Xcalibur

LCquan

Configuring LCquan for Compliance with
21 CFR Part 11

Administrator Guide

DOCUMENTATION
SURVEY

Thermo
SCIENTIFIC

For Research Use Only. Not for use in diagnostic procedures.

Contents

Preface

The LCquan™ 2.6.0 application is part of the Xcalibur™ mass spectrometry data system. This administrator guide describes how to configure the Xcalibur and LCquan applications to help an organization comply with the Electronic Records and Electronic Signatures Rule, published by the United States Food and Drug Administration as 21 CFR Part 11. The intended audience includes both laboratory administrators and local IT professionals who have administrative privileges for the system.

> **IMPORTANT** Some of the instructions in this guide assume an understanding of the security settings for Microsoft™ Windows™ operating system. Thermo Fisher Scientific strongly recommends that you enlist your local IT professional to perform these tasks.

To provide us with comments about this document, click the link below. Thank you in advance for your help.

DOCUMENTATION
SURVEY

Related Documentation

The following LCquan manuals are available on the LCquan software CD as PDF files:

- *LCquan Administrator Guide* describes how to configure the application for compliance with 21 CFR Part 11.

- *LCquan User Guide* describes how to use the LCquan application to perform quantitative analysis of compounds.

- *LCquan Tutorial* describes step-by-step procedures to perform quantitative analysis with sample data.

If you are using a Watson laboratory information management system (LIMS), refer to *Installing and Using the Peak View Gateway Between Watson and LCquan*.

If you are using the Thermo Scientific Web Access Suite™, refer to the *Web Access Administrator Guide* for instructions on adding the LCquan application to the programs served by Web Access.

❖ **To view the installed LCquan manuals**

Go to **Start > Programs > Thermo Xcalibur > Manuals > LCquan**.

❖ **To open the LCquan Help**

1. From the LCquan window, choose **Help > LCquan Help**.

2. To locate a particular topic, use the Help Contents, Index, or Search panes.

Special Notices

Make sure you follow the precautionary statements presented in this guide. The special notices appear in boxes.

> **IMPORTANT** Highlights information necessary to prevent damage to software, loss of data, or invalid test results; or might contain information that is critical for optimal performance of the system.

> **Note** Highlights information of general interest.

> **Tip** Highlights helpful information that can make a task easier.

Contacting Us

There are several ways to contact Thermo Fisher Scientific for the information you need.

❖ **To contact Technical Support**

Phone	800-532-4752
Fax	561-688-8736
E-mail	us.techsupport.analyze@thermofisher.com
Knowledge base	www.thermokb.com

Find software updates and utilities to download at mssupport.thermo.com.

❖ **To contact Customer Service for ordering information**

Phone	800-532-4752
Fax	561-688-8731
E-mail	us.customer-support.analyze@thermofisher.com
Web site	www.thermo.com/ms

❖ **To copy manuals from the Internet**

Go to mssupport.thermo.com and click **Customer Manuals** in the left margin of the window.

❖ **To suggest changes to documentation or to Help**

• Fill out a reader survey online at
http://www.surveymonkey.com/s.aspx?sm=R7gKOvhLXn3NTkpK2BefHQ_3d_3d.

• Send an e-mail message to the Technical Publications Editor at
techpubs-lcms@thermofisher.com.

Introduction

This chapter briefly describes the major requirements for the Electronic Records and Electronic Signatures Rule, published by the United States Food and Drug Administration as 21 CFR Part 11.[1] It also provides an overview of the tasks required to configure the Xcalibur and LCquan applications to help ensure technical compliance with 21 CFR Part 11.

Note that 21 CFR Part 11 requires both technical and procedural compliance. To achieve technical compliance, you must use software that provides technical controls such as security features and functions. To accomplish procedural compliance, you must establish standard operating procedures and policies that define how to use processes and systems in a manner that complies with 21 CFR Part 11.

Contents

- Major Requirements of 21 CFR Part 11
- Compliance with 21 CFR Part 11
- LCquan Folder Structure
- Prerequisites To Configuring the System
- Understanding the Administrator Tasks

---

[1] Electronic Records: Electronic Signature Final Rule. *Code of Federal Regulations,* Part 11, Title 21, Food and Drugs; *Fed. Regist.* **1997**, *62* (54).

The final rule is also available electronically at http://www.fda.gov.

Major Requirements of 21 CFR Part 11

In August 1997, the United States Food and Drug Administration published a rule for electronic records and electronic signatures under the current good manufacturing practice (GMP) regulations in the Code of Federal Regulations (21 CFR Part 11). The rule provides criteria to make electronic records and electronic signatures equivalent to paper records and handwritten signatures. It also permits the widest possible use of electronic technology.

To comply with 21 CFR Part 11, you must implement rules to ensure that proper methods, procedures, and controls are in place. These rules address the following issues:

- Prevention of Data Falsification

- Data Reconstruction

- System Security

Prevention of Data Falsification

You can falsify electronic data in several ways:

- Direct modification

- Indirect modification by deleting records

- Indirect modification by using readily available tools

To prevent falsification, you must implement a number of controls. These controls can be procedural in nature or can be functionally implemented within the system generating the electronic records. Normally, achieving compliance requires a combination of both methods.

To help prevent data falsification, the Xcalibur data system uses audit trails and system security.

Data Reconstruction

Showing how data is generated is just as important as showing that you have not falsified data. You cannot reconstruct raw data; however, it is possible to regenerate all other records derived from the original raw data files.

To confirm that all electronic records generated from the raw data can be regenerated, an efficient and comprehensive audit trail must fulfill these criteria:

- Account for all events and actions that are required to regenerate the records.

- Add new audit trail entries to existing records only. Do not overwrite or obstruct other records.

- Prevent the user from having any control of the audit trail records or modifying the configuration of the audit trail.

The audit trails that the Xcalibur data system creates meet these requirements.

System Security

To prevent unauthorized access to data, most organizations implement strict security procedures for their computer networks. In this context, *unauthorized access* means:

- Access by an individual (external or internal to the organization) who has not been granted the authority to use, manipulate, or interact with the system

- Access by using the identity of another individual—for example, by using a colleague's user name and password

The 21 CFR Part 11 rule defines a number of controls to ensure that only the individuals who have some level of responsibility toward the system that generates electronic records can access them. The rule includes both procedural controls and functionality controls.

The Xcalibur data system directly implements some of these controls and relies on the security functions in the Microsoft Windows XP Professional operating system for other controls, for example:

- The Finnigan™ Security Server controls secure file operations.

- The laboratory administrator restricts user access through Thermo Foundation Authorization Manager (an administrative utility), which relies on Windows XP Professional user groups.

- The laboratory administrator controls software feature access through the Thermo Foundation Authorization Manager.

- Windows XP Professional security functions handle user authentication.

- Windows XP Professional security functions maintain electronic record security and, in particular, the NTFS permission rights.

Compliance with 21 CFR Part 11

To comply with 21 CFR Part 11, you can take advantage of security features and functions added to certain Xcalibur applications. To fully implement these security features, the laboratory administrator must work with the IT professional in achieving the proper Xcalibur configuration.

Configuring Software Applications

Configuring applications for compliance with 21 CFR Part 11 requires two steps:

- Protecting Records

- Setting Up User Access Controls

Protecting Records

To establish secure file operations, as the laboratory administrator, you must restrict access permissions for specific folders and files. Set permissions so that only you can delete or alter records. The use of protected folders and files ensures that unauthorized users cannot obscure previous records by using a utility such as Windows Explorer.

Setting Up User Access Controls

To control user access, you must define secure user groups and grant access permissions for each group. You can restrict defined groups of users from performing various functions within the application. This restriction can range from complete prohibition, through several levels of password-required access, to no restrictions. You set user access controls by using Thermo Foundation Authorization Manager.

After the security settings are defined for at least one group, users who are not in a secure group are denied access to the application.

> **IMPORTANT** If no secure groups are defined, then users have access to all features of the application.

Security Features Within the Xcalibur Application

After the appropriate file protections and user access controls are in place, the Xcalibur application employs several built-in features to ensure the security of the data and to meet 21 CFR Part 11 requirements.

The Xcalibur application performs Cyclic Redundancy Checks (CRCs) to protect against malicious changes to data files. A CRC can detect file corruption and attempted changes to data files outside the application. The CRC calculates checksums for sets of data, using mathematical formulas, and embeds the value within the file. Each time you open the file, the CRC recalculates the checksums and compares them with the stored values. When you modify or process data within the application, the CRC recalculates and stores new checksums.

In addition, the Xcalibur application includes a file tracking system that maintains a database of the files created in or used by the application. When you open an existing project, the Xcalibur application displays a warning if files within that project have been moved or modified (as determined from the CRC value).

A comprehensive audit trail ensures that you can generate all electronic records from the raw data. The audit trail comprises three parts: the history log, the event log, and the file tracking log. The history log contains information about every parameter change a user has made within an LCquan workbook. The event log contains information about all the events that have occurred within the application, such as the creation of a workbook or the execution of a command that is under authorization control. The file tracking log tracks changes made to files contained within an LCquan workbook.

Prerequisites To Configuring the System

As the laboratory administrator, you must plan how the laboratory will function before performing the procedures in this guide. At a minimum, address the following:

- How Users Perform Sample Acquisition

- LCquan Folder Structure

- Secure User Groups

How Users Perform Sample Acquisition

The Scenarios for LCquan Sample Acquisition diagrams illustrate how users can perform sample acquisitions and where the LCquan system can store the acquired sample data:

- Scenario A—Acquired sample data stored on a standalone workstation (local users)

- Scenario B—Acquired sample data stored on a workstation that is on a network (domain users)

- Scenario C—Acquired sample data stored on a network server (domain users)

A scenario B or C configuration can be integrated with a laboratory information management system, such as the Watson LIMS. If you are using a Watson LIMS, refer to *Installing and Using the Peak View Gateway Between Watson and LCquan*.

For scenario C, the LCquan system supports the Citrix Presentation Server™ environment for LCquan workstations that are for data review only. The Citrix server can provide application virtualization to manage LCquan configuration and maintenance. An instance of the LCquan application running on a Citrix server cannot be used for acquisition. The IT professional is responsible for installing LCquan software on the Citrix server.

For scenario C, the LCquan system supports the Thermo Scientific Web Access Server environment for LCquan workstations that are for data review only. Web Access can provide application virtualization to manage LCquan configuration and maintenance. An instance of the LCquan application running on a Web Access server cannot be used for acquisition. The IT professional is responsible for installing LCquan software on the Web Access server.

For scenario C, the LCquan system supports remote acquisition. During remote acquisition, the application time-stamps rawfiles and creates a time-stamped folder:

- Remotely stored rawfiles are time-stamped with the submission time.

- All rawfiles in a sequence share the same time stamp.

- Pausing during acquisition does not change the time stamp.

- The time stamp for the rawfiles folder and the time stamp for the rawfiles are not necessarily the same.

Figure 1. Scenarios for LCquan Sample Acquisition

A. Acquisition to a standalone LCquan system
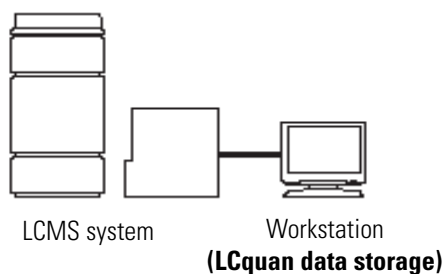
Local acquisition
Local user
Standalone workstation

LCMS system   Workstation
                (LCquan data storage)

B. Acquisition to a standalone LCquan system on a network
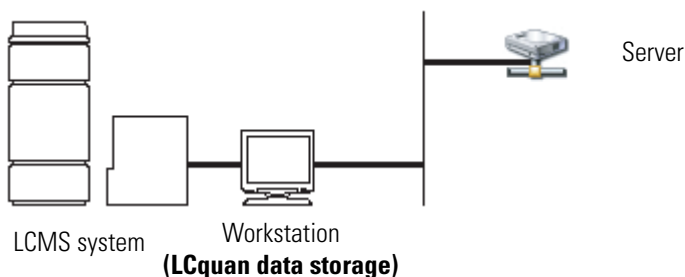
Server

Local acquisition
Domain users
Networked workstation but data stored locally
(LIMS option)

LCMS system   Workstation
                (LCquan data storage)

C. Acquisition to a network server
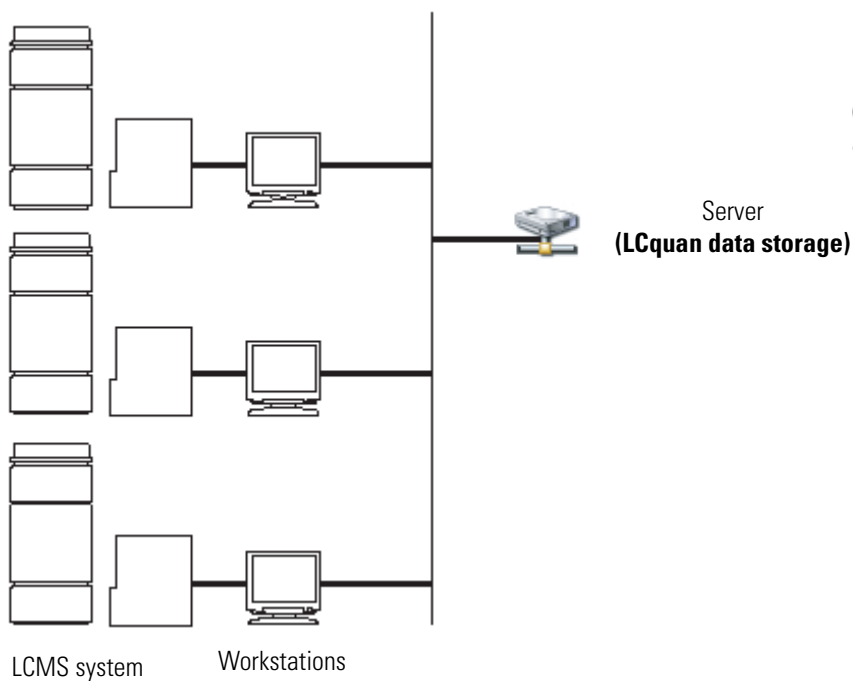
Network acquisition
Domain users
Networked workstations
(LIMS option, Web Access option,
and Citrix option)

Server
(LCquan data storage)

LCMS system   Workstations

LCquan Folder Structure

The LCquan folder structure includes the following:

- Security folder—Contains the configuration files. Thermo Foundation Authorization Manager retrieves the controlled feature information from the configuration files in the Security folder. The file path for the security folder is as follows:

  C:\Documents and Settings\All Users\Application Data\Thermo Scientific\INI

- Root folder or folders—Contain the LCquan projects.

  - For storing the acquired data locally, you can use the default folder, \Xcalibur\QuanRoot, or you can create your own LCquan root folder. Go to Scenarios for LCquan Sample Acquisition, scenario A.

  - For storing the acquired data on a network server, you must designate a folder on the network server as the LCquan root folder.

For each new project, the LCquan application creates the following hierarchical folder structure within the designated root folder (see Figure 2).

- Study folder—Top-level folder within the root folder. Each study folder contains one or more workbook folders. The study folder can contain any number of workbook folders, but each workbook must have a unique name.

- Workbook folder—Contains all the information that the LCquan application uses for an individual quantitative analysis project. The workbook folder contains the LCquan file (.lqn), the instrument method file (.meth), and an audit database (.mdb). The workbook folder also contains the following:

  - Exports folder—Stores copies of all files that the application exports, such as report files.

  - Imports folder—Stores a copy of legacy files that you import into the workbook, such as instrument method files, processing method files, or sequence files.

  - Rawfiles folder—Contains acquired data files (.raw files) and any imported raw data files.

  - Temp folder—Contains temporary files used by the LCquan application.

Figure 2. LCquan folder structure
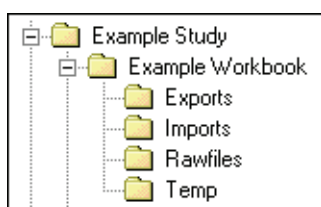
Secure User Groups

The LCquan application requires both the security features of the Windows XP operating system and the Foundation Authorization Manager to define the LCquan secure user groups and permissions. Typically, the IT professional is responsible for establishing Windows user accounts and user groups. The laboratory administrator is responsible for setting up the permission levels in Foundation Authorization Manager and, if necessary, private groups.

- **Windows user groups**

  - The IT professional creates and manages domain user accounts and user groups. Go to Scenarios for LCquan Sample Acquisition, scenarios B and C.

  - You or the IT professional can create standalone workstation user accounts and user groups. Go to Scenarios for LCquan Sample Acquisition, scenario A.

  > **IMPORTANT** Each Windows user account must be associated with a user ID, a password, and a full description. These items are required for the system to store the auditing information in the designated database.

- Authorization Manager private groups—A group can be either a preexisting Windows user group or a private group that you configure within the Foundation Authorization Manager.

  - Networked workstation—A user must be a member of a domain user group before you can add the user to a private group. If an intended user is not a user on the domain, the IT professional must create a user account for the user. Go to Scenarios for LCquan Sample Acquisition, scenarios B and C.

  - Standalone workstation—A user must have a logon account for the workstation before you can add the user to a private group. You or the IT professional must create a user account for each intended user. Go to Scenarios for LCquan Sample Acquisition, scenario A.

As the laboratory administrator, you must make the following decisions before asking your IT professional to configure Windows user groups for domain users or before configuring private groups in the Foundation Authorization Manager:

- Types of user roles, for example, administrator, supervisor, scientist, technician, auditor, or quality assurance

- Individuals assigned to each user role and their projects

- Permissions for a given user role, such as the authority to create methods and acquire data, signature authority, or read-only access to workbooks

  For example, a laboratory might have standard operating procedures that prohibit technicians from performing certain operations with the software. But the same laboratory might not have any restrictions on software operations that the scientists can perform. In this case, you must create at least two user groups—one for scientists and one for technicians.

A user can belong to more than one user group. In the following example, users 1, 2, and 3 belong to more than one user group.

Figure 3. LCquan system users and user groups example
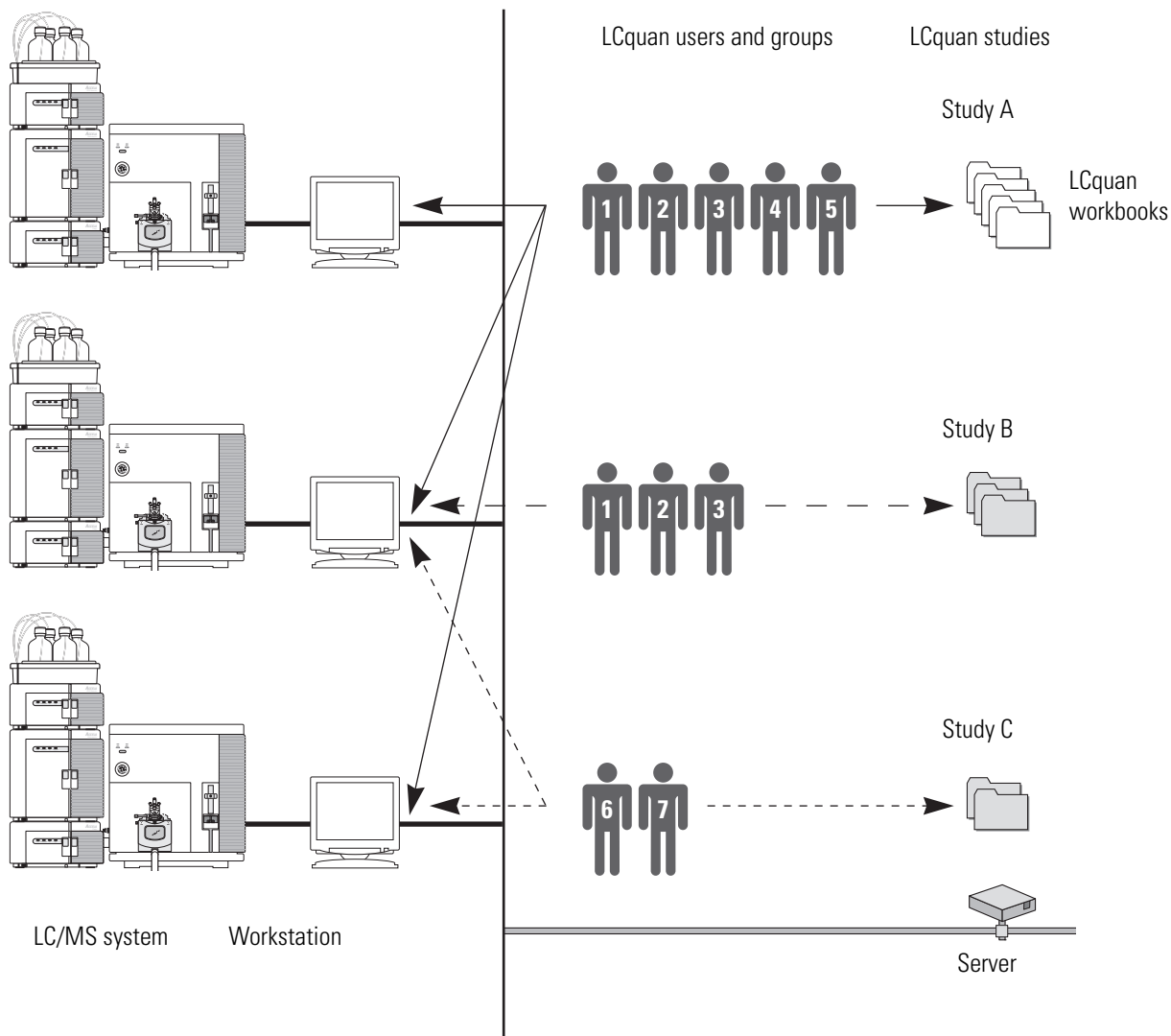
Understanding the Administrator Tasks

As the laboratory administrator, you must work with your IT professional to configure the system for compliance with 21 CFR Part 11.

- The 21 CFR Part 11 Compliance Checklist shows the tasks for both your role and the role of the IT professional.

- Configuration workflows for both domain users on page 12 and local users on page 13 show how the tasks can vary for different laboratory configurations.

> **IMPORTANT** The local IT administrator must configure the security features and settings for Windows.

Complete the procedures that are outlined in the 21 CFR Part 11 Compliance Checklist and described in detail in the following chapters. Otherwise, the Xcalibur data system might not fully comply with 21 CFR Part 11 requirements.

Table 1. 21 CFR Part 11 Compliance Checklist (Sheet 1 of 2)

Task	Refer to topic	Role	Completed?
1. Install software for Xcalibur and LCquan on the designated workstations.	Installation instructions packaged with the software CDs	IT professional or laboratory administrator	
2. Run the database configuration application.	"Using the Database Configuration Manager" on page 15	IT professional (Oracle™ database) or laboratory administrator	
3. Ensure that the Finnigan Security Server is properly configured and running.	"Verifying the Properties of the Finnigan Security Server" on page 20	IT professional or laboratory administrator	
4. Determine which folder to use as the LCquan secure root folder and identify the secure user groups.	"LCquan Folder Structure" on page 7 and "Secure User Groups" on page 8	Laboratory administrator	
5. Configure security settings for Windows: a. Set up users and groups. b. Specify the password lockout parameters for failed logon attempts. Refer to your company's guidelines. c. Restrict access to the secure root folder. Ensure users have permissions to write to the secure root folder.	"Configuring Security Settings for Folders and Files" on page 25	IT professional (Laboratory administrator can also restrict access to the secure root folder.)	
6. Configure sequential user logon and automatic logoff.	"Specifying the Way Users Log On and Off" on page 39	IT professional or laboratory administrator	

Table 1. 21 CFR Part 11 Compliance Checklist (Sheet 2 of 2)

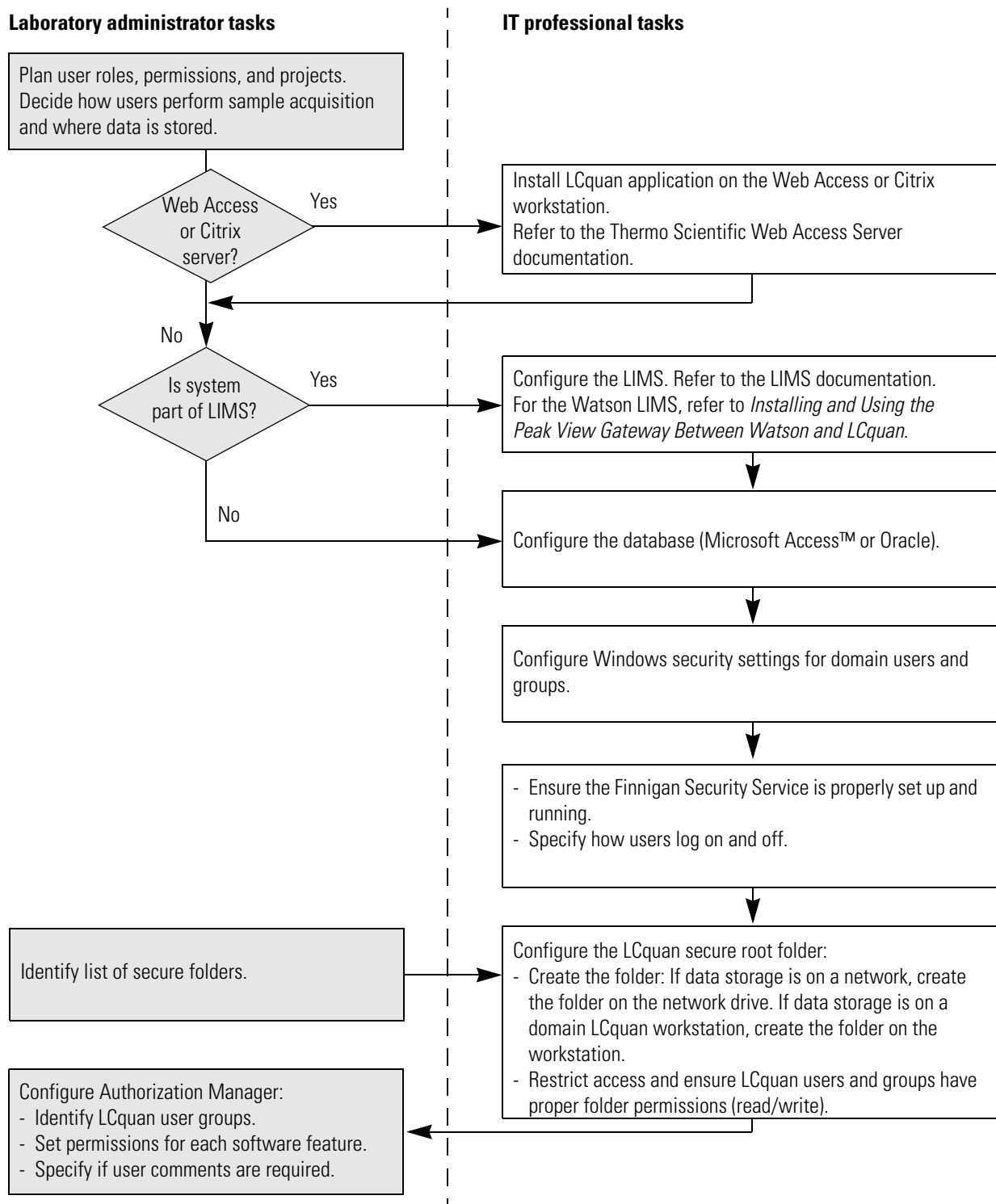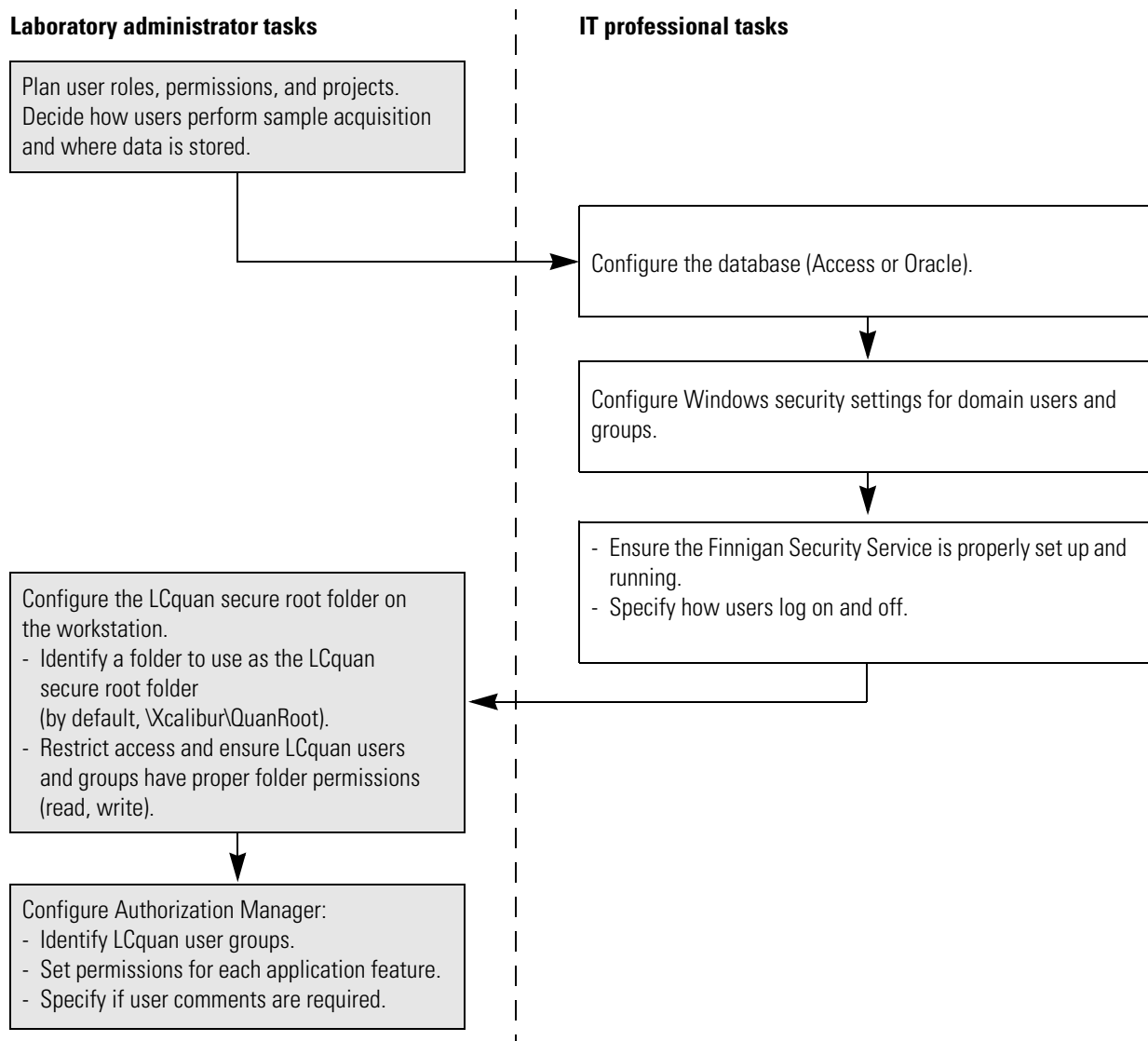| Task	Refer to topic	Role	Completed?
7. Configure Authorization Manager settings for the LCquan application:	"Using the Authorization Manager" on page 44	Laboratory administrator	
a. Define LCquan user groups.	"Setting Up Secure User Groups" on page 45		
b. Set permission levels for software features for each LCquan user group.	"Setting Permissions" on page 48, and "Permission Level Settings in the LCquan Application" on page 69		
c. If users are permitted to change the secure root folder, define the list of secure folders.	"Defining the List of Secure Folders" on page 53		
d. Specify whether users are required to make comments.	"Viewing the Authorization Manager History Log" on page 58		
e. Save the configuration settings.	"Saving the Security Settings" on page 59		

Figure 4. Configuration tasks of the laboratory administrator and IT professional for domain users

Laboratory administrator tasks | **IT professional tasks**

Plan user roles, permissions, and projects. Decide how users perform sample acquisition and where data is stored.

Web Access or Citrix server? — Yes → Install LCquan application on the Web Access or Citrix workstation.
Refer to the Thermo Scientific Web Access Server documentation.

No ↓

Is system part of LIMS? — Yes → Configure the LIMS. Refer to the LIMS documentation.
For the Watson LIMS, refer to *Installing and Using the Peak View Gateway Between Watson and LCquan*.

No →

Configure the database (Microsoft Access™ or Oracle).

Configure Windows security settings for domain users and groups.

- Ensure the Finnigan Security Service is properly set up and running.
- Specify how users log on and off.

Identify list of secure folders. →

Configure the LCquan secure root folder:
- Create the folder: If data storage is on a network, create the folder on the network drive. If data storage is on a domain LCquan workstation, create the folder on the workstation.
- Restrict access and ensure LCquan users and groups have proper folder permissions (read/write).

Configure Authorization Manager:
- Identify LCquan user groups.
- Set permissions for each software feature.
- Specify if user comments are required.

Figure 5. Configuration tasks of the laboratory administrator and IT professional for local users

Laboratory administrator tasks   **IT professional tasks**

Plan user roles, permissions, and projects.
Decide how users perform sample acquisition
and where data is stored.

Configure the database (Access or Oracle).

Configure Windows security settings for domain users and
groups.

- Ensure the Finnigan Security Service is properly set up and
  running.
- Specify how users log on and off.

Configure the LCquan secure root folder on
the workstation.
- Identify a folder to use as the LCquan
  secure root folder
  (by default, \Xcalibur\QuanRoot).
- Restrict access and ensure LCquan users
  and groups have proper folder permissions
  (read, write).

Configure Authorization Manager:
- Identify LCquan user groups.
- Set permissions for each application feature.
- Specify if user comments are required.

Using the Database Configuration Manager

This chapter describes how to use the Database Configuration Manager to configure your compliance database. The compliance database keeps a record of auditable events and changes made to files that the Xcalibur data system creates and manages. Until you run the Database Configuration Manager, all applications run without auditing and the system is *not* in compliance with 21 CFR Part 11.

Contents

- Using Microsoft and Oracle Databases

- Configuring Your Auditing Database

Using Microsoft and Oracle Databases

The LCquan application uses a Microsoft Access database to store each LCquan workbook audit trail. To store the Xcalibur Global audit trail, you can use either of the following:

- Oracle database on a network workstation or server (remote system)

- Microsoft Access database on a standalone or networked workstation or server

Note If you already ran the Database Configuration Manager program as part of configuring Xcalibur 2.0 for 21 CFR Part 11 compliance, you do not need to run the program again.

If the Watson LIMS is part of the workflow, refer to the Watson documentation for database setup instructions that are specific to the Watson LIMS.

To use an Oracle database, make sure that you complete the following tasks:

1. If the site does not have an Oracle server, install an Oracle database on an accessible remote server. For more information, see "Installing the Oracle Server" on page 78 or consult your Oracle database administrator.

2. Install the Oracle client software on your local system. For more information, see "Installing the Oracle Client" on page 86 or consult your Oracle database administrator.

3. If you do not know the user name, password, and Oracle Net Service Name of your Oracle database, obtain this information from your Oracle database administrator.

IMPORTANT Ensure that no other Xcalibur applications are running at the same time as the Database Configuration manager. Auditing of Xcalibur applications cannot take place while running the Database Configuration manager.

Configuring Your Auditing Database

This section describes how to use the Database Configuration manager to configure your auditing database.

❖ **To configure your auditing database**

1. From the Windows XP taskbar, choose **Start > Programs > Thermo Foundation 1.0 > Database Configuration**.

   The Auditing Database Configuration Manager opens.
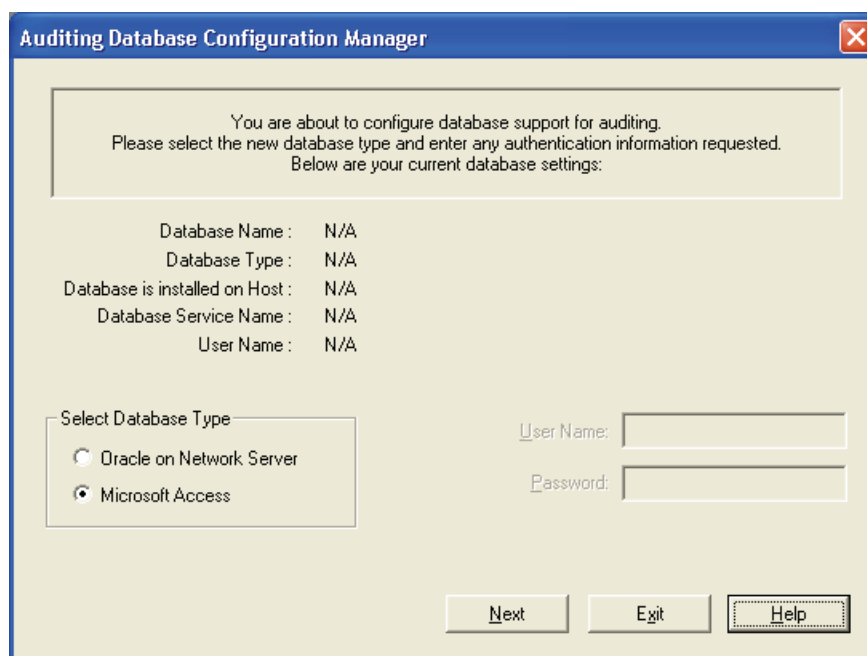
2. In the Select Database Type area, select the database type:

   • If you are using an Access database, select the **Microsoft Access** option and go to step 4.

   • If you are using an Oracle database, select the **Oracle on Network Server** option and go to step 3.

3. For an Oracle database, specify the Oracle database parameters:

   a. In the User Name box, type the database user name.

   b. In the Password box, type the database password.

   c. In the Oracle Net Service Name list, select the Oracle Net Service Name for your database.

   Note Be sure to use the Oracle user name and password provided by your Oracle database administrator.

4. Click **Next**.

The DatabaseConfigManager dialog box opens.
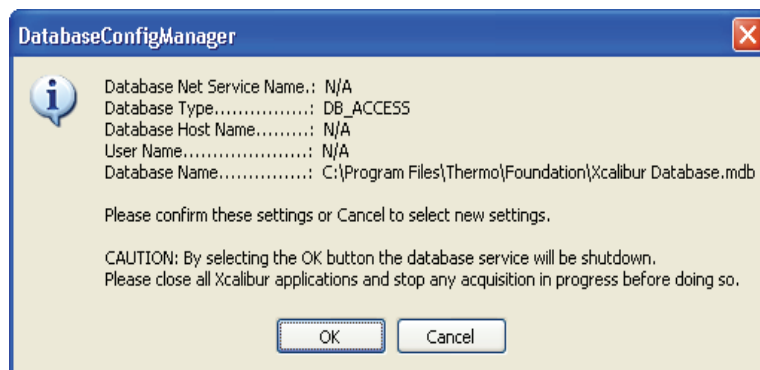
5. Verify that the settings in the DatabaseConfigManager dialog box are correct and click **OK**.

   The next page of the Auditing Database Configuration Manager opens.
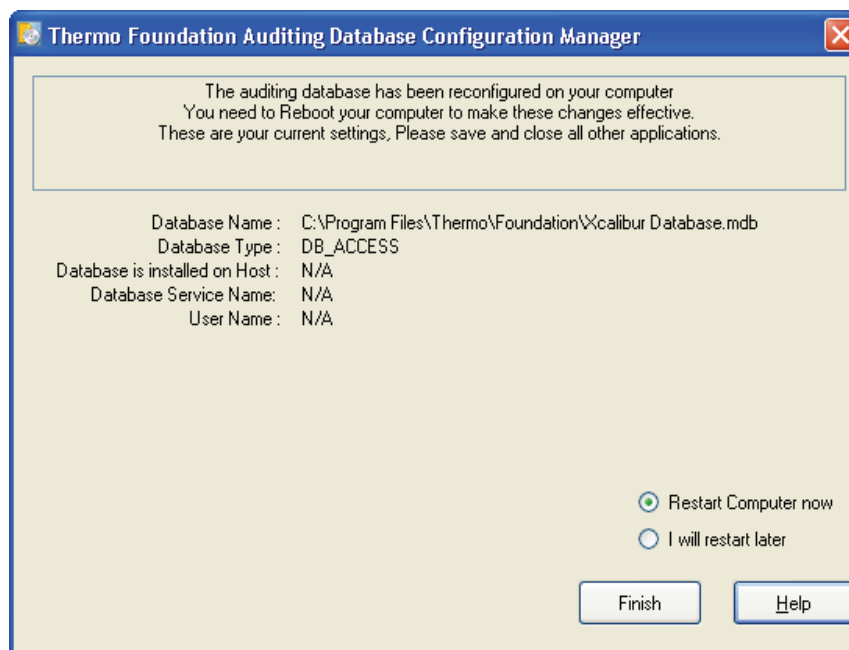
6. Select a restart option:

   • To automatically restart the computer, select the **Restart computer now** option.

   • To manually restart the computer at a later time, select the **I will restart later** option.

   > **Note** The changes made in the Database Manager take effect after restarting the computer.

7. Click **Finish** to save your settings and close the Auditing Database Configuration Manager.

Establishing Secure File Operations

The 21 CFR Part 11 rule requires that previously recorded information cannot be obscured by record changes. This rule also requires that records be protected to allow for their accurate and ready retrieval.

To comply with these requirements, you must store all electronic records in protected folders and you must establish standard operating procedures for precise and systematic record archiving.

Contents

- Verifying the Properties of the Finnigan Security Server
- Verifying the Properties of Thermo Foundation DatabaseService
- Configuring Security Settings for Folders and Files
- Configuring Security Settings for the Database Registry Key
- Specifying the Way Users Log On and Off
- Removing and Archiving Files

Verifying the Properties of the Finnigan Security Server

The Finnigan Security Server has two main functions:

- User authentication—If you select authentication for certain events using the Foundation Authorization Manager, the Security Server verifies user names and passwords whenever they are entered.

- Secure file operations—You can set the Security Server to take ownership of the data folders and files. This security measure prevents users from deleting data they own.

When you install the application, the Security Server is installed and started. It is configured to start automatically every time the computer is restarted.

> **IMPORTANT** You must prevent unauthorized users from stopping the Security Server. If the Security Server is stopped, the security features in the application do not function properly.
>
> Only the system administrator who installed the application software and the Security Server, or who has administrative rights, can stop the server.

❖ **To verify that the properties of the Security Server are set correctly**

1. Open the Windows Services feature as follows:

    a. From the Windows XP taskbar, choose **Start > Settings > Control Panel.**

    b. Double-click **Administrative Tools**.

    c. Double-click **Services**.

2. Right-click **Finnigan Security Server**, and choose **Properties** from the shortcut menu.

    The Finnigan Security Server Properties dialog box opens to the General page.

3. On the General page, set Startup type to **Automatic**.

4. Ensure that the Service status reads **Started**.
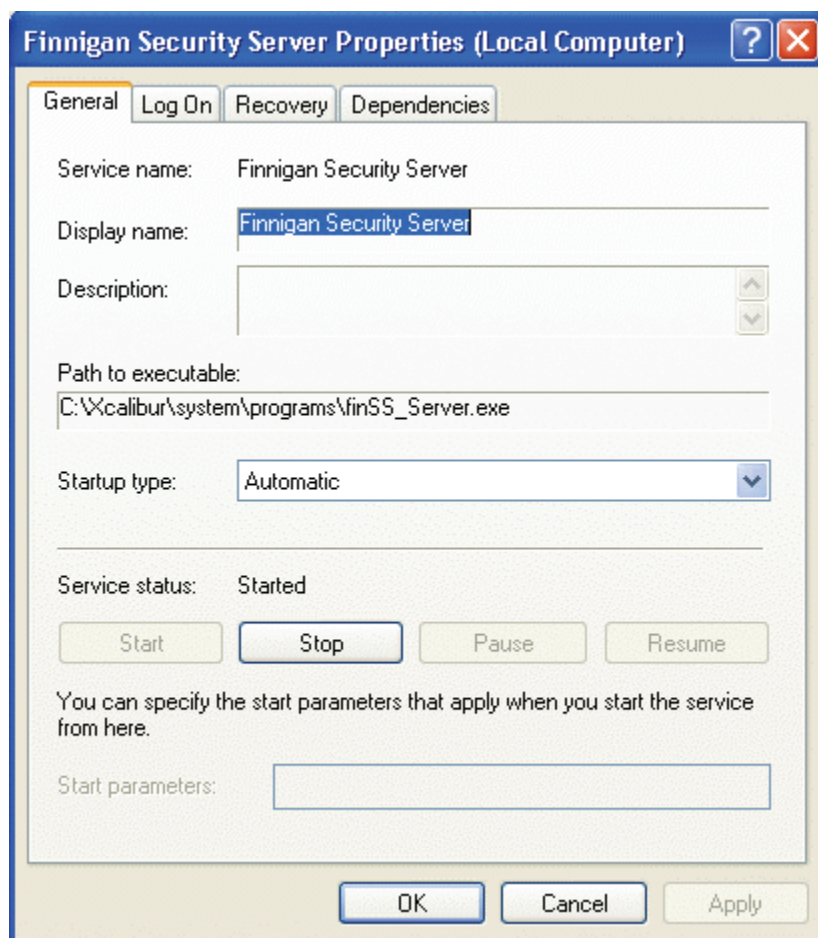
5. Click the **Log On** tab.
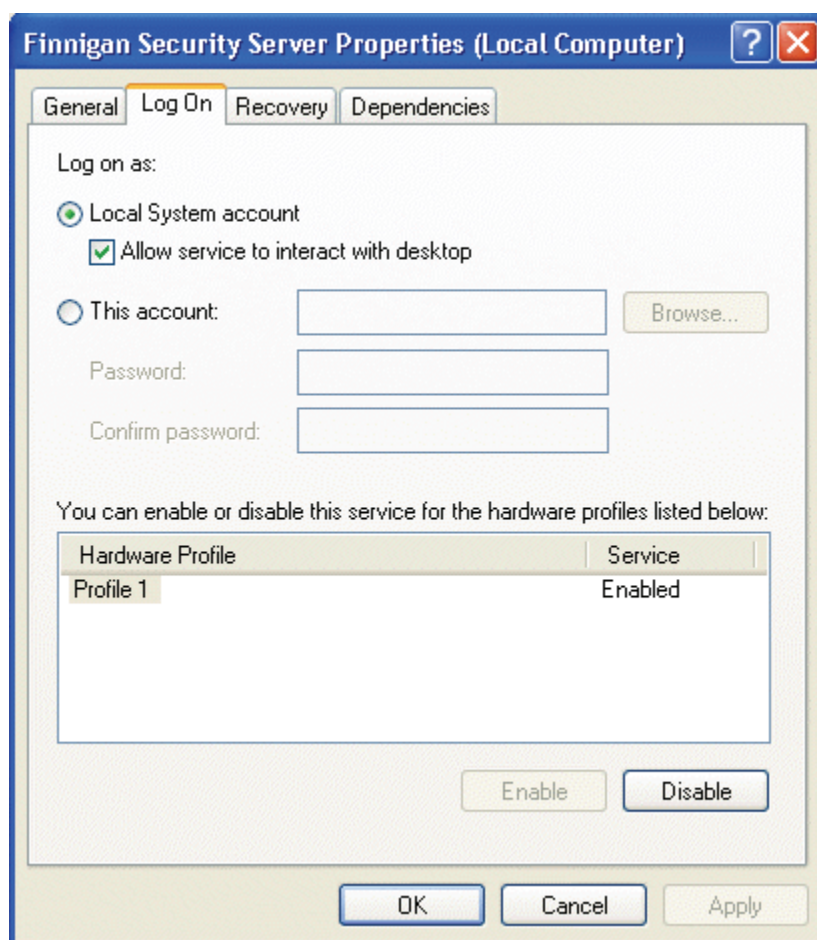
6. On the Log On page, select the **Local System account** option.

7. Select the **Allow service to interact with desktop** check box.

8. Click **OK** to close the Finnigan Security Server Properties dialog box.

9. Close the Services window, and then close the Administrative Tools window.

You have now confirmed that the Security Server is properly set up.

Verifying the Properties of Thermo Foundation DatabaseService

Using Thermo Foundation DatabaseService, Xcalibur applications can access the auditing database and make auditing entries.

Verify that the properties of the Foundation Database Service are correctly specified.

❖ **To verify properties of Foundation Database Service**

1. Open the Windows Services feature:

   a. From the Windows XP taskbar, choose **Start > Control Panel**.

   b. Double-click **Administrative Tools**.

   c. Double-click **Services**.

2. Verify properties for Foundation DatabaseService:

   a. Right-click **Thermo Foundation DatabaseService**, and choose **Properties** from the shortcut menu.

   The Thermo Foundation DatabaseService Properties dialog box opens.
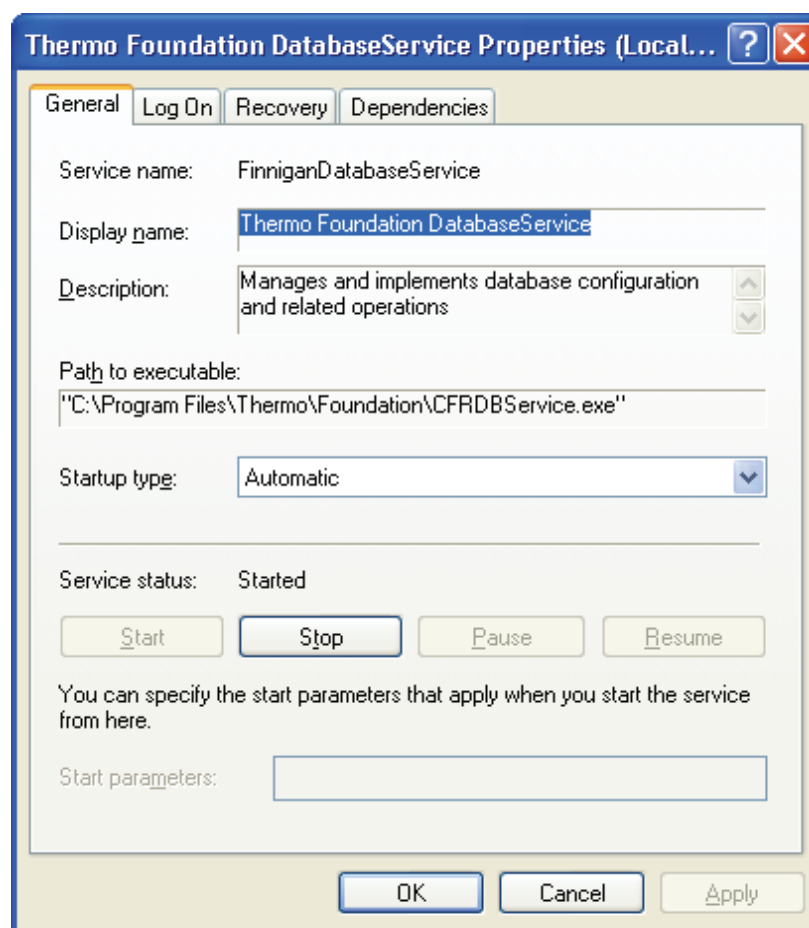
b. On the General page, ensure that Startup type is set to **Automatic**.

c. Ensure that the Service status reads **Started**.

d. Click the **Log On** tab.
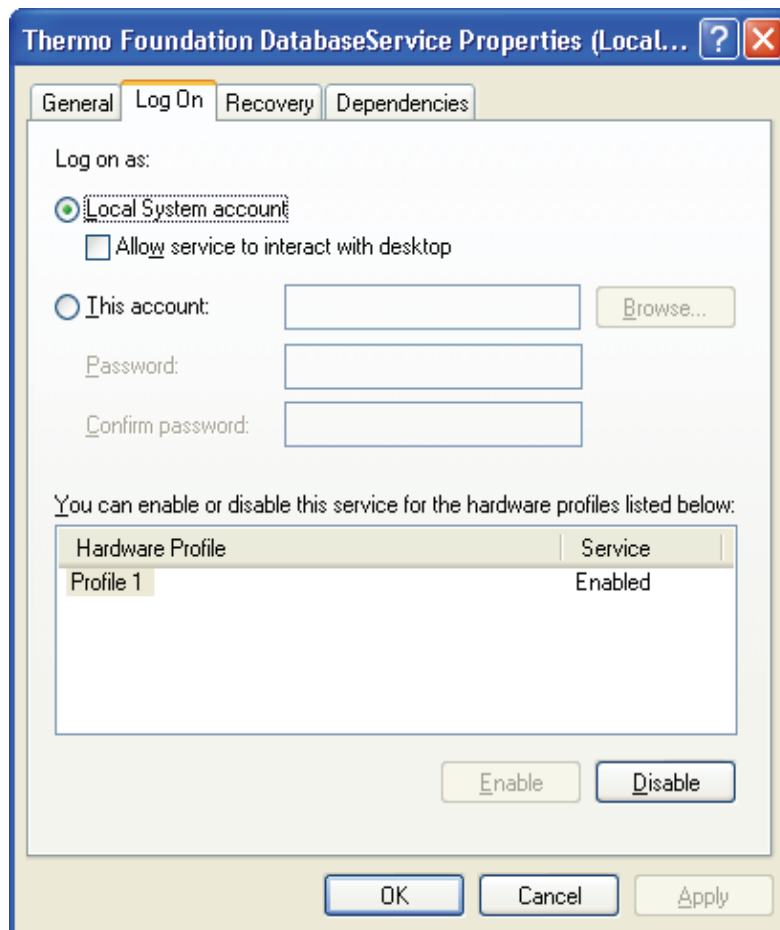
e. Ensure that the **Local System account** option is selected.

f. Ensure that the **Allow service to interact with desktop** check box is cleared.

g. Click **OK** to close the Thermo Foundation DatabaseService Properties dialog box.

3. Close the Services window, and then close the Administrative Tools window.

You have now confirmed that the services are properly set.

Configuring Security Settings for Folders and Files

To ensure the security of your data, you must restrict access to the following folders and the files contained within them:

- Root folder or folders—Contain the LCquan projects. See "LCquan Folder Structure" on page 7. You cannot permit non-administrators to delete files within the root folder.

- Security folder—Contains the configuration files. Because the Foundation Authorization Manager reads the controlled feature information from the configuration files, you must prohibit non-administrators from accessing these files. The security folder is located in the following folder:

  C:\Documents and Settings\All Users\Application Data\Thermo Scientific\INI

With the New Technology File System (NTFS—an advanced file system used within the Windows XP operating system), you can set the access permissions for folders and files for specific user groups. When you set up permissions, you specify the level of access for user groups. For example, you can do the following:

- Allow members of one user group to read the contents of a file.

- Allow members of another user group to make changes to the file.

- Prevent members of all other user groups from accessing the file.

New subfolders and files inherit folder permissions. You can make existing subfolders and files inherit new permissions that have been applied to the parent folder by using the Properties dialog box for the folder. (See "Preparing a Root Folder" on page 26.)

After you set the appropriate permissions, an unauthorized user cannot maliciously or accidentally alter previously recorded information using utilities such as Windows Explorer.

This section contains the following topics:

- Configuring Security Settings for the Root Folder

- Configuring Settings for the Security Folder

Configuring Security Settings for the Root Folder

You must create a root folder or folders for your data and configure the proper security settings for each folder. To do this, use the Security tab of the Properties dialog box to add users and groups and set the permissions for each.

In the procedures that follow, add an administrative user (or administrative group) and the group Everyone to the Group Or User Names list. Then, grant the administrator full access to the folder and grant limited access to everyone else.

> **Tip** To further restrict access to folders and files, you can grant access to specific user groups only. To do this, first set up appropriate user groups, as described in "Adding Windows Users and Groups" on page 30, and then perform the procedures that follow, using your specific user groups instead of the group Everyone.

Continue with the following topics:

- Preparing a Root Folder
- Adding Windows Users and Groups
- Removing Unnecessary Users
- Setting Permissions

Preparing a Root Folder

To prepare a root folder, first turn off Use Simple File Sharing in folders. You can then create a root folder for storing all your projects.

❖ **To turn off Use Simple File Sharing**

1. Log on to the system as a user with administrative privileges.

2. From the Windows XP taskbar, choose **Start > Programs > Accessories > Windows Explorer**.

3. In the Windows Explorer window, choose **Tools > Folder Options** to open the Folder Options dialog box. Then click the **View** tab.

4. In the Advanced settings list, scroll to the bottom.

5. Clear the **Use simple file sharing** check box.

Clear this check box.
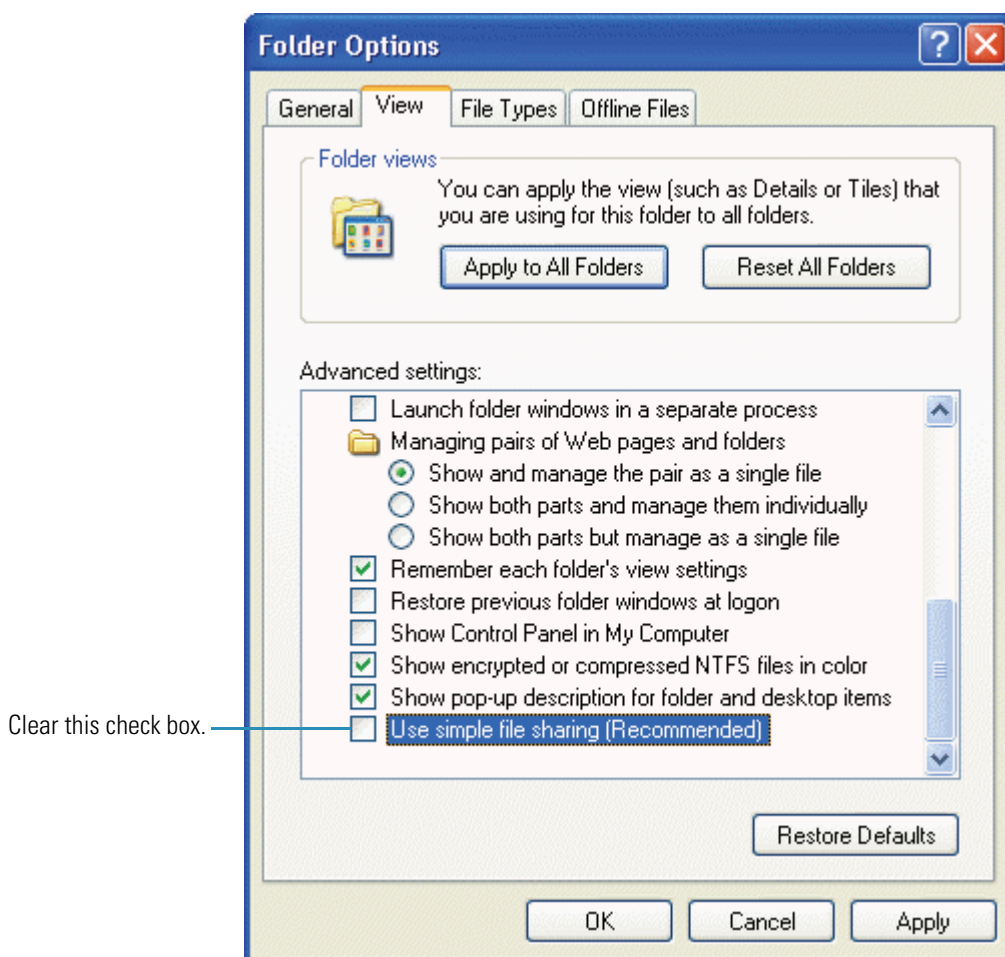
6. Click **OK** to save the change and close the Folder Options dialog box.

❖ **To create or locate a folder to use as the root folder for storing all projects**

1. Create or use any folder (except the Xcalibur folder).

   For example, you can use the QuanRoot folder (located in the Xcalibur folder) as the root folder for LCquan projects. This folder is created on your system when you load the LCquan software.

   > **IMPORTANT** Do not use the Xcalibur folder as your root folder. If you change the permission settings for this folder, Xcalibur applications will not run correctly. Instead, create a new folder or use another existing folder as your root folder.

2. Right-click the folder and choose **Properties** from the shortcut menu.

   The Study Properties dialog box for the folder opens.

3. Click the **Security** tab.
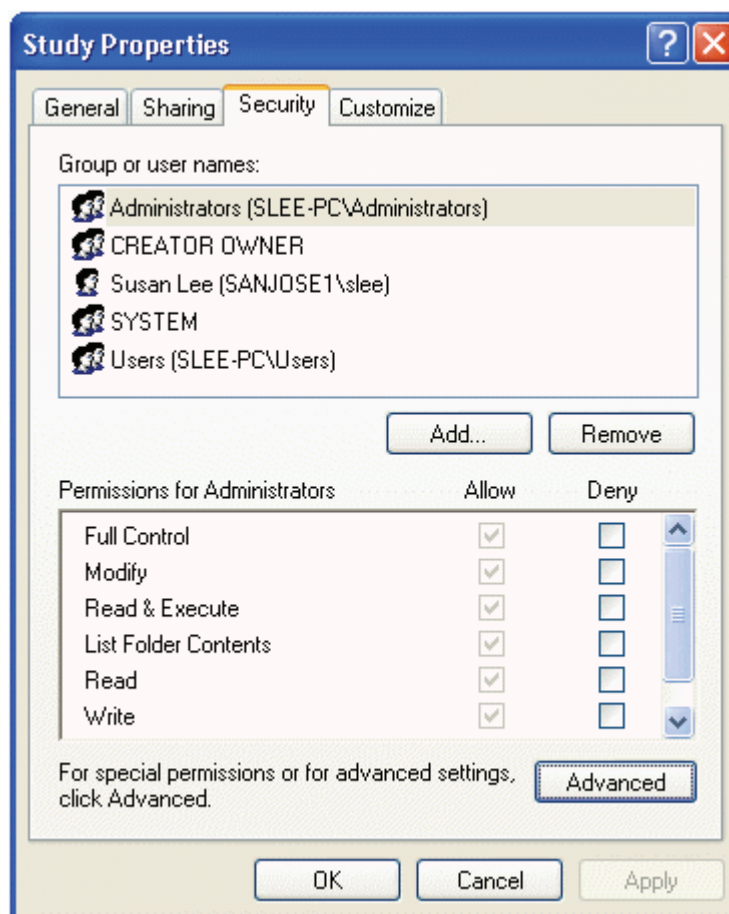
IMPORTANT When you create a new root folder, the permissions from the parent folder automatically propagate to the new folder, indicated by:

- Shaded check boxes in the Permissions list.

- In the Advanced Security Settings dialog box, the check box labeled "Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here." is selected.

IMPORTANT Normally, you do not want to allow your secure root folder to inherit permissions from the parent folder. You prevent this inheritance by clearing the Inherit from parent… check box in the next steps. You then correct the permissions in the topic "Setting Permissions" on page 32.

4. Click **Advanced** to open the Advanced Security Settings for Study dialog box.
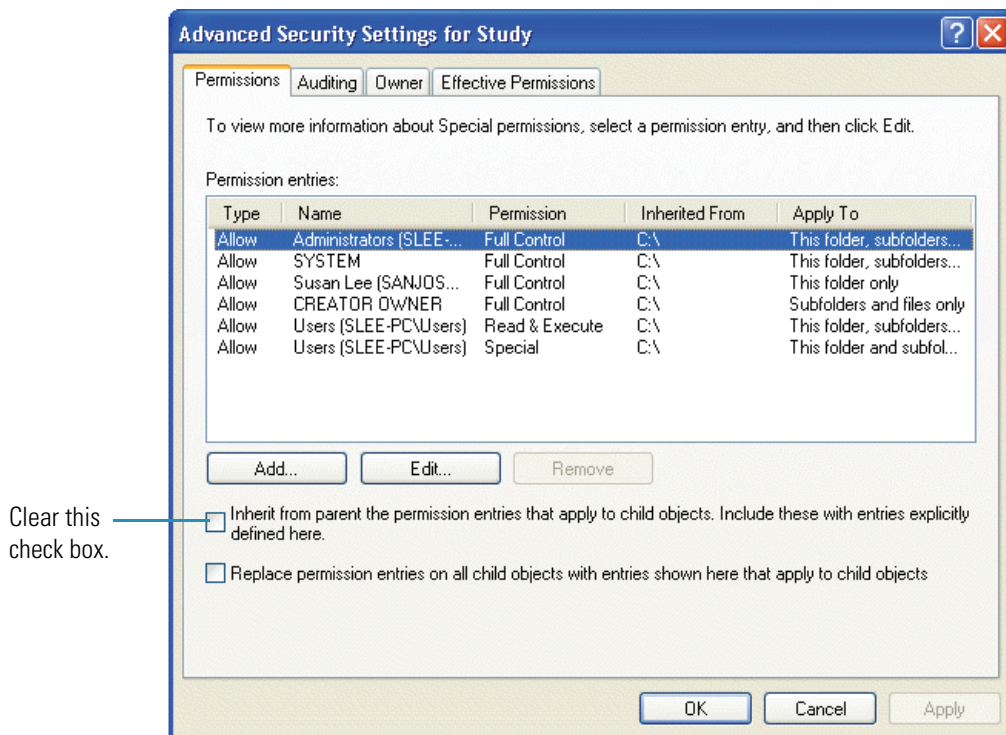
Clear this check box.

5. Clear the **Inherit from parent…** check box.

The Security dialog box opens.
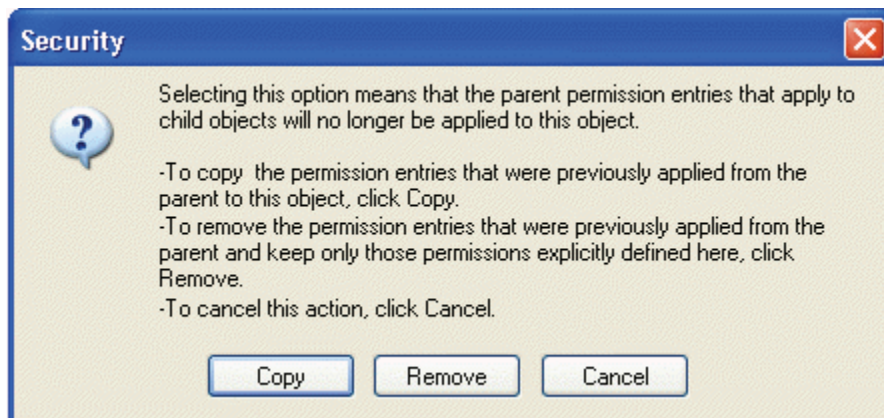
6. To copy the inherited permissions to the new folder, click **Copy**.

7. Click **OK** to close the Advanced Security Settings dialog box.

You will correct the permission settings later.

> **Note** After you clear the Inherit from parent… check box and copy the inherited permissions to the new folder, the new root folder no longer inherits permissions from the parent folder. If someone then changes the permission settings of the parent folder, the permission settings of the new root folder do not change. However, any subfolders created under the new root folder still inherit the permissions from the root folder.

8. In the Properties dialog box, examine the Group or user names list and notice which groups or users appear in the list.

   You want only the group **Everyone** and your administrator name (or the name of the administrator group) to appear in this list.

   - If either is missing from the list, go to the next topic "Adding Windows Users and Groups."

   - If both appear in the list, and additional groups or users also appear in the list, go to "Removing Unnecessary Users" on page 32.

   - If both appear in the list, and no additional groups or users appear in the list, go to "Setting Permissions" on page 32.

Adding Windows Users and Groups

In preparation for setting permission levels for the folder, you might need to add users and groups to the Group or user names box on the Security page.

> **IMPORTANT** Each Windows user account must be associated with a user ID, password, and full description. These items are required for the system to store the auditing information in the designated database.

❖ **To add users and groups**

1. On the Security page of the Properties dialog box, click **Add**.

   The Select Users, Computers, or Groups dialog box opens.

For example, users and administrator

Network name
(if domain users on network)
or
workstation name
(if local users on standalone workstation)
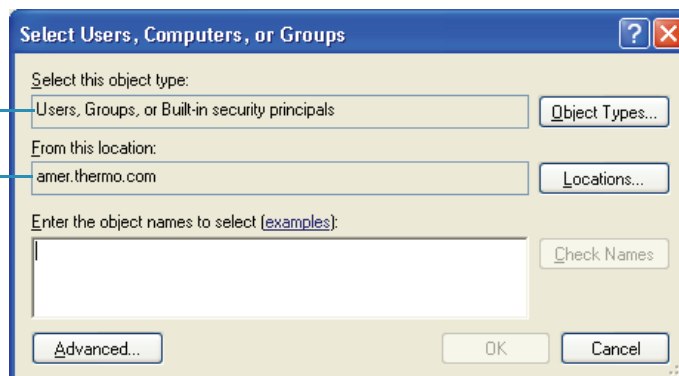
2. Ensure that the Select this object type box contains the object types that you require (Users, Groups, or Built-in security principals).

   To change the list of objects, click **Object Types**. In the Object Types dialog box, edit the list of objects and click **OK**.

3. Ensure that the From this location box lists the root location that contains your users and groups.

   To change the location, click **Locations**. In the Locations dialog box, specify a new location and click **OK**.

4. In the Enter the object names to select box, type the names of the users or groups that you want to add:

   • If the group Everyone is missing from the Group or user names list on the Security tab, type **Everyone.**

   • If your administrator name (or the name of the administrator group) is missing from the Group or user names list on the Security page, type the appropriate user name or group name.

   > **Tip** You can enter multiple object names at the same time by separating the names with a semicolon.

5. To search for the specified users or groups, click **Check Names**.

   All similar or matching object names that were found appear underlined in the Enter the object names to select box.
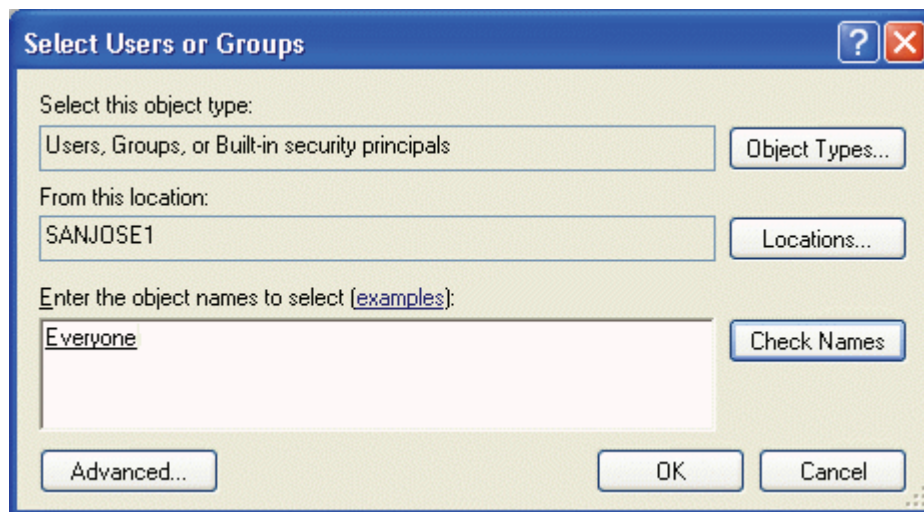
6. In the Enter the object names to select box, ensure that only the correct object name or names appear and click **OK**.

7. In the Study Properties dialog box, click the **Security** tab.

   Ensure that only the following entries appear in the Group or user names box:

   - Administrators (administrator name)

   - Everyone

   If no additional groups or users appear, go to Setting Permissions.

   If additional groups or users appear, you must remove them. Go to Removing Unnecessary Users.

Removing Unnecessary Users

You must remove unnecessary users or groups from the Group or user names box on the Security page.

❖ **To remove the names**

1. In the Group or user names box, select the name of the unnecessary user or group and click **Remove**.

2. Repeat this step to remove any other unnecessary users or groups.

Setting Permissions

After the correct users and groups are in the Group or user names box on the Security page of the Properties dialog box, set the permissions.

❖ **To set the permissions**

1. In the Group or user names box, select the administrator (or the administrator group).

2. In the Permissions for Administrators list, select the **Allow** check box for Full Control.

   All the other check boxes in the Allow column are automatically selected.

Ensure that only these two entries appear.

Administrator permissions
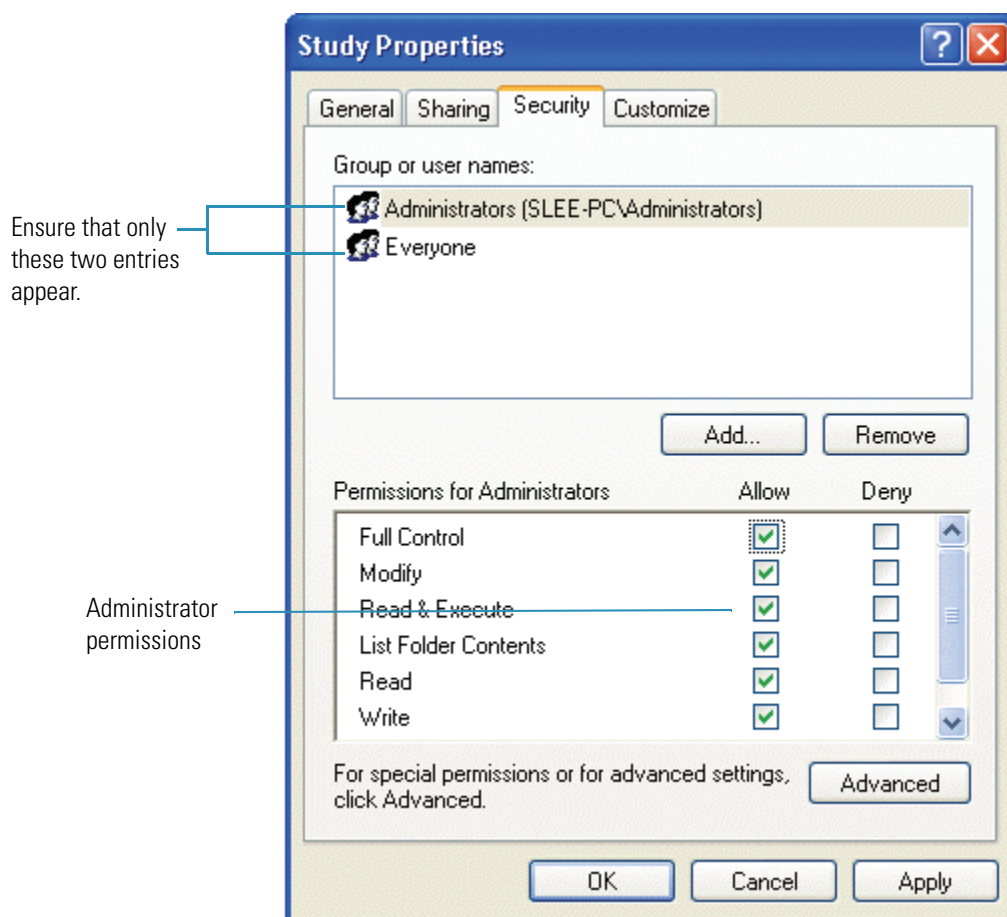
IMPORTANT Groups or users who are granted Full Control for a folder can delete files and subfolders within that folder, regardless of the permissions protecting the files and subfolders.

3. In the Group or user names box, select **Everyone**.

4. In the Permissions for Administrators list, select **Allow** for each of the following:

   • Read & Execute

   • List Folder Contents

   • Read

   • Write

5. Clear the **Allow** check box for all other actions in the list.

Note Setting these permissions ensures that none of the files in the folder can be deleted by using Windows Explorer.

6. Ensure that the inheritance setting is correct as follows:

   a. Click **Advanced**.

      The Advanced Security Settings dialog box opens.

   b. Ensure that the **Inherit from parent…** check box is cleared.

   c. Click **OK**.

7. In the Study Properties dialog box, click **OK**.

You have configured the security settings for the root folder. You are now ready to configure the security settings for the Security folder.

Configuring Settings for the Security Folder

The procedure for configuring the security folder is similar to that for configuring the root folder. For the security folder, you must grant full access rights only to the administrator and read-only access rights to everyone else.

For additional information about any step, see "Configuring Security Settings for the Root Folder" on page 26.

❖ **To configure the Security folder**

1. Use Windows Explorer to locate the Security folder.

   The folder path is as follows:

      C:\Documents and Settings\All Users\Application Data\Thermo Scientific\INI

2. Right-click the **Security** folder and choose **Properties** from the shortcut menu to open the Study Properties dialog box.

3. Click the **Security** tab.

4. Click **Advanced** to open the Advanced Security Settings dialog box for the Security folder.

5. Clear the **Inherit from parent…** check box.

6. When the Security dialog box opens, click **Copy**.

7. Click **OK** to close the Advanced Security Settings dialog box.

8. Ensure that the Group or user names box contains only your administrator name (or the administrator group) and the group **Everyone**.

   • If Administrator (or the Administrator group) does not appear in the list, add it.

   • If the group Everyone does not appear in the list, add it.

   • If any other users or groups appear in the list, remove them.

9. Set the permissions for the folder:

   a. In the Group or user names box, select **Administrator**.

   b. In the Permissions list, select the **Allow** check box for Full Control.

      All the other Allow check boxes are automatically selected.

   c. In the Group or user names box, select **Everyone**.

   d. In the Permissions list, select the **Allow** check box for Read and clear the **Allow** check box for all the other options.

   e. In the Advanced Security Settings dialog box, ensure that the **Inherit from parent…** check box is cleared.

   f. Click **OK** to close the Advanced Security Settings dialog box.

10. Click **OK** to save the permission assignments and close the Properties dialog box.

You have configured the security settings for the Security folder.

Configuring Security Settings for the Database Registry Key

When you run the Database Configuration tool for the first time, the tool creates a Windows XP registry key that stores information about the database. To ensure the security of the auditing database, set the security settings for this registry key so that only the workstation administrator can make changes to the key.

❖ **To configure the security settings for the database registry key**

1. From the Windows XP taskbar, choose **Start > Run** to open the Run dialog box.

2. In the Run dialog box, type **regedit** and click **OK**.

   The Registry Editor dialog box opens.
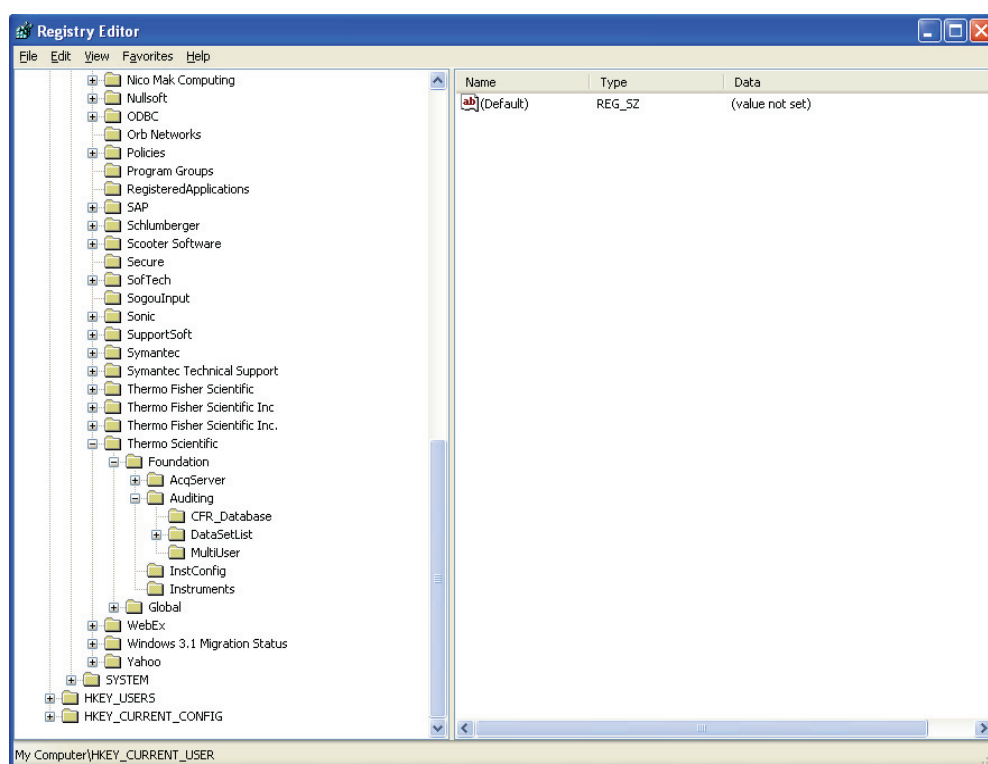
3. In the left pane of the Registry Editor dialog box, locate the folder:

   My Computer\HKEY_LOCAL_MACHINE\SOFTWARE
   \Thermo Scientific\Foundation\Auditing\CFR_Database

4. Right-click the **CFR_Database** folder and choose **Permissions** from the shortcut menu to open the Permissions dialog box for this registry key.

5. Click **Advanced**.

The Advanced Security Settings dialog box opens.
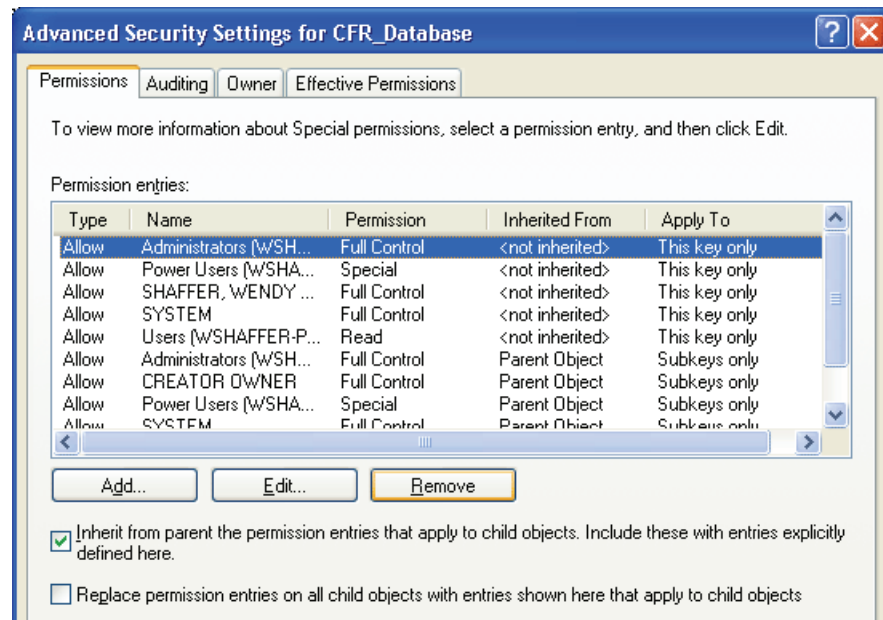
6. Clear the **Inherit from parent…** check box.

The Security dialog box opens.
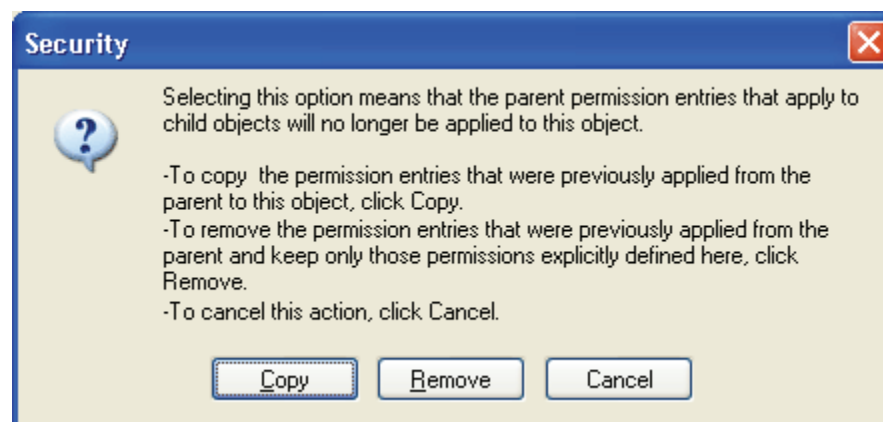
7. Click **Copy** to copy the inherited permissions to the CFR_Database registry key.

8. Click **OK** to close the Advanced Security Settings dialog box.

9. In the Study Properties dialog box, examine what groups or users appear in the Group or user names box. You want only your administrator name (or the administrator group) and the group **Everyone** to appear in this box.

   • If your administrator name (or the administrator group) does not appear in the box, add it. (See "Adding Windows Users and Groups" on page 30.)

   • If the group **Everyone** does not appear in the box, add it. (See "Adding Windows Users and Groups" on page 30.)

- If other users or groups appear in the box, remove them.
  (See "Removing Unnecessary Users" on page 32.)

10. Set the permissions for the registry key:

    a. In the Group or user names box, select your administrator name (or the
        administrator group).

    b. In the Permissions list, select the **Allow** check box for Full Control.

        The **Read** check box in the Allow column is automatically selected.
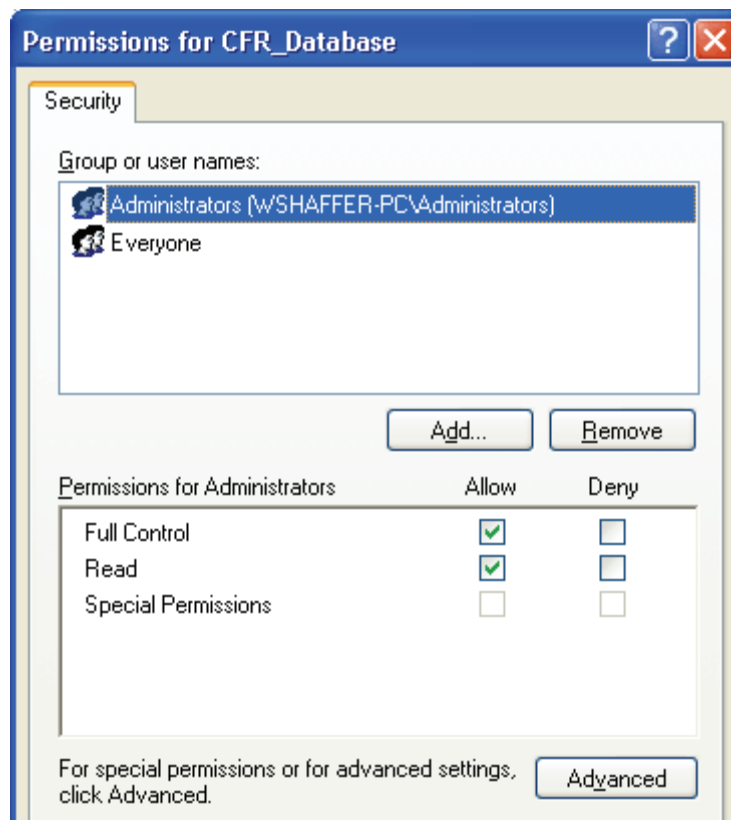
    c. In the Group or user names box, select **Everyone**.

    d. In the Permissions list, select the **Allow** check box for Read, and clear the **Allow**
        check box for all other actions in the list.

11. Click **OK**.

12. Choose **File > Exit** to close the Registry Editor.

Specifying the Way Users Log On and Off

This section describes the following:

- Turning Off Fast User Switching for Local Workstations

- Sequential User Logon and Automatic Logoff

- Removing and Archiving Files

Turning Off Fast User Switching for Local Workstations

Turning off fast user switching is important because if you as a system administrator do not turn off fast user switching, two users could log on at the same time, which can cause strange behavior when they try to control their mass spectrometer. The acquisition service can only handle one user logged in at a time. We recommend all labs turn off fast user switching, regardless of whether secure file operations is important to them or not.

Depending on the operating system, you can switch between users without actually logging off from the computer. You can turn off this feature, called Fast User Switching, so that the current user must log off before another user logs on.

To maintain secure file operations, turn off the Fast User Switching feature on all computers.

- Windows XP Professional: Fast User Switching is featured on computers that are not members of a network domain.

- Windows Vista: Fast User Switching is featured on all computers.

❖ **To turn off Fast User Switching**

1. From the Windows XP taskbar, choose **Start > Control Panel** to open the Control Panel.

2. Double-click **User Accounts**.

3. Under Pick A Task, click **Change The Way Users Log On And Off** to open the Select Logon And Logoff Options page.

4. Clear the **Use Welcome Screen** check box.

5. Clear the **Use Fast User Switching** check box.

6. Click **Apply Options**.

7. Close the User Accounts dialog box and close the Control Panel.

When a user logs off, the computer automatically shuts down any programs that are running.

Sequential User Logon and Automatic Logoff

> **IMPORTANT** To ensure compliance with 21 CFR Part 11, you must use sequential user logon and automatic logoff. If Sequential User Logon is NOT enabled, you must ensure that the Automatic Logoff feature is also NOT enabled. Failing to turn off Automatic Logoff when Sequential User Logon is off could result in incomplete data acquisitions.

With the Sequential User Logon feature, a user can log on to a workstation, start data acquisition, and log off while the system continues to acquire the data. A subsequent user can log on to the workstation and can queue acquisition sequences and process data while the acquisition the first user started continues.

Set up the sequential user logon feature through Xcalibur Instrument Configuration by selecting Enable Multi-user Login when you configure each device. You can select that option only if all the configured devices support sequential user logon.

❖ **To enable or disable automatic logoff**

1. Choose **Start > All Programs > Thermo Foundation 1.0 > AutoLogoff**.

   The Automatic Logoff Setup dialog box opens.

    By default, automatic logoff is disabled
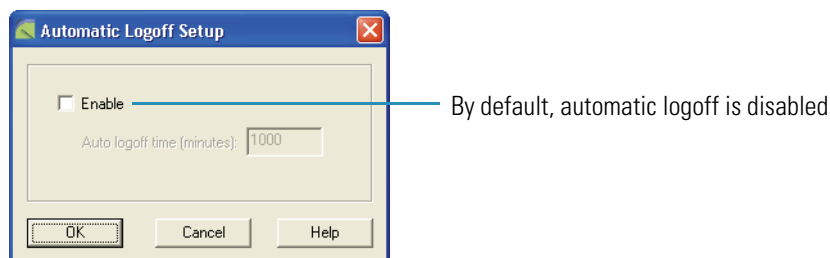
2. Do one of the following:

   - To turn on the feature, select the **Enable** check box and type a value (1–1000) in the Auto logoff time (minutes) box to specify how long the system waits before logging off the current user.

   - To turn off the feature, clear the **Enable** check box.

3. Click **OK**.

If the Windows XP screen saver is set to appear on the computer at an earlier time than the Auto Logoff time, the automatic logoff still occurs at the specified time, even though the user cannot see evidence of the logoff because the screen saver is active.

> **IMPORTANT** If your LCquan system is on a computer that has Windows Vista installed, provide the following instruction to users after you turn on AutoLogoff: "Each time you log on, Vista asks if you permit the system to run AutoLogoff in the background. Choose **Allow** each time." Add this instruction to your standard operating procedures. If this is not acceptable, run the LCquan application on a Windows XP system.

Removing and Archiving Files

To fully comply with 21 CFR Part 11, you must have proper procedures in place for long-term archiving and retrieving of electronic records—including raw data, processed data, and metadata. You must also have a procedure for ensuring that retrieved records can be read. Generally, this requires you to convert records to a new format or to keep and maintain the tools for reading the records in their current format.

To archive files, use third-party software designed for this purpose. In addition, to protect the archived data, develop and implement standard operating procedures for archiving files and security procedures to protect the archived data.

Defining Secure User Groups and Permissions

As the laboratory administrator, you control access to the Xcalibur data system and certain application features by using Thermo Foundation Authorization Manager to define secure user groups and grant these groups appropriate permission levels. Every member of a secure user group has the same permissions. Only those users in a designated secure user group can perform authorized actions. All others are prohibited access.

Follow these procedures to use the Foundation Authorization Manager to configure the secure groups and set permissions for controlled features in the Xcalibur data system.

Contents

- Using the Authorization Manager
- Setting Up Secure User Groups
- Setting Permissions
- Defining the List of Secure Folders
- Requiring User Comments
- Setting Up Secure Reports
- Viewing the Authorization Manager History Log
- Printing the Security Settings
- Saving the Security Settings

Using the Authorization Manager

With Thermo Foundation Authorization Manager and the security features of the Windows XP operating system, define user groups and set permission levels for these groups. The Authorization Manager ensures that only individuals who have some level of responsibility for the records can access them.

❖ **To start the Authorization Manager**

From the Windows XP taskbar, choose **Start > Programs > Thermo Foundation 1.0 > Authorization Manager**.

The Thermo Foundation Authorization Manager opens.

Figure 6.   Thermo Foundation Authorization Manager
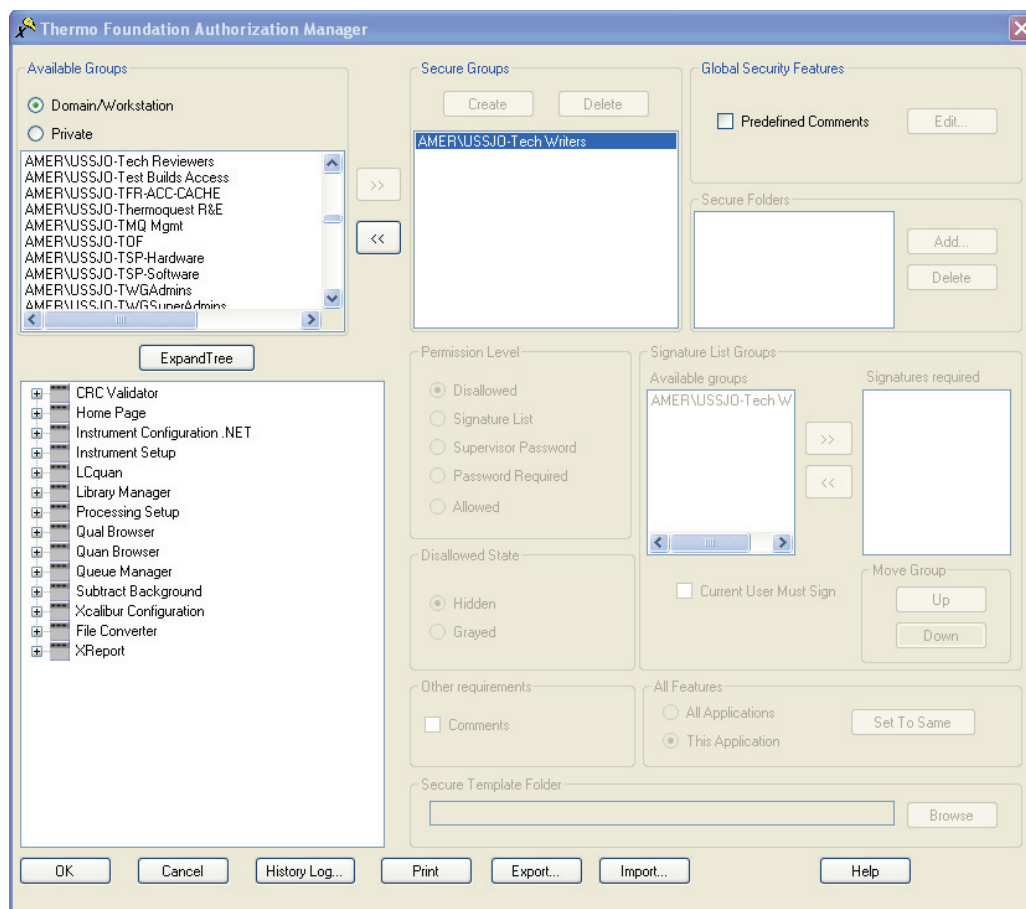
Setting Up Secure User Groups

To set up the secure user groups in Thermo Foundation Authorization Manager, you can use either preexisting Windows user groups or create your own private groups in the Authorization Manager.

The LCquan application places no limit on the number of user groups you can define. For simplicity, if all users are to have the same privileges, you can define a single user group.

> **IMPORTANT** You must define secure user groups; otherwise, the LCquan system is not secure. If no secure groups are defined, all users can access all features of the software.

A single user can belong to more than one user group. If the groups have different permission levels, the most lenient permission level applies to the user.

Defining User Groups

❖ **To define user groups**

1. In the Authorization Manager, select the appropriate Available Groups option to specify the type of user group:

   - To use preexisting Windows XP logon groups, select the **Domain/Workstation** option. Contact your domain administrator to create or change logon groups.

     Continue to step 2.

   - To use (or create) a local user group, select the **Private** option. The lab administrator can create private groups.

     Skip to step 3.

2. To define secure domain/workstation logon groups, select a group in the Available Groups list and click the right arrow.

   The group name appears in the Secure Groups box.
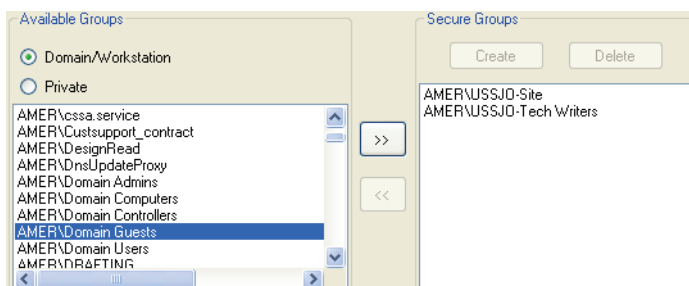
   Repeat this step to define more secure groups. When you are finished creating groups, go to "Editing User Groups" on page 47.

3. To define secure private groups, do the following:

   a. In the Secure Groups area, click **Create**.

      The Create private group dialog box opens.
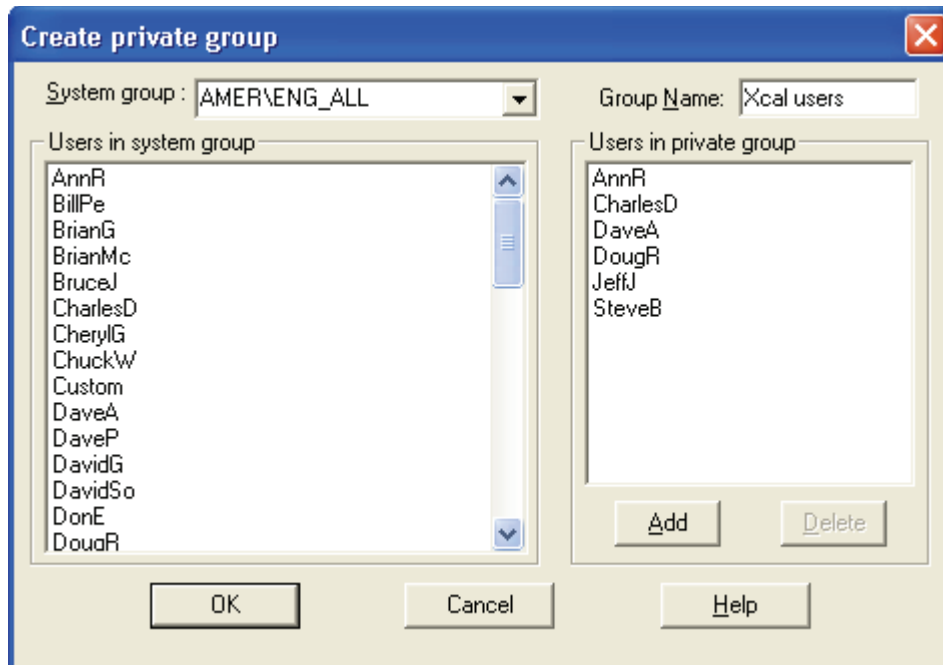
   b. In the Group Name box, type a name for the group.

   c. In the System group list, select a domain.

      The domain user accounts are displayed in the Users in system group list.

   d. In the Users in system group list, select a user account and click **Add**.

      The user account appears in the private group box.

   e. To add users in other domains to the private group, repeat steps c and d.

   f. Click **OK**.

      The new private group appears in the Secure Groups box.

   g. To create additional private groups, repeat steps a through f.

   Note Private groups are necessary only if the required groups are not available as
   Windows XP logon groups.

Editing User Groups

After you define a secure user group, you can view and (for private groups only) edit the members of the group.

❖ **To view and edit the members of a group**

In the Secure Groups box, right-click the user group and choose **Members** from the shortcut menu.

- If the group is a private group, the Edit user list of private group dialog box opens. To add or remove names from the user group, click **Add** or **Delete**.
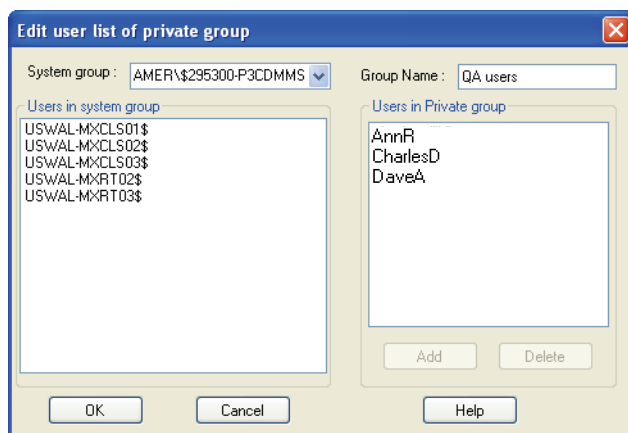
- If the group is a domain/workstation logon group, the Users in group dialog box opens. Because membership in these groups is controlled by the domain administrator, the lists are read-only. To make changes to domain/workstation logon groups, contact your domain administrator.
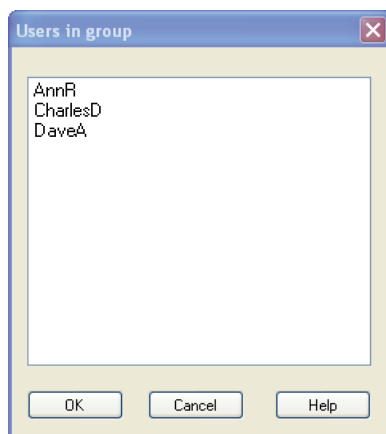
Setting Permissions

For each secure user group, you can set the permission levels for certain features in the software. You set permissions in the Permission Level section of the Thermo Foundation Authorization Manager.

The following table lists the available permission levels. All new secure user groups, whether domain/workstation groups or private groups, have all features set to **Disallow**.

Table 2. Permission levels

Permission Level	Description
Disallowed	Not permitted. You can specify whether the user interface control for the disallowed operation is hidden or grayed out.
Signature List	Enter the names and passwords of everyone on the required signature list to perform the authorized action.
	In the Signature List Groups area, you specify the groups whose signatures are required. A representative from each group on the required signature list must enter the user ID and password before the action is authorized.
	A user who belongs to more than one group on the required signature list can sign on behalf of each group by entering his or her user ID and password for each group.
Supervisor Password	Enter the supervisor name and password to perform the action. Anyone who has permission to perform the Allowed or Password Required actions can sign as a supervisor.
Password Required	The user must enter a password before continuing to perform the authorized action.
Allowed	No restrictions.

You can set permission levels by doing the following:

- Changing the Permission Level of a Feature

- Setting All Permissions

- Inheriting Permissions

- Exporting and Importing Permissions

Note For a list of the permission level settings required for your particular application to ensure compliance with 21 CFR Part 11, go to Appendix A, "Permission Level Settings in the LCquan Application."

Changing the Permission Level of a Feature

This section provides a general procedure for changing the permission level for most features.

❖ **To change the permission level of a feature**

1. In the Authorization Manager, select a user group from the Secure Groups box.

2. In the controlled features list to the lower left of the Authorization Manager, select the name of your software application.

3. To show the entire list of controlled features for the application, click **Expand Tree**.
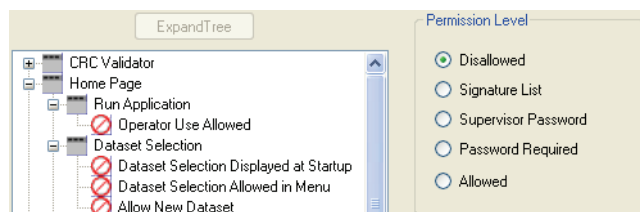
4. From the list, select a feature and select one of the following Permission Level options:

   • Disallowed

   • Signature List

   • Supervisor Password

   • Password Required

   • Allowed
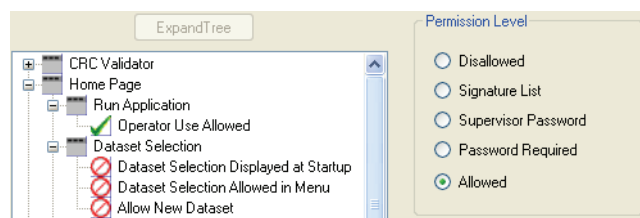
Note You can set permissions only for individual features, such as Allow New Dataset. You cannot set permissions for groups, such as Dataset Selection. When you select a feature, the Permission Level options for that feature are available.

Tip Right-click a feature to select the permission level from the shortcut menu.

5. If you selected Permission Level: Disallowed, select how the user interface appears for the disallowed state.

- To hide the unavailable control, select the **Hidden** option.

- To gray out the unavailable control, select the **Grayed** option.

6. If you set the permission level to Signature List, use the Signature List Groups–Available groups area to define the signature list groups:

a. In the Available groups box, select a user group and click the right arrow. The group appears in the Signatures required box.

b. To add other groups to the signatures required list, repeat step a.

c. To require that the current user of the application be placed on the signature list, select the **Current User Must Sign** check box.

d. To rearrange the order of the groups in the Signatures required box, select a group and click the Move Group buttons: **Up** or **Down**.

> **Note** When a user uses a feature with a permission level of Signature List, a series of password dialog boxes appears, one dialog box for each signature (name and password of a member of the designated group).
>
> The order of the groups in the Signature List Groups: Available Groups box defines the display order of the password dialog boxes.

7. If you want the users to enter a comment when they perform an action, select the **Comments** check box in the Other requirements area.

This option is available for all permission settings except **Disallowed**. When a user enters a comment, it appears in the audit log for the software.

8. Set the permission levels for any or all remaining features as follows:

   • To set the permission level of an individual feature, repeat steps 4 to 7.

   • To set the permission levels of the other features in the currently selected application to the same permission level you just set, select the **This Application** option and click **Set To Same**.
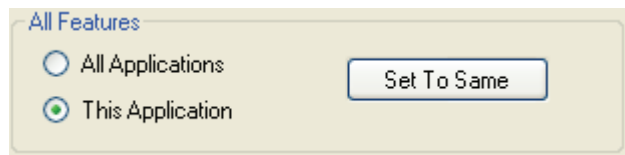
   • If you want to set the permission levels of all the features in all the applications to the same permission level you just set, select the **All Applications** option and click **Set To Same**.

     The Permission Level setting, the Disallow State setting (if applicable), and the Comments setting are copied to all the other features.

9. To set the permission levels for other user groups in the Secure Groups list, repeat steps 1 through 8.

> **Note** The Authorization Manager retains permission level settings if you move a user group out of the Secure Groups box and into the Available Groups box. If you move the group back into the Secure Groups box, the permission settings remain intact; however, if you delete a user group from the Secure Groups box, all permission settings are lost.

Setting All Permissions

You can set every feature to the same permission level in one of two ways.

❖ **To set features to the same permission level**

• After you set the permission level for one feature, click the **All Applications** option and click **Set To Same**.

–Or–

- Right-click the user group name in the Secure Groups box and choose **Globally set to >** *permission level* from the shortcut menu.
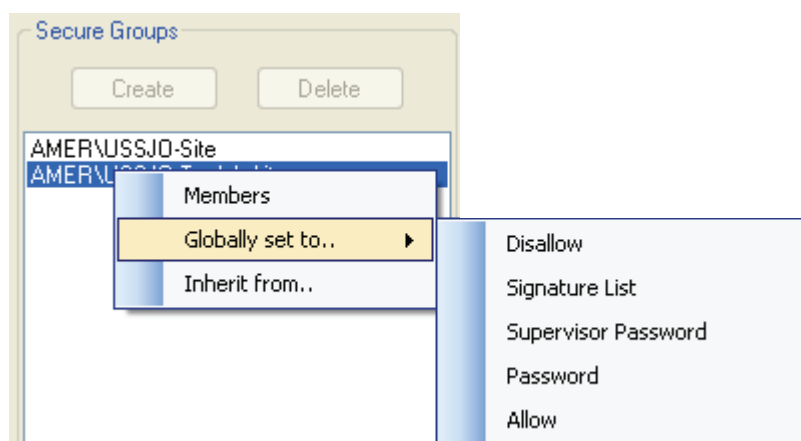
Inheriting Permissions

You can copy a complete set of permission levels from one secure user group to another secure user group.

❖ **To copy permission levels from one secure user group to another secure user group**

1. In the Secure Groups box, select the user group to receive the set of permission levels.

2. Right-click the selected group and choose **Inherit from** from the shortcut menu.
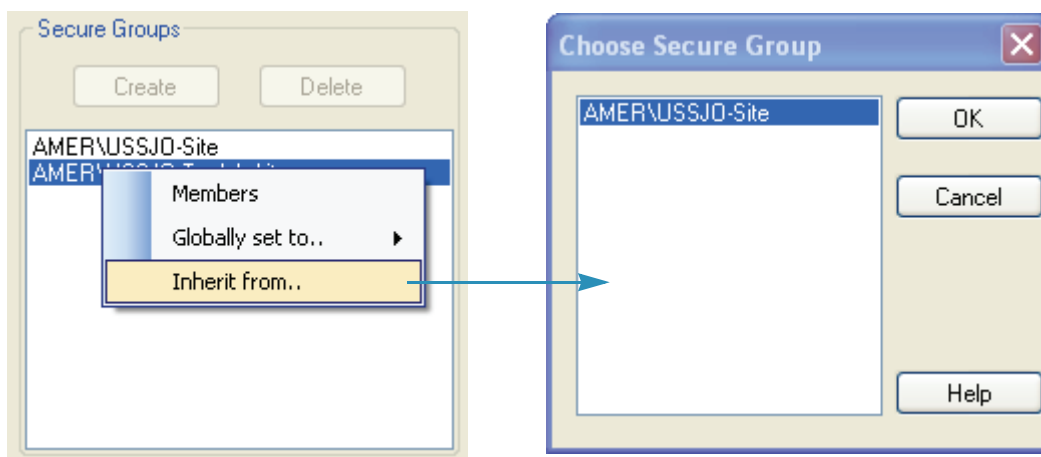
The Choose Secure Group dialog box opens and displays a list of the secure groups (minus the currently selected group).

3. Select the group whose permission levels you want to copy and click **OK**.

Both user groups now have the same set of permission levels.

Exporting and Importing Permissions

You can import the permission list that contains the user groups and permissions from another computer. Doing this saves time if you have more than one computer in your lab and you want to allow users access to all computers. Instead of setting up identical user groups on each computer, you can import the permission list from a computer that has the user groups and access permissions that you require.

> **Note** To maintain the security of the permission list, you must export it to a secure location. The Security folder (with proper security settings) on the current computer is an ideal location.

❖ **To export and import the permission list**

1. On the system where the correct users and permission levels are set, start the Thermo Foundation Authorization Manager.

2. In the Foundation Authorization Manager, click **Export**.

   The Save As dialog box opens.

3. Save the permission list in the Security folder as a file with the file extension **.eperm**.

   (The path for the security folder is \Xcalibur\system\security. The default file name is permissions.eperm.)

4. Copy the file into the Security folder on the new system.

5. On the new system, start Thermo Foundation Authorization Manager and click **Import.**

   The Open dialog box opens.

6. Select the permission list file (*filename*.**eperm**) and click **Open**.

   The user groups and permission levels appear in the Foundation Authorization Manager.

7. Confirm that the user groups and permissions are correct and click **OK** to save the settings and close Thermo Foundation Authorization Manager.

Defining the List of Secure Folders

To comply with the requirements of 21 CFR part 11, all electronic records must be in protected folders. To ensure the LCquan root folder is protected, do not permit users to change the root folder to an unprotected folder.

> **IMPORTANT** If you have not configured the security settings to protect your root folders, do so before setting the root folder feature permissions. See Chapter 3, "Establishing Secure File Operations."

The Foundation Authorization Manager list of controlled features includes the following two features for each application:

- Allow Arbitrary Selection of Root Folder—Allows users to change the root folder to any folder that they choose. You must ensure that the Allow Arbitrary Selection of Root Folder feature is set to Disallowed.

- Allow Change of Root Folder—Allows users to change the root folder to another secure folder. You can set the Allow Change of Root Folder feature to any permission level. If you set the permission level to anything other than Disallowed, you must define a list of secure folders from which the user can select a new root folder.

Tip To display these two features in the Foundation Authorization Manager, double-click **LCquan** in the controlled features list and double-click **Root Folder**.

❖ **To define the list of secure folders**

1. In the Secure Folders box, click **Add**.

   The Browse For Folder dialog box opens.

Note You should define secure folders by using fully qualified path names. Use of mapped drive paths might result in network disconnection upon auto-logoff.
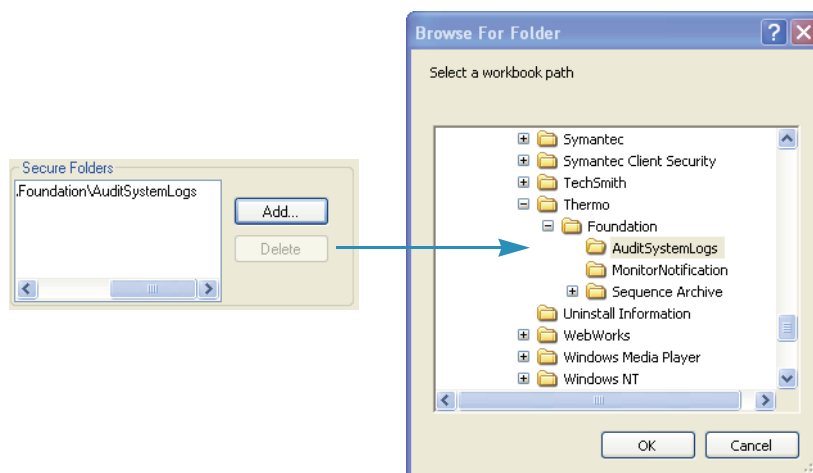
2. Select the secure folder that you want to add to the Secure Folders box and click **OK** to close the dialog box.

   The folder appears in the list in the Secure Folders box.

3. Repeat steps 1 and 2 for each folder that you want to add to the Secure Folders box.

After the permission levels and the Secure Folders box have been correctly set up, a user cannot change the root folder to a folder that is not secure. The user must select the new folder from the Secure Folders box from within the application. The secure folders information is saved as part of the configuration in a protected folder. For more information, see "Saving the Security Settings" on page 59.

Requiring User Comments

For details about how to require users to enter comments when they perform a controlled action, see "Changing the Permission Level of a Feature" on page 49. When a user enters a comment, it appears in the audit log for the application. (This option is available for all permission settings except Disallowed.)

❖ **To restrict users comments to a predetermined list of comments**

1. Select the **Predefined Comments** check box in the Global Security Features area and click **Edit**.

   The Comment List dialog box opens.
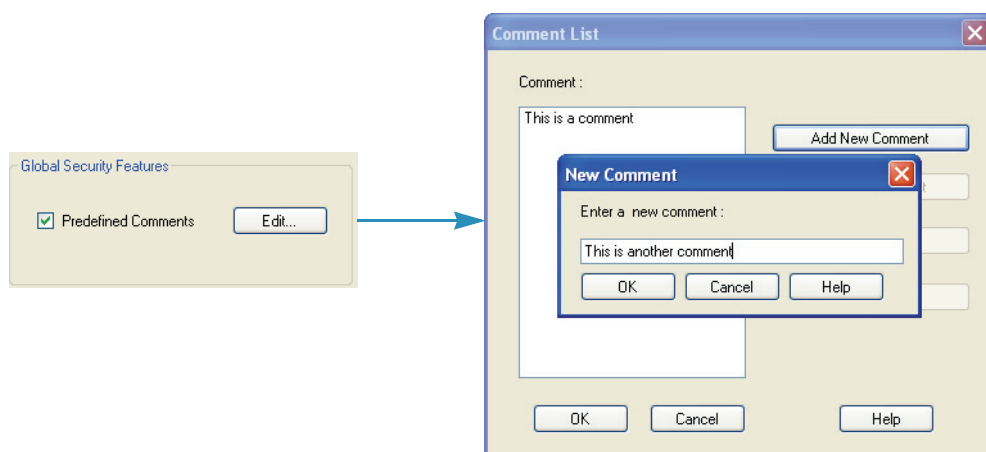
2. Click **Add New Comment**.

   The New Comment dialog box opens.

3. Enter the comment and click **OK**.

   The new comment appears in the Comment box.

4. Repeat steps 2 and 3 for each new comment that you want to enter.

   The Comment box displays the predefined comments in the order that you entered them in. You can rearrange the order of the comments by clicking Move Up or Move Down, or delete a comment by selecting it and clicking Remove Comment.

5. When you are finished, click **OK**.

Setting Up Secure Reports

You can limit a user group's authorization for creating LCquan quantitation reports to the secure XReport templates that you specify. After you configure the secure XReport templates feature, the user groups with this permission level can use only the templates from the specified secure templates folder. Users are limited to saving only, and the file format is limited to PDF files. In the LCquan Review Reports view, the options to print reports and create new XReport templates are not available.

About the Secure Reports

Users create secure reports when they use the secure XReport templates in the secure templates folder. The secure reports have the following characteristics:

- The only option available for creating a secure report is to save the report as a PDF file. The PDF document properties allow for printing only.

   The application changes any other preexisting report formats in the given workbook to PDF and tracks the changes in the audit trail.

- A watermark design appears on the background of each page of a secure report.

- A unique serial number appends to the footer of each page:

   workbookName_timestamp_n

   where n is a counter for the number of reports printed from a workbook.

The serial number increments for each report generated from a given LCquan workbook. If user groups with different security privileges create reports from the same workbook, both the secure and non-secure reports are included in the total count of reports when assigning the serial number.

Setting Up a Secure Template Folder

Secure XReport templates are available in the designated secure templates folder. You can specify only one secure templates folder. Templates that are not in the secure templates folder are not available to the user, even if the templates were previously available in another workbook.

Use the following guidelines when setting up a secure templates folder:

- To prevent users from adding any unapproved templates to the folder, assign read-only access to the folder.

- For a locked workbook, make sure to designate the folder that already contains the templates for the locked workbook.

- Ensure the secure template folder contains only the approved XReport template files (.xrt).

Configuring Secure Reports

❖ **To configure secure reports**

1. In the Foundation Authorization Manager, select a user group from the Secure Groups area.

2. In the list of controlled features (lower left side), select **LCquan** and click **Expand Tree**.

3. In the Quantitative Section, select **Secure XReport Template**.

   Figure 7. LCquan controlled features
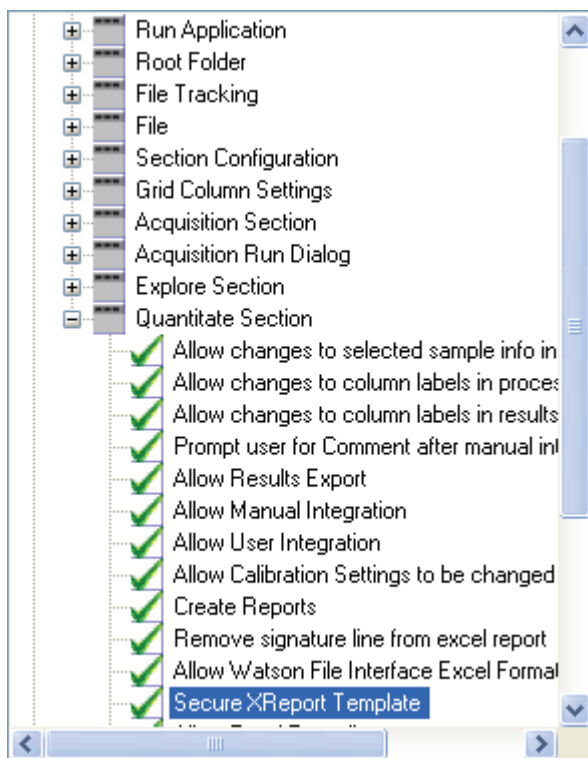
4. In the Permission Level area, select **Allowed**.

   For the Secure XReport Template feature, Allowed is the most restrictive setting.

5. In the Secure Template Folder area, click **Browse**.
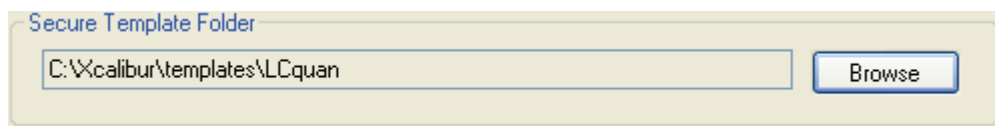
6. In the Browse for Folder dialog box, select the folder that contains the secure templates and click **OK**.

Viewing the Authorization Manager History Log

Thermo Foundation Authorization Manager automatically maintains a history log to record all changes made to the security settings. The log records the following events:

- The creation of a private group

- The addition or deletion of members from a group

- A change in group permissions

- A switch between private and domain/workstation groups

- The manipulation of the signature list

❖ **To display the history log**

In Thermo Foundation Authorization Manager, click **History Log**.

The audit view window opens, showing the history log for the Authorization Manager.
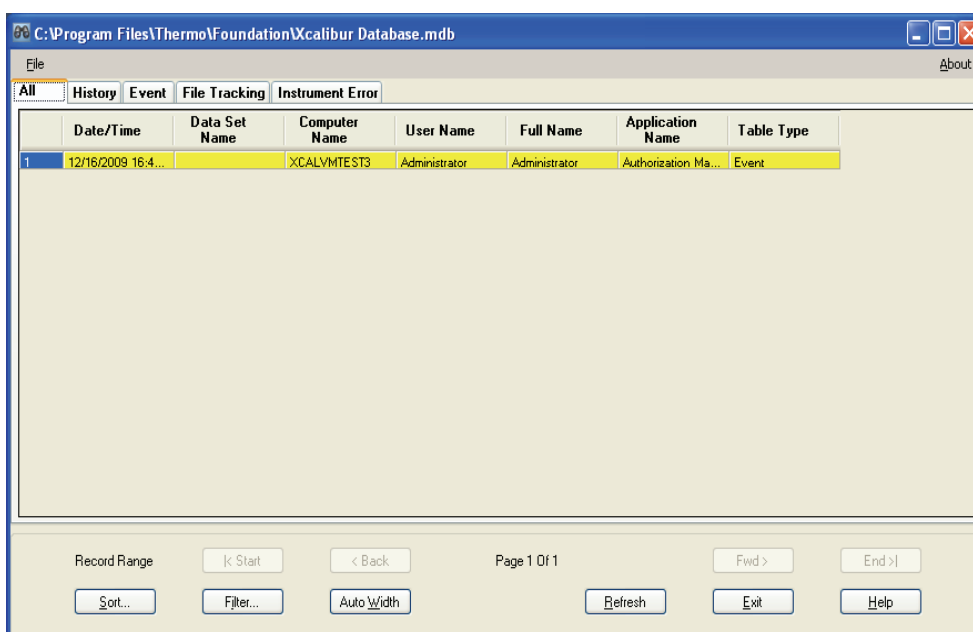
Each entry in the history log contains the time and date, and the user ID and full name. You can sort and filter the entries in the history log by field (for example, you can sort and filter by date and time). You can also print the log.

Printing the Security Settings

You can print a report of the security settings for each secure user group. The report contains a listing of the members of the group, the controlled features information for each application, and the names of any secure folders for each application.

❖ **To print the security settings**

1. In Thermo Foundation Authorization Manager, click **Print**.

    The Print dialog box opens.

2. Select the print options, and click **OK**.

Figure 8. Sample Security Settings printout

```
Xcalibur Security Settings for secure group : AMER\USSJO-Site
Thursday, June 05, 2008 12:48:05 PM
User dana.powers
Computer USSJO-LGUZZE-PC
Xcalibur Version 3.0


Members
-----------------------------------------------------------------------------------------------
nick.chavez
don.mcmichael

Application                  Secure Folders
-----------------------------------------------------------------------------------------------
CRC Validator                [none]
Home Page                    [none]
Instrument Configuration .NET [none]
Instrument Setup             [none]
LCquan                       C:\Program Files\Thermo\Foundation\AuditSystemLogs
Library Manager              [none]
Processing Setup             [none]
Qual Browser                 [none]
Quan Browser                 [none]
Queue Manager                [none]
Subtract Background          [none]
Xcalibur Configuration       [none]
File Converter               [none]
XReport                      [none]

Application              Feature                              Permission  Comment  Disallowed  Signature
                                                              Required?   State    List
-----------------------------------------------------------------------------------------------
CRC Validator   Run Application|Operator Use Allowed          DisAllowed  n/a      Hidden      n/a
Home Page       Run Application|Operator Use Allowed          DisAllowed  n/a      Hidden      n/a
Home Page       Dataset Selection|Dataset Selection Displayed.. DisAllowed n/a     Hidden      n/a
Home Page       Dataset Selection|Dataset Selection Allowed i.. DisAllowed n/a     Hidden      n/a
Home Page       Dataset Selection|Allow New Dataset          DisAllowed  n/a      Hidden      n/a
Home Page       Analysis|Start Analysis                      DisAllowed  n/a      Hidden      n/a
Home Page       Analysis|Stop  Analysis                      DisAllowed  n/a      Hidden      n/a
Home Page       Analysis|Pause Analysis                      DisAllowed  n/a      Hidden      n/a
Home Page       Devices|Devices On                           DisAllowed  n/a      Hidden      n/a
Home Page       Devices|Devices StandBy                      DisAllowed  n/a      Hidden      n/a
```

Saving the Security Settings

After you have defined your user groups, set the appropriate permission levels, and specified the type of application auditing, click **OK** to save your settings and exit the Authorization Manager.

The controlled features information is saved in a configuration file in the following folder:

\Xcalibur\system\security

You must properly set the security for this folder to prohibit access by nonadministrators. If you have not already done this, go to Chapter 3, "Establishing Secure File Operations."

Auditing

This chapter describes how to use the Audit Viewer utility for auditing functions. You can display all auditable events and changes made to files created or managed by the LCquan application, view a history of what has been done during data acquisition and data processing to produce results, and get information about all events that have occurred within the application.

Contents

- Accessing the Auditing Databases
- Viewing the Audit Viewer Pages
- Filtering the Audit Viewer Entries
- Sorting the Audit Viewer Entries
- Printing the Audit Viewer Entries

Accessing the Auditing Databases

The LCquan application writes to the Global Auditing database and maintains the LCquan workbook databases to ensure compliance with 21 CFR Part 11. The Global Auditing database stores LCquan start and stop events. All other LCquan events are stored in the LCquan workbook databases.

> **IMPORTANT** Before you can access the Global Auditing database, you must configure the database in the Auditing Database Configuration Manager. For instructions, see "Using the Database Configuration Manager" on page 15.

> **IMPORTANT** Each Windows user account must be associated with a user ID, password, and full description. The system requires these items to store the auditing information in the designated database.

You can access either of the following types of databases using Audit Viewer:

- The Global Auditing database, which keeps a log of auditable events for all the Xcalibur-related data files and applications it recognizes. The Xcalibur-related data files include the raw files that you acquire in the LCquan application.

- The LCquan workbook database, which keeps a log of auditable events associated with the current workbook, including the entries that have not been saved to the database. Each workbook database also includes a log about the raw files that are acquired as part of the workbook.
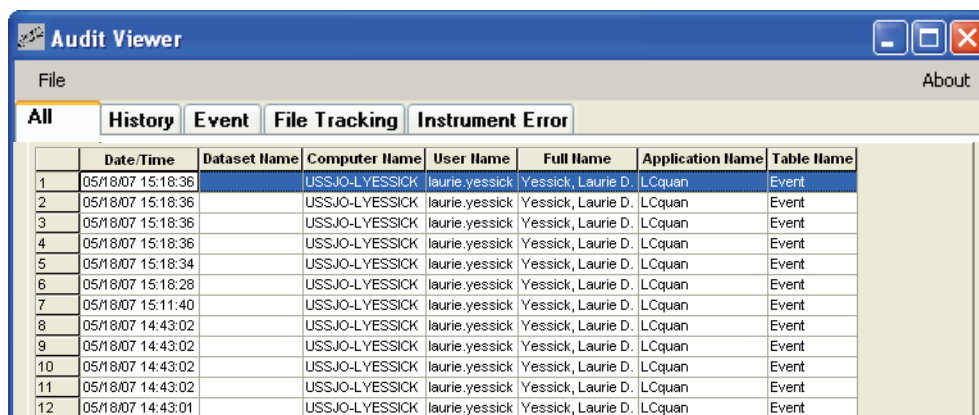
Accessing the Global Auditing Database

You can access the Global Auditing database when you start Audit Viewer from the Windows desktop.

❖ **To start Audit Viewer from your Windows taskbar**

Choose **Start > Programs > Thermo Foundation 1.0 > Audit Viewer**.

The Audit Viewer opens.

Accessing an LCquan Workbook Database

Each LCquan workbook has its own database. When you start Audit Viewer from an LCquan workbook, Audit Viewer displays the saved and unsaved entries for the current workbook. The unsaved entries are highlighted in yellow in the Audit Viewer window.

Note The Audit Viewer entries can also include unsaved changes from another workbook if the changes are still in memory.

❖ **To access the auditing database for a workbook**

1. Open the LCquan workbook.

2. From the LCquan interface, choose **File > Audit Trail**.

   The Audit Viewer opens and displays the entries for the open workbook. Unsaved entries are highlighted in yellow.

To access the auditing database for a different workbook, repeat steps 1 and 2. A second instance of Audit Viewer starts and displays the entries for that workbook.

Viewing the Audit Viewer Pages

The Audit Viewer window contains the following tabs, each with a different function:

- The All tab provides a summary of all entries for the current database.

  To display the Audit Viewer page associated with an entry on the All page, double-click the entry on the All page.

- The History tab provides a chronological listing of all the changes made to method files and result lists.

- The Event tab lists all user-initiated auditable events. All events that are subject to authorization control are auditable.

- The File Tracking tab provides the following type of information:

  – Global Auditing database: Lists the changes that are made by any program to the Xcalibur-created files.

  – LCquan workbook database: Lists the changes made within the application to any LCquan-owned files in the workbook, including the workbook file (.lqn), processing method (.pmd), instrument method (.meth), sequence (.sld), and any imported sample data files (.raw). The File Tracking page does not include the data files (.raw) acquired from within the LCquan workbook, which are tracked in the Global Auditing database.

    If any of the workbook files are modified outside the system, the LCquan application displays a file-tracking error message.

    Note The LCquan application does not save entries to the database until you **s**ave the workbook. The Audit Viewer headlights the unsaved entries in yellow.

- The Instrument Error tab lists significant events that occur to instruments that the Xcalibur data system creates or manages.

Filtering the Audit Viewer Entries

By applying a filter, you can display a subset of the entries in the Audit Viewer window. You can set up two types of filters: filters that are based on dates and filters that are not based on dates (non-date filters). You can use a combination of the two types of filters.

❖ **To set up a non-date filter**

1. In the Audit Viewer window, click **Filter**.

   The Filter Entries dialog box opens.
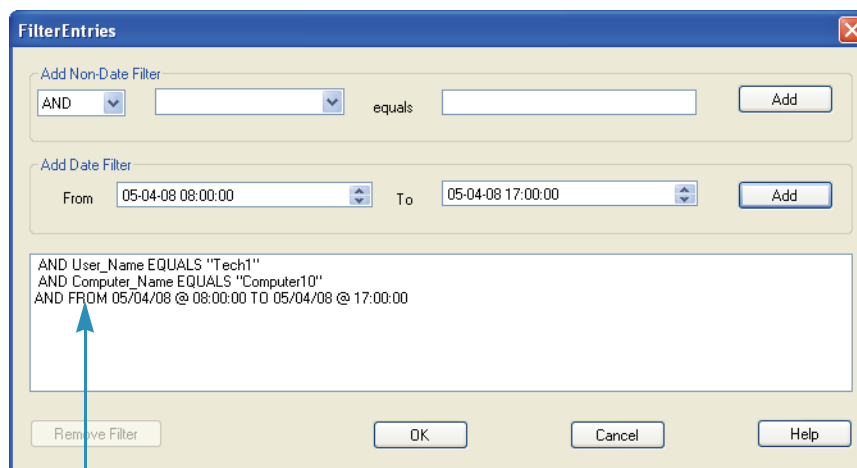
Searches for records created by Tech1 on Computer10
between 8:00 A.M. and 5:00 P.M. on May 4, 2008.

2. In the Add Non-Date Filter area, select **AND** or **OR** from the first list.

   • AND filters for entries that match ALL the specified criteria.

   • OR filters for entries that match ANY of the criteria.

3. Specify a filter in the form of ***Column Name*** equals ***string***.

   a. From the dropdown list, select a column to filter on.

   b. In the adjacent box, type the text string to match.

   c. Click **Add**.

   The filter criteria appear in the space below.

4. To add additional filters, repeat steps 2 and 3.

   If you select an OR filter, records must match only one of the filters. If you selected an AND match, records must match ALL the specified filters.

> **Note** The non-date filter accepts partial matches. For example, if you have a user name of `john.doe`, then a filter string of `john` or `doe` will match entries for that user name.

❖ **To set up a date filter**

1. In the Add Date Filter area, select or type the beginning date and time in the From box.

2. Enter the ending date and time in the To box.

3. Click **Add**.

❖ **To remove a filter**

1. In the Filter Entries dialog box, select the filter statement.

2. Click **Remove Filter**.

❖ **To search for filter criteria**

When you have defined all your filters, click **OK**.

The Audit Viewer window displays the results on the All page.

Sorting the Audit Viewer Entries

You can sort entries by the column headings on each of the Audit Viewer pages.

❖ **To sort entries on an Audit Viewer page**

1. In the Audit Viewer window, click the tab of the page you want to view.

2. Click **Sort**.

The Sort Entries dialog box opens.
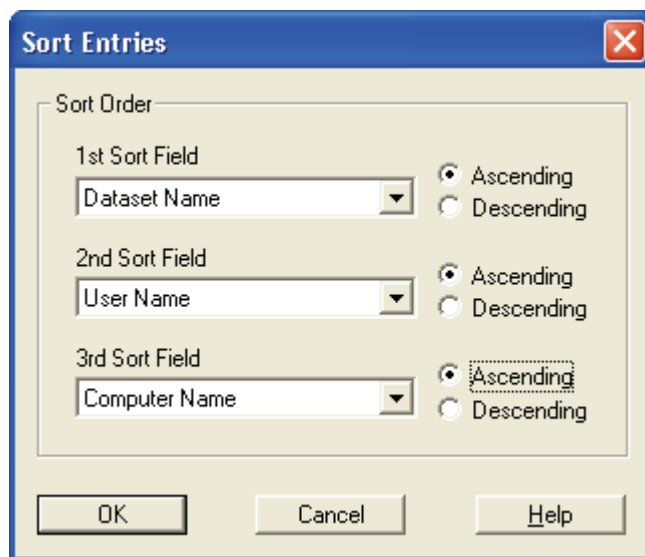
3. In the 1st Sort Field list, select a column heading and select the **Ascending** or **Descending** option.

   Repeat this step for the 2nd Sort Field and 3rd Sort Field.

4. Click **OK**.

   The Audit Viewer page displays the entries in the specified sort order.

Printing the Audit Viewer Entries

The printing options vary depending on whether you are printing the audit trail for the Global Auditing Database or a workbook database. For a workbook database, you must save all displayed records on the Audit Viewer page before you can print the entries.

❖ **To print the audit trail for the Global Auditing database**

1. From the Windows desktop, choose **Start > Programs > Thermo Foundation 1.0 > Audit Viewer**.

2. In the Audit Viewer, click the tab of the page you want to print.

3. Click **Print**.

4. In the Print Options dialog box, select your printing options and click **OK**.

❖ **To print the audit trail for an LCquan workbook database**

1. In the LCquan window, choose **File > Audit Trail**.

   If you already saved workbook entries, go to step 3.

   If the workbook contains unsaved entries, a View Audit Trail message appears prompting you to save the workbook before continuing.

2. In the View Audit Trail dialog box, do one of the following:

   • To save the workbook entries, click **Yes**.

      The Xcalibur data system logs the automatic save in the audit trail and starts Audit Viewer.

   • To start Audit Viewer without saving the workbook, click **No**.

   Note If you select the Don't tell me about this again check box, the application automatically applies the last requested behavior (Save or Not Save) each time you start Audit Viewer when the workbook contains unsaved entries. To restore the message, choose **Options > Enable Warnings**.

3. In the Audit Viewer, click the tab of the page that you want to print.

4. Make sure the displayed page contains only saved entries. The rows of unsaved entries are highlighted in yellow.

   If you have a mix of saved and unsaved entries, you can do one of the following:

   • In the LCquan Workbook window, choose **File > Save** to save the LCquan workbook. In the Audit Viewer window, click **Refresh**.

   • In the Audit Viewer window, click **Filter**, and then add filter rules so that only the saved records appear on the page you want to print. For details about adding filter rules, see "Filtering the Audit Viewer Entries" on page 65.

5. Click **Print**.

6. In the Print Options dialog box, select printing options and click **OK**.

Permission Level Settings in the LCquan Application

This appendix discusses the different LCquan permission levels and how they interact, including which features must be set to **disallow** to comply with 21 CFR Part 11.

Contents

- Permission Level Settings that You Must Set to Disallow

- Permission Level Settings and Interactions

Permission Level Settings that You Must Set to Disallow

To ensure compliance with 21 CFR Part 11, set the permission level for each of the following LCquan features to **Disallowed**:

- Allow Arbitrary selection of Root Folder

    You can find this feature in the Foundation Authorization Manager console tree. Look for Root Folder under the LCquan folder.
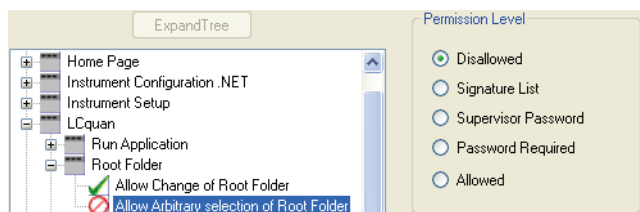
- Allow Opening of Workbooks with filetracking errors

    You can find this feature in the Foundation Authorization Manager console tree. Look for File Tracking under the LCquan folder.
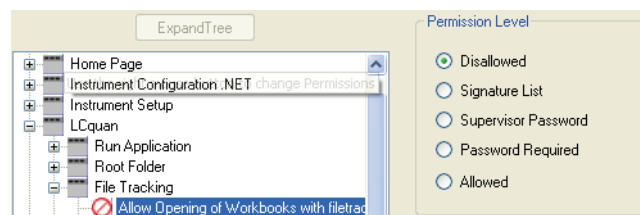
Set the permission levels for the other features to best suit your needs. For a list of the controlled LCquan features, see "Permission Level Settings" on page 71.

Permission Level Settings and Interactions

Certain permission level settings override other settings. In addition, some features are unavailable—regardless of their permission level settings—if a workbook is locked or has been opened in review mode.

The Permission Level Settings table lists the LCquan features that you can configure in the Foundation Authorization Manager.

Figure 9. Permission Level Settings (Sheet 1 of 5)

LCquan feature	Description
Run Application	
Operator Use Allowed	If you set this feature to Disallowed, the user cannot open the application. As a result, the permission level settings for the other features are irrelevant.
	If a user whose permission is set to Disallowed tries to access the system, the LCquan application makes an entry in the Global Auditing Database history log.
Root Folder	
Allow Change of Root Folder	If you enable this feature (set it to Signature List, Supervisor Password, Password Required, or Allowed), define a list of secure folders where the user can select a new root folder.
Allow Arbitrary Selection of Root Folder	Set this permission to Disallowed to ensure compliance with 21 CFR Part 11.
File Tracking	
Allow Opening of Workbooks with Filetracking Errors	Set this permission to Disallow to ensure compliance with 21 CFR Part 11.
Allow Opening of Workbooks Already Marked as Opened	If you set this permission to Allowed, the user can open workbooks that the application flags as opened.
	When a user opens an LCquan workbook, the application flags the workbook as opened to prevent the workbook from being opened by multiple instances of the application. If the application is forced to close abnormally, the flag might not be removed even though the workbook is no longer open. To open the workbook, set this permission to Allow. The next time the workbook is closed, the open flag is removed.

Figure 9. Permission Level Settings (Sheet 2 of 5)

LCquan feature	Description
File	
Save	If you set this permission to Disallowed, the user can lock the workbook only if it has not been changed. If it has been changed, the user cannot lock the workbook.
Save As	If you set this permission to Disallowed, the user cannot use the Save As command.
Create New Workbook	(No special information or interactions.)
Create Locked Version of Workbook	If you set this permission to Disallowed, the user does not have the option to lock a workbook.
Section Configuration	
Show Instrument Setup Section	If you set this permission to Disallowed, the user cannot display the Instrument Setup Section nor can the user make changes to the Instrument Methods.
Show Acquisition Section	If you set this permission to Disallowed, the user cannot create or modify an acquisition sequence nor can the user acquire data.
Show Explore Section	If you set this permission to Disallowed, the user cannot explore new quantitation methods.
Show Quantitate Section	If you set this permission to Disallowed, the user cannot: • Create or change a processing method. • Create or modify processing sequences. • Survey and review all the results. • Create reports from this section and process the data to produce quantitative results.
Grid Column Settings	
Allow Changes to Column setup info	If you set this permission to Disallowed, the user cannot change the number and arrangements of columns in the Results table.
Acquisition Section	
Start Acquisition Dialog	If you set this permission to Disallowed, the user cannot open the Run Sequence dialog box from the Acquisition view.

Figure 9. Permission Level Settings (Sheet 3 of 5)

LCquan feature	Description
Allow Changes to Selected Sample Info in Acquisition Sequence	If you set this permission to Disallowed, the user cannot make changes to the sample information, such as Sample Name, Comment, Study, Client, Laboratory, and so on, in the acquisition sequence.
Allow Changes to Column Labels in Acquisition Sequence	If you set this permission to Disallowed, the user cannot make changes to the column labels in the acquisition sequence.
Acquisition Run Dialog	
OK Button	If you set this permission to Disallowed, the user can view the Run Sequence dialog box but cannot start a data acquisition because the OK button is unavailable in the Run Sequence dialog box.
Explore Section	
Allow Import of Peak Lists	If you set this permission to Disallowed, the user cannot import a Peak Name List.
Allow Export of Peak Lists	If you set this permission to Disallowed, the user cannot export a Peak Name List.
Quantitate Section	
Allow Changes to Selected Sample Info in Processing Sequence	If you set this permission to Disallowed, the user cannot make changes to the sample information, such as Sample Name, Comment, Study, Client, Laboratory, and so on, in the processing sequence.
Allow Changes to Column Labels in Processing Sequence	If you set this permission to Disallowed, the user cannot change the column labels in the processing sequence.
Allow Changes to Column Labels in Results	If you set this permission to Disallowed, the user cannot change the column labels on the Survey or Review All pages of the LCquan Quantitate section.
Prompt User for Comments after Manual Integration	If you set this permission to Allow, the user must enter a comment before proceeding with a manual integration. Whenever the user performs a manual integration, the Chromatogram Comment dialog box opens and prompts the user for a comment before proceeding.
Allow Results Export	If you set this permission to Disallowed, the user cannot export results.
Allow Manual Integration	If you set this permission to Disallowed, the user cannot manually adjust the peak integration.

Figure 9. Permission Level Settings (Sheet 4 of 5)

LCquan feature	Description
Allow User Integration	If you set this permission to Disallowed, the user cannot adjust the peak integration settings for an individual peak.
Allow Calibration Settings to Be Changed	If you set this permission to Disallowed, the user cannot change the Calibration settings of a particular component.
Create Reports	If you set this permission to Allow, the user can create two types of reports: • Microsoft Excel™ Workbook with data and results • XReport report
Remove Signature Line From Excel Report	(Required for the Watson file interface) An Allow setting removes the signature line from the exported quantitation reports so that the Watson system can import the exported Excel spreadsheet via the file interface. See "Recommended Settings for Excel Reports" on page 93 in Appendix C, "Watson Interface."
Allow Watson File Interface Excel Format Reports	(Recommended for the Watson file interface) An Allow setting fixes the format of the Acq Date column entries in the exported quantitation reports so that the Watson file system can correctly import the acquisition date and time. See "Recommended Settings for Excel Reports" on page 93 in Appendix C, "Watson Interface."
Secure XReport Template	An Allowed setting prevents the user from creating quantitation reports with XReport other than reports that use the secure XReport templates. After you specify a secure template folder, users can save secure reports only as PDF files using the templates from the specified folder. For details, see "Setting Up Secure Reports" on page 56 in Chapter 4, "Defining Secure User Groups and Permissions."

Figure 9. Permission Level Settings (Sheet 5 of 5)

LCquan feature	Description
Allow Excel Rounding	An Allowed setting restricts the number of decimal places in the exported Excel reports. The values for Area, Height, Response, ISTD Area, ISTD Height, and ISTD Response are restricted to zero decimals. All other values are limited to three decimals.
	The Allowed setting changes the behavior in the LCquan Column Arrangement dialog box for Excel reports, preventing the user from changing the precision. Any previous value settings are overridden with a restricted number of decimals and the values are not editable. The Allow setting does not affect the behavior of the LCquan grid views, the exported results, or the reports generated using XReport.
	Important Before the Excel rounding feature takes effect for the Watson digital interface, you must start and exit the LCquan application at least one time. See "Recommended Settings for Excel Reports" on page 93.

Installing an Oracle Database

This appendix describes the procedure that Thermo Fisher Scientific Inc. uses to install the Oracle Server and Client software. Consult your Oracle database administrator for advice and instructions about how to install this software for your application.

The installation information in this appendix supplements the documentation provided by Oracle and does not replace it. Refer to your Oracle documentation for installation and configuration details.

Note The procedures contained in this appendix describe the installation of the Oracle9*i* Database. The installation procedures for other versions or releases of the database can differ from those described here.

Contents

- Installing the Oracle Server
- Installing the Oracle Client

Installing the Oracle Server

❖ **To install the Oracle Server**

1. Insert the Oracle database CD.

   The **Autorun** installation program automatically starts. If the installation program does not automatically start, find and double-click the setup.exe file.
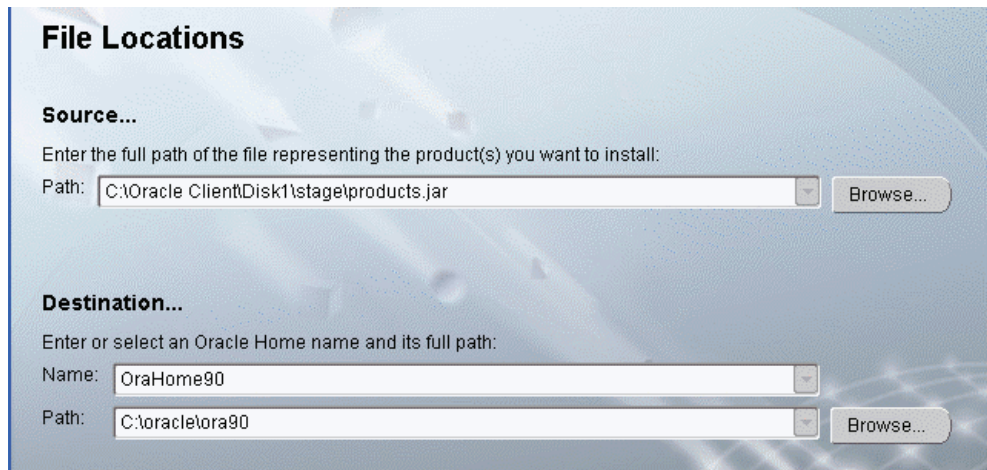

2. In the installation program, click **Install/Deinstall Products**.

The Oracle Universal Installer: Welcome page opens.
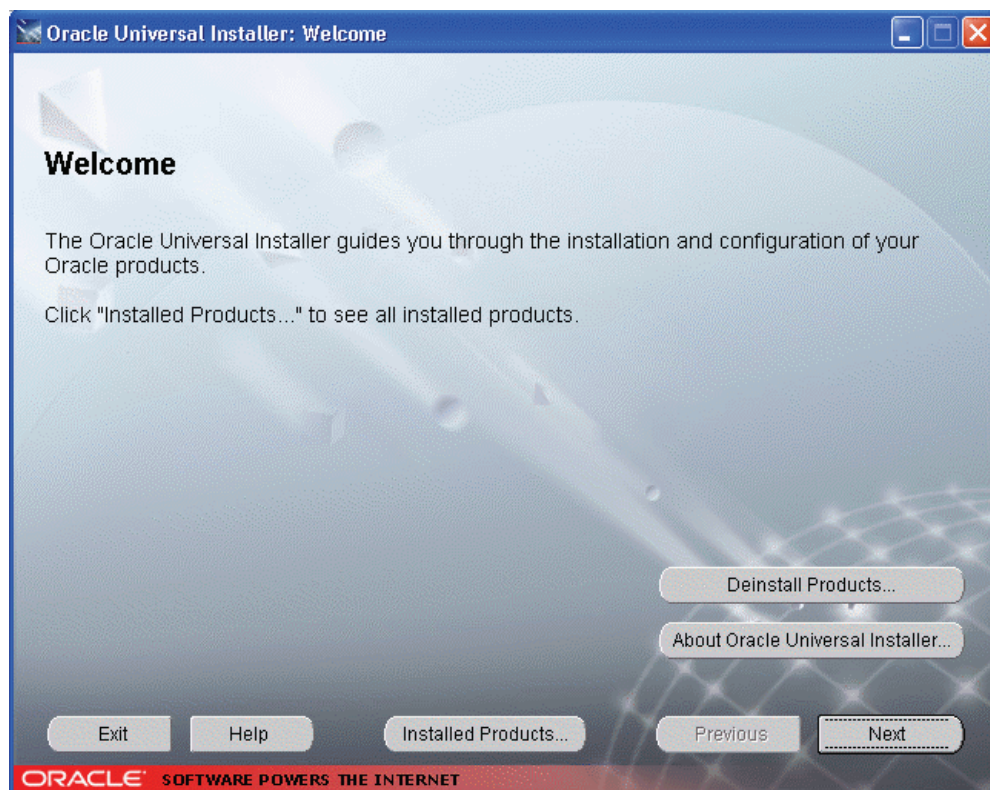
> **Note** Do not install the Oracle server in an existing Oracle environment with a previous version of the software already installed. Remove any previous versions before installing the new version. If you have data in the other database, *back up your data* and use the Oracle Data Migration Assistant to migrate it to the new database during or after the installation. Refer to the Oracle documentation for more information.

3. To remove a previous version of the Oracle server before proceeding with this installation, click **Deinstall Products.**

   The Inventory dialog box opens.

4. Select the previous version from the list and click **Remove**.

5. On the Welcome page, click **Next**.

The File Locations page opens.

> **IMPORTANT** The Source Path box automatically fills in the location of the installation files. Do not change the path.

6. Enter the Oracle Home name and its full path:

   a. In the Destination Name box, type or select a name for the Oracle Home.

   b. In the Destination Path box, type or select the location where the Oracle components will be installed.

   c. Click **Next**.

   The Available Products page opens.

7. Select the product to install and click **Next**.

The Installation Types page opens.
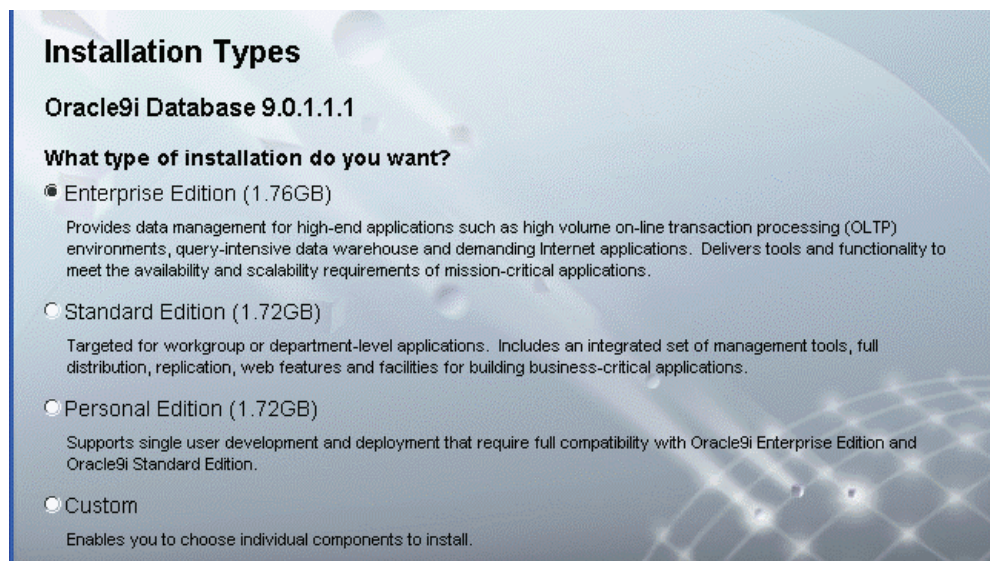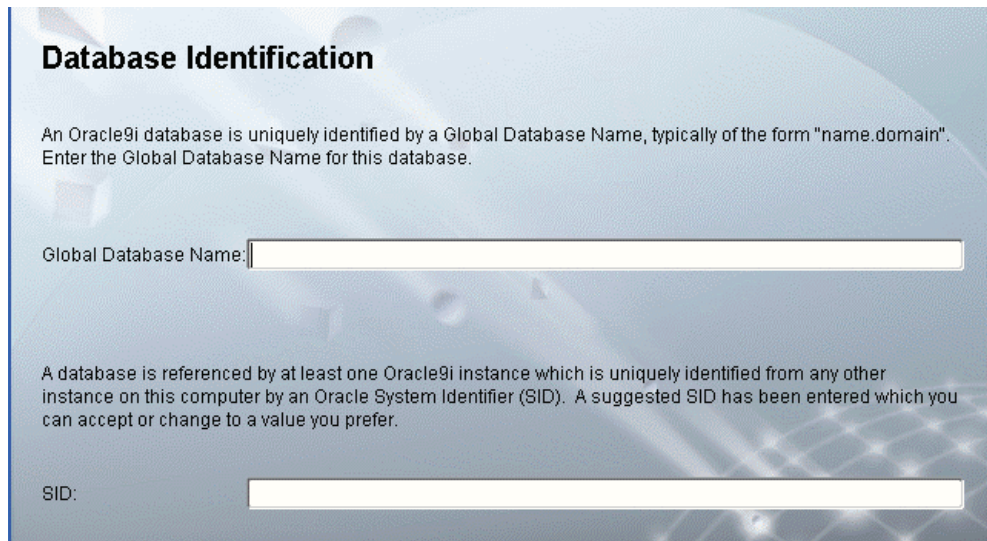
8. Select the type of installation you want and click **Next**.

The Database Configuration page opens.
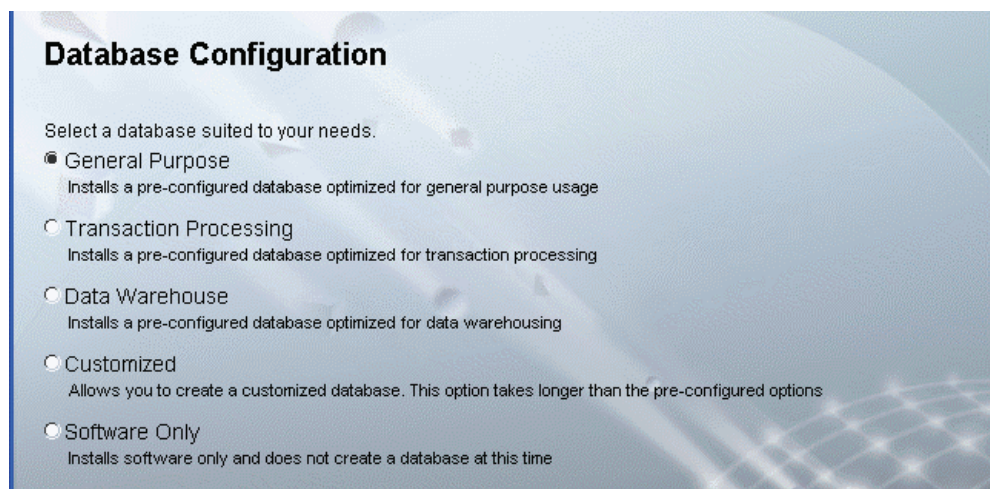
9. Select an appropriate database and click **Next**.

The Database Identification page opens.
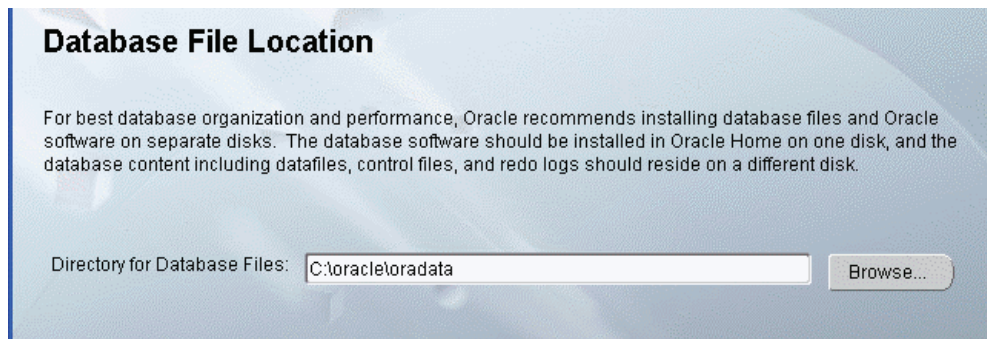
10. Type the Global Database Name for the database, type the Oracle System Identifier (SID) name, and click **Next**.

The Database File Location page opens.

11. Type the directory location for the database files (Directory for Database Files) and click **Next**.

The directory location must be a mapped drive.

The Database Character Set page opens.
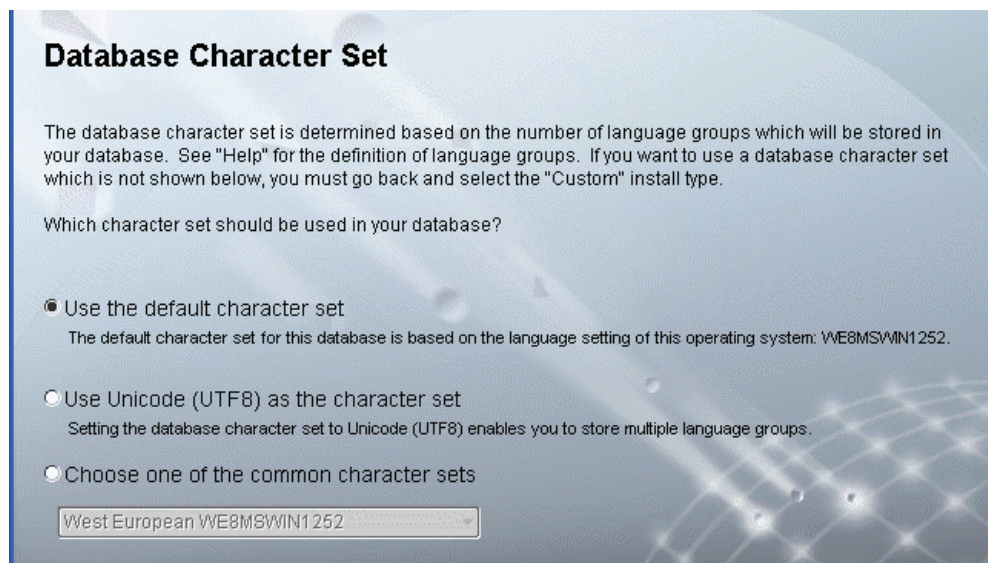
12. Select the character set to use in your database and click **Next**.

The Summary page opens.
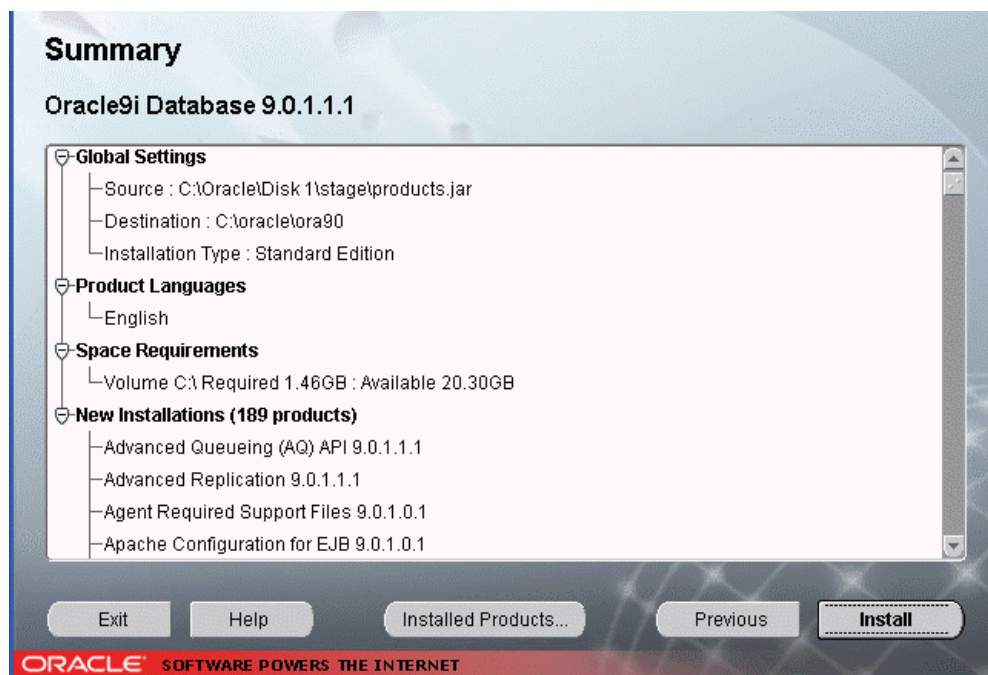
13. Review the space requirements to ensure that you have enough disk space and click **Install** to start the installation.

When the installation is complete, the Configuration Tools page opens and a series of tools automatically starts to create and configure your database and the Oracle Net Services environments.

The Configuration Tools page displays the results.
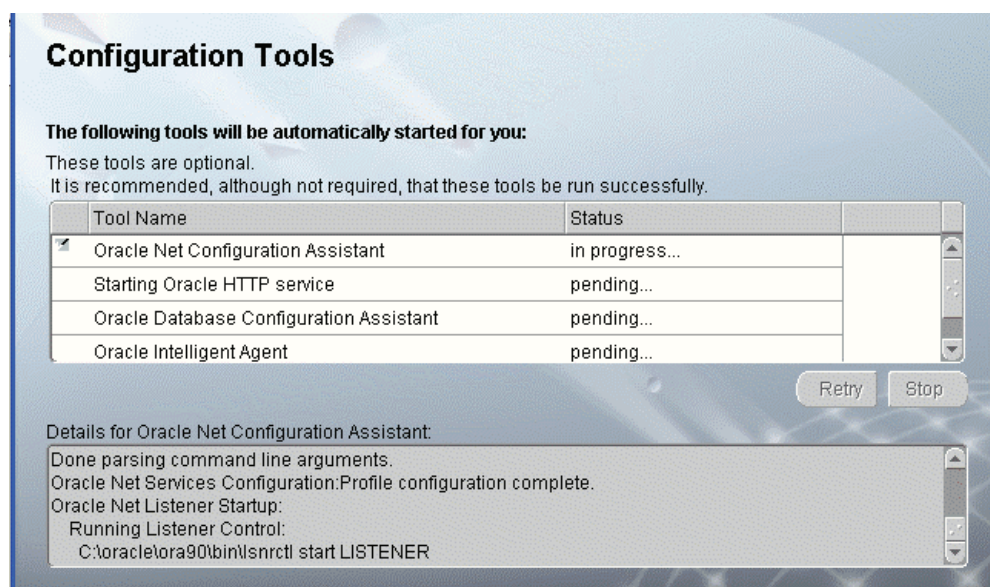
- If the Oracle Database Configuration Assistant tool runs, continue with step 14.

- If the Oracle Database Configuration Assistant tool does not run, go to step 15.

14. If the Oracle Database Configuration Assistant tool runs, change the default passwords that it sets. After the tool completes its run, the Oracle Database Configuration Assistant dialog box opens:

    a. Make note of the database information listed in this dialog box.
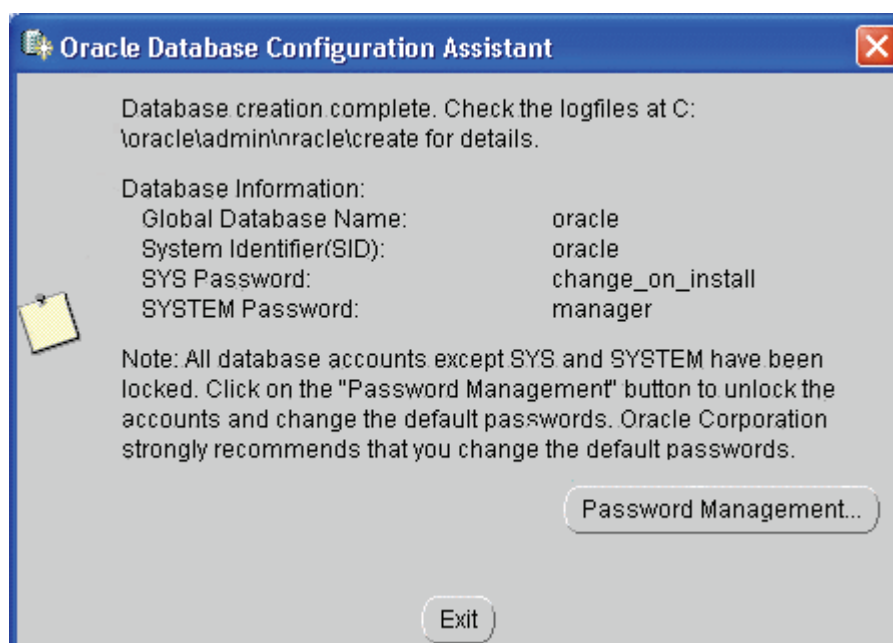
    b. In the Oracle Database Configuration Assistant dialog box, click **Password Management.**

The Password Management dialog box opens.
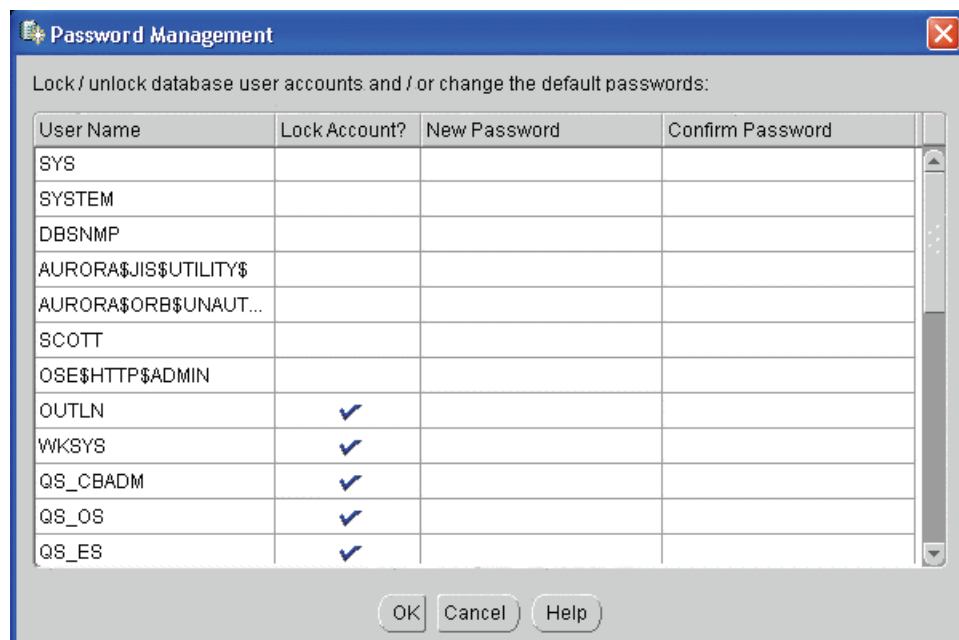
c. Change the default passwords.

d. Lock or unlock the database user accounts as necessary.

e. Click **OK** to save the changes and close the Password Management dialog box.

15. When all the tools on the Configuration Tools page have finished running, click **Next**.

    The End Of Installation page opens.

16. Click **Exit** to exit from the Oracle Universal Installer.

    The database is installed.
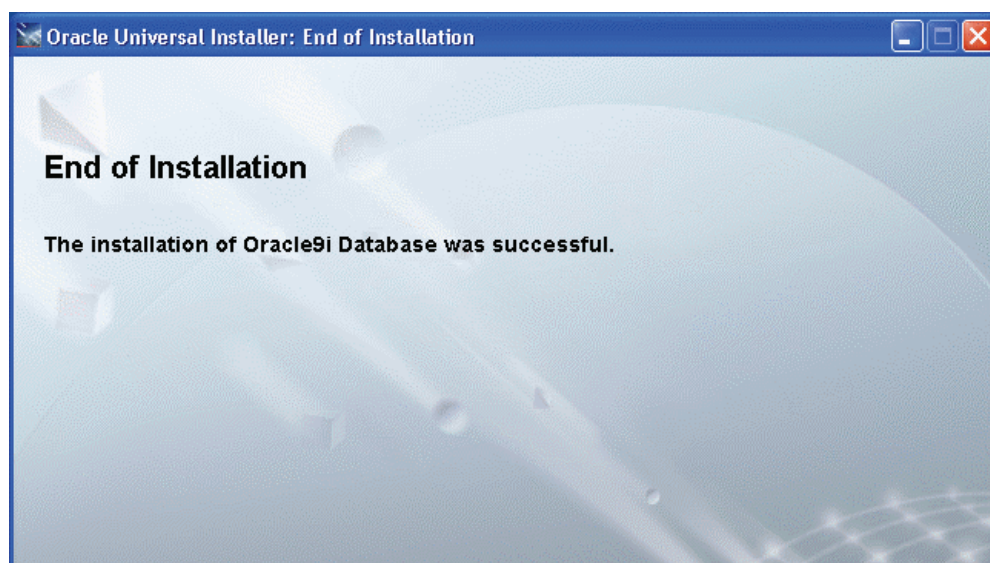
Installing the Oracle Client

❖ **To install the Oracle client software**

1. Insert the Oracle database client CD.

   The Autorun installation program automatically starts. If it does not, locate and double-click the setup.exe file.

> **Note** Do not install the Oracle application into an existing Oracle environment that contains another installation of the client. Remove any previous versions before installing a new version. Refer to your Oracle documentation for more information.

2. In the installation program, click **Install/Deinstall Products**.

   The Oracle Universal Installer: Welcome page opens.

3. Remove a previous version of the Oracle database client before proceeding with this installation as follows:

   a. Click **Deinstall Products**.

      The Inventory dialog box opens.

   b. Select the previous version from the list and click **Remove**.

4. On the Welcome page, click **Next**.

The File Locations page opens.

IMPORTANT The Source Path box automatically fills with the location of the installation files. Do not change the path.

5. Enter the Oracle Home name and its full path:

   a. In the Destination Name box, type or select a name for the Oracle Home.

   b. In the Destination Path box, type or select the location where the Oracle components will be installed.

   c. Click **Next**.

   The Installation Types page opens.

6. Select the type of installation that you want and click **Next**.

The Summary page opens.
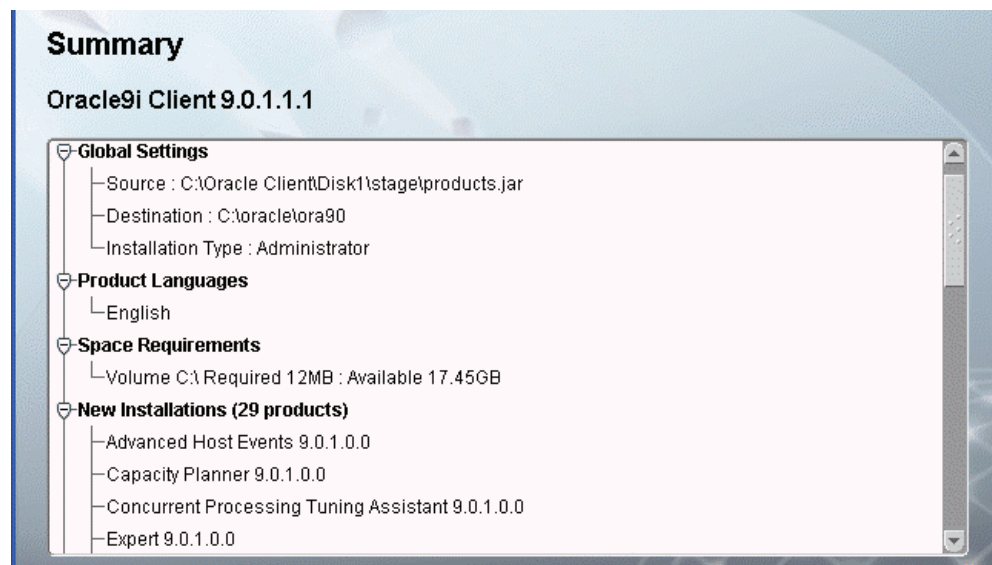
7. Review the space requirements to confirm that your system has enough disk space and click **Install**.

When the installation is complete, the Configuration Tools page opens and a series of tools automatically starts to create and configure your database and Oracle Net Services environments.

The Configuration Tools page displays the results.
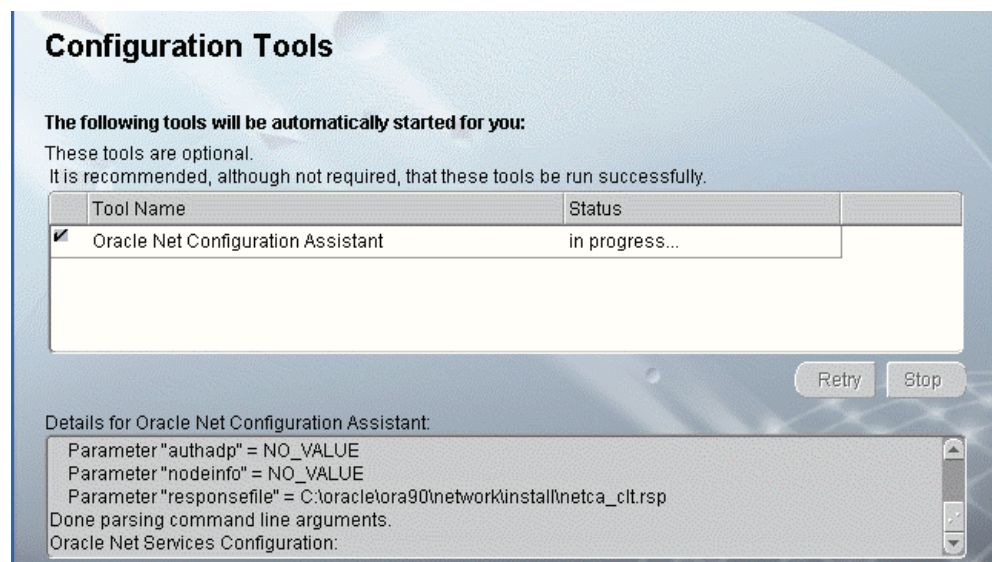
- If the Oracle Net Configuration Assistant runs, continue with step 8.

- If the Oracle Net Configuration Assistant does not run, go to step 15 on page 92.
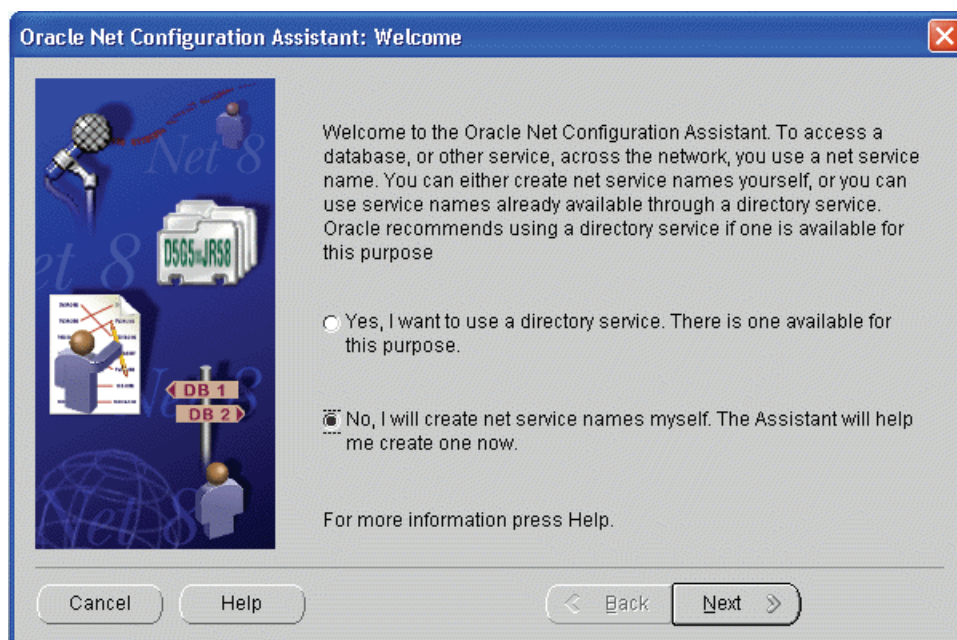
8. On the Oracle Net Configuration Assistant: Welcome page, select the **No, I will create net service names myself** option and click **Next**.

   The Net Service Name Configuration, Database Version page opens.

9. Select the **Oracle8i or later database or service** option and click **Next**.

The Net Service Name Configuration, Service Name page opens.
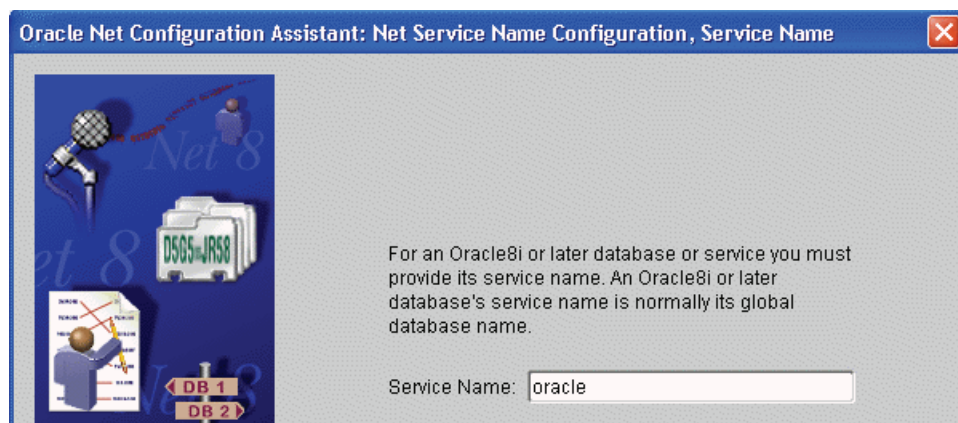
10. Type the global database name and click **Next**.

The Net Service Name Configuration, Select Protocols page opens.
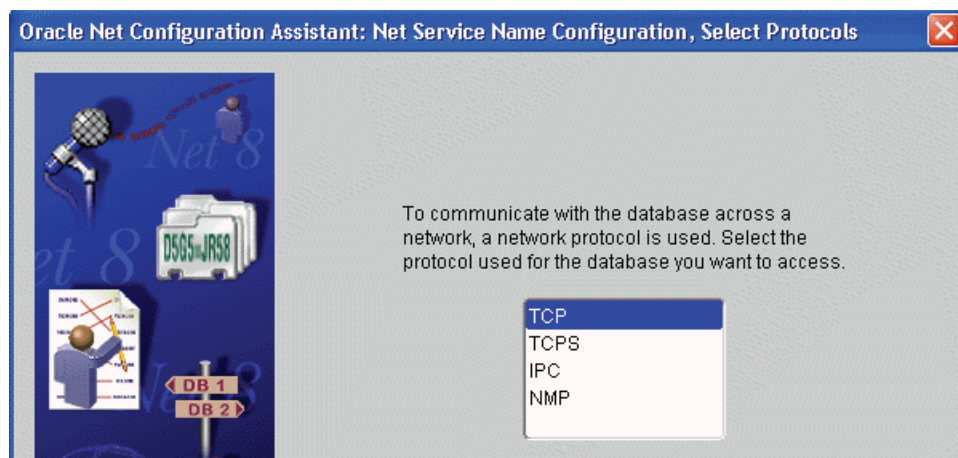
11. Select the protocol used for the database that you want to access and click **Next**.

The next page that opens depends on what protocol you selected.

For example, if you selected the TCP protocol, the Net Service Name Configuration, TCP/IP Protocol page opens and you are prompted to provide protocol parameter information.
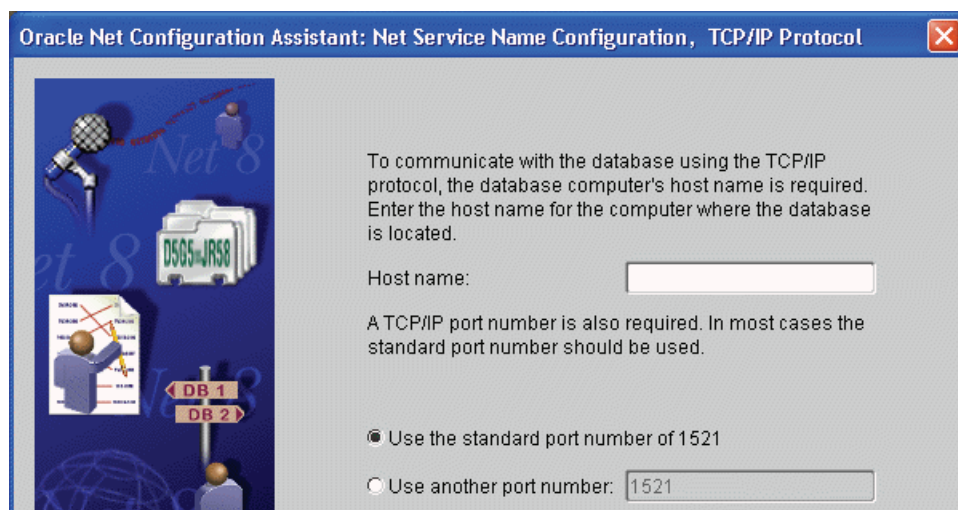
12. Based on your choice of protocol, complete the specification of the protocol and click **Next**.

For example, on the previous Net Service Name Configuration, TCP/IP Protocol page, enter the host name for the system where the database is located, select the **Use the standard port number** option, and click **Next**.

The Net Service Name Configuration, Test page opens.

13. Select the **Yes, perform a test** option and click **Next**.

The Net Service Name Configuration, Connecting page opens and a connection test is performed.

- If the test is successful, click **Next**. The Net Service Name Configuration, Net Service Name page opens.
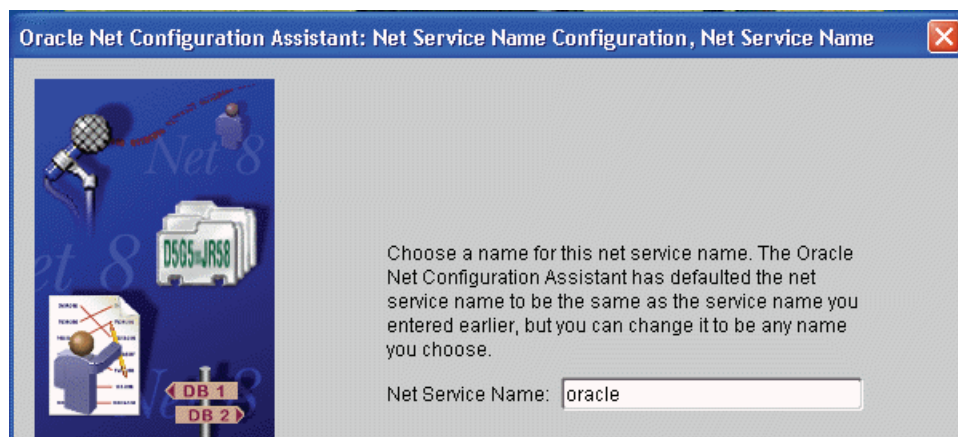
- If the test fails, click **Back** to review the information you entered. Make any necessary changes and try the test again.

14. On the Net Service Name Configuration, Net Service Name page, do the following:

    a. Accept the default net service name or type another net service name.

       The name you enter must be unique to the client.

    b. Click **Next**.

       The Net Service Name Configuration, Another Net Service Name? page opens.

    c. Specify whether or not to configure another net service name for this client.

       • If you select **Yes** and click **Next**, the Oracle Net Configuration Assistant leads you through the process of configuring another net service name.

       • If you select **No** and click **Next**, the Net Service Name Configuration Done page opens. Click **Next** again and click **Finish** to complete the Oracle Net Configuration Assistant.

         The installer returns you to the Oracle Universal Installer: Configuration Tools page.

15. On the Oracle Universal Installer: Configuration Tools page, click **Next**.

    The installation is complete.

Watson Interface

This appendix describes Thermo Foundation Authorization Manager settings for the Watson interface.

> **Contents**
>
> - Recommended Settings for Excel Reports
> - About the Watson Digital Interface

Recommended Settings for Excel Reports

For the Watson file interface, set the following features in Thermo Foundation Authorization Manager to ensure that you can correctly import Excel reports from the LCquan application:

- Remove Signature Line from Excel Reports—This setting removes the signature line from the exported quantitation reports.

- Allow Watson File Interface Excel Format Reports—This setting corrects the format of the acquisition date and time entries in the exported quantitation reports.

Rounding the Decimal Places

For the Watson digital interface, you can ensure consistency in the number of decimal places displayed in the Excel reports that the LCquan application exports. To do this, use the Allow Excel Rounding feature.

If you specify Excel rounding, the exported values are restricted to three decimal places consistently in the Excel reports. However, if you use this feature, the Excel reports do not include a full precision value.

To use the Excel rounding feature, set the permission level to **Allowed** in the Foundation Authorization Manager (Setting the Excel Features). Before the Excel rounding feature takes effect for the Watson digital interface, you must start and exit the LCquan application.

Setting the Excel Features

❖ **To set the Excel features for LCquan reports**

1. From the Windows XP taskbar, choose **Start > Programs >**

   Thermo Foundation 1.0 > Authorization Manager.

   Thermo Foundation Authorization Manager opens.
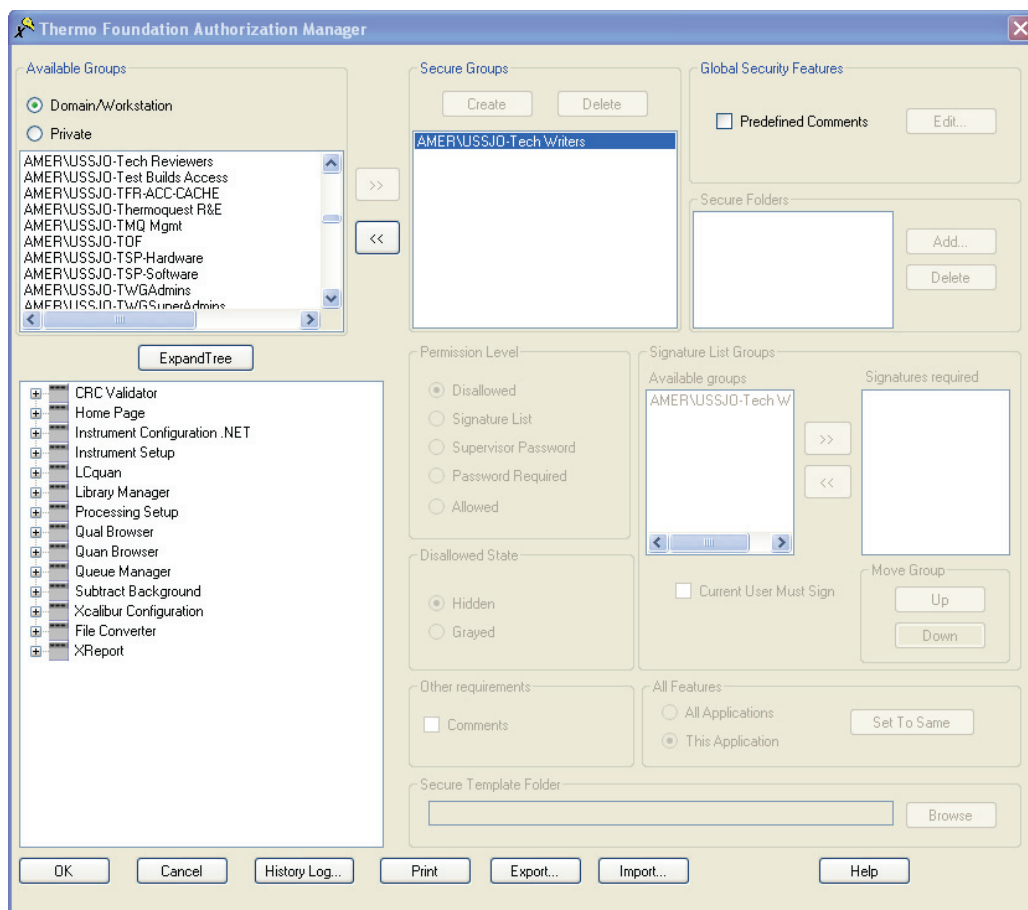
2. In the Secure Groups area, select the group.

3. In the controlled features list (lower left side), select **LCquan**, and click **Expand Tree**.

   The LCquan list of controlled features appears.

Figure 10. LCquan quantitate section features list
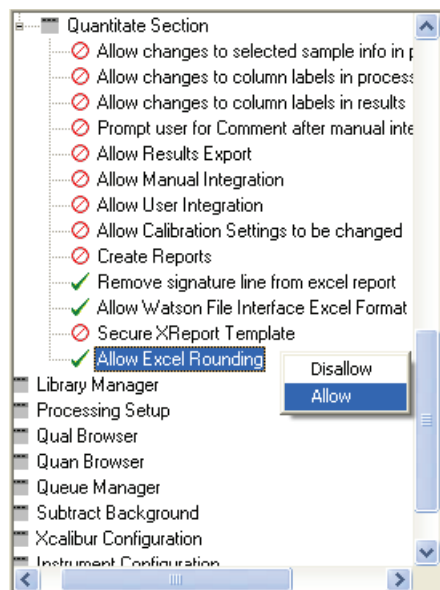
4. Under Quantitate Section, right-click the feature and choose **Allow** from the shortcut menu for each of the following:

   • Remove signature line from Excel report

   • Allow Watson file interface Excel format

   • Allow Excel Rounding

Figure 11. LCquan quantitate section features list
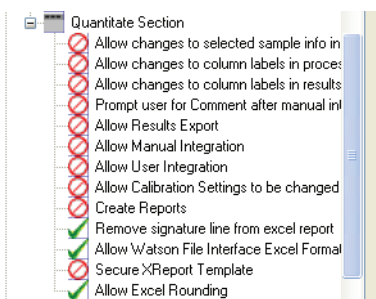
A check mark appears next to each allowed feature.

5. Click **OK** to apply the changes and close the Foundation Authorization Manager.

About the Watson Digital Interface

The following fields are exported to the Watson application using the digital interface for each sample/analyte combination:

- Peak area

- Peak height

- Retention time

See "Rounding the Decimal Places" on page 93.

To use the digital interface with Watson 7.2 or later, refer to the instructions in the manual *Installing and Using the Peak View Gateway Between Watson and LCquan.*

IT Considerations

To ensure that both the Xcalibur and LCquan applications work properly, review these IT issues.

Contents

- Avoid Antivirus Scanning During Data Acquisition
- Do Not Delete the Xcalibur System Account
- Ensure that a Firewall Exception Exists for the Instrument

Avoid Antivirus Scanning During Data Acquisition

Schedule utilities that actively scan the hard drive—such as antivirus, defragmenting, and backup utilities—to run at times other than during data acquisition. These utilities can monopolize computer resources, interfere with data acquisition, or cause loss of communication with the instrument.

These directories are typically used during data acquisition:

- C:\Documents and Settings*Current User*\Local Settings\Temp

- C:\Xcalibur\methods *or* the directory where the instrument method (.meth) and processing method (.pmd) files are stored

- C:\Xcalibur\data *or* the directory where raw files (.raw) are stored

- C:\Xcalibur\system\programs\

Do Not Delete the Xcalibur System Account

With sequential user logon, a user can log on, start an acquisition, and then log out. When sequential user logon is enabled, an extra user account—Xcalibur System—is created. This account runs in the background during data acquisition. Do not delete this account.

Ensure that a Firewall Exception Exists for the Instrument

Firewall settings must include an exception for the instrument in use. If the firewall exception is not configured, the computer is unable to communicate with the instrument. During installation, instrument software now automatically configures the required exception for the Microsoft Windows firewall.

Index