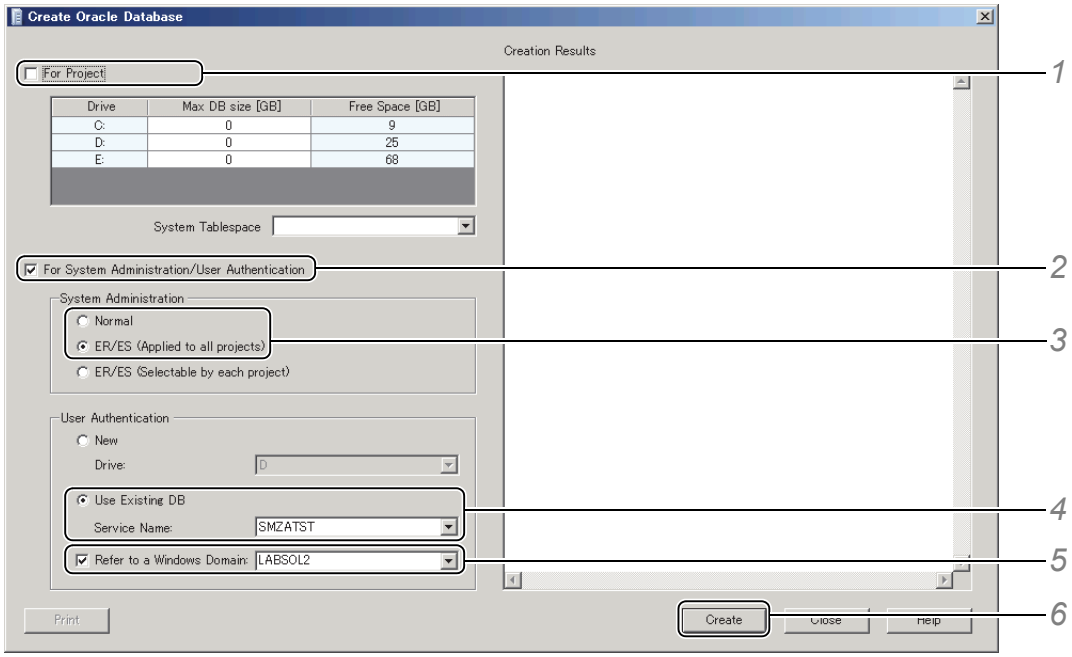
1 **Log into Windows as a user with administrator rights.**

When using a Windows domain, log into the target domain.

2 **Start up "C:\Program Files\LabSolutions\LSSCreateOracleDb.exe".**

NOTE

- "C:\Program Files\" is the default installation directory folder. Enter the installation directory folder if the installation directory folder is changes.
- Use [Run as administrator] to start up "LSSCreateOracleDb.exe" on Windows 7/Windows Vista.



1 Deselect [For Project].

2 Select [For System Administration/User Authentication].

3 If the existing CLASS-Agent is set to the ER/ES mode, select [ER/ES (Applied to all projects)].
If the existing CLASS-Agent is set to the Normal mode, select [Normal].

4 Select [Use Existing DB].
Specify the service name of the existing authentication database.

5 Select [Refer to a Windows Domain] to set the user to the same user as the Windows domain user.
Specify the domain to link to.

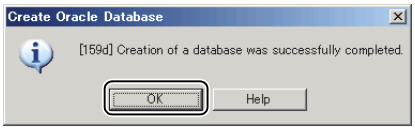
NOTE

Once the [Refer to a Windows Domain] is selected, it cannot be deselected.

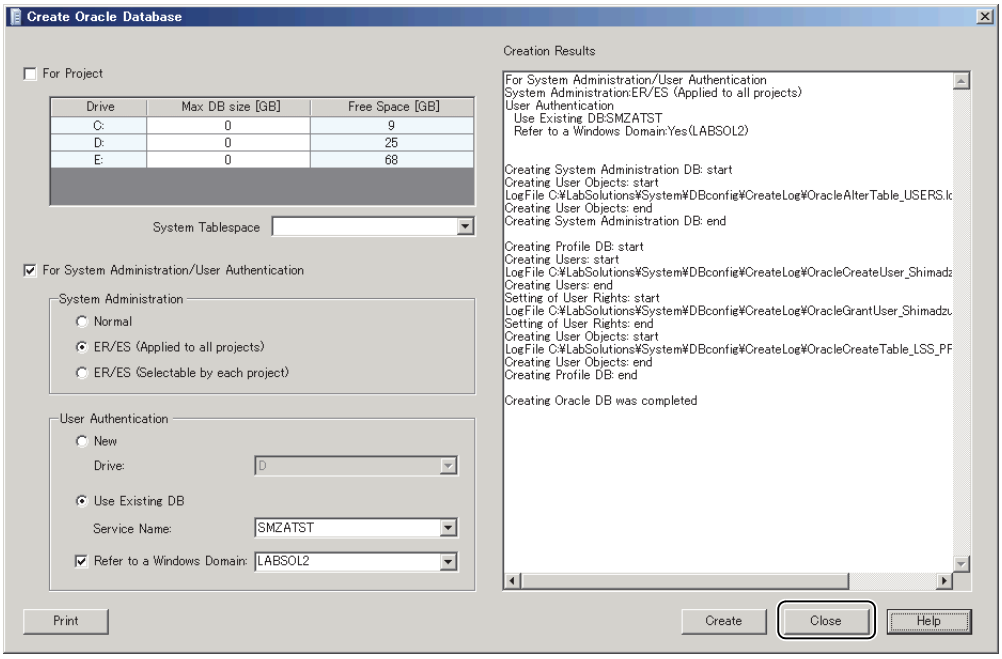
6 Click [Create].

7 Click [OK].

8 Click [OK].



9 Click [Close].



This completes the database creation. Link LabSolutions to the CLASS-Agent user authentication database.

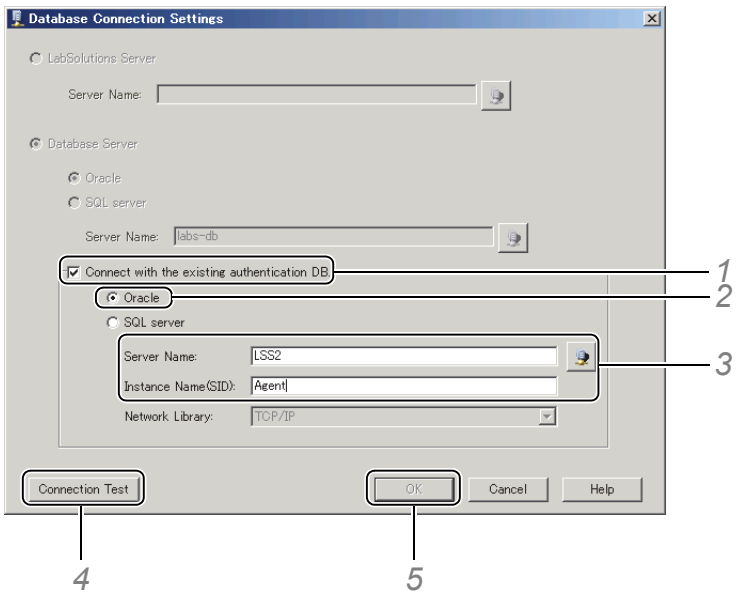
NOTE

Perform the following procedure on all LabSolutions clients.

3 Start up “C:\Program Files\LabSolutions\LSSSetDbConnection.exe”.

NOTE

Use [Run as administrator] to start up “LSSSetDbConnection.exe” on Windows 7/Windows Vista.



1 Select [Connect with the existing authentication DB].

2 Select [Oracle].

3 Specify the [Server Name] where the existing authentication database is installed and [Instance Name (SID)] of the authentication database.

4 Click [Connection Test].

NOTE

Correspond as follows when the existing authentication DB is Oracle.

- Set the following contents to Environment Variables in Windows.

  Variable : Oracle home

  Value : Installation Path of Oracle Client (ex. C:\Oracle\product\10.2.0\db_1)

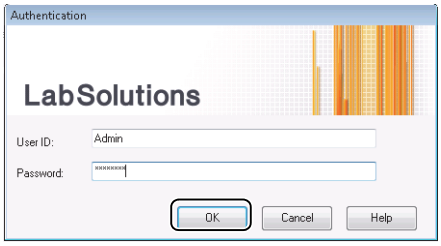
- Install Oracle Data Provider for .NET (ODP).

  ODP is stored in the media for Client of Oracle.

  The version of ODP and the version of Oracle should be same.

5 If the test is successful, [OK] is enabled. Click [OK].

6 Wait for the LabSolutions [Authentication] sub-window to be displayed. Enter the [User ID] and [Password] of the user with administrator rights, and click [OK].



The sub-window closes when the authentication process ends.

This completes the process of linking LabSolutions to the user authentication database. Proceed to *"2.5.3 Store Result Data on the CLASS-Agent Database" P.52* to store the result data to the CLASS-Agent database.

■ Mdb CLASS-Agent User Authentication Database

1 **Log into Windows as a user with administrator rights.**

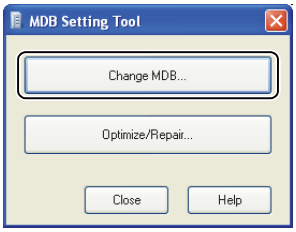
When using a Windows domain, log into the target domain.

2 **Start up “C:\Program Files\LabSolutions\LSSSetMdbForm.exe”.**

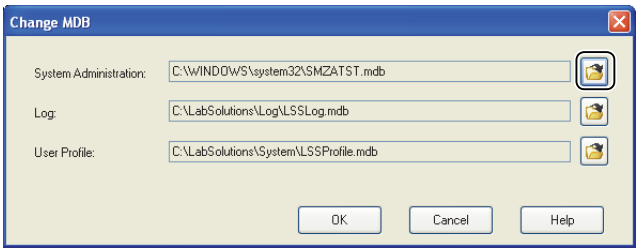
NOTE

- “C:\Program Files\” is the default installation directory folder. Enter the installation directory folder if the installation directory folder is changes.
- Use [Run as administrator] to start up “LSSSetMdbForm.exe” on Windows 7/Windows Vista.

1 Click [Change MDB].

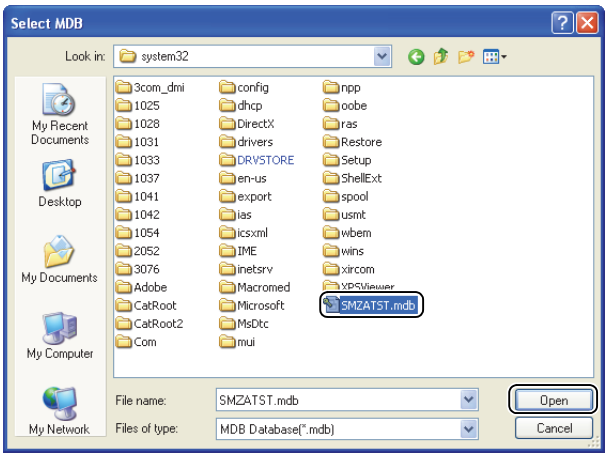


2 Click  of [System Administration].

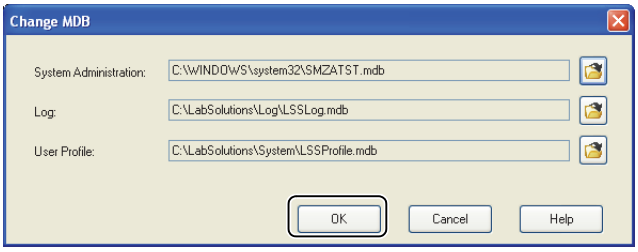


3 Select SMZATST.mdb in the directory the Shimadzu User Authentication Tool is installed, and click [Open].

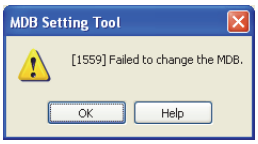
The default directory becomes C:\Windows\system32.



4 Click [OK].



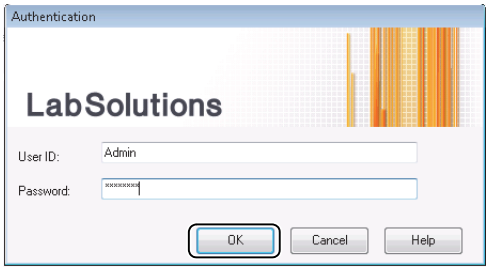
5 Click [OK].



6 Wait for the LabSolutions [Authentication] sub-window to be displayed. Enter the [User ID] and [Password] of the user with administrator rights, and click [OK].

NOTE

Use LabSolutions after restarting the PC if [Cancel] is selected.



The sub-window closes when the authentication process ends.

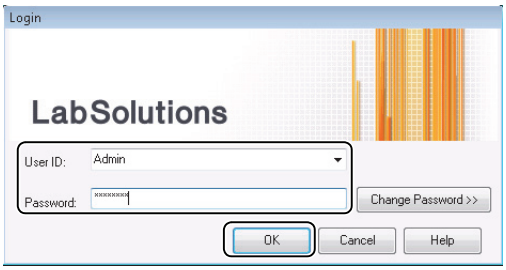
This completes the process of linking LabSolutions to the user authentication database. Proceed to *"2.5.3 Store Result Data on the CLASS-Agent Database" P.52* to store the result data to the CLASS-Agent database.

2.5.3 Store Result Data on the CLASS-Agent Database

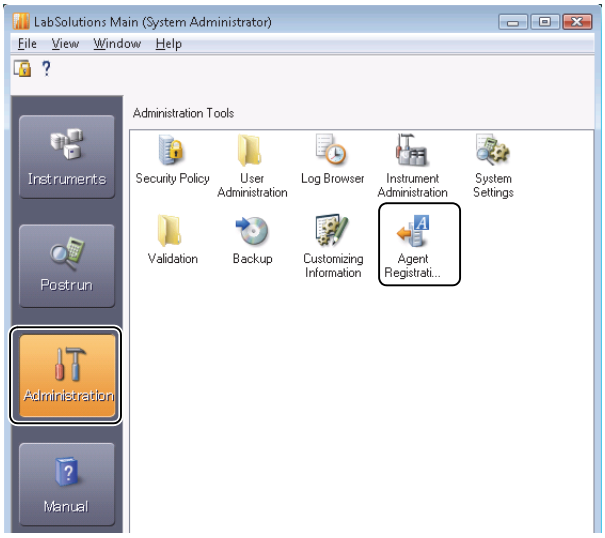
NOTE
Perform the following procedure on all LabSolutions clients.

1 **Double-click the  (LabSolutions) icon on the Desktop.**

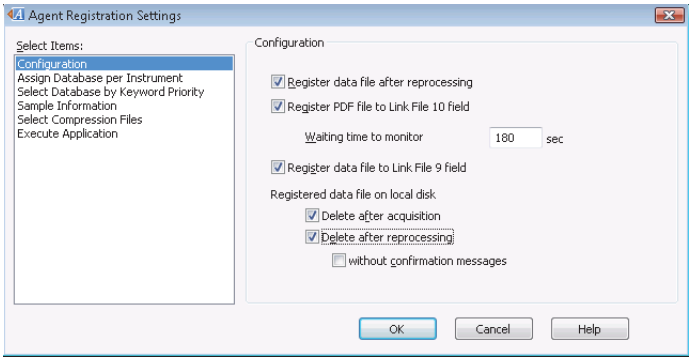
2 **Enter the [User ID] and [Password] of the user with administrator rights, and click [OK].**

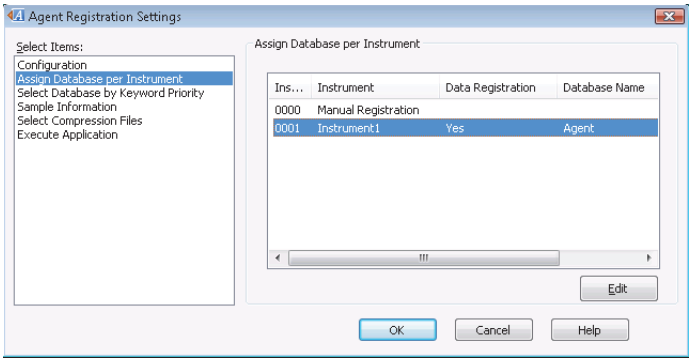


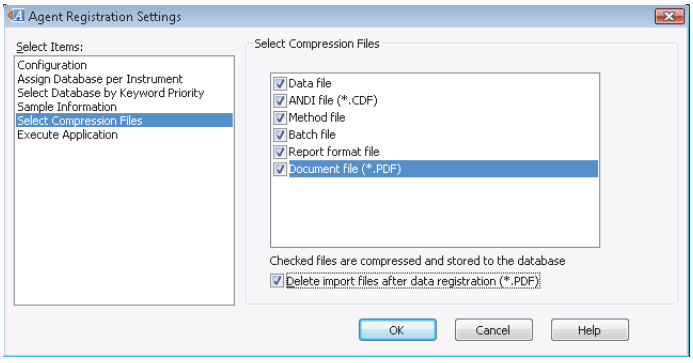
3 **Click  , and double-click [Agent Registration Settings].**



4 Set the registration method, registration destination database, compression file, and other settings.



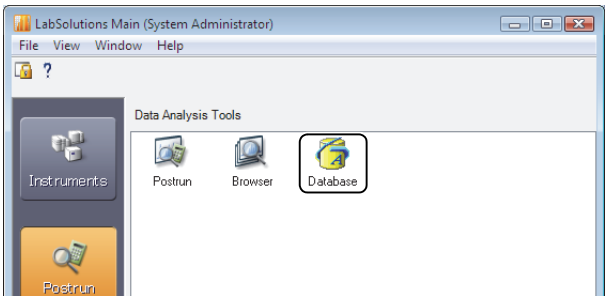




NOTE

When Class-Agent is installed, the [Database] icon is displayed in the 

window. Click the [Database] icon to start up CLASS-Agent.



(Restart the PC to display the [Database] icon if CLASS-Agent is installed after LabSolutions.)

3 Audit Trail Function

The software can create an “audit trail log” of changes made to data acquisition or data analysis parameters. This chapter describes the procedure for setting the audit trail and checking the histories.

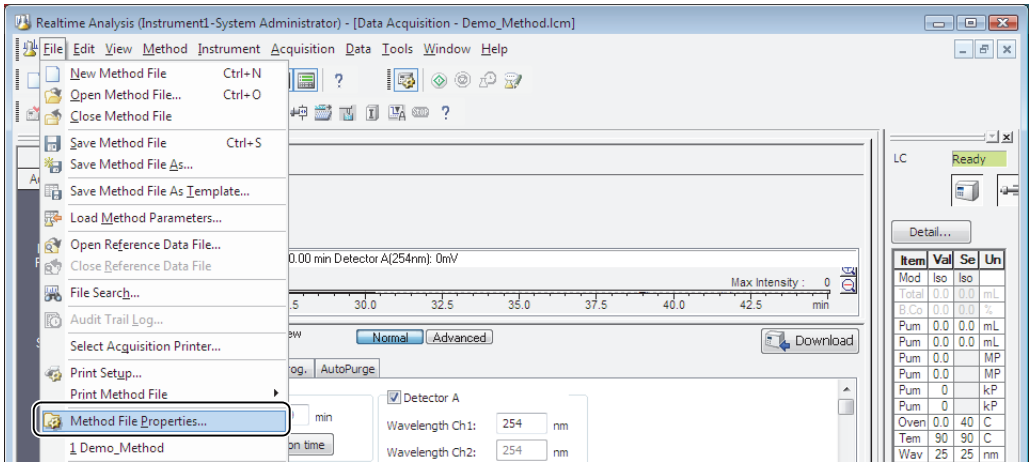
3.1 Audit Trail Log Setup

The audit trail log can be activated for data files, system configuration files, and method/batch/report format files.

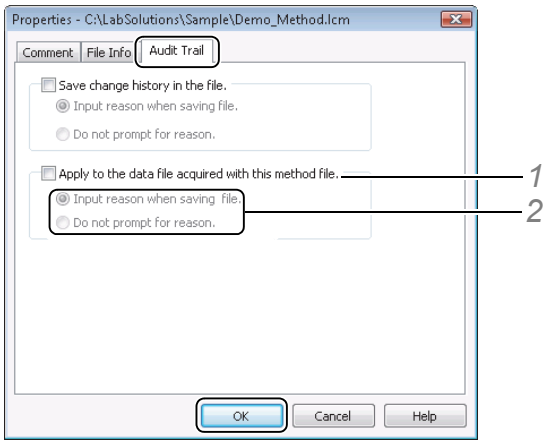
3.1.1 Audit Trail Log in Data Files

This section describes the audit trail log setup in a data file for a method file in the [Data Acquisition] window.

1 **Click [Method File Properties] on the [File] menu in the [Data Acquisition] window.**



2 **Click the [Audit Trail] tab, set each item, and click [OK].**



1 Select the [Apply to the data file acquired with this method file.] item. Once an audit trail is attached to a data file, it can never be canceled.

2 Select [Input reason when saving file.] to require a comment (e.g. reason for the change) be entered each time that a change is saved.
Select [Do not prompt for reason.] to create a log that contains only the date of the change, and the name of user who made the change.

NOTE

The audit trail settings cannot be made to “Untitled” files. First save the new file, then change these settings.

3 Acquire data (by single run) using this method file.

When the data file is obtained using this method file, a history of changes made to the data is created in the data file as an audit trail log.
This records a history of changes made to the method and format in the data.

NOTE

Although the above describes an example of how data is acquired from a single run, the result is the same when a data file is obtained in the [Realtime Batch] window using the method described above.

■ The [Properties] Sub-Window of the Method File

The [Properties] sub-window of the method file can be opened from the following locations.

File Type	Sub-window + Menu
Method File	[File] - [Method File Properties] in the following windows • [Data Acquisition] window • [Method Editor] window • [Calibration Curve] window • [Quant Browser] window

Reference

- If the [Apply audit trail function when creating method file] item is selected in the security policy settings, the audit trail is automatically enabled when a new method file is created. Once the audit trail function is activated in the security policy it is activated for all (new and existing) method files and it cannot be canceled.
  For more details about setting security policies, refer to *"1.2.1 System Administration Policy (Security Policy)" "Instrument Policies" P.8*.
- For details on checking the audit trail log in data files, refer to *"3.3.4 Audit Trail Log" P.66*.
- For details on data files, refer to *"2.1 File Formats" P.29*.

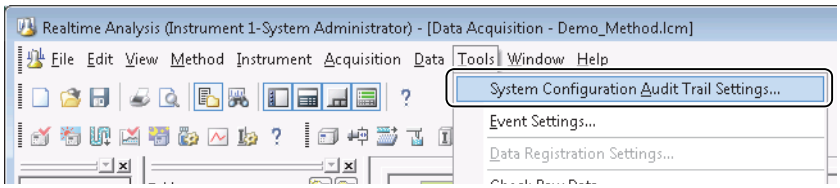
3.1.2 Audit Trail Log in System Configuration Files

When the audit trail function is enabled in the system configuration, a history is maintained for changes made to the system configuration information of the instrument.

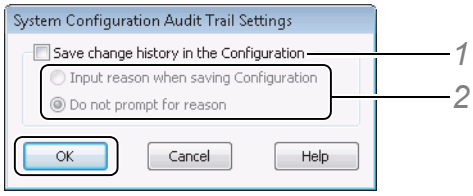
1 **Click [System Configuration Audit Trail Settings] on the [Tools] menu in the [Data Acquisition] window.**

NOTE

Use the same procedure to set the system configuration audit trail in the [Realtime Batch] window.



2 **Set each item, and click [OK].**



1 Select [Save change history in the Configuration].

2 Select [Input reason when saving Configuration.] to require a comment (e.g. reason for the change) be entered each time that a change is saved.
Select [Do not prompt for reason.] to create a log that contains only the date of the change, and the name of user who made the change.

NOTE

Once an audit trail log is created for a file, it cannot be canceled. This feature assures the integrity of the history logs.

Reference

- If the [Apply audit trail function for system configuration] item is selected in the security policy settings, the system configuration audit trail log is automatically activated.
  For more details about setting security policies, refer to *"1.2.1 System Administration Policy (Security Policy)" "Instrument Policies" P.8*.
- For details on checking the audit trail log in the system configuration information, refer to *"3.4.1 Audit Trail Log in System Configuration Information" P.71*.
- For details on system configuration files, refer to *"2.1 File Formats" P.29*.

3.1.3 Audit Trail Log in Method Files, Batch Files and Report Format Files

This section describes the setup for attaching an audit trail log to method files in the [Data Acquisition] window.

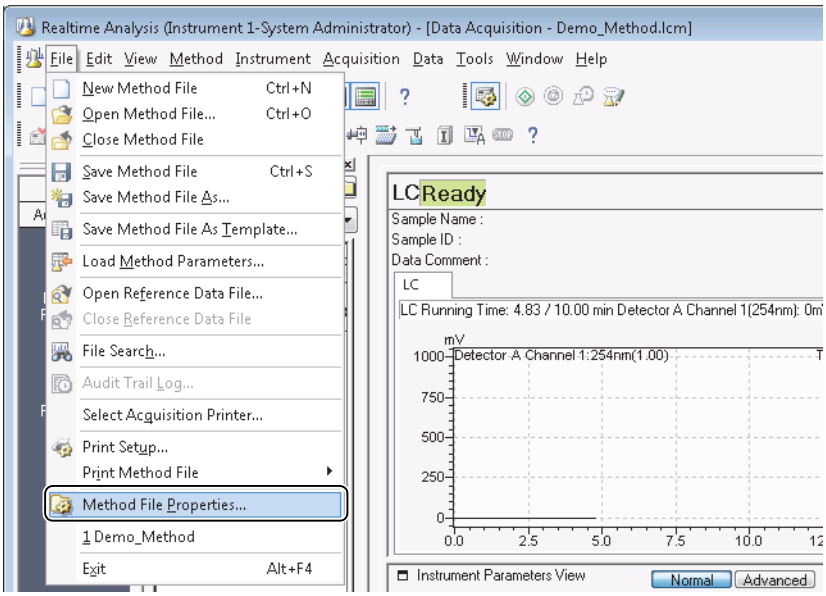
The following items must be selected to enable the security policy settings for making new files.

File	Item
Method File	Apply audit trail function when creating method file.
Batch File	Apply audit trail function when creating batch file.
Report Format File	Apply audit trail function when creating report format file.

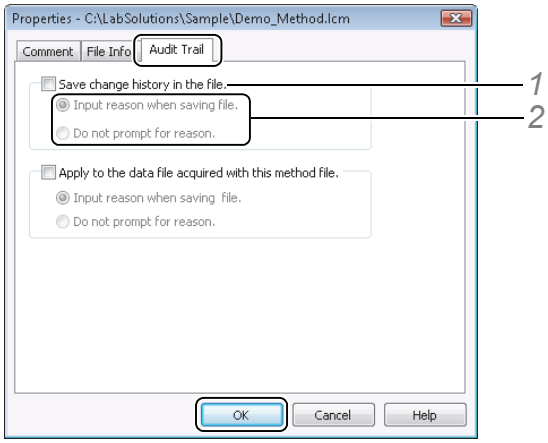
☞ Reference

- For more details about setting security policies, refer to *"1.2.1 System Administration Policy (Security Policy)" "Instrument Policies" P.8*.
- For details on checking the audit trail log in metadata files, refer to *"3.4.2 Audit Trail Log in Method Files, Batch Files and Report Format Files" P.72*.
- For details on each of the metadata files (method, batch and report format files), refer to *"2.1 File Formats" P.29*.

1 Click [Method File Properties] on the [File] menu in the [Data Acquisition] window.



2 Click the [Audit Trail] tab, set each item, and click [OK].



1 Select [Save change history in the file.].

2 Select [Input reason when saving file.] to require a comment (e.g. reason for the change) be entered each time that a change is saved.
Select [Do not prompt for reason.] to create a log that contains only the date of the change, and the name of user who made the change.

When the method file parameters are changed, a history of changes are saved in the method file as an audit trail log.
In the same manner, the history of changes made to the instrument parameters and data processing parameters are also saved to their respective files.

NOTE

- Once an audit trail log is attached to a file, it cannot be canceled. This feature assures the integrity of the history logs.
- The audit trail settings cannot be made to “Untitled” files. First save the new file, then change these settings.

■ The [Properties] Sub-Window of the Metadata File

The [Properties] sub-window for each metadata file type can be opened from the following locations.

File Type	Sub-window + Menu
Method File	[File] - [Method File Properties] in the following windows • [Data Acquisition] window • [Method Editor] window • [Calibration Curve] window • [Quant Browser] window
Batch File	[File] - [Batch File Properties] in the following windows • [Realtime Batch] window • [Batch Editor] window • [Postrun Batch] window
Report Format File	[File] - [Report Format File Properties] in the [Report] window **NOTE** • A history is not maintained for changes made to parameters in report items pasted in report format files. • The [Properties] sub-window can also be opened from the [Data Report] window. However, this [Properties] window does not have the [Audit Trail] tab. A history of changes made to data formats can be created if the audit trail log is activated in data files.

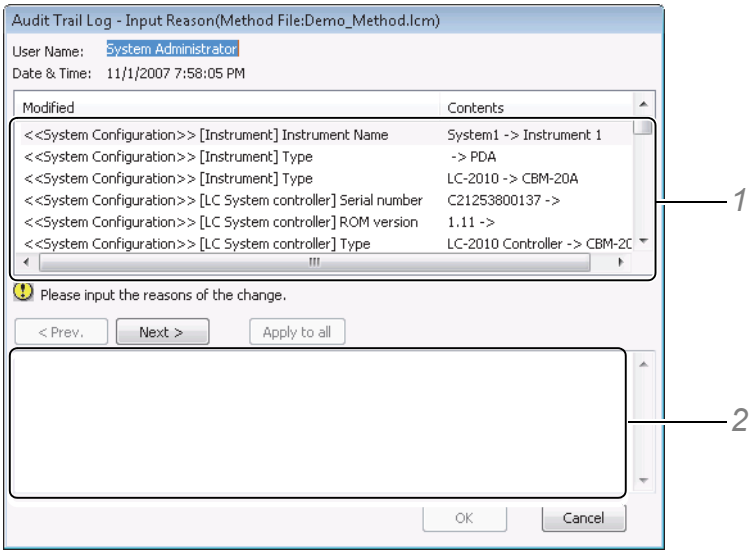
3.2 Reasons for Changes

In files that are set up to leave behind a reason for a change in the audit trail log, a sub-window prompting the user to enter the reason for the change opens when the user tries to save changes made to a file. This sub-window can be closed only by entering the reason for the change.

This section describes an example of the procedure when instrument parameters in a method file have been changed in the [Data Acquisition] window.

1 **Drag-and-drop a method file that requires entry of a reason for the change into the [Data Acquisition] window from the [Data Explorer] sub-window.**

2 **Change a few of the instrument parameters, and click (Save) on the toolbar.**



1 Click the desired row in the [Modified/Contents] list.

Click [Prev.] and [Next] to move the selection row up and down in the list. Toggle through the items in the list and enter or review the reason for the change.

2 Enter the reasons for the changes.

Empty text strings, such as spaces and tabs, are not regarded as reasons for changes. Enter an accurate reason for the change.

3 To edit the change reason or add more information re-select the desired item and edit the reason.

After all of the reasons for changes are entered, click [OK].

NOTE

To enter the same reason for the change to all of the items in the list, enter the first reason and click [Apply to all].

The new parameters are saved, and the audit trail log including the reasons for changes is recorded in the method file.

Reference

For details on editing instrument parameters, refer to the Operators Guide.

3.3 View the Data File History

Data files store the following content:

- Chromatograms
- Method files (data processing parameters, instrument parameters used for data acquisition, and system configuration parameters)
- Batch Tables if the analysis used realtime batch/postrun batch
- Report formats

Data acquisition-related information is recorded as part of the data file even if the audit trail is not activated.

NOTE
Data files are in an All-In-One structure that allows various information to be saved.

3.3.1 Data File Properties

Open the data files properties to view sample information, acquisition date, or the name of the method file.

The data file [Properties] sub-window can be opened from the following locations.

Window	Menu
Data Analysis	[File] - [Data File Properties]
Calibration Curve	[Data] - [Data File Properties]
Quant Browser	[Data] - [Data File Properties]
Data Browser	[File] - [Data File Properties]
Data Comparison	Each of the data files at [File] - [Data File Properties]

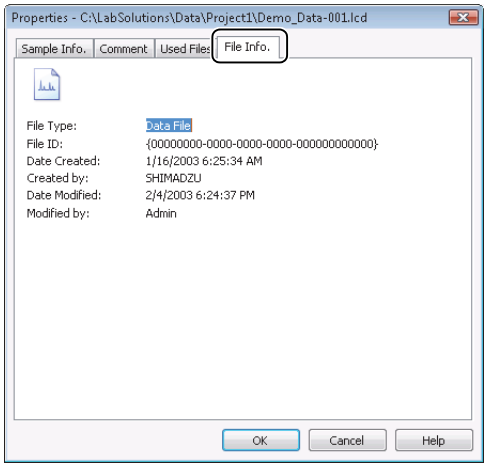
This section describes the procedure for checking the properties of data files from the [Data Analysis] window.

1 **Click [Data File Properties] on the [File] menu in the [Data Analysis] window.**

2 **Review the content of the data files on each of the tabs.**

■ [File Info.] Tab

The [File Info.] tab displays information such as the date that the data was created, who created the data, modification date and the editor.

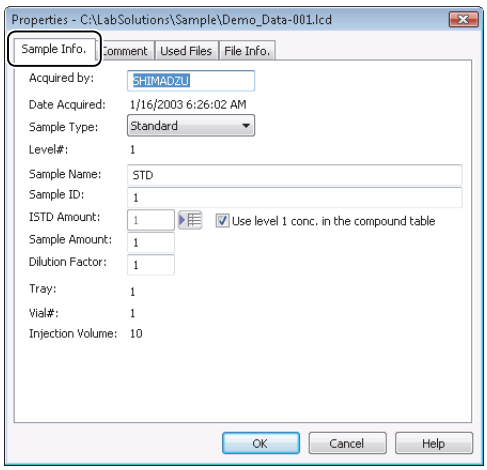


NOTE

The “file ID” is a unique ID that is assigned to all data files.

■ [Sample Info.] Tab

The [Sample Info.] tab displays the information used for data acquisition, the data acquisition date and the operator at the time of analysis.

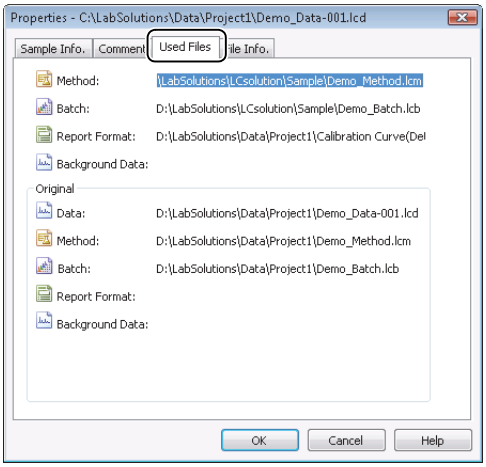


NOTE

The content of the [Sample Info.] tab can be edited. If the [ISTD Amount], [Sample Amount] or [Dilution Factor] are edited, the data is automatically recalculated and the quantitation results change.
If the audit trail function is enabled, a history of that change is recorded.

■ [Used Files] Tab

The [Used Files] tab displays the names of files, such as method files and batch files, used to acquire the data.



NOTE

The method files, batch files and report format files displayed on the [Used Files] tab can be exported from the data file and used for data acquisition and analysis.

Reference

Refer to the Operators Guide or to *"3.3.6 Export Batch Tables" P.70* for details on exporting files.

■ Other Tabs

Two other tabs may also be displayed, the [Comment] tab for displaying data file comments and the [Option Info.] tab for displaying optional Batch Table column names.

NOTE

- Refer to Help for information on Batch Table options.
- The [Option Info.] tab is displayed when additional Batch Table columns (Option 1 to Option 10) are used.

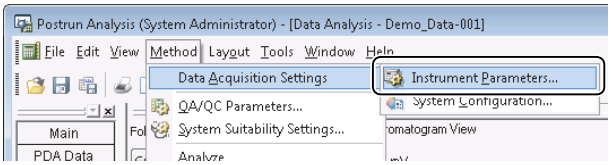
3.3.2 Instrument Parameters and System Configuration

The instrument parameters and system configuration can be checked throughout data analysis on the various analysis windows such as, [Data Analysis], [PDA Data Analysis], and [MS Data Analysis].

This section describes the procedure for checking the instrument parameters and system configuration information saved in the data files.

■ Instrument Parameters

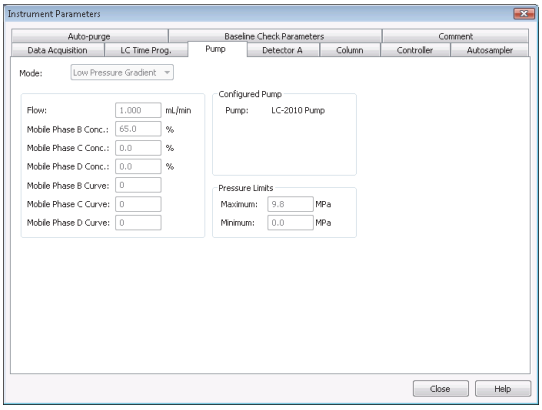
1 **Select [Data Acquisition Settings] on the [Method] menu in the [Data Analysis] window, and click [Instrument Parameters].**



2 **Examine the parameters on each of the instrument tabs.**

NOTE

The information contained on the tabs of this sub-window cannot be edited.



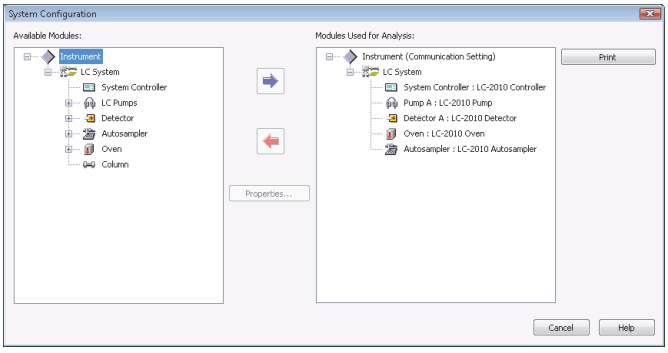
■ System Configuration Information

1 **Select [Data Acquisition Settings] on the [Method] menu in the [Data Analysis] window, and click [System Configuration].**

2 **Examine the system configuration information.**

NOTE

The information contained on the tabs of this sub-window cannot be edited.



3.3.3 Data Acquisition History

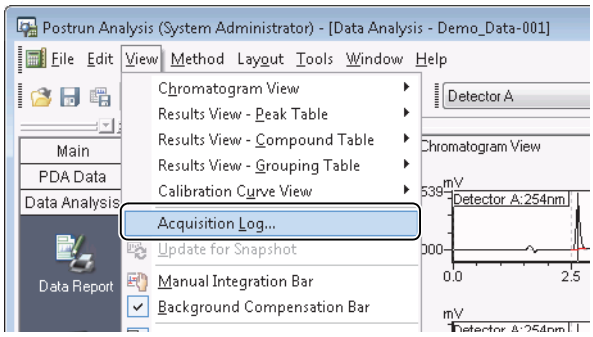
The software records a history of errors that occur during data acquisition and of changes made to data acquisition settings. Use this record to determine whether the data file has been properly acquired.

The acquisition history log can be reviewed throughout the data analysis process.

This section describes the procedure for checking the acquisition history log that is saved in the data files.

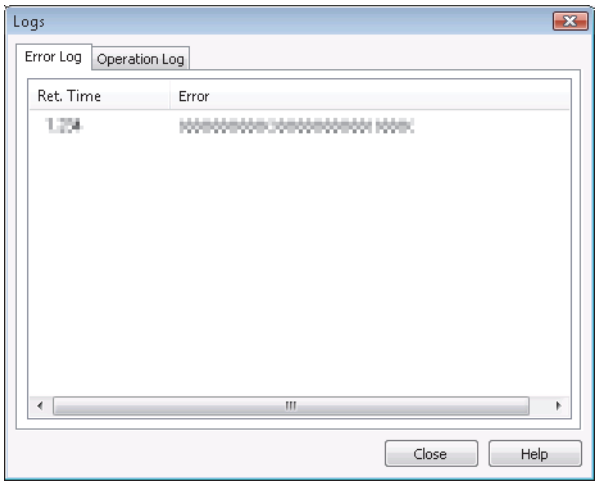
■ [Error Log]

1 **Click [Acquisition Log] on the [View] menu in the [Data Analysis] window.**



2 **Click the [Error Log] tab.**

The [Error Log] tab displays errors that occur during data acquisition in chronological order.

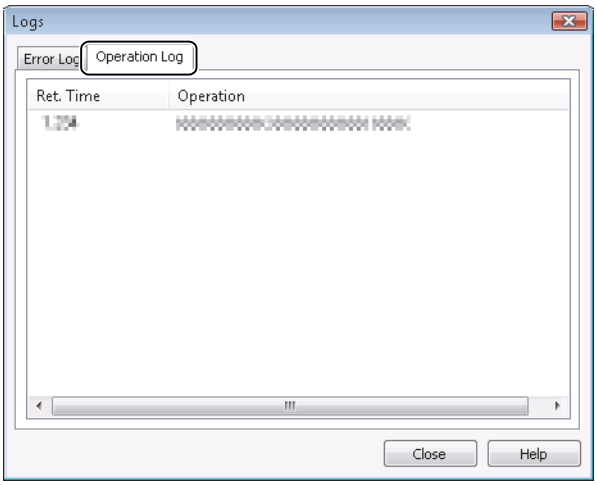


■ [Operation Log]

1 **Click [Acquisition Log] on the [View] menu in the [Data Analysis] window.**

2 **Click the [Operation Log] tab.**

The [Operation Log] tab displays the operation log created during data acquisition. It contains information such as changes made directly to instrument parameters by the instrument monitor.



3.3.4 Audit Trail Log

The audit trail log saves a history of changes that are made to postrun data such as manual peak integration, changes made to data processing parameters, or when report formats are edited. This audit trail log is saved in the data file.

The audit trail log can be reviewed throughout the data analysis process.

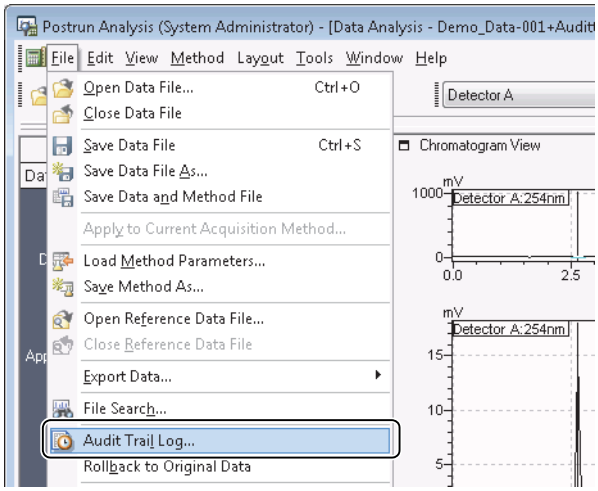
This section describes the procedure for checking the audit trail log saved in the data files from the [Data Analysis] window.

☞ Reference

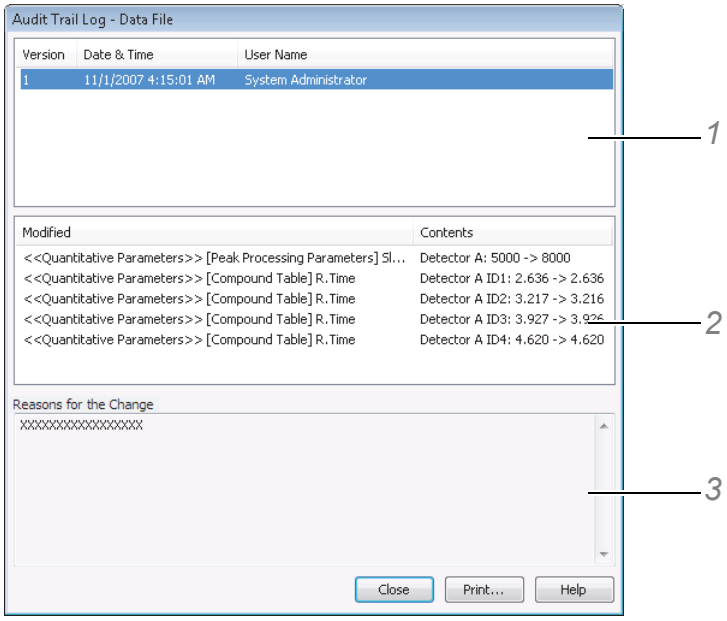
When the audit trail log is attached to a method file, a history of changes is maintained in the data file after data acquisition ends.

For details on enabling the audit trail function for data files, refer to *"3.1.1 Audit Trail Log in Data Files" P.55*.

1 Click [Audit Trail Log] on the [File] menu in the [Data Analysis] window.



2 Check the modified location, contents and reasons for change.



1 Click the a row in the [Version/ Date & Time/User Name] list to display the change history.
The details of the changes are displayed in the [Modified/Contents] list.

2 Click a row in the [Modified/Contents] list to display the reasons for the change.

3 If reasons for the change were entered it is displayed in the [Reasons of the Change] box.
If multiple modifications were made, repeat step *2*, to review the reasons for all of the changes.

4 Repeat steps *1* through *3* to review multiple versions.

NOTE
Click [Print] in the [Audit Trail Log] sub-window to print the logs.

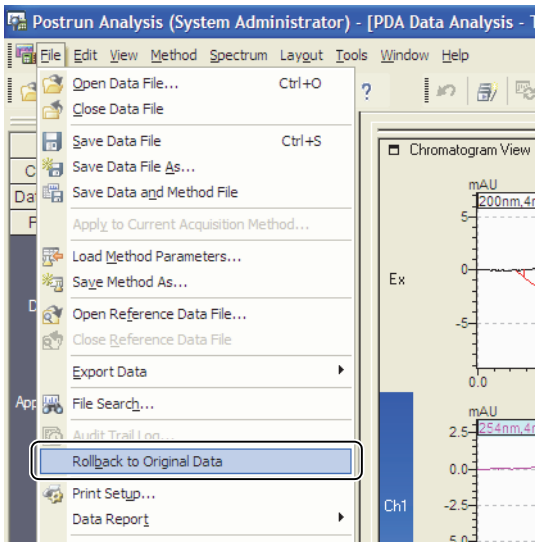
3.3.5 Restoration of Original Data

Data files store two sets of method file information, the data acquisition method file and the latest data analysis method file. This allows processed data to be restored to the original data.

This function is available at any point throughout the data analysis process.

This section describes the procedure for rolling data analysis results back to the original data in the [Data Analysis] window.

1 **Click [Rollback to Original Data] on the [File] menu in the [Data Analysis] window.**



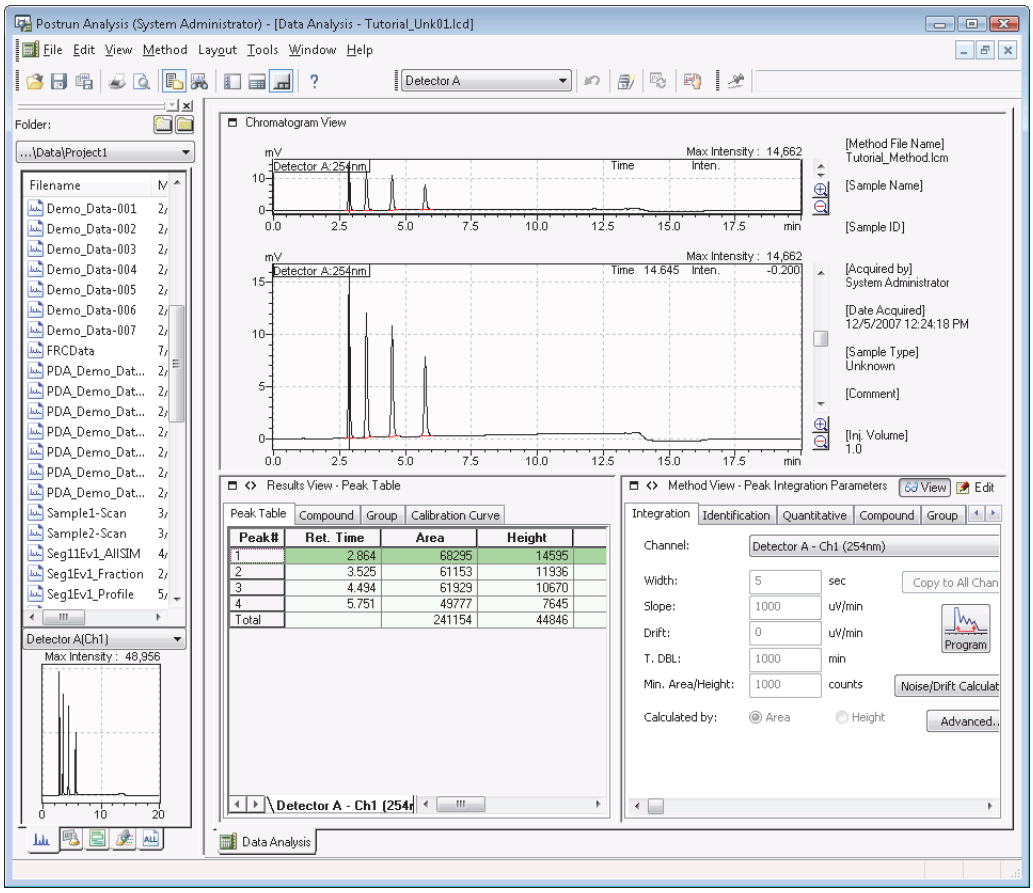
NOTE

A confirmation box opens to prevent operational error. Check the original data against the processed data without deleting the processed data by selecting [Rollback to Original Data] but do not save the file.

2 **Click [Yes] in the confirmation box.**

Data analysis is performed using the data processing parameters that were active when the data was acquired, and the original results are displayed.
Report formats information stored in the data file also return to the state that was active at data acquisition.

3 Check the data file in the [Data Analysis] window.



Reference

The data acquisition method file information and the latest data processing method file information can be exported from the data files and used to perform data acquisition and postrun analysis. Refer to the Operators Guide for details on exporting method files from data files.

To check report formats in data files, click [Data Report] - [Edit Format] on the [File] menu to display the [Report (Report in Data File)] sub-window.

NOTE

Report formats can be exported from data files by clicking [Save Report Format File As] on the [File] menu in the [Report (Report in Data File)] sub-window.

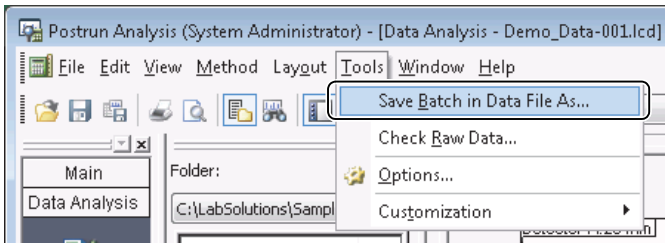
3.3.6 Export Batch Tables

Data files store two sets of Batch Table information, the acquisition Batch Table information and the latest postrun Batch Table information. Batch Table information in data files can be exported by using the Batch Table export function.

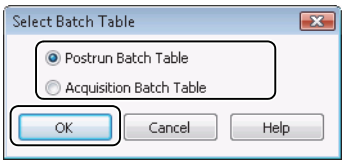
This function is available at all points throughout the data analysis window.

This section describes the procedure for exporting batch files in the [Data Analysis] window.

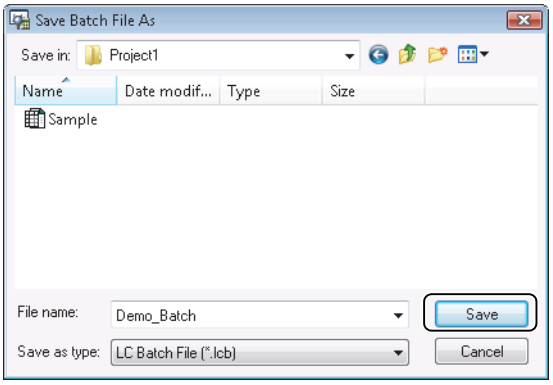
1 **Click [Save Batch in Data File As] on the [Tools] menu in the [Data Analysis] window.**



2 **Select the Batch Table to be exported, and click [OK].**



3 **Enter the [File name], and click [Save].**



The selected Batch Table is exported as a batch file.

3.4 Histories of Other Files

The histories of changes made to method files, batch files and other files can be viewed in addition to the history of data files.

Reference

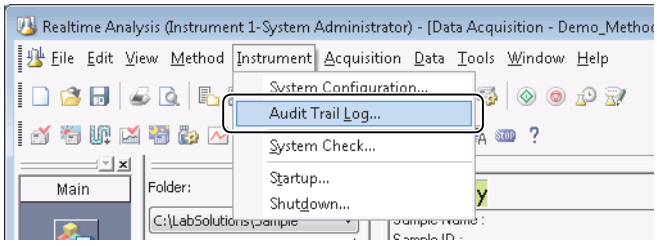
After the audit trail log has been activated, histories can be reviewed for changes made in system configuration information and metadata files (method/batch/report format files).

Refer to *"3.1 Audit Trail Log Setup" P.55* for details on activating the audit trail function.

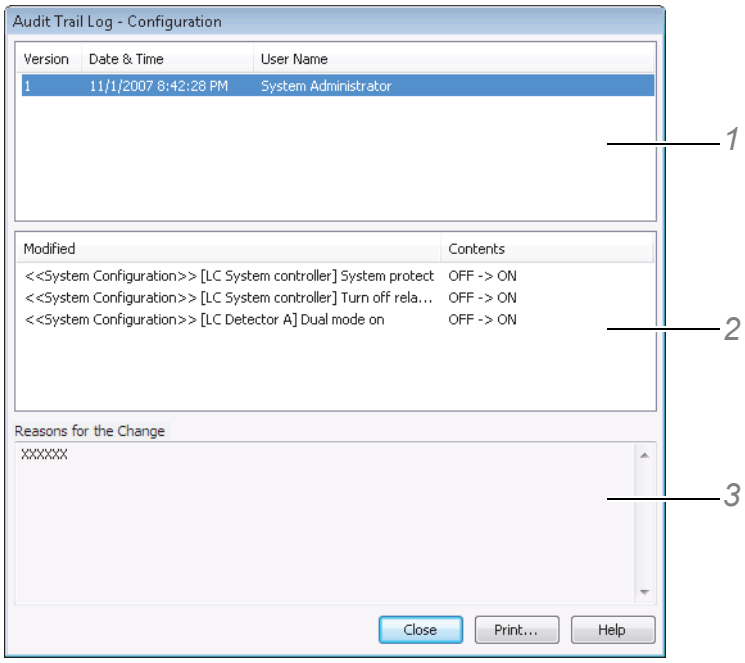
3.4.1 Audit Trail Log in System Configuration Information

Histories of changes made to the system configuration information can be reviewed using [Audit Trail Log] on the [Instrument] menu.

1 **Click [Audit Trail Log] on the [Instrument] menu in the [Data Acquisition] window.**



2 **Check the modified location, contents and reasons for the change.**



1 Click the a row in the [Version/ Date & Time/User Name] list to display the change history.
The details of the changes are displayed in the [Modified/Contents] list.

2 Click a row in the [Modified/Contents] list to display the reasons for the change.

3 If reasons for the change were entered it is displayed in the [Reasons of the Change] box.
If multiple modifications were made, repeat step *2*, to review the reasons for all of the changes.

4 Repeat steps *1* through *3* to review multiple versions.

NOTE

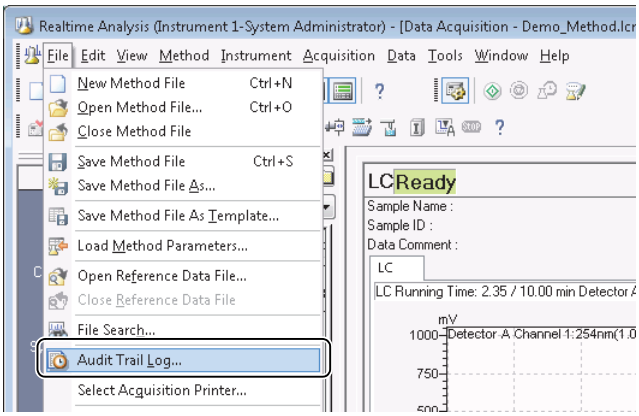
Click [Print] in the [Audit Trail Log] sub-window to print the logs.

3.4.2 Audit Trail Log in Method Files, Batch Files and Report Format Files

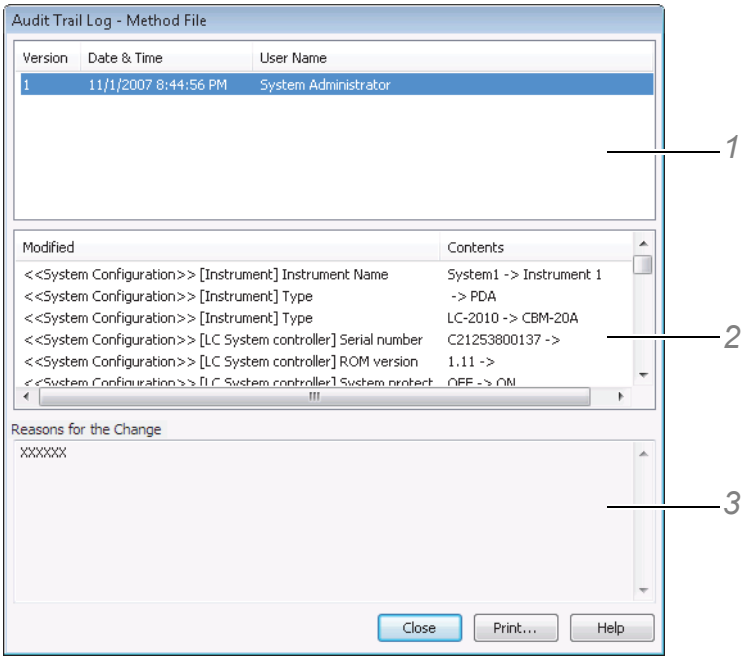
The history of changes stored in the metadata files (method/batch/report format files), can be reviewed in the [Audit Trail Log] sub-window.

This section describes how to display an audit trail log in method files.

1 **Click [Audit Trail Log] on the [File] menu in the [Data Acquisition] window.**



2 **Check the modified location, contents and reasons for the change.**



1 Click the a row in the [Version/ Date & Time/User Name] list to display the change history.
The details of the changes are displayed in the [Modified/Contents] list.

2 Click a row in the [Modified/Contents] list to display the reasons for the change.

3 If reasons for the change were entered it is displayed in the [Reasons of the Change] box.
If multiple modifications were made, repeat step *2*, to review the reasons for all of the changes.

4 Repeat steps *1* through *3* to review multiple versions.

NOTE

Click [Print] in the [Audit Trail Log] sub-window to print the logs.

■ The [Audit Trail Log] Sub-Window of the Metadata File

The [Audit Trail Log] sub-windows of each of the metadata files can be opened from the following locations.

File Type	Sub-window + Menu
Method File	[File] - [Audit Trail Log] in the following windows • [Data Acquisition] window • [Method Editor] window • [Calibration Curve] window • [Quant Browser] window
Batch File	[File] - [Audit Trail Log] in the following windows • [Realtime Batch] window • [Batch Editor] window • [Postrun Batch] window
Report Format File	[File] - [Audit Trail Log] in the [Report] window

4 System Suitability Test

Execute the system suitability test before the start of data acquisition to verify that the system can be used stably for a specific data acquisition. The realtime batch can be stopped if the results of the system suitability check are not adequate. This process allows for the preservation of important samples.

4.1 Save Test Conditions in Method Files

The system suitability test parameters must be saved to a method file to execute the system suitability test.

This section describes the procedure for entering the system suitability test parameters in a method file and checking peak area repeatability.

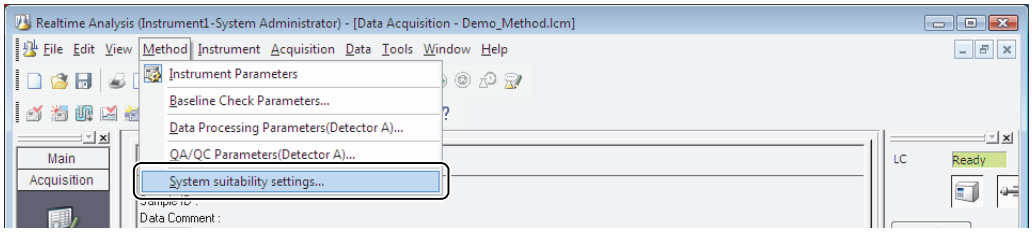
1 **Drag-and-drop the method file onto the [Data Acquisition] window from the [Data Explorer] sub-window.**

The method file is loaded.

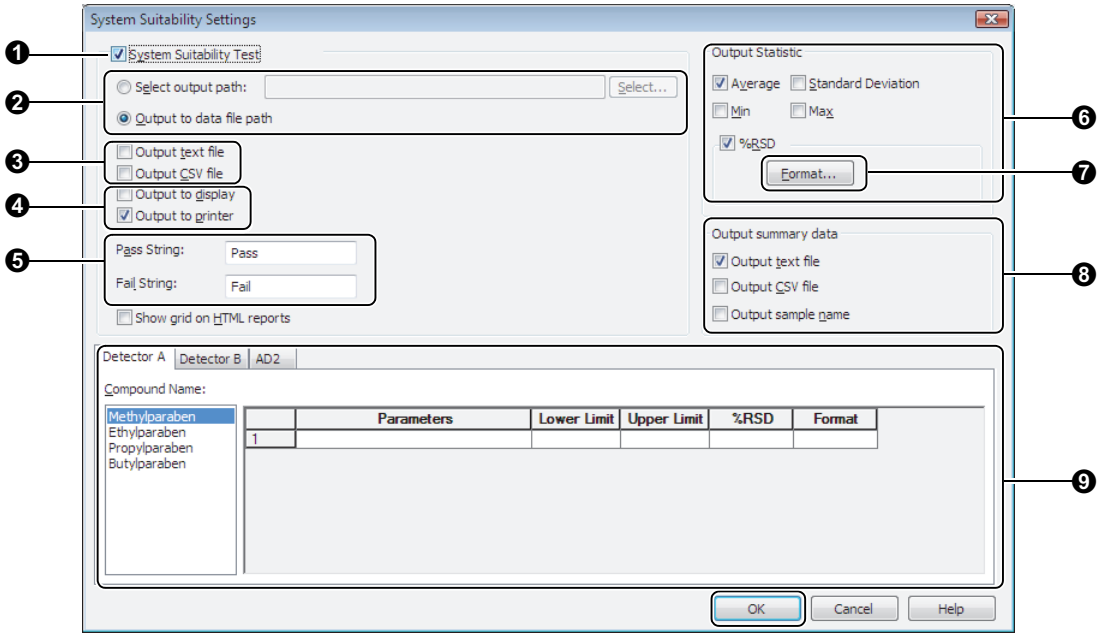
Reference

If column performance results such as [Resolution] and [Tailing F.] are used, select the calculation method according to the respective pharmacopoeia.
Refer to the Operators Guide for details on selecting the calculation.

2 **Click [System Suitability Settings] on the [Method] menu.**

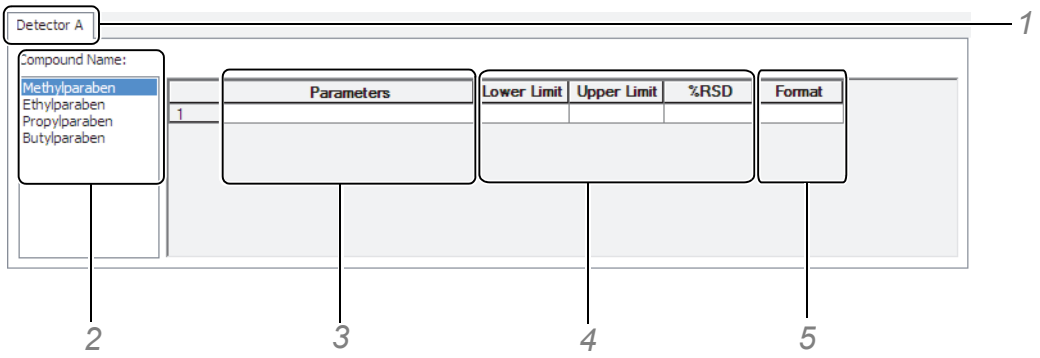


3 Make the following settings in the [System Suitability Settings] sub-window, and click [OK].



No.	Explanation
❶	Select this item to execute the system suitability test using the currently displayed method.
❷	Enter the destination of the result report. • When [Select output path] is selected, click the [Select] button on the right to specify the destination. • When [Output to data file path] is selected, the result report is saved to the folder that contains the realtime batch data file.
❸	Select either text format or CSV format for the format of the result report.
❹	Select whether the HTML result report will be viewed on the monitor or sent to a printer. **NOTE** The HTML result report is output to the Windows default printer.
❺	Enter the text string that is displayed in the result report for evaluations that pass or fail
❻	Select the statistical values that are used in the evaluation and included in the result report. **NOTE** The [Average], [Min] and [Max] statistical values are rounded according to the format of the check values set at ❾.
❼	Click the [Format] button to open the [Format Settings] sub-window, then enter the rounding procedure and number of displayed digits of the relative standard deviation. **Reference** The [Format Settings] sub-window is common to the [Format Settings] sub-window that appears in ❾. See the description for ❾ or refer to Help for more details.
❽	Select how the summary data will be output.
❾	Enter the check items and check criteria to be executed during the system suitability test.

Use the following procedure to set the check items and check criteria.



1 Select the tab for the detector to be used in execution of the system suitability test.

NOTE

If multiple detectors are used to execute the system suitability test, click the tab for each detector and set the check items for each detector.

2 Click the name of the compound to be checked.

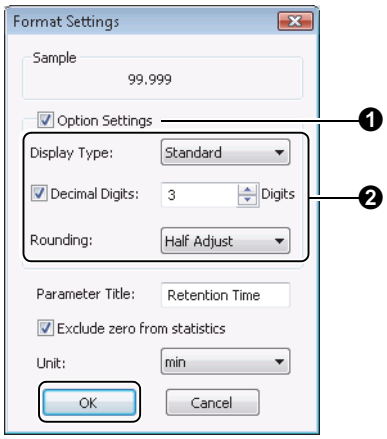
3 Click a cell on the [Parameters] column, and select the check item from the list that is displayed.

4 Enter the following pass/fail criteria for each check item.

- [Lower] - lowest passing value
- [Upper] - highest passing value
- [%RSD] - highest passing relative standard deviation value
- [Format]

Leave the check criteria blank or enter [-] to not set a check criteria.

5 Click a cell on the [Format] column to change the rounding method or the displayed format of numeric values.



No.	Explanation
❶	Select [Option Settings] to change the rounding method and the number of displayed digits for the selected check item. **Reference** By default, the calculation results are displayed according to numeric value processing set by the system. Refer to *"1.2.4 Numerical Rounding and Number of Displayed Digits" P.17* for details on how the system processes numeric value.

No.	Explanation
❷	Select the rounding method and the number of displayed digits for the selected check item. • [Display Type] - [Default], [Exponential], [Significant Digits] • [Rounding] - [Half Adjust], [Round Up], [Round Down] • [Decimal Digits] - If [Display Type] is changed to [Significant Digits] this item changes to [Significant Digits].

NOTE

- Repeat steps 2 through 5 to set different check items to other compounds.
- Repeat steps 3 through 5 to check a single compound using multiple items.
- A total of up to 100 different check items can be set.
- Values for check items such as [Resolution] and [Tailing Factor] are calculated according to the method selected on the [Performance] tab in [Method View]. If multiple formulas were selected on the [Performance] tab, all values for each calculation method are output to the result report.
- The check result is failed if even one calculated value does not satisfy the check criteria.

4 Click [OK] in the [System Suitability Settings] sub-window, and click (Save) on the toolbar.

The system suitability settings are saved to the method file.

Reference

The system suitability test settings must be saved to both the method file and batch file to execute the system suitability test.
Refer to *"4.2 Set Test Conditions to Batch Tables" P.78* for details on how to save the system suitability settings in batch files. Refer to *"4.3 Realtime Batch Control Based on Test Results" P.80* for details on how to control realtime batch by the system suitability check results.

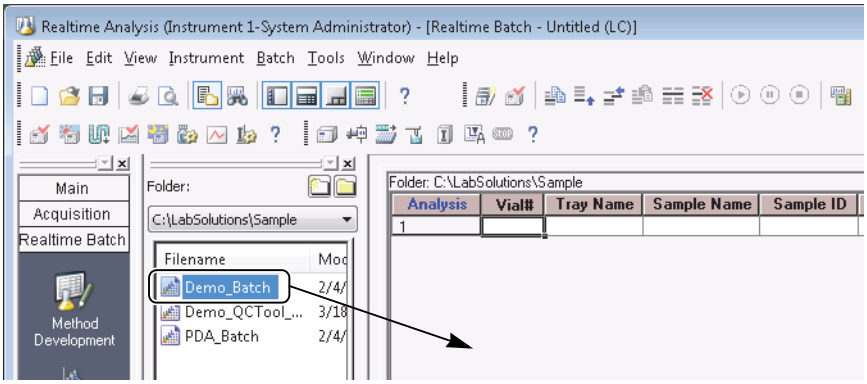
4.2 Set Test Conditions to Batch Tables

This section describes the procedure for saving the system suitability test condition in the Batch Table. When data acquisition is initiated with a prepared batch file, the system suitability test is executed and the result report is output.

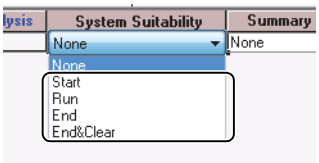
1 Drag-and-drop the batch file onto the [Realtime Batch] window from the [Data Explorer] sub-window.

Reference

Refer to *"4.1 Save Test Conditions in Method Files" P.75* for details on saving the system suitability test to a method file.



The batch file is loaded.



Reference

The [System Suitability] column is not displayed in the default Batch Table. Right-click on the Batch Table, and click [Table Style] to display the [Table Style] sub-window. Add the [System Suitability] column to the Display Items box, and click [OK].
Refer to the Operators Guide for details on the [Table Style] sub-window.

1 Click the [System Suitability] cell in the 1st row where the system suitability test is to be executed, and select [Start].

[Start] initializes the system suitability test data list and adds the data file from that row of the Batch Table to the list.

2 Click the [System Suitability] cells on the subsequent system suitability rows and select [Run].

[Run] adds the data file for that row of the Batch Table to the list.

3 Click the [System Suitability] cell on the final row of the system suitability test, and select [End].

[End] adds the data file for that row of the Batch Table to the list. The check items of the system suitability test are calculated and checked for the data in the list, and the result report is output.

NOTE

- Select [End & Clear] in the [System Suitability] cell to execute the system suitability test for only 1 row.
- System suitability test execution rows do not need to be adjacent on the Batch Table.

Reference

Refer to the Operators Guide for details on other items in the Batch Tables.

2 Click (Save) on the toolbar.

The settings are saved to batch file.

3 Click the (Start Realtime Batch) icon on the assistant bar.

Realtime batch is started.
The result report is output to the specified folder after data acquisition of the row with [End & Clear] or [End] in the [System Suitability] column ends.

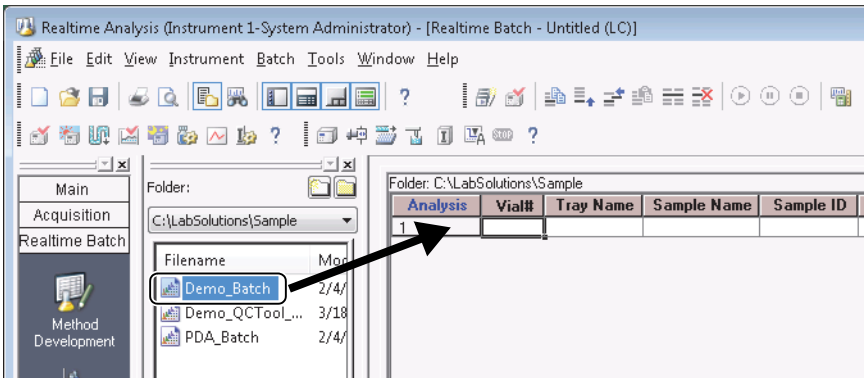
NOTE

- The result report file is named according to the following rule:
  (batch file name)_(No. of row with [End & Clear] or [End]).html
- The result data file is a file name conforming to the same rule as above, and its file extension is ".txt" (text file) or ".csv" (CSV file).
- In the case of summary data files, the file name conforming to the same rule as above is appended with the detector name, and followed with the file extension (".txt" or ".csv").
- If a file of the same name exists, the original file is overwritten with the new file.

4.3 Realtime Batch Control Based on Test Results

This section describes how to cancel realtime batch using the Batch Table actions if the system suitability test fails.

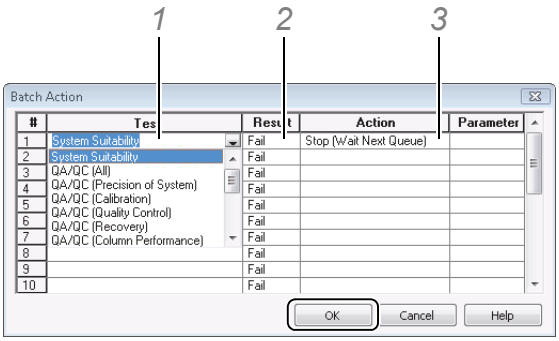
1 **Drag-and-drop the batch file into the [Realtime Batch] window from the [Data Explorer] sub-window.**



The batch file is loaded.

2 **Click the [Action] cell in the row that contains [End & Clear] or [End] in the system suitability column.**

3 **Set each item, and click [OK].**



1 Click the [Test] cell, and select [System Suitability] from the list.
2 Click the [Result] cell, and select [Fail] from the list.
3 Click the [Action] cell, and select [Stop (Wait Next Queue)] from the list.

Reference

The [Test] cell allows the choice to base the check on the QA/QC calculation result and the system check result.
Refer to Help for details about the QA/QC calculation.
Refer to the Operators Guide for details on the system check, and on saving the system check in batch processing.

NOTE

[Pass] can also be selected in the [Result] cell. The following actions can also be selected in the [Action] cell.

Action Item	Operation
Pause	Pauses batch processing.
Stop (Run Next Queue)	Stops the current batch processing, and executes the next batch in the batch queue.
Stop (Wait Next Queue)	Stops the current batch processing, and does not start the next batch in the batch queue.
Reinject	Repeats the processing of that row. The data file name is appended with a number such as -1 and -2 when reinjection is performed.
Execute User Program	Executes the commands specified in parameters.
Goto	Processing moves to the specified row.
Restore Method	Restores a data processed method file to its original file using the method saved before batch execution.
Return	Returns to the row where Goto was executed.

4 **Click (Save) on the toolbar.**

The settings are saved to batch file.

Reference

Refer to the Operators Guide for details on setting other items in Batch Tables.

5 **Click the (Start Realtime Batch) icon on the assistant bar.**

Realtime batch is started.
Realtime batch is stopped if the system suitability test fails.

NOTE

- If multiple calculation methods were selected on the [Performance] tab, the check result is failed if even one calculated value does not satisfy the check criteria. For example, if [Resolution] is performed according to multiple calculation methods (JP method and USP method), the check result is failed if the USP method passes and the JP method fails.
- Stop realtime batch and shut down the instrument according to the following procedure.

  1 Click the [Action] cell, and select [Goto] from the list.
  2 Enter the last row No. of the Batch Table at [Parameter].
  3 Enter the method file to perform shutdown in the final row of the Batch Table.

  This procedure executes the final row of the Batch Table when the check result fails and the instrument is shut down according to the instrument parameters of the method file in the final row.

5 Appendices

This chapter describes how to set instrument information, output reports in PDF format, and validate the software.

5.1 Instrument Information

Double click the [Instrument Administration] icon in the [System Administrator] window. Enter the system name and type of the analytical instruments to connect to the PC in the [Instrument Administration] sub-window.

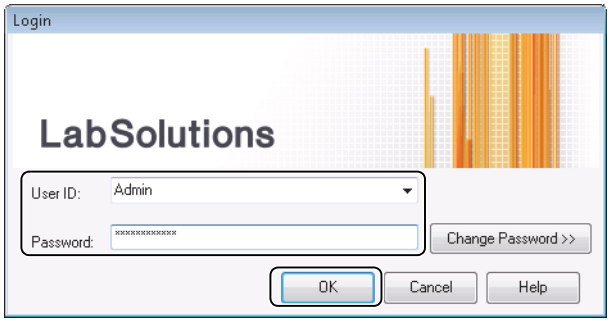
This section describes the procedure for administering the analytical instruments connected to the software system.

NOTE

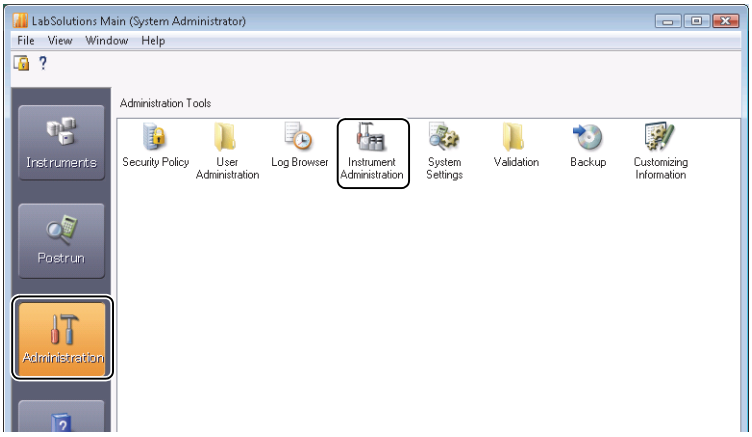
To change instrument registration and instrument information, log in as a user ID having the [Instrument Administration] rights.

1 **Double-click the (LabSolutions) icon on the Desktop.**

2 **Enter a [User ID] and [Password] for a user having the [Instrument Administration] rights, and click [OK].**

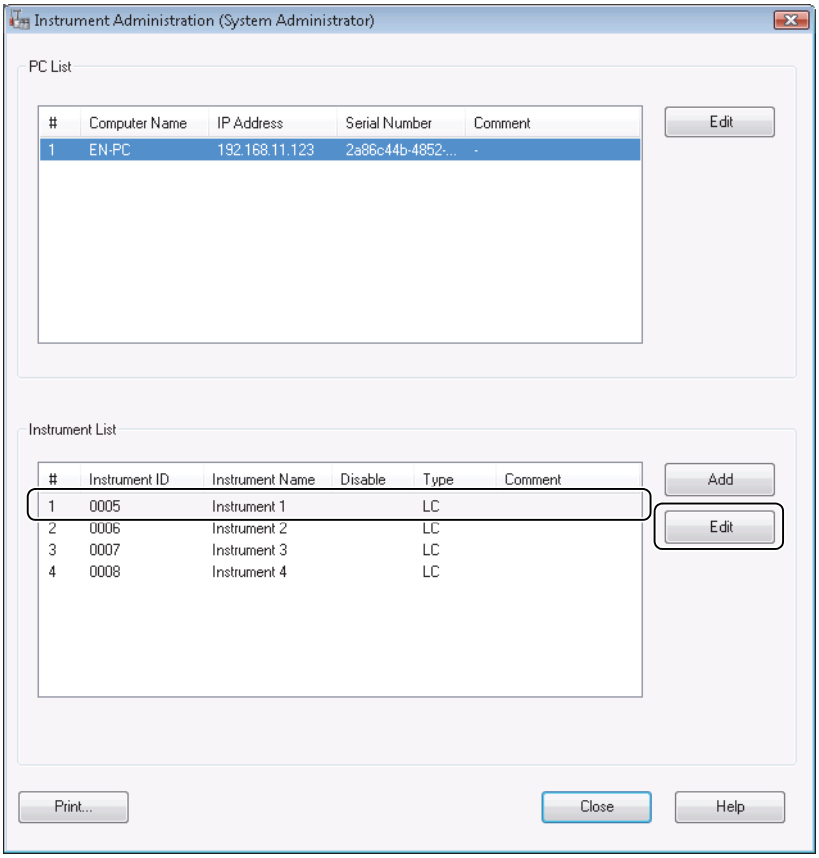


3 **Click the (Administration) icon, and double-click the [Instrument Administration] icon.**

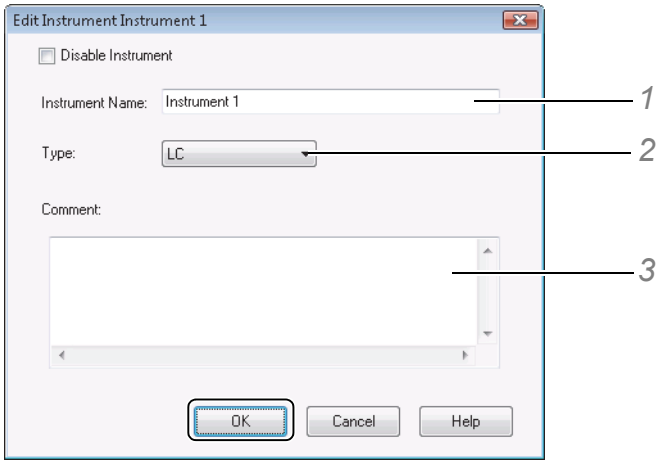


4 **Select the 1st row from [Instrument List] in the [Instrument Administration] sub-window, and click [Edit].**

The following example describes the procedure for displaying the settings of the analytical instrument connected as the 1st instrument.



5 **Enter an [Instrument Name], select the [Type], and add a [Comment], then click [OK].**



1 Enter the instrument name. This instrument name becomes the [Instrument Name] in the [LabSolutions Main] window, [Realtime Analysis] sub-window display, and system information report.

2 Select the type of the instrument.

NOTE

Select “LCMS-QP” for LCMS systems.

Select “GC” for GC systems.

3 Enters a comment to display in the instrument administration sub-window.

6 **Click [Add] to connect other instruments to the same PC.**

The [Add Instrument] sub-window opens. Follow the procedure in step *5* to enter the additional instrument information. The [Add Instrument] sub-window opens.

NOTE

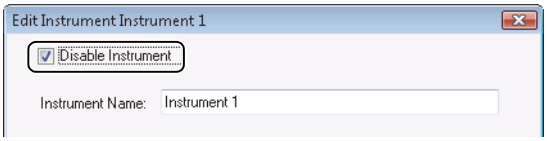
- A maximum of 16 instruments can be registered to a system.
- Log in as a user ID having the [Instrument Administration] rights to change instrument registration and information.
- The maximum of 4 instruments can be connected to an individual PC. Only two of those may contain a PDA detector and only one of those systems may contain an MS.
- Control of one LCMS, one PDA detector and one LC is possible.

■ Disable Instruments

Disable instruments to take them temporarily offline from the system, for example, for instrument maintenance.

1 **Select the name of the instrument to disable from [Instrument List] in the [Instrument Administration] sub-window, and click [Edit].**

2 **Select [Disable Instrument].**



3 **Click [OK].**

[Disable] is displayed in the [Disable] field of the [Instrument List].

NOTE

Disabled instruments are not displayed in the [Instrument] sub-window of the [LabSolutions Main] window. The method files, batch files, report format files, and system configuration information of the instrument are stored.

5.2 PDF Reports

The software is able to output data acquisition result reports as PDF (Portable Document Format) files. The electronic signature information, etc. is automatically appended to the output PDF files.

5.2.1 Output of PDF Reports

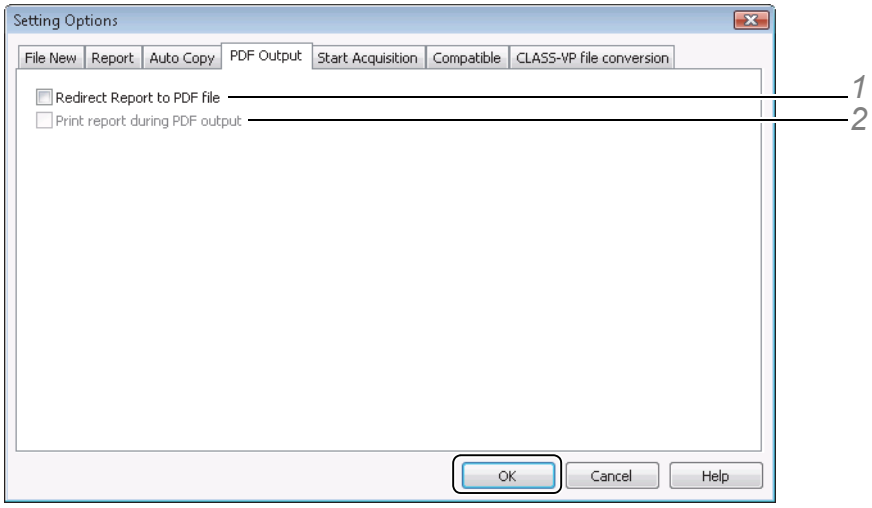
Select PDF output in the [Setting Options] sub-window to output data acquisition result reports to print image files in the PDF format after data acquisition and realtime batch or postrun analysis.

This section describes the procedure for setting PDF output from the [Data Acquisition] sub-window.

1 **Click [Options] on the [Tools] menu.**

2 **Click the [PDF Output] tab.**

3 **Set each item, and click [OK].**



1 Select [Redirect Report to PDF file].

2 Select [Print report during PDF output] to print the data acquisition results and output to a PDF file.

NOTE

- This setting is stored for each software user. If another user has logged into the software, that user must set the output of PDF files to generate the PDF file.
- Output PDF files are saved using the following names.
  - (data file name).pdf (example: Demo_Data-001.pdf) - for data acquisition results
  - (batch file name)_output date/time.pdf (example: Demo_Batch_20060216124536.PDF) - for summary reports

5.2.2 Other PDF File Output Methods

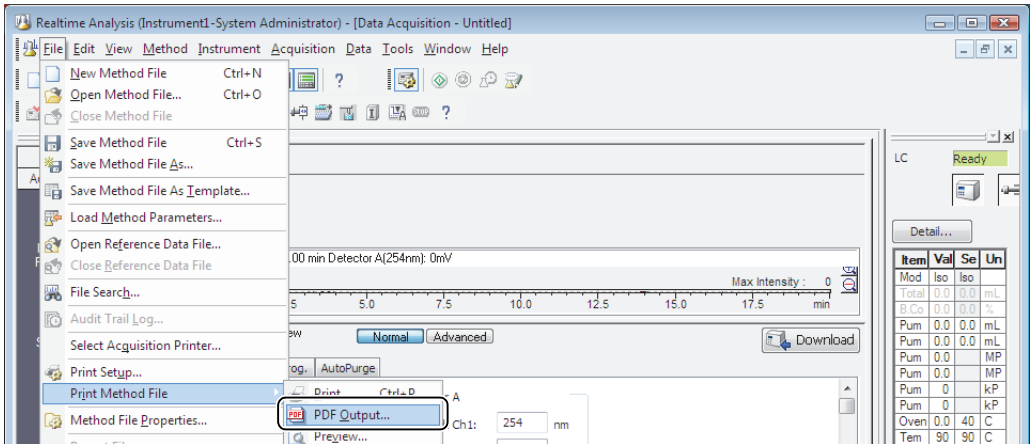
The software also has functions to output parameter information of method files displayed in the [Data Acquisition] window and print images of chromatograms overlaid on the [Data Comparison] window as PDF files.

■ Output Print Images as PDF Files

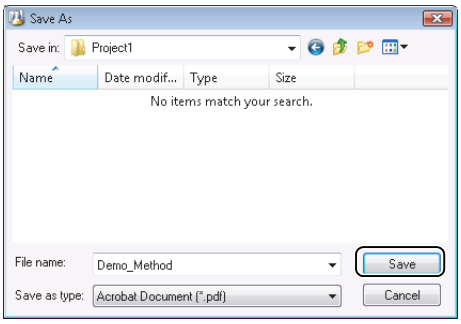
Screen captures can be output to a PDF file by clicking the [PDF Output] sub-menu in the print menu under the [File] menu of each window.

This section describes the procedure for using exclusive system report formats to output the parameter information of method files loaded in the [Data Acquisition] window as PDF files.

1 **From the [Data Acquisition] window, click on the [File] menu then select [Print Method File] and choose [PDF Output].**



2 **Specify the folder to save the file to, enter the PDF file name, and click [Save].**



The PDF file is created.

NOTE

- The [Print] sub-menu in the [File] - [Print Method File] menu sends a print image file to the destination set in *"5.2.1 Output of PDF Reports"*.
- The following names are displayed as default names in the [Save As] sub-window.
  - (file name).pdf (example: Demo_Data-001.pdf) - for information
  - (system exclusive report format name).pdf (example:Data_Comparison_Report.pdf) - for graph images

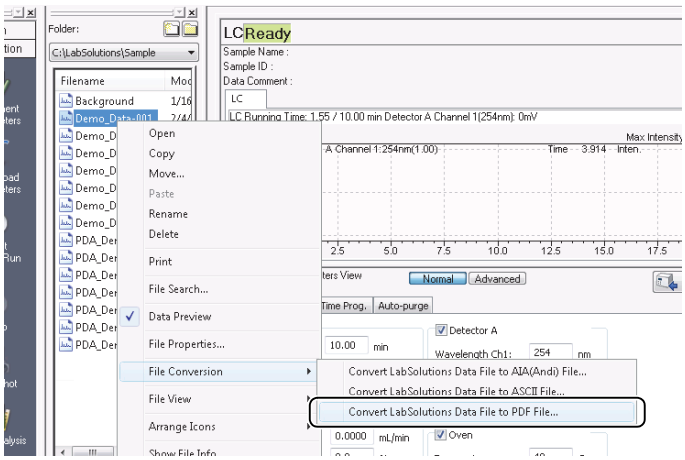
■ File Conversion in Data Explorer

The [Data Explorer] sub-window has a file conversion function to convert data files in other software to this software file format, save them as new files, and export these files to AIA or ASCII format files.

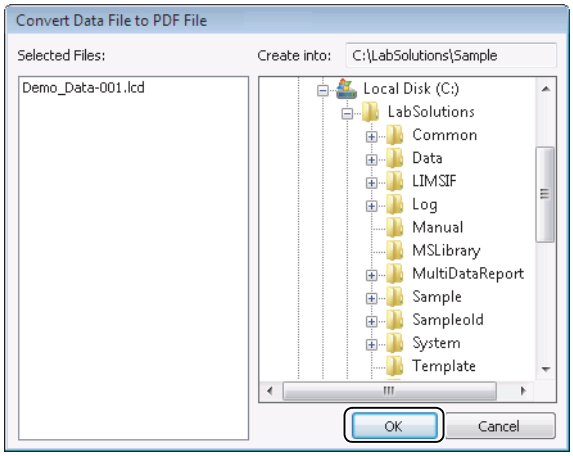
This section describes the procedure for batch-output of data reports in selected data files to the PDF format using the file conversion function.

1 **Right-click a data file from in the [Data Explorer] sub-window.**

2 **Click [File Conversion] then [Convert LabSolutions Data File to PDF File].**



3 **Select the PDF file output destination, and click [OK].**



The PDF file is created at that output destination.

NOTE

- To select multiple data files in the [Data Explorer] sub-window, either click the files with the [Ctrl] key held down, or click two files with the [Shift] key held down to select continuous files between the two files.
- Files of other types can also be converted to target files using the same procedure.

5.3 Software Validation

The software can confirm whether an installed program has been changed, and confirm whether chromatogram information in the data files has been altered.

5.3.1 Check the Program

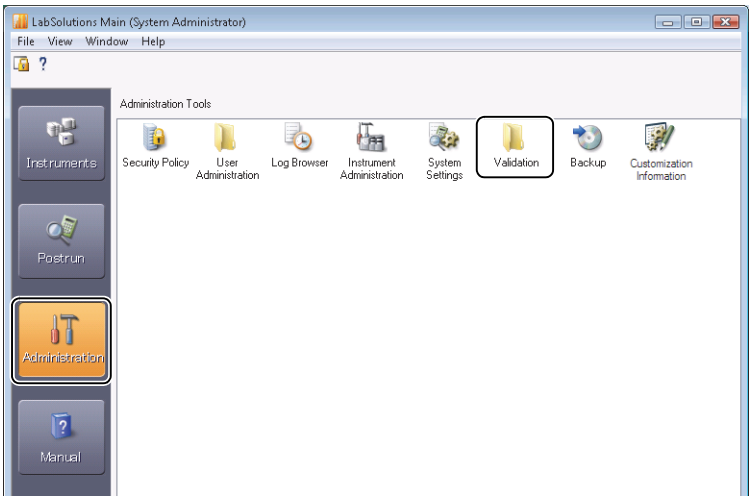
Execute [Check the Program Files] to compare each of the software programs to the original installed state to determine whether they have been tampered with or deleted.

This section describes the [Check the Program Files] procedure.

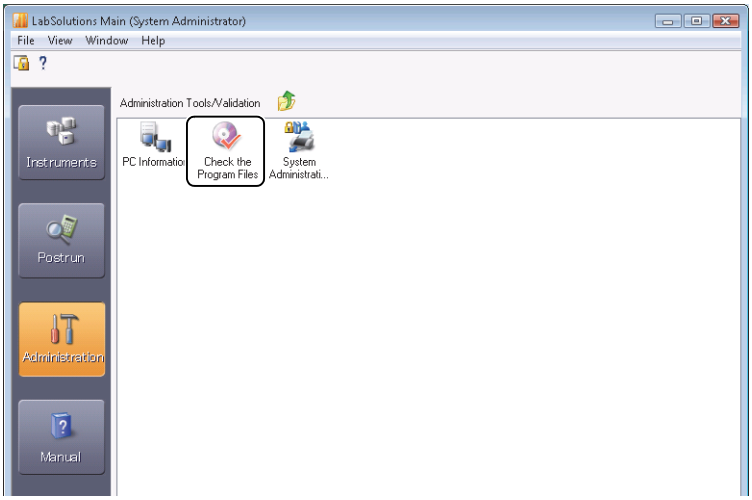
NOTE

To execute [Check the Program Files], log in as a user ID having the [Perform Validation Support] rights.

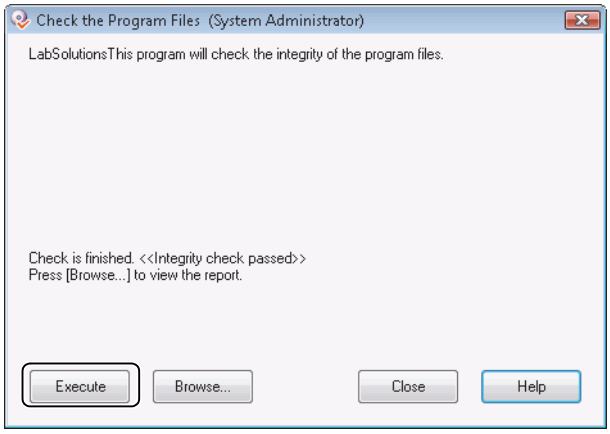
1 **Double-click the [Validation] folder icon in the [System Administrator] sub-window of the [LabSolutions Main] window.**



2 **Double-click the (Check the Program Files) icon.**

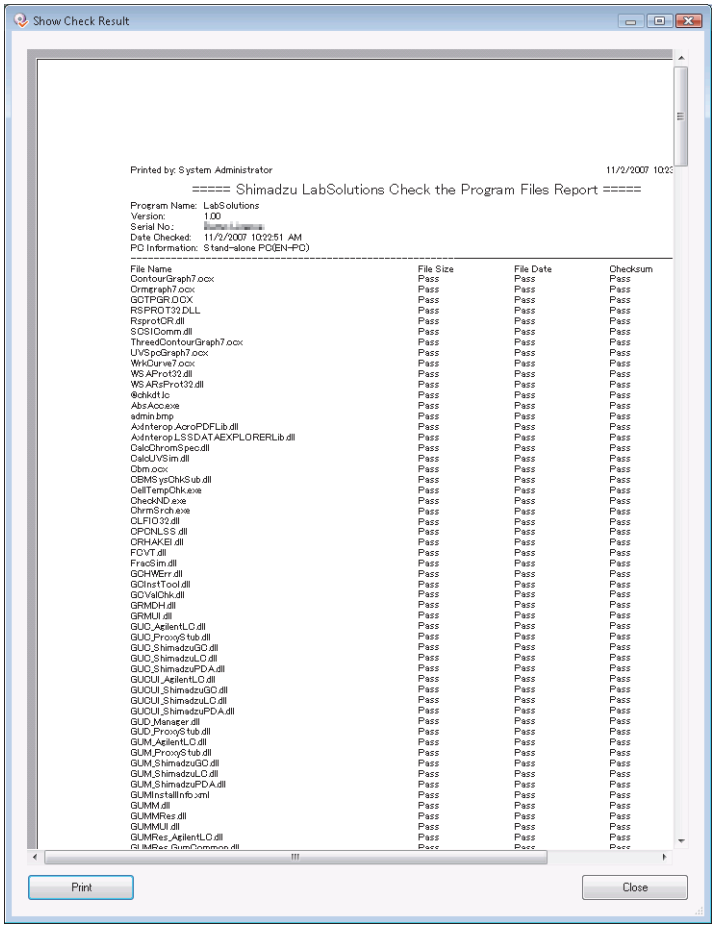


3 Click [Execute].



The program files check is executed.
When the check ends, the result is displayed in the sub-window.

4 To check detailed information of each program, click [Browse].



NOTE

Click [Print] in the [Show Check Result] sub-window to print the results of the program check.

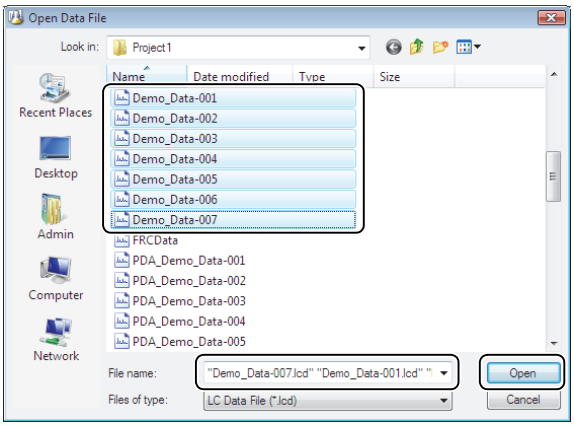
5.3.2 Check Raw Data

When [Check Raw Data] is executed, the raw (waveform) data for the chromatograms in the data file can be examined to see if it has been tampered with by a computer virus or other illegal means.

This section describes an example of how to check the raw data of a data file from the [Data Analysis] window.

1 **Click [Check Raw Data] on the [Tools] menu in the [Data Analysis] window.**

2 **Select the file, and click [Open].**

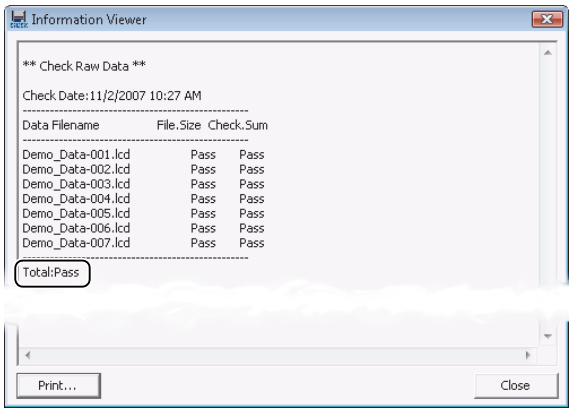


The raw data check is executed.

NOTE

The raw data check can be executed for multiple data files.
To select multiple data files, either click each file with the [Ctrl] key held down, or click two files with the [Shift] key held down to select continuous files between the two files.

3 **Check that [Total:Pass] is displayed in the [Information Viewer] sub-window.**



NOTE

Click [Print] in the [Information Viewer] sub-window to print the results of the raw data check.

Index

M

N

O

P

R

S

T

U

V

W