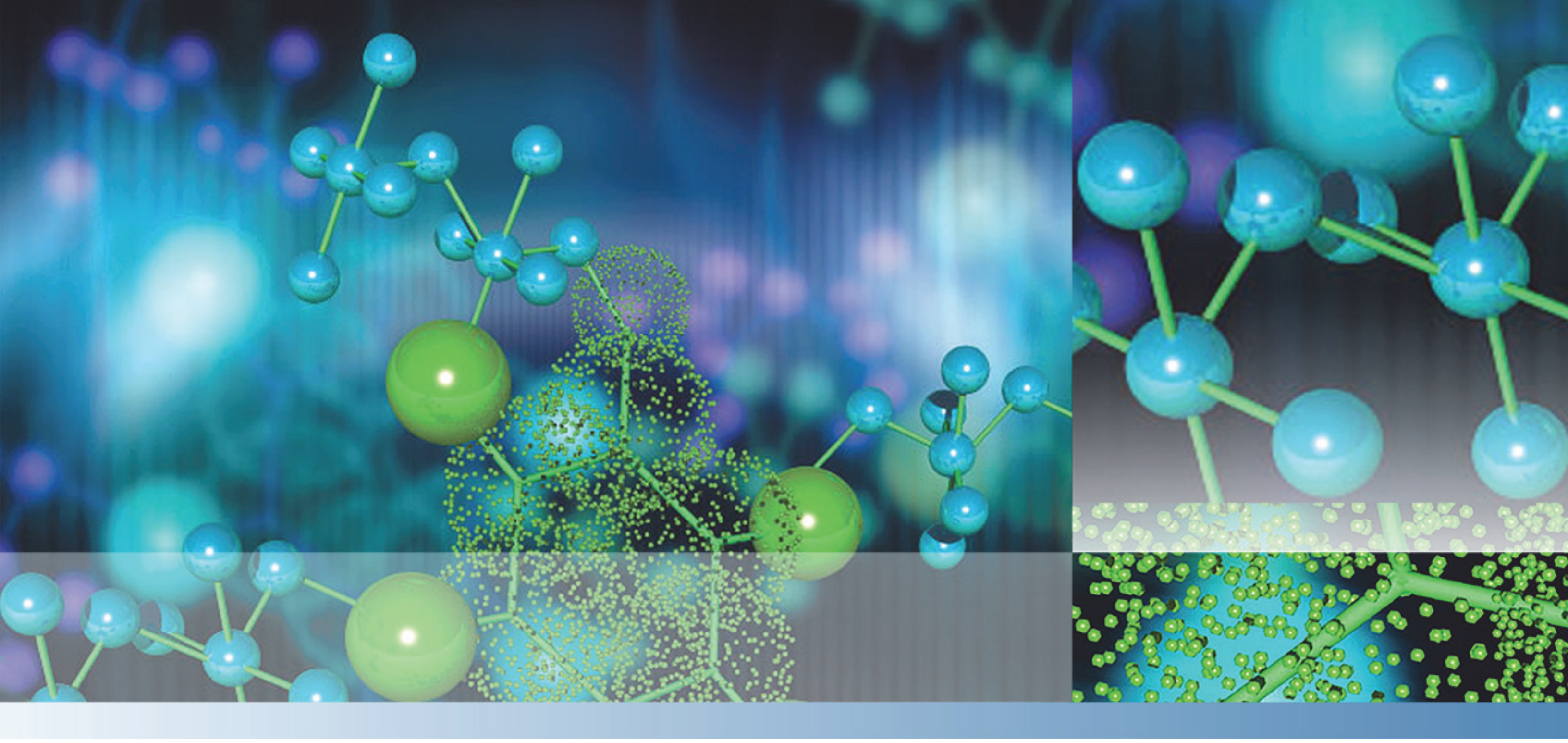


Thermo

Foundation

Administrator Guide

Software Version 3.1

XCALI-97619 Revision A August 2014

DOCUMENTATION SURVEY

Thermo SCIENTIFIC

The contents of this document are subject to change without notice. All technical information in this document is for reference purposes only. System configurations and specifications in this document supersede all previous information received by the purchaser.

This document is not part of any sales contract between Thermo Fisher Scientific Inc. and a purchaser. This document shall in no way govern or modify any Terms and Conditions of Sale, which Terms and Conditions of Sale shall govern all conflicting information between the two documents.

Release history: Revision A, August 2014

Software version: Foundation platform version 3.1 and later

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

Contents

Preface

This administrator guide describes how to configure instruments and the Xcalibur™ and LCquan™ applications for security and compliance. 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 the Microsoft™ Windows™ operating system. Thermo Fisher Scientific strongly recommends that you enlist your local IT professional to perform these tasks.

Contents

❖ To suggest changes to documentation or to Help

Complete a brief survey by clicking the button below.
Thank you in advance for your help.

DOCUMENTATION SURVEY

Related Documentation

The documentation for the Thermo Foundation platform includes this guide and Help.

❖ To access the administrator guide from the data system computer

Choose **Start > All Programs (or Programs) > Thermo Foundation *x.x* > Manuals**.

System Requirements

Ensure that the system meets these requirements.

System	Requirements
Computer	Minimum requirements: • Dual-core processor processing speeds of 3.3 GHZ • Installed memory (RAM): 4 GB • System type: 64-bit operating system • 250 GB hard drive • DVD drive • Video card and monitor capable of 1280 × 1024 resolution • NTFS format
Software	• Adobe™ Reader™ 10 or later • Microsoft™ Office 2010
Operating system	Microsoft Windows™ 7 Professional with Service Pack 1 (64-bit)

For information about maintaining communication between the data system computer and the Thermo Scientific™ instruments that it controls, see Chapter 10, "Maintaining Communication with the Instruments."

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.

For Thermo Scientific™ products	Access by phone, fax, email, or website
Technical Support	(U.S.) Phone: 1 (800) 532-4752 Fax: 1 (561) 688-8736 Email: us.techsupport.analyze@thermofisher.com Web—for product support, technical documentation, and knowledge bases: www.thermoscientific.com/support
Customer Service (Sales and service)	(U.S.) Phone: 1 (800) 532-4752 Fax: 1 (561) 688-8731 Email: us.customer-support.analyze@thermofisher.com Web—for product information: www.thermoscientific.com/lc-ms Web—for customizing your service request: 1. From any Products & Services web page, click **Contact Us**. 2. In the Contact Us box, complete the information requested, scroll to the bottom, and click **Send**.
User Documentation	Web—for downloading documents: mssupport.thermo.com 1. On the Terms and Conditions web page, click **I Agree**. 2. In the left pane, click **Customer Manuals**. 3. To locate the document, click **Search** and enter your search criteria. For Document Type, select **Manual**. Email—to send feedback directly to Technical Publications: techpubs-lcms@thermofisher.com Web—to complete a survey about this Thermo Scientific document: www.surveymonkey.com/s/PQM6P62

1

Introduction

You can use Thermo Scientific applications to develop methods, create or import sequences, acquire, process, and review data, and create reports, all within a secure environment. This chapter provides an overview of security and compliance considerations and describes how to use the Foundation platform, the Xcalibur data system, and the LCquan application to address them.

Contents

System Security

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

- 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 Xcalibur data system and the LCquan application directly implement some of these controls and rely on the security functions in the Microsoft Windows 7 Professional operating system for other controls:

- The Thermo Foundation Security Service controls secure file operations.
- The laboratory administrator restricts user software access through Thermo Foundation Authorization Manager (an administrative utility), which relies on Windows user groups. The Authorization Manager does not configure user access to the workstation. However, it can define application roles and feature access for the users.
- Windows security functions handle user authentication.
- Windows security functions maintain electronic record security and, in particular, the NTFS permission rights.

Configuration Tasks of the Laboratory Manager and IT Professional

As the laboratory administrator, you must work with your IT professional to configure the security features. Table 1 lists the tasks the laboratory administrator and IT professional perform.

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

To verify that the system is appropriately configured, see these topics:

- Configuration Checklist
- Configuration Flowchart

Configuration Checklist

Review the following checklist.

Table 1. Configuration tasks checklist (Sheet 1 of 2)

Task	Reference	Role	Completed?
1. Install software for Xcalibur and LCquan on the designated workstations.	The install guide for the appropriate software.	IT professional or laboratory administrator	
2. Run the database configuration application.	Chapter 2, "Using the Database Configuration Manager."	IT professional (for Oracle™ database) or laboratory administrator	
3. Ensure that the Thermo Foundation Security Service is properly configured and running.	"Configuring Security Settings for Folders and Files" on page 25.	IT professional or laboratory administrator	
4. Determine which folder to use as the application secure root folder and identify the secure user groups.	"LCquan Folder Structure" on page 141 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 but not to delete objects.	"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 45.	IT professional or laboratory administrator	

Table 1. Configuration tasks checklist (Sheet 2 of 2)

Task	Reference	Role	Completed?
7. Configure Authorization Manager settings for applications:	Chapter 4, "Using the Authorization Manager."	Laboratory administrator	
a. Define user groups.	"Using the Authorization Manager to Set Up Secure User Groups" on page 53	Same as above	
b. Set permission levels for software features for each user group.	"Step 2: Setting the Permission Levels" on page 73	Same as above	
c. If users are permitted to change the secure root folder, define the list of secure folders.	"Setting Up the List of Secure Folders for the LCquan Application" on page 82	Same as above	
d. Specify whether users are required to make comments.	"Step 3: Setting Up a List of Predefined Comments" on page 79	Same as above	
e. Save the configuration settings.	"Step 5: Saving the Security Settings" on page 86.	Same as above	

Configuration Flowchart

Figure 1 and Figure 2 show flowcharts of the configuration process for domain users and local users, respectively.

Figure 1. Configuration tasks of the laboratory administrator and IT professional for domain users

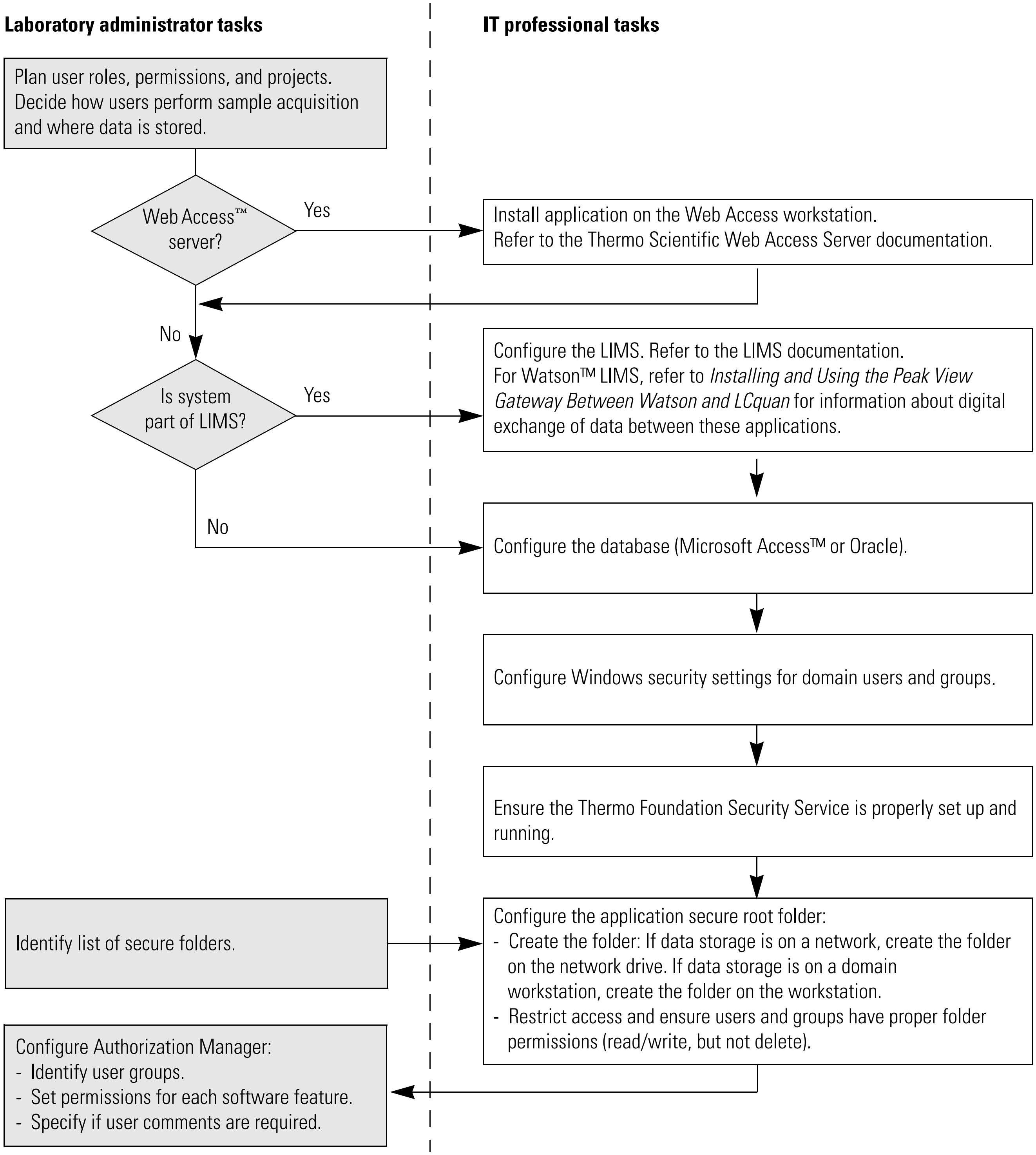
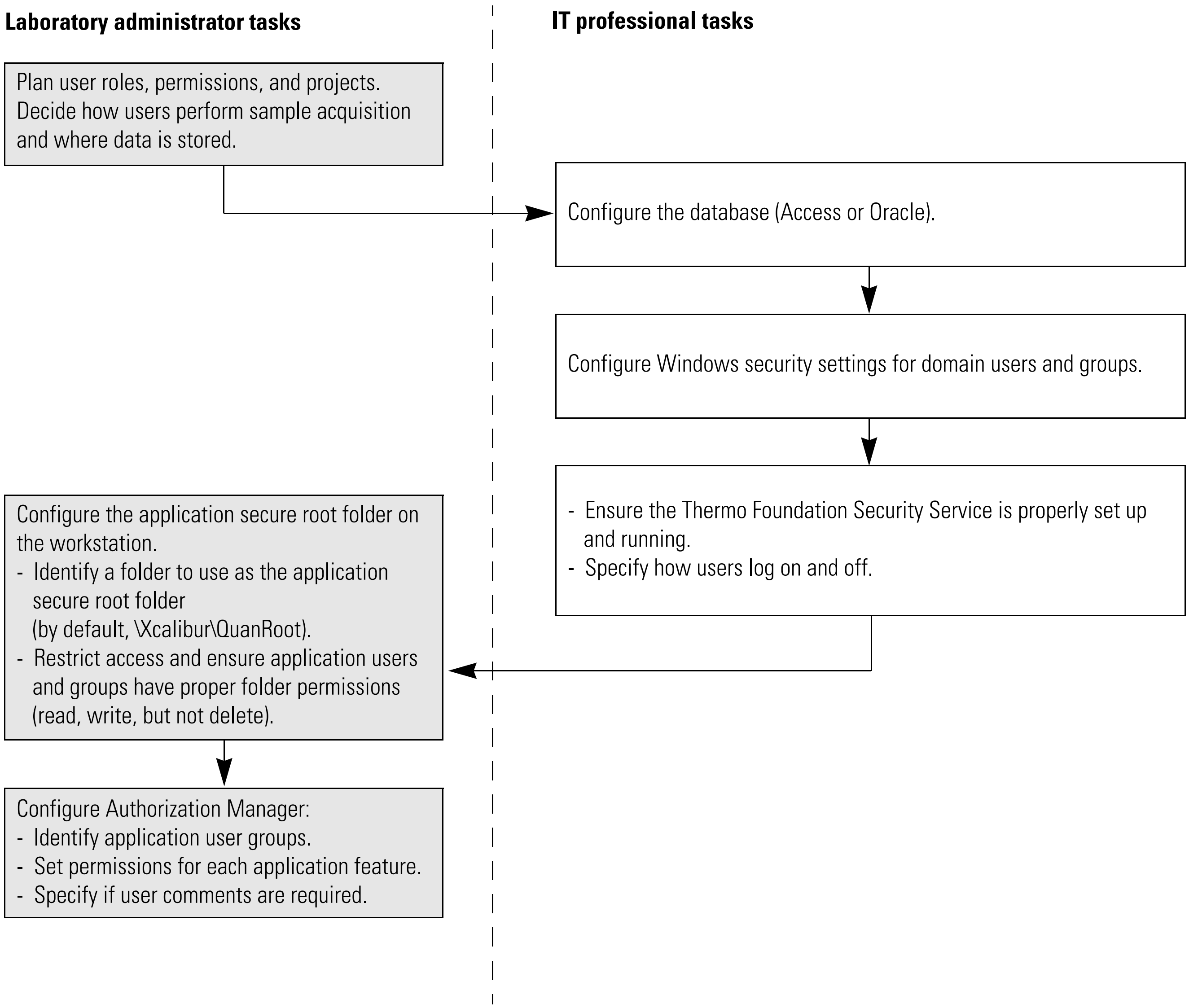

Laboratory administrator tasks
IT professional tasks
Plan user roles, permissions, and projects. Decide how users perform sample acquisition and where data is stored.
Web Access™ server?
Yes
Install application on the Web Access workstation. Refer to the Thermo Scientific Web Access Server documentation.
No
Is system part of LIMS?
Yes
Configure the LIMS. Refer to the LIMS documentation. For Watson™ LIMS, refer to *Installing and Using the Peak View Gateway Between Watson and LCquan* for information about digital exchange of data between these applications.
No
Configure the database (Microsoft Access™ or Oracle).
Configure Windows security settings for domain users and groups.
Ensure the Thermo Foundation Security Service is properly set up and running.
Identify list of secure folders.
Configure the application 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 workstation, create the folder on the workstation.
- Restrict access and ensure users and groups have proper folder permissions (read/write, but not delete).
Configure Authorization Manager:
- Identify user groups.
- Set permissions for each software feature.
- Specify if user comments are required.

Figure 2. 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 Thermo Foundation Security Service is properly set up and running.
- Specify how users log on and off.

Configure the application secure root folder on the workstation.

- Identify a folder to use as the application secure root folder (by default, \Xcalibur\QuanRoot).
- Restrict access and ensure application users and groups have proper folder permissions (read, write, but not delete).

Configure Authorization Manager:

- Identify application user groups.
- Set permissions for each application feature.
- Specify if user comments are required.

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 and Store Data
- Secure User Groups

How Users Perform Sample Acquisition and Store Data

Users can perform sample acquisitions and store the acquired sample data in various places. Refer to your application user guide for supported configurations. These are the most likely mass spectrometer and data storage configurations:

- Local users can store acquired sample data on a standalone workstation.
- Domain users can store acquired sample data on a workstation that is on a network.
- Multiple domain users can store acquired sample data on a network server.

You can integrate application data with a laboratory information management system (LIMS), such as Watson LIMS. If you are using Watson LIMS, refer to *Installing and Using the Peak View Gateway Between Watson and LCquan*.

Some applications support the Thermo Scientific Web Access Server environment for workstations that are for data review only. Web Access can provide application virtualization to manage configuration and maintenance. You cannot use an instance of the application running on a Web Access server for acquisition. The IT professional is responsible for installing Thermo software on the Web Access server.

Some applications support remote acquisition. During remote acquisition, you can have the application time-stamp raw files created by the Xcalibur application during acquisition and create a time-stamped folder:

- Remotely stored raw files are time-stamped with the submission time.
- Pausing during acquisition does not change the time stamp.
- The time stamp for the raw files folder and the time stamp for the raw files are not necessarily the same.

Or, you can prevent the application from time-stamping the raw files during a remote acquisition by setting the permission from the Expand Tree list if the application permits this activity. Refer to your application user guide for more information.

IMPORTANT An application might be able to overwrite a raw file of the same name if you turn off time-stamping.

Secure User Groups

Your application requires both the security features of the Windows 7 operating system and the Thermo Foundation Authorization Manager to define the secure user groups and permissions. Typically, the IT professional is responsible for establishing Windows user accounts and user groups (domain groups). The laboratory administrator is responsible for setting up the permission levels in the Authorization Manager and, if necessary, private groups. You can create user groups that are either identified Windows user groups or private user groups that you define. You cannot create a collection of groups that is a combination of these two options.

- Windows user groups
  - The IT professional creates and manages domain user accounts and user groups.
  - You or the IT professional can create standalone workstation user accounts and user groups.

  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 an existing 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 view the user name so 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.
  - 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.

As the laboratory administrator, you must define the following 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 define at least two user groups—one for scientists and one for technicians.

Configuring Software Applications

Thermo Scientific applications are installed as a group, installing the different applications in the correct order to support the interdependencies of the software. The Foundation platform supports the other applications, providing a variety of cross-application functions. The Xcalibur data system is the base application and the LCquan application is a layered application. The LCquan application has better tools and features for operating in a secure environment.

To view version information about all installed Thermo Scientific applications, see "Viewing and Saving System Version Information" on page 123.

To fully implement the security features for applications, the laboratory administrator must work with the IT professional to achieve the proper data system configuration. Configuring applications for security and compliance requires three steps:

- Defining User Requirements
- Protecting Records
- Setting Up User Access Controls

Defining User Requirements

To define user requirements, consider all aspects of how the system will be configured and how you want authorized users to use the configured system.

If the system is to be used in an agency-regulated environment, perform a full system validation. Create a formal user requirements document and a system configuration document that address the bullet points below. Create and execute test scripts that address each of the requirements.

If you do not plan to use the system in a regulated environment, define how the system should be used. This might include the following elements that will help you to conduct the system configuration steps throughout this document:

- Define authorized user groups on the system, categorized by user type, which defines the level of access to the system functionality as well as access to data.
- Create a detailed process workflow showing how each user type uses the system to control instruments and to perform sample acquisition, analysis, and reporting.
- Create a list of all discrete software functionality of the system, organized according to the applications list in the Authorization Manager module.

Protecting Records

To establish secure file operations, as the laboratory administrator, you or an assistant laboratory administrator must restrict access permissions for specific folders and files. Set permissions so that only you or an assistant administrator 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 you define the security settings for at least one group, the application automatically denies access to user that are not in that group.

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

2

Using the Database Configuration Manager

This chapter describes how to use the Database Configuration Manager to configure your database. The 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.

Contents

Using Microsoft and Oracle Databases

To store the Foundation 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 The LCquan application uses a Microsoft Access database to store each LCquan Workbook Audit Trail.

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

Use the Thermo Foundation Auditing Database Configuration Manager to configure either a Microsoft Access database on your local computer or an Oracle database on a remote computer.

For information about installing and configuring the Oracle Server and Client software, version 11g or later, refer to the Oracle manuals. Consult with your Oracle database administrator and your Thermo Fisher Scientific service representative for advice and instructions about how to install this software for your application.

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

1. If the site does not have an Oracle server, version 11g or later, install an Oracle database on an accessible remote server. For more information, consult your Oracle database administrator.
2. Install the Oracle client software on your local system. For more information, 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.

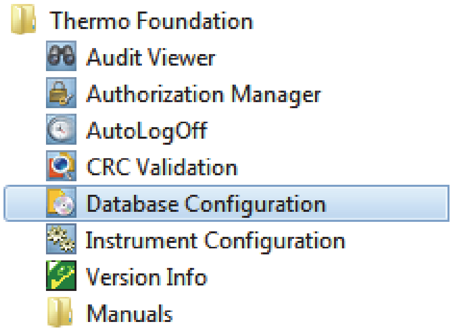
Configuring Your Auditing Database

This topic describes how to use the Auditing Database Configuration Manager to configure your auditing database.

For information about the parameters in the Thermo Foundation Auditing Database Configuration Manager wizard, see "Auditing Database Configuration Manager Parameters" on page 15.

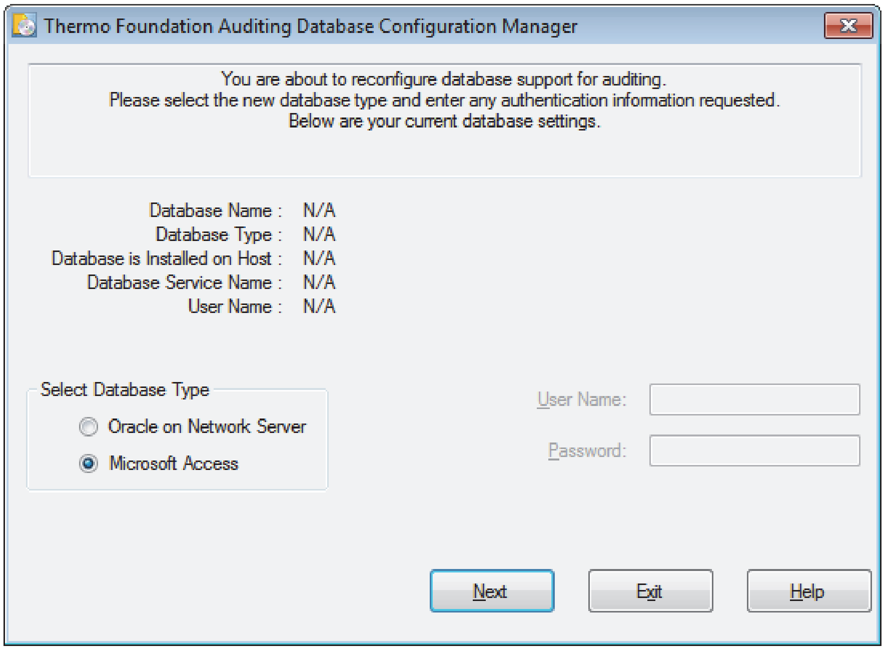
❖ To configure your auditing database

1. From the Windows taskbar, choose **Start** > **Programs** (or **All Programs**) > **Thermo Foundation *x.x*** > **Database Configuration**, where *x.x* is the version.



The Thermo Foundation Auditing Database Configuration Manager opens (Figure 3).

Figure 3. Foundation Auditing Database Configuration Manager dialog box



Thermo Foundation Auditing Database Configuration Manager

You are about to reconfigure database support for auditing.
Please select the new database type and enter any authentication information requested.
Below are your current database settings.

Database Name : N/A
Database Type : N/A
Database is Installed on Host : N/A
Database Service Name : N/A
User Name : N/A

Select Database Type

○ Oracle on Network Server

● Microsoft Access

User Name:

Password:

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. This option creates a relational database that cannot be accessed or edited in the MS Access application.

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

   > **IMPORTANT** If you are using Oracle version 11 or later, you might need to contact Technical Support for information about configuring your database. See "Contacting Us" on page ix for contact information.

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.

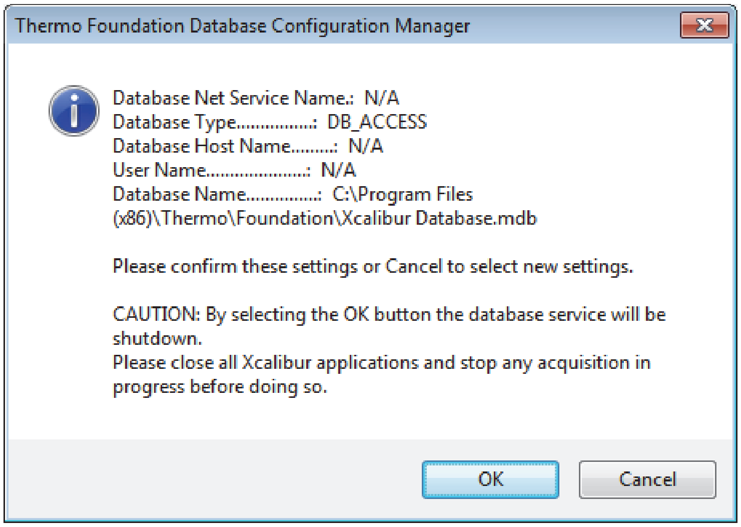
   c. In the Oracle Net Service Name list, select the Oracle Net Service Name for your database.

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

4. Click **Next**.

   The Thermo Foundation Database Configuration Manager dialog box opens (Figure 4).

Figure 4. Foundation Database Configuration Manager dialog box



Thermo Foundation Database Configuration Manager

Database Net Service Name.: N/A
Database Type...............: DB_ACCESS
Database Host Name.........: N/A
User Name.....................: N/A
Database Name..............: C:\Program Files (x86)\Thermo\Foundation\Xcalibur Database.mdb

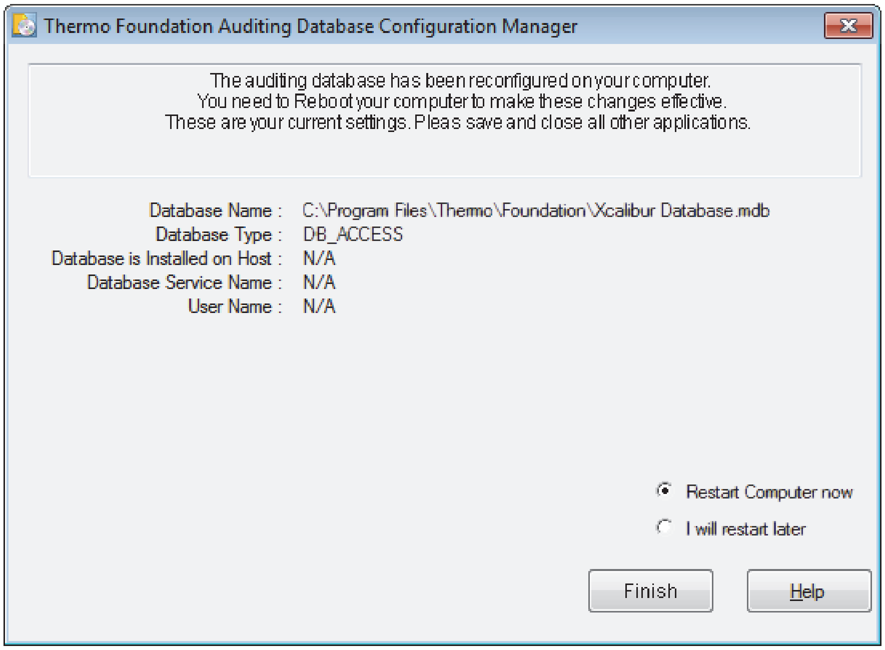
Please confirm these settings or Cancel to select new settings.

CAUTION: By selecting the OK button the database service will be shutdown.
Please close all Xcalibur applications and stop any acquisition in progress before doing so.

5. Confirm that the settings in the Thermo Foundation Auditing Database Configuration Manager dialog box are correct and click **OK**.

   The final page of the Thermo Foundation Auditing Database Configuration Manager opens (Figure 5).

Figure 5. Auditing Database Configuration Manager dialog box with Finish button



Thermo Foundation Auditing Database Configuration Manager

The auditing database has been reconfigured on your computer.
You need to Reboot your computer to make these changes effective.
These are your current settings. Pleas save and close all other applications.

Database Name : C:\Program Files\Thermo\Foundation\Xcalibur Database.mdb
Database Type : DB_ACCESS
Database is Installed on Host : N/A
Database Service Name : N/A
User Name : N/A

● Restart Computer now
○ I will restart later

6. Select a restart option:

   - To automatically restart the computer after you click Finish, 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 Auditing Database Configuration Manager take effect after restarting the computer.

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

Auditing Database Configuration Manager Parameters

Use the Thermo Foundation Auditing Database Configuration Manager to select and configure the auditing database. Follow the instructions in the box at the top of the Auditing Database Configuration Manager wizard. You must restart your computer to make the changes effective.

Not all of the parameters are displayed at every step in the configuration process.

Note If you are using Oracle as the database back end, install at least one relational database on an accessible server and install the Oracle client on the system computer before using the Auditing Database Configuration Manager.

Table 2 describes the parameters for the Auditing Database Configuration Manager.

Table 2. Auditing Database Configuration Manager parameters (Sheet 1 of 3)

Parameter	Description
Read-only information	
Database Name	Displays the currently configured database. This line does not appear if this is the first time that you are running the Auditing Database Configuration Manager.
Database Type	Displays the database type. The database must be an Oracle database on a remote server or a Microsoft Access database on a local computer. This line does not appear if this is the first time that you are running the Auditing Database Configuration Manager.

Table 2. Auditing Database Configuration Manager parameters (Sheet 2 of 3)

Parameter	Description
Database Is Installed On Host	Displays where the Oracle database is installed on the host computer. (When using a Microsoft Access database, this line is blank.) This line does not appear if this is the first time that you are running the Auditing Database Configuration Manager.
Security Name	Displays the Oracle database service name. (When using a Microsoft Access database, this line is blank.) This line does not appear if this is the first time that you are running the Auditing Database Configuration Manager.
User Name	Displays the logon name for the Oracle database. (When using a Microsoft Access database, this line is blank.) This line does not appear if this is the first time that you are running the Auditing Database Configuration Manager.
Select Database Type area	
Oracle On Network Server	Select to use a remote server to run the Oracle database. You must enter a valid user name and password to access the database. When you select this option, the Oracle Net Service Name list appears below the Password box.
Microsoft Access	Select to use a local database based on Microsoft Access.
Additional parameters for the Oracle database selection	
User Name	Displays the Oracle database logon name. (When using a Microsoft Access database, this box is grayed out.)
Password	Displays the Oracle database password. (When using a Microsoft Access database, this box is grayed out.)
Oracle Net Service Name	Displays the name of the Oracle Net Service that the database administrator set up during the Oracle Client configuration that provides database connection information. All available names appear in the list. (When using a Microsoft Access database, this list does not appear.)
Final wizard page parameters	
Restart Computer Now	Restarts the computer automatically when you click Finish.

Table 2. Auditing Database Configuration Manager parameters (Sheet 3 of 3)

Parameter	**Description**
I Will Restart Later	Ends the database configuration without restarting the computer when you click Finish. You must restart your computer to make the changes effective.
Buttons	
Next	Moves to the second page of the Auditing Database Configuration Manager.
Exit	Closes the wizard without accepting the new entries.
Cancel	Returns to the first page of the wizard where you can change the entries.
OK	Accepts the entries and go to the Auditing Database Configuration Manager.
Finish	Closes the Auditing Database Configuration Manager. If you selected the Restart Computer Now option, save and close all other applications before clicking this button.

Establishing Secure File Operations

To allow for accurate and ready retrieval of data and preserve previously recorded information from being overwritten by record changes, store all electronic records in protected folders and establish standard operating procedures for precise and systematic record archiving.

Contents

Recovering the Xcalibur System Account

To support system security, the Foundation platform sets up the Xcalibur_System account. The account is not interactive. No one ever logs in to this account except the Xcalibur data system itself. The Foundation platform creates this account with administrative privileges. The account name and password are embedded.

The Xcalibur_System account is located in the following directory:

drive:\Users\Xcalibur_System

If you accidentally delete the Xcalibur_System account, recover it as follows.

❖ To recover the account name for the Foundation platform

Reinstall the Foundation platform.

Configuring the Thermo Foundation Services

The authorization and auditing functions of a layered application installed on the Thermo Foundation platform rely on two system services:

- Thermo Foundation Security Service for user authentication and secure file operations—If certain events require authentication, this service verifies the user names and passwords entered. You can set the Security Service to take ownership of the data folders and files. This security measure prevents users from deleting data they own. This service installs when you install the Xcalibur data system.
- Thermo Foundation Database Service—To access the auditing database and make auditing entries using any Thermo layered application. This service installs when you install the Foundation platform.

Both services automatically start whenever a user restarts a workstation.

Layered applications use the Thermo Foundation Database Service to access the auditing database and make auditing entries.

To ensure that these services operate correctly, follow these procedures:

- Opening the Services Window
- Confirming the Thermo Foundation Database Service Settings
- Configuring the Properties of Thermo Foundation Security Service

Opening the Services Window

You access the Thermo Foundation services from the Services window.

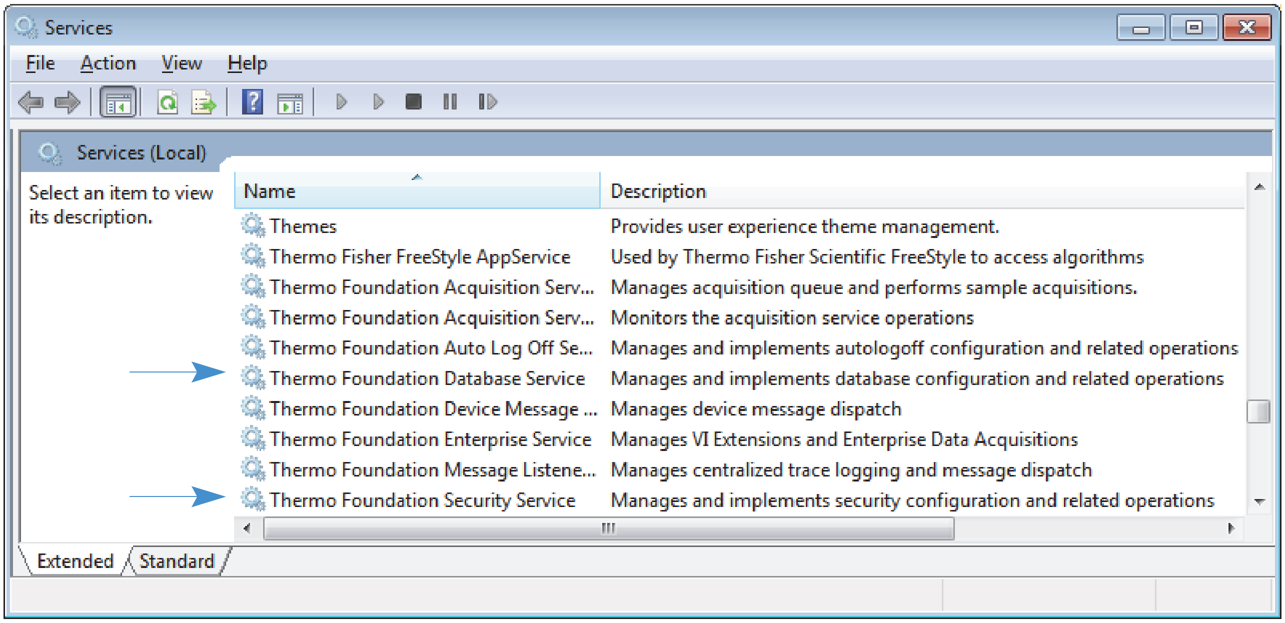
❖ **To open the Services window**

1. From the Windows taskbar, choose **Start > Control Panel**.
2. On the Adjust your computer’s settings page, do the following:
   a. In the View By list, select **Category**.
   b. Click **System and Security**.
3. On the System and Security page, click **Administrative Tools**.

4. Double-click **Services**.

   The Services window opens (Figure 6).

Figure 6. Services window with a view of the Thermo Foundation services



Select an item to view its description.

Name	Description
Themes	Provides user experience theme management.
Thermo Fisher FreeStyle AppService	Used by Thermo Fisher Scientific FreeStyle to access algorithms
Thermo Foundation Acquisition Serv...	Manages acquisition queue and performs sample acquisitions.
Thermo Foundation Acquisition Serv...	Monitors the acquisition service operations
Thermo Foundation Auto Log Off Se...	Manages and implements autologoff configuration and related operations
Thermo Foundation Database Service	Manages and implements database configuration and related operations
Thermo Foundation Device Message ...	Manages device message dispatch
Thermo Foundation Enterprise Service	Manages VI Extensions and Enterprise Data Acquisitions
Thermo Foundation Message Listene...	Manages centralized trace logging and message dispatch
Thermo Foundation Security Service	Manages and implements security configuration and related operations

Confirming the Thermo Foundation Database Service Settings

Make sure that the Allow Service to Interact with Desktop setting is set to No (clear check box).

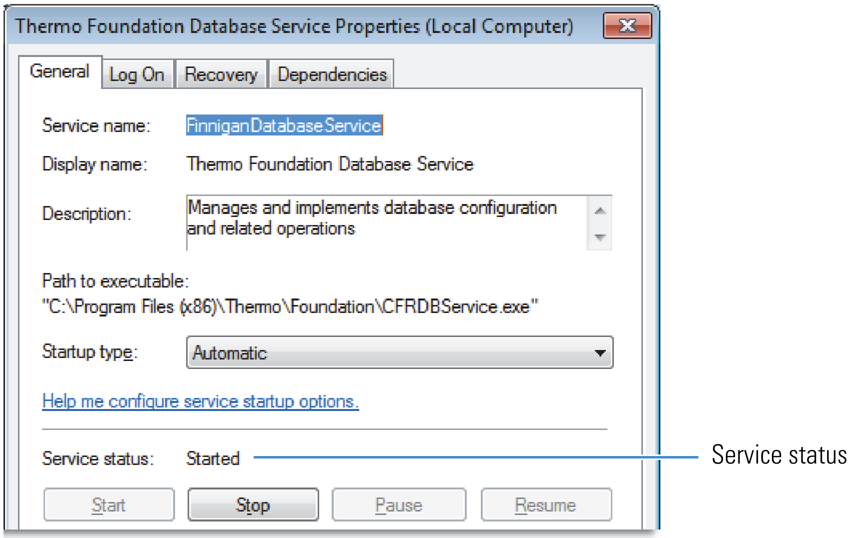
❖ To confirm that the Thermo Foundation Database Service is set correctly

1. Open the Services window. See "Opening the Services Window."

2. Double-click **Thermo Foundation Database Service**.

   The Thermo Foundation Database Service Properties dialog box opens to the General page (Figure 7).

Figure 7. Foundation Database Service Properties – General page



Thermo Foundation Database Service Properties (Local Computer)

General | Log On | Recovery | Dependencies

Service name: FinniganDatabaseService

Display name: Thermo Foundation Database Service

Description: Manages and implements database configuration and related operations

Path to executable:
"C:\Program Files (x86)\Thermo\Foundation\CFRDBService.exe"

Startup type: Automatic

Help me configure service startup options.

Service status: Started

Start | Stop | Pause | Resume

Service status

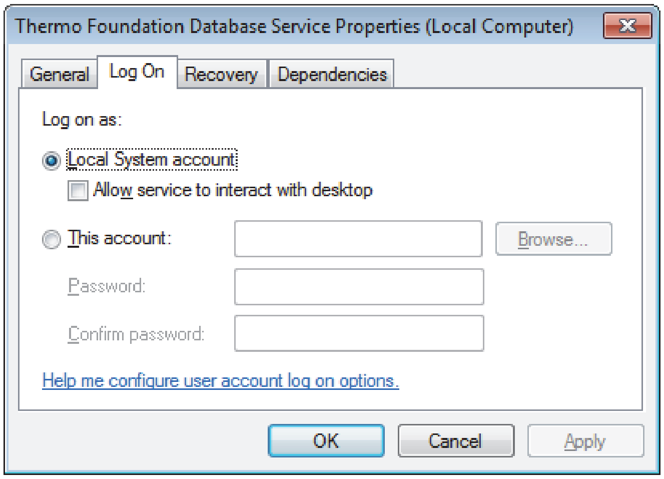
3. On the General page of the Database Service Properties dialog box, do the following:

   a. In the Startup Type list, select **Automatic**.

   b. Confirm that Service Status reads **Started**.

4. Click the **Log On** tab to display the Log On page (Figure 8).

Figure 8. Thermo Foundation Database Service Properties – Log On page



Thermo Foundation Database Service Properties (Local Computer)

General | Log On | Recovery | Dependencies

Log on as:

● Local System account

☐ Allow service to interact with desktop

○ This account: Browse...

Password:

Confirm password:

Help me configure user account log on options.

OK | Cancel | Apply

5. On the Log On page of the Thermo Foundation Database Service Properties dialog box, do the following:

   a. Under Log On As, select the **Local System Account** option.

   b. Clear the **Allow Service to Interact with Desktop** check box.

6. Click **OK** to close the dialog box.

7. Close the Services window and close the Administrative Tools window.

Configuring the Properties of Thermo Foundation Security Service

Make sure that the Allow Service to Interact with Desktop setting is set to Yes (select the check box).

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

❖ To configure the properties of the Thermo Foundation Security Service

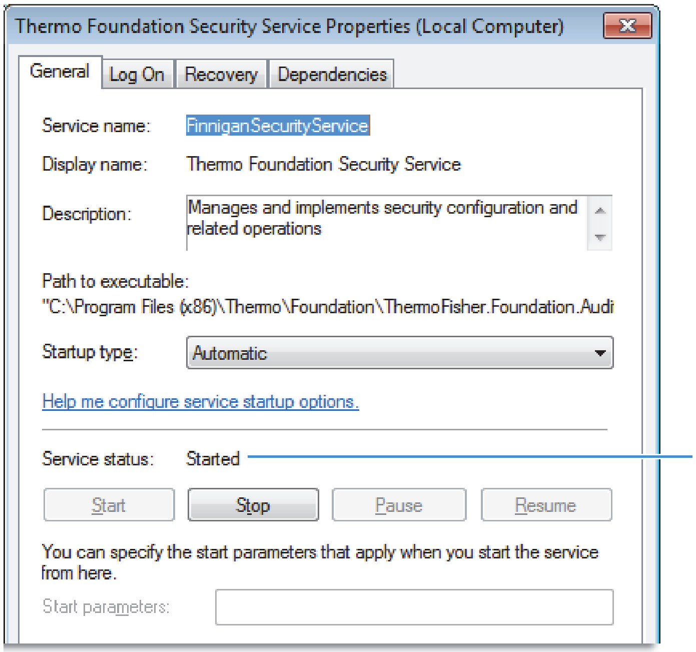
1. Open the Services window (see "Opening the Services Window" on page 20).
2. Double-click **Thermo Foundation Security Service**.

   The Thermo Foundation Security Service Properties dialog box opens to the General page.
3. On the General page of the Thermo Foundation Security Service Properties dialog box, do the following:

   a. Set the Startup Type to **Automatic**.

   b. Make sure that the Service Status reads **Started** (Figure 9).

Figure 9. Foundation Security Service Properties – General page


Thermo Foundation Security Service Properties (Local Computer)
General
Log On
Recovery
Dependencies
Help me configure service startup options.
Start
Stop
Pause
Resume
Service status

Service name: FinniganSecurityService
Display name: Thermo Foundation Security Service
Description: Manages and implements security configuration and related operations
Path to executable:
"C:\Program Files (x86)\Thermo\Foundation\ThermoFisher.Foundation.Audi
Startup type: Automatic
Service status: Started
You can specify the start parameters that apply when you start the service from here.
Start parameters:

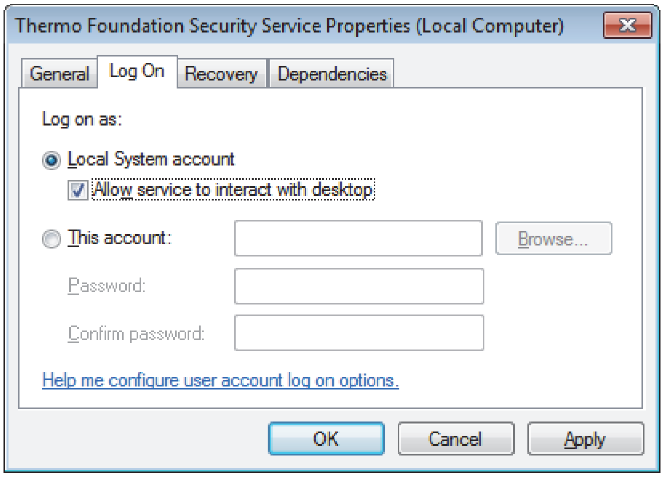
4. Click the **Log On** tab.

5. On the Log On page of the Security Service Properties dialog box, select the following:

   a. Select the **Local System Account** option.

   b. Select the **Allow Service to Interact with Desktop** check box (Figure 10).

Figure 10. Thermo Foundation Security Service Properties dialog box



Thermo Foundation Security Service Properties (Local Computer)

General | Log On | Recovery | Dependencies

Log on as:

● Local System account

☑ Allow service to interact with desktop

○ This account: Browse...

Password:

Confirm password:

Help me configure user account log on options.

OK Cancel Apply

6. Click **OK** to close the Thermo Foundation Security Service Properties dialog box.

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

> **Note** Once you set the properties of the Thermo Foundation Security Service, various actions can change the properties, such as IT policies that generally are passed down to computers. Review properties regularly to avoid changes that interfere with expected auditing behavior.

Configuring Security Settings for Folders and Files

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

- Foundation folder—Contains the executable (EXE) files, the dynamic library link (DLL) files, the log files, and so on that make up the Foundation platform.

  The Foundation folder is located in the following directory for Windows 7 (64 bit):

  drive:\Program Files (x86)\Foundation

- INI folder—Contains the configuration files. Because the Thermo Foundation Authorization Manager reads the controlled feature information from the configuration files, prohibit write or delete access to these files by non-administrators.

  The INI folder for the Windows 7 operating systems is located in *drive*:\ProgramData\Thermo Scientific.

Note The folder that contains the configuration files is hidden by default in Windows.

To make the INI folder appear, from the Windows 7 taskbar, choose **Start > Control Panel > Appearance and Personalization*** **> Folder Options > View > Hidden Files and Folders**, and select **Show Hidden Files and Folders**.

*If you do not see the Appearance and Personalization category, select **Category** in the View By list on the upper-right portion of the Adjust Your Computer's Settings page.

To add an administrative user (or administrative group) to the Security page Group, or to add a specific group or groups to the User Names list and grant the administrator full access to the security folder and read-only access to everyone else, follow these procedures:

1. Configuring Security Settings for the Root Folder
2. Adding and Removing Users Within Folders
3. Setting Folder Permissions for Users and Groups

Tip When you require more restricted access to folders and files, grant access only to specific user groups. To set up appropriate user groups, see "Using the Authorization Manager" on page 50.

As you follow these procedures, use your specific user group.

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 a group or groups to the Permission Entries 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 and Removing Users Within Folders" on page 30, and then perform the procedures that follow, using your specific user groups.

To prepare a root folder, first turn off Use Sharing Wizard in the Folder Options dialog box. You can then create a root folder for storing all your projects.

Follow these procedures:

- To turn off the File Sharing Wizard
- To create or locate a folder to use as the root folder for storing all projects

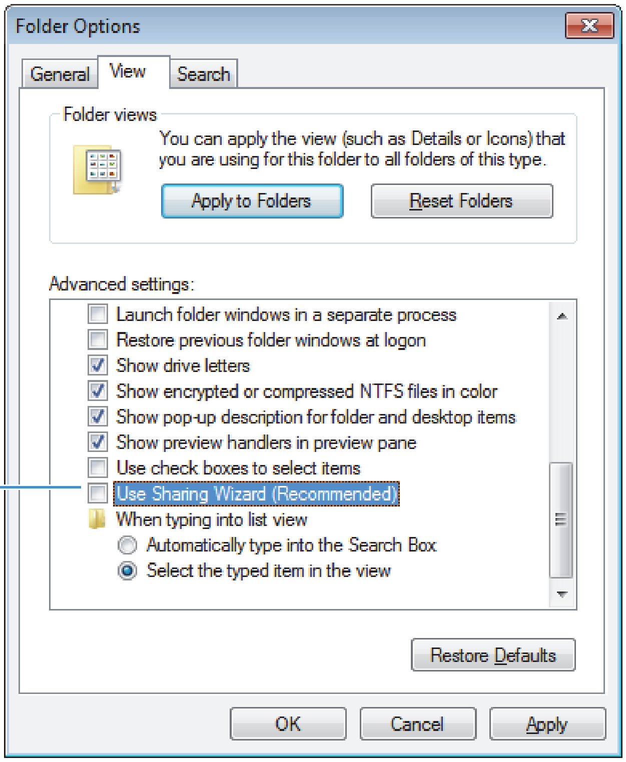
❖ To turn off the File Sharing Wizard

1. Log on to the system as a user with administrative privileges.
2. From the Windows taskbar, choose **Start > All Programs > Accessories > Windows Explorer**.
3. In the upper-left side of the view, choose **Organize > Folder and Search Options**.

   The Folder Options dialog box opens.
4. Click the **View** tab.

5. In the Advanced Settings list, at the bottom, clear the **Use Sharing Wizard** check box (Figure 11).

Figure 11. Folder Options – View page



Folder views

You can apply the view (such as Details or Icons) that you are using for this folder to all folders of this type.

Advanced settings:

□ Launch folder windows in a separate process
□ Restore previous folder windows at logon
☑ Show drive letters
☑ Show encrypted or compressed NTFS files in color
☑ Show pop-up description for folder and desktop items
☑ Show preview handlers in preview pane
□ Use check boxes to select items
□ Use Sharing Wizard (Recommended)
When typing into list view
○ Automatically type into the Search Box
● Select the typed item in the view

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).

   In this example, the folder is named Study.

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

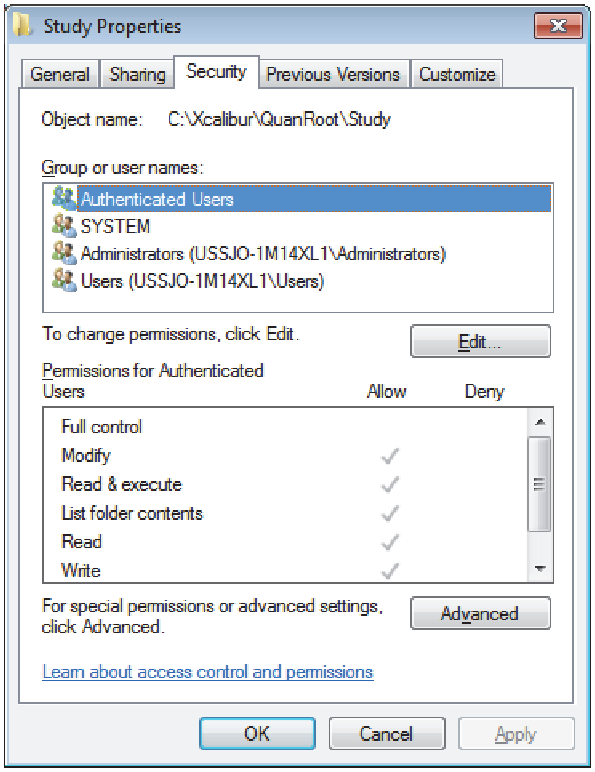
   IMPORTANT Do not use the Xcalibur folder as your root folder. If you change the permission settings for this folder, Xcalibur applications will not run correctly. Instead, create a new folder or use another existing folder as your root folder.

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

   The Properties dialog box for the folder opens.

3. Click the **Security** tab (Figure 12).

Figure 12. Properties dialog box – Security tab



Object name: C:\Xcalibur\QuanRoot\Study

Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (USSJO-1M14XL1\Administrators)
- Users (USSJO-1M14XL1\Users)

To change permissions, click Edit.

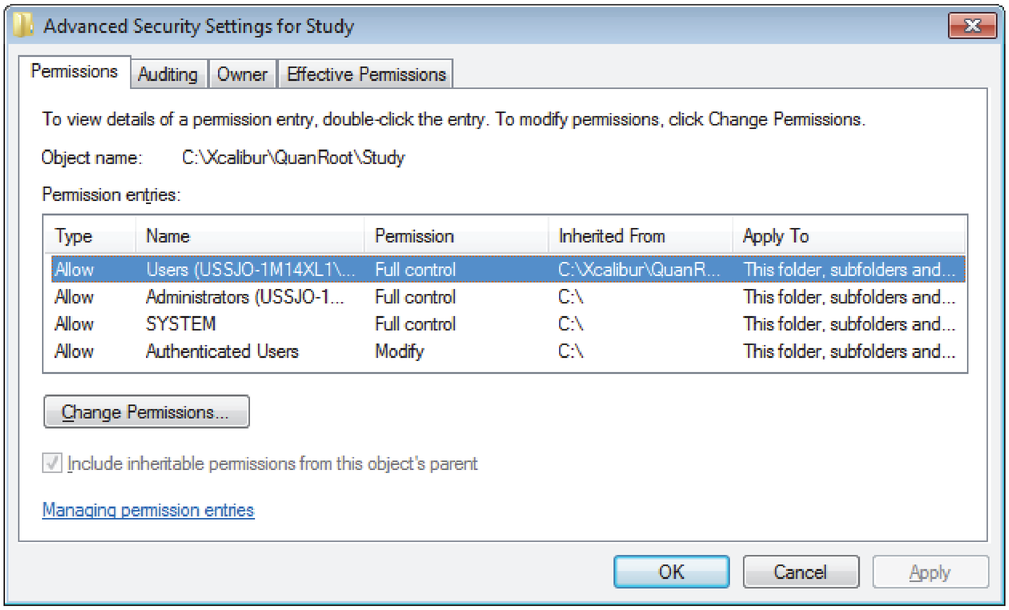
Permissions for Authenticated Users	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

4. Click **Advanced**.

The Permissions page of the Advanced Security Settings for Study dialog box opens (Figure 13).

Figure 13. Properties dialog box – Security tab – Advanced Settings



To view details of a permission entry, double-click the entry. To modify permissions, click Change Permissions.

Object name: C:\Xcalibur\QuanRoot\Study

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Users (USSJO-1M14XL1\...	Full control	C:\Xcalibur\QuanR...	This folder, subfolders and...
Allow	Administrators (USSJO-1...	Full control	C:\	This folder, subfolders and...
Allow	SYSTEM	Full control	C:\	This folder, subfolders and...
Allow	Authenticated Users	Modify	C:\	This folder, subfolders and...

☑ Include inheritable permissions from this object's parent

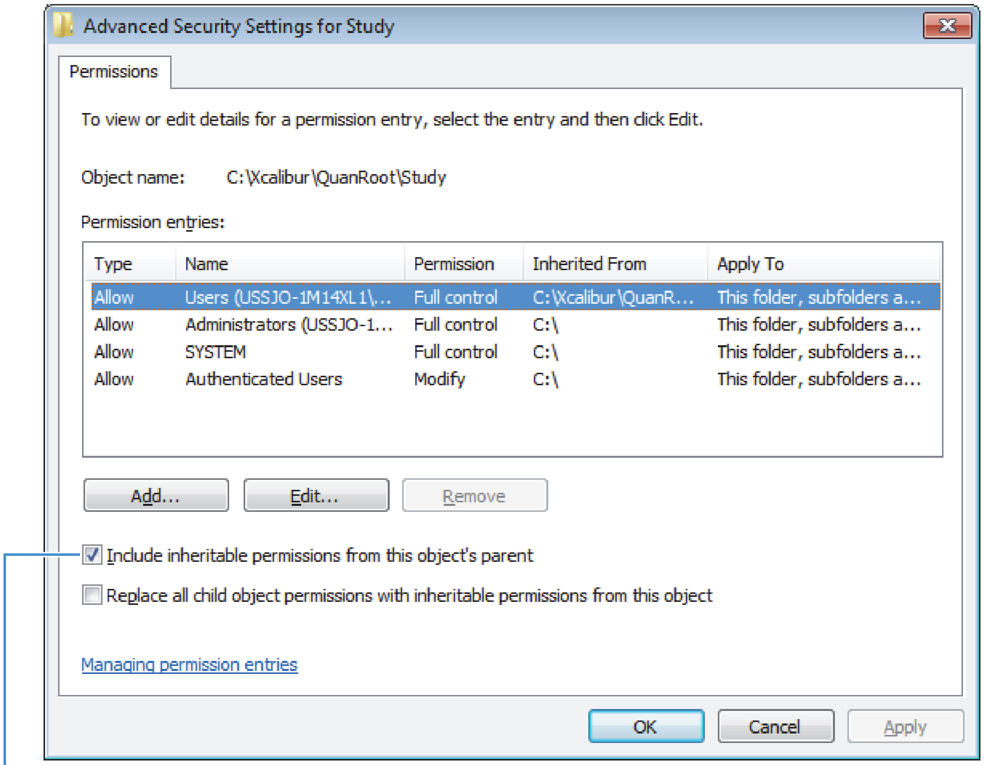
When you create a new root folder, the permissions from the parent folder automatically propagate to the new folder, indicated by shaded check boxes in the Permissions list.

In the Advanced Security Settings dialog box, the check box labeled "Include inheritable permissions from this object's parent" is automatically selected and grayed out. For a root folder, you must change this option.

> **IMPORTANT** Normally, you do not want to allow your secure root folder to inherit permissions from the parent folder. If someone changes the permission settings of the parent folder, the permission settings of the new root folder do not change if you select the Inherit From Parent… option.
>
> Prevent this inheritance by clearing the Inherit From Parent… check box in the next steps. Then correct the permissions in the section "Setting Folder Permissions for Users and Groups" on page 35.
>
> Subfolders created under the new root folder still inherit the permissions from the root folder.

5. Click **Change Permissions** to display the permission entries (Figure 14).

Figure 14. Advanced Security Settings for *Selected Folder* dialog box



Advanced Security Settings for Study

To view or edit details for a permission entry, select the entry and then click Edit.

Object name: C:\Xcalibur\QuanRoot\Study

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Users (USSJO-1M14XL1\…	Full control	C:\Xcalibur\QuanR…	This folder, subfolders a…
Allow	Administrators (USSJO-1…	Full control	C:\	This folder, subfolders a…
Allow	SYSTEM	Full control	C:\	This folder, subfolders a…
Allow	Authenticated Users	Modify	C:\	This folder, subfolders a…

☑ Include inheritable permissions from this object's parent

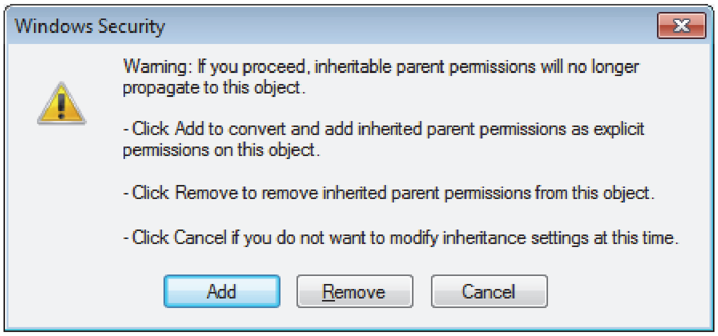
☐ Replace all child object permissions with inheritable permissions from this object

Clear this check box.

6. Clear the **Include Inheritable Permissions…** check box.

   The Windows Security dialog box opens (Figure 15).

   Figure 15. Windows Security dialog box



Windows Security

Warning: If you proceed, inheritable parent permissions will no longer propagate to this object.

- Click Add to convert and add inherited parent permissions as explicit permissions on this object.

- Click Remove to remove inherited parent permissions from this object.

- Click Cancel if you do not want to modify inheritance settings at this time.

7. To copy the inherited permissions to the new folder, click **Add**.

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

   You will correct the permission settings later.

9. On the Security page of the Properties dialog box, examine the Group or User Names list and notice which groups or users appear in the list.

   You want only your selected group or groups 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 "Adding and Removing Users Within Folders."
   - If both appear in the list, and additional groups or users also appear in the list, go to "Removing Unnecessary Users from Folders" on page 34.
   - If both appear in the list, and no additional groups or users appear in the list, go to "Setting Folder Permissions for Users and Groups" on page 35.

Adding and Removing Users Within Folders

Before setting permission levels for a folder or registry key, you might need to modify the Groups or User Names list on the Security page for the folder by adding or removing users as described in these topics:

- Adding Users to Folders
- Removing Unnecessary Users from Folders

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.

Adding Users to Folders

To modify the users list for the INI and Foundation folders, follow these procedures:

- To add users and groups to a folder
- To remove users or groups from the Group or User Names list

❖ To add users and groups to a folder

1. Using Windows Explorer, locate the folder of interest: INI or Foundation.

   Note By default, the Foundation and INI folders are in these directories.

   - For Windows 7 (64 bit), the Foundation folder is located in the following directory:

     drive:\Program Files (x86)\Thermo

   - For Windows 7, the INI folder is located in the following directory:

     drive:\ProgramData\Thermo Scientific\

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

   The *Folder Name* Properties dialog box opens.

3. If the Security page is unavailable, do the following:

   a. Choose **Start > Control Panel.**

   b. Choose **Appearance and Personalization > Folder Options.**

      The Folder Options dialog box opens.

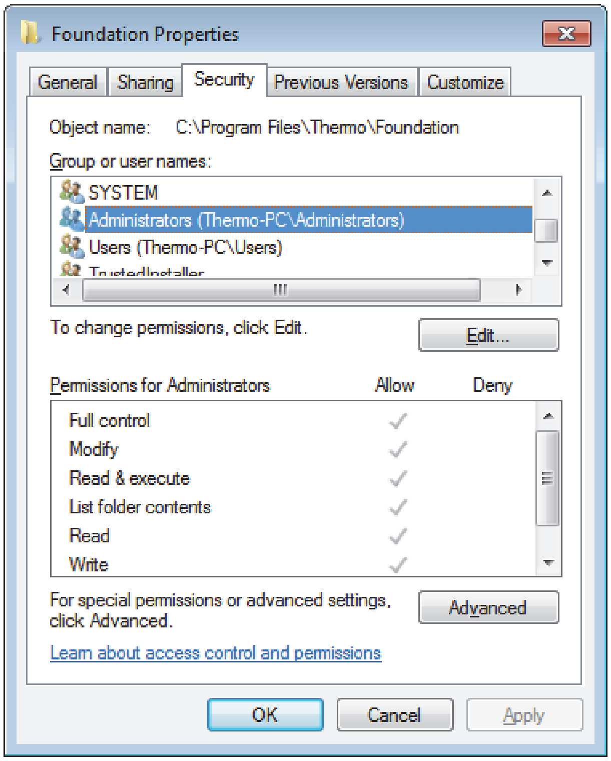
   c. Click the **View** tab.

   d. In the Advanced Settings box, clear the **Use Sharing Wizard** check box, and then click **OK** to accept the setting and close the Folder Options dialog box.

   e. Close the Control Panel.

4. Click the **Security** tab to display the Security page (Figure 16).

Figure 16. Foundation Properties – Security page



Object name: C:\Program Files\Thermo\Foundation

Group or user names:

- SYSTEM
- Administrators (Thermo-PC\Administrators)
- Users (Thermo-PC\Users)
- TrustedInstaller

To change permissions, click Edit.

Permissions for Administrators	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

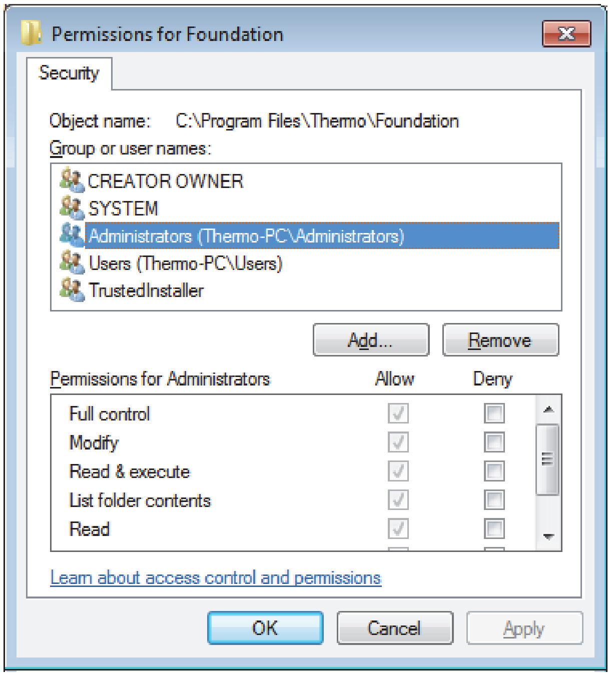
For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

5. Click **Edit**.

The Permissions for *Folder Name* dialog box opens (Figure 17).

Figure 17. Permissions for *Folder Name* dialog box



Object name: C:\Program Files\Thermo\Foundation

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (Thermo-PC\Administrators)
- Users (Thermo-PC\Users)
- TrustedInstaller

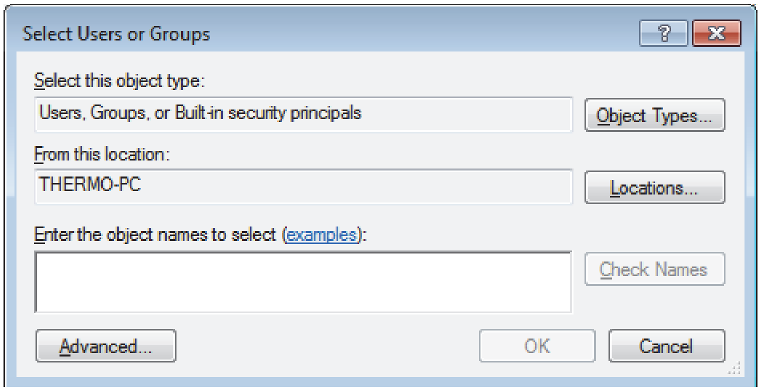
Permissions for Administrators	Allow	Deny
Full control	☑	☐
Modify	☑	☐
Read & execute	☑	☐
List folder contents	☑	☐
Read	☑	☐

Learn about access control and permissions

6. To add users or groups, click **Add**.

   The Select Users or Groups dialog box opens. To select a user or a group, the Select This Object Type list must contain the appropriate object types and the From This Location box must contain the root location of your users and groups as shown in Figure 18.

Figure 18. Select Users or Groups dialog box



Select Users or Groups

Select this object type:
Users, Groups, or Built-in security principals

From this location:
THERMO-PC

Enter the object names to select (examples):

7. Confirm 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 (for example, Users and Administrator) and click **OK**.

8. Confirm 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**.

9. In the Enter the Object Names to Select box, enter the new users or groups:

   - If the name of a specific user group was missing from the Group or User Names list on the Security page, type the name of the group.

   - If the user name of the administrator (or the name of the administrator group) was missing from the Group or User Names list on the Security page, type the user name or group name.

   > **Tip** To enter multiple object names at the same time, separate the names with a semicolon.

10. To verify that the new user or group name is now in the list, do the following:

    a. Click **Check Names** to search for users or groups with the names that you specified in the Enter the Object Names to Select box.

       All similar or matching object names that were found appear underlined in the box.

    b. Confirm that only the correct object name or names are listed in the box. Then click **OK** to close the Select Users or Groups dialog box and return to the Permissions for *Folder Name* dialog box.

11. Examine the Group or User Names list again.

    The user groups and the name of the administrator are now available in the list.

    - When additional groups or users appear in the Group or User Names list, go to "Removing Unnecessary Users from Folders."

    - If no additional groups or users appear, go to "Setting Folder Permissions for Users and Groups" on page 35.

❖ To remove users or groups from the Group or User Names list

1. If it is not already open, open the Permissions for *Folder Name* dialog box (see step 1 through step 5 of "To add users and groups to a folder" on page 31).

2. For each user of group that you want to remove, do the following:

   a. Select the name of the user or group.

   b. Click **Remove** to remove the selected user or group.

You are now ready to set the permission levels for your users and groups.

Removing Unnecessary Users from Folders

You must remove unnecessary users or groups from the Group or User Names box on the Security page.

❖ To remove the names of unnecessary users or groups

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

   The Permissions dialog box opens.

2. In the Group or User Names box, select the name of the unnecessary user or group and click **Remove**.

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

Setting Folder Permissions for Users and Groups

After the correct users and groups are in the Group or User Names list on the Security page of the *Folder Name* Properties dialog box, set the folder permissions for the users and groups.

❖ To set the permissions for users and groups

1. Open the Security page for the folder as follows:

   a. Right-click the folder and choose Properties.

      The Properties dialog box opens.

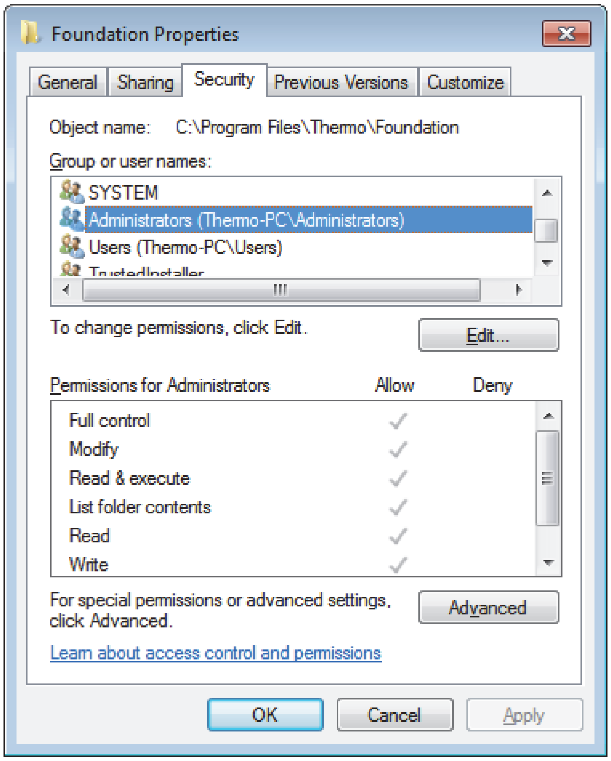
   b. Click the **Security** tab.

2. Set up the permission levels for the administrator as follows:

   a. In the Group or User Names list, select the administrator (or the administrator group) and click **Edit**.

      The Permissions for Folder dialog box opens (Figure 19).

Figure 19. *Folder Name* Properties dialog box



Object name: C:\Program Files\Thermo\Foundation

Group or user names:

SYSTEM
Administrators (Thermo-PC\Administrators)
Users (Thermo-PC\Users)
TrustedInstaller

To change permissions, click Edit.

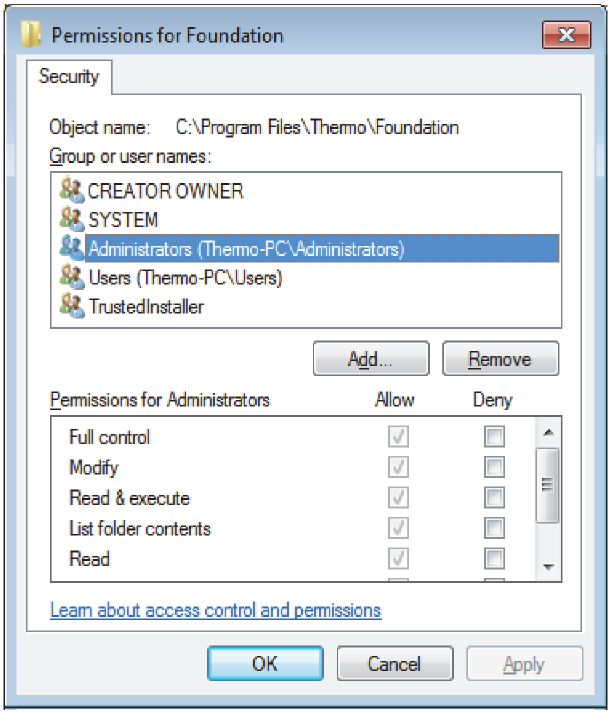
Permissions for Administrators	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

b. In the Permissions for *Folder Name* dialog box, select the **Allow** check box for the Full Control option.

All of the other check boxes in the Allow column are automatically selected (Figure 20).

Figure 20. Permissions for *Folder Name* dialog box



Permissions for Foundation

Security

Object name: C:\Program Files\Thermo\Foundation

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (Thermo-PC\Administrators)
- Users (Thermo-PC\Users)
- TrustedInstaller

Permissions for Administrators	Allow	Deny
Full control	☑	☐
Modify	☑	☐
Read & execute	☑	☐
List folder contents	☑	☐
Read	☑	☐

Note Groups or users granted Full Control for a folder can delete files and subfolders within that folder regardless of the permissions protecting the files and subfolders.

3. Set up the permissions levels for a group as follows:

a. In the Group or User Names list, select the group name.

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

Note Setting these permissions confirms that you cannot delete any of the files in the folder using Windows Explorer.

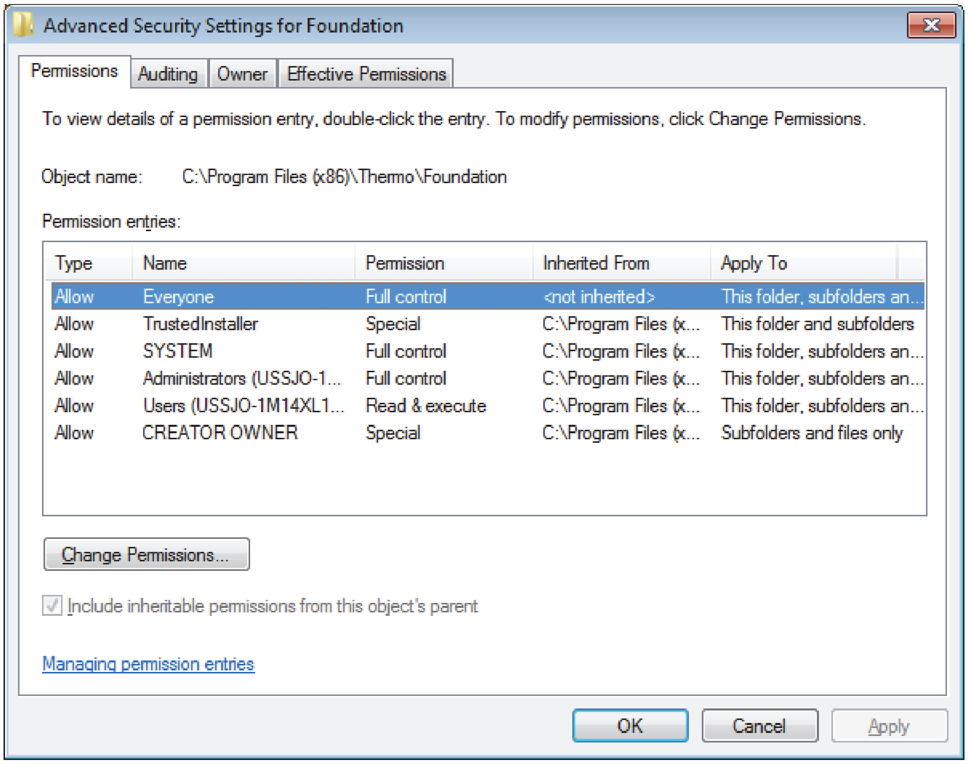
4. Click **OK** to close the Permissions for Foundation dialog box and return to the Security page of the Foundation Properties dialog box.

5. To confirm that the inheritance setting is correct, do the following:

   a. On the Security page, click **Advanced**.

   The Advanced Security Settings dialog box opens (Figure 21).

Figure 21. Advanced Security Settings for *Folder Name*



To view details of a permission entry, double-click the entry. To modify permissions, click Change Permissions.

Object name: C:\Program Files (x86)\Thermo\Foundation

Permission entries:

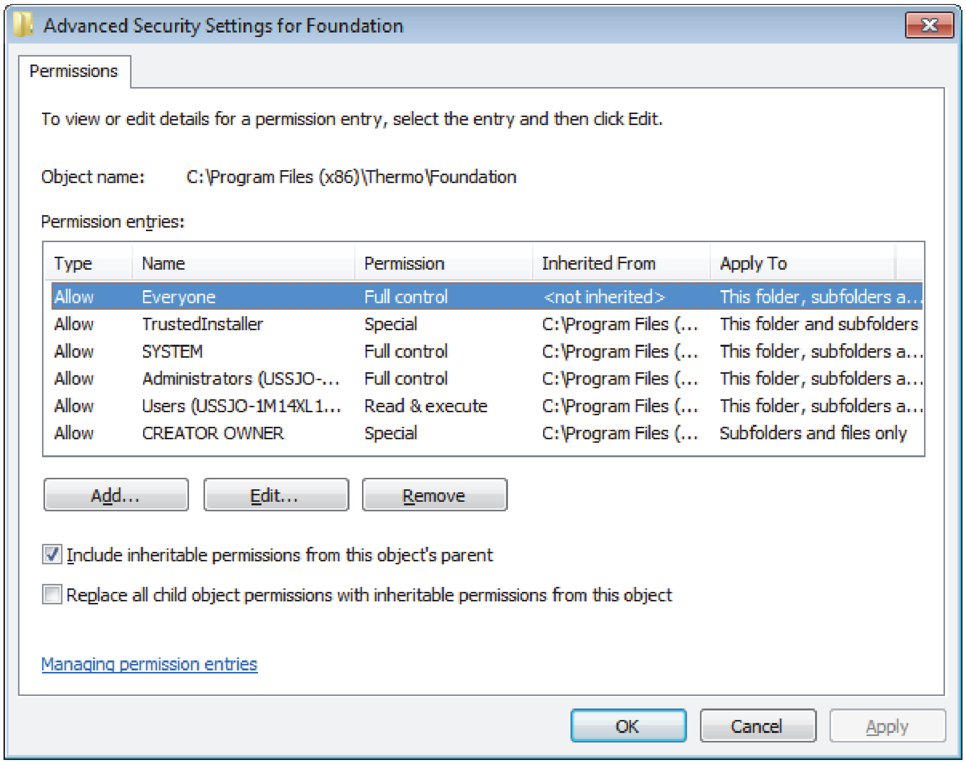
Type	Name	Permission	Inherited From	Apply To
Allow	Everyone	Full control	<not inherited>	This folder, subfolders an...
Allow	TrustedInstaller	Special	C:\Program Files (x...	This folder and subfolders
Allow	SYSTEM	Full control	C:\Program Files (x...	This folder, subfolders an...
Allow	Administrators (USSJO-1...	Full control	C:\Program Files (x...	This folder, subfolders an...
Allow	Users (USSJO-1M14XL1...	Read & execute	C:\Program Files (x...	This folder, subfolders an...
Allow	CREATOR OWNER	Special	C:\Program Files (x...	Subfolders and files only

☑ Include inheritable permissions from this object's parent

b. Click **Change Permissions**.

The Permissions page opens (Figure 22).

Figure 22. Advanced Security Settings – Permissions page



Advanced Security Settings for Foundation

Permissions

To view or edit details for a permission entry, select the entry and then click Edit.

Object name: C:\Program Files (x86)\Thermo\Foundation

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Everyone	Full control	<not inherited>	This folder, subfolders a...
Allow	TrustedInstaller	Special	C:\Program Files (...	This folder and subfolders
Allow	SYSTEM	Full control	C:\Program Files (...	This folder, subfolders a...
Allow	Administrators (USSJO-...	Full control	C:\Program Files (...	This folder, subfolders a...
Allow	Users (USSJO-1M14XL1...	Read & execute	C:\Program Files (...	This folder, subfolders a...
Allow	CREATOR OWNER	Special	C:\Program Files (...	Subfolders and files only

☑ Include inheritable permissions from this object's parent

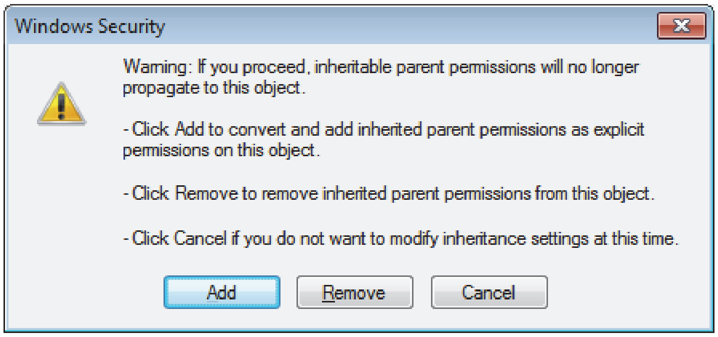
☐ Replace all child object permissions with inheritable permissions from this object

Managing permission entries

c. Clear the **Include Inheritable Permissions from This Object's Parent** check box.

The Windows Security dialog box opens (Figure 23).

Figure 23. Windows Security dialog box



Windows Security

Warning: If you proceed, inheritable parent permissions will no longer propagate to this object.

- Click Add to convert and add inherited parent permissions as explicit permissions on this object.

- Click Remove to remove inherited parent permissions from this object.

- Click Cancel if you do not want to modify inheritance settings at this time.

d. Click **Add** and then **OK** to close the dialog box and return to the Permissions page.

e. Click **OK** to return to the Security page.

6. Click **OK** to close the *Folder Name* Properties dialog box and save the permission assignments.

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 give full access rights only to the administrator and give 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:\ProgramData\Thermo Scientific\INI

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

   The Properties dialog box opens.

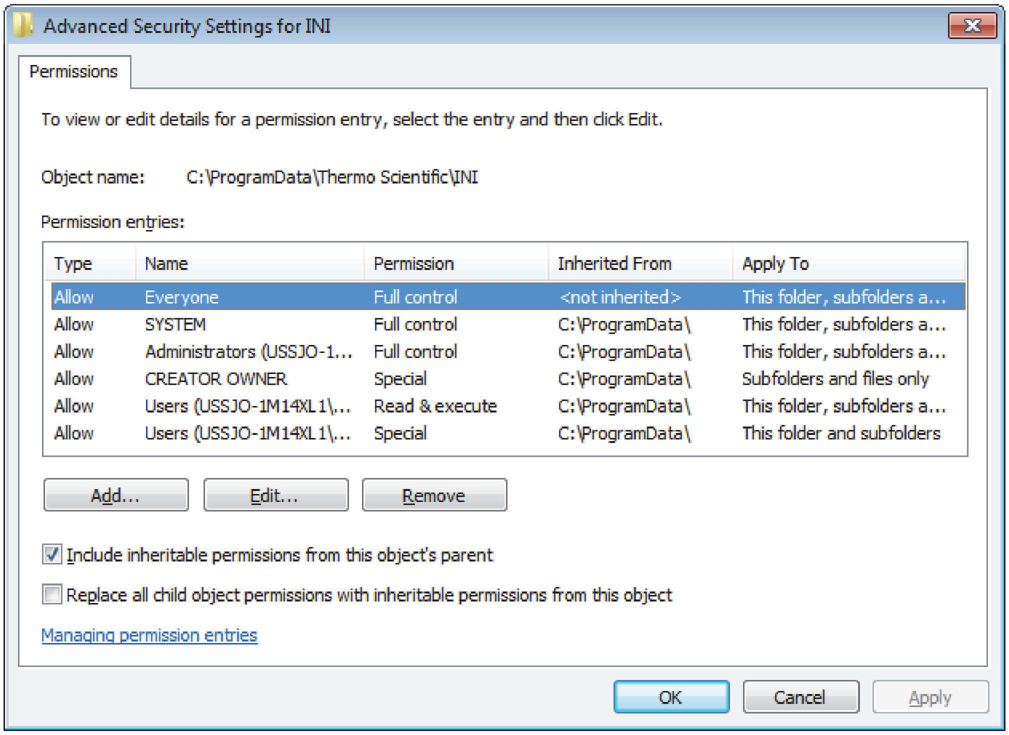
3. Click the **Security** tab.

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

5. Click **Change Permissions**.

   The Permissions page opens (Figure 24).

Figure 24. Permissions page for the INI folder


Advanced Security Settings for INI
Permissions
Add...
Edit...
Remove
Managing permission entries
OK
Cancel
Apply

To view or edit details for a permission entry, select the entry and then click Edit.

Object name: C:\ProgramData\Thermo Scientific\INI

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Everyone	Full control	<not inherited>	This folder, subfolders a...
Allow	SYSTEM	Full control	C:\ProgramData\	This folder, subfolders a...
Allow	Administrators (USSJO-1...	Full control	C:\ProgramData\	This folder, subfolders a...
Allow	CREATOR OWNER	Special	C:\ProgramData\	Subfolders and files only
Allow	Users (USSJO-1M14XL1\...	Read & execute	C:\ProgramData\	This folder, subfolders a...
Allow	Users (USSJO-1M14XL1\...	Special	C:\ProgramData\	This folder and subfolders

☑ Include inheritable permissions from this object's parent

☐ Replace all child object permissions with inheritable permissions from this object

6. Clear the **Include Inheritable Permissions from This Object's Parent** check box.
7. When the Windows Security dialog box opens, click **Add**.
8. Confirm that the Permission Entries box contains only your administrator name (or the administrator group) and the groups you want to add.
    - If Administrator (or the Administrator group) does not appear in the list, add it.
    - If a group does not appear in the list, add it.
    - If any other users or groups appear in the list, select and remove them.
9. Set the permissions for the folder:
    a. In the Permission Entries box, select **Administrator**.
    b. Click **Edit**.
    c. In the Permissions list, select the **Allow** check box for Full Control.

    All the other Allow check boxes are automatically selected.

    d. Click **OK**.
    e. In the Permission Entries box, select the group name.
    f. Click **Edit**.
    g. In the Permissions list, select the **Allow** check box for Read and clear the **Allow** check box for all the other options to prevent removal of information.
    h. In the Advanced Security Settings dialog box, confirm that the **Inherit From Parent…** check box is cleared.
    i. Click **OK** twice to close the Advanced Security Settings dialog box.
10. Click **OK** to save the permission assignments and close the Properties dialog box.

Configuring Security Settings for the Database Registry Key

When you run the Database Configuration tool for the first time, the tool creates a Windows 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.

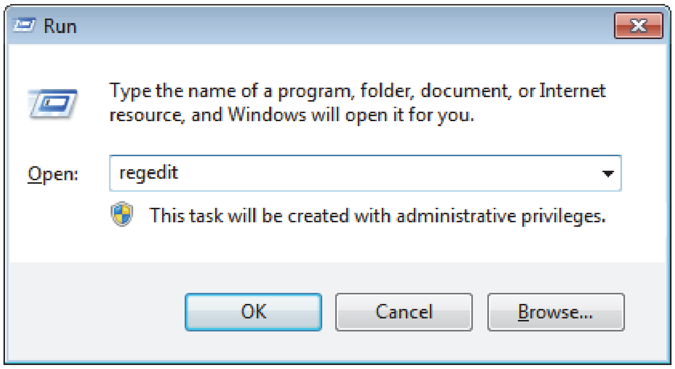
Note You must configure the database registry key whenever you create a new global database.

❖ To configure the security settings for the database registry key

1. From the Windows taskbar, choose **Start > Run**.

   The Run dialog box opens (Figure 25).

   Figure 25. Run dialog box



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

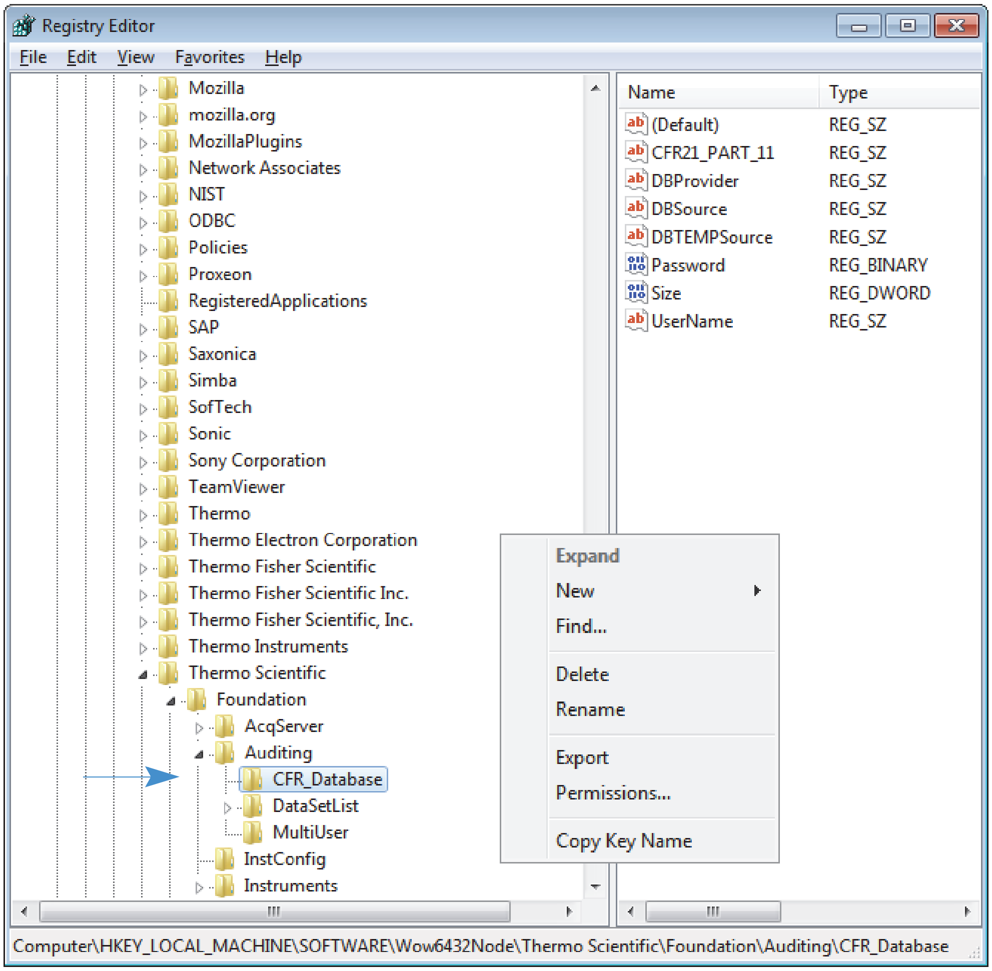
Open: regedit

This task will be created with administrative privileges.

2. Type **regedit** and click **OK**.

   The Registry Editor window opens (Figure 26).

Figure 26. Registry Editor dialog box with the CFR_Database key selected



Name	Type
(Default)	REG_SZ
CFR21_PART_11	REG_SZ
DBProvider	REG_SZ
DBSource	REG_SZ
DBTEMPSource	REG_SZ
Password	REG_BINARY
Size	REG_DWORD
UserName	REG_SZ

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Thermo Scientific\Foundation\Auditing\CFR_Database

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

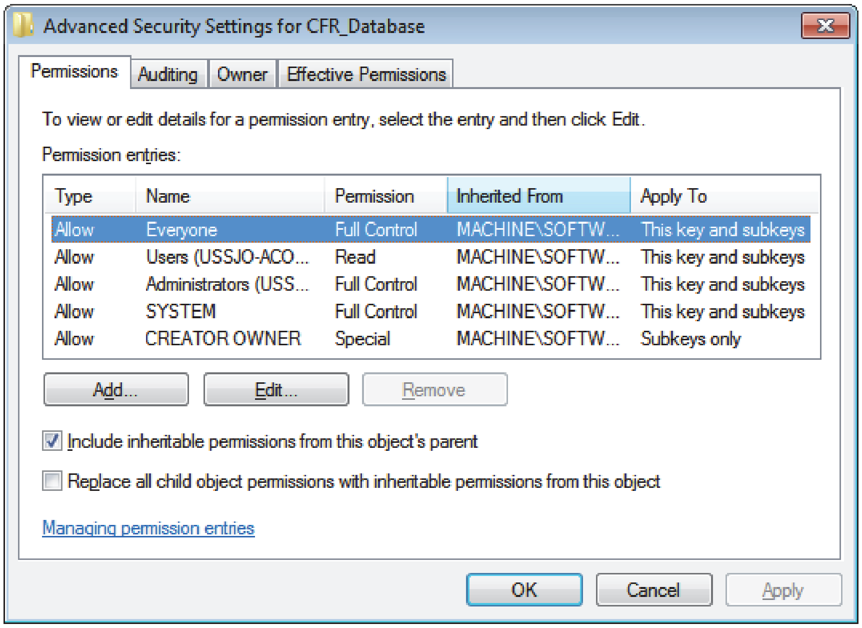
   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Thermo Scientific\Foundation\Auditing\CFR_Database

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 (Figure 27).

Figure 27. Advanced Security Settings dialog box



To view or edit details for a permission entry, select the entry and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Everyone	Full Control	MACHINE\SOFTW...	This key and subkeys
Allow	Users (USSJO-ACO...	Read	MACHINE\SOFTW...	This key and subkeys
Allow	Administrators (USS...	Full Control	MACHINE\SOFTW...	This key and subkeys
Allow	SYSTEM	Full Control	MACHINE\SOFTW...	This key and subkeys
Allow	CREATOR OWNER	Special	MACHINE\SOFTW...	Subkeys only

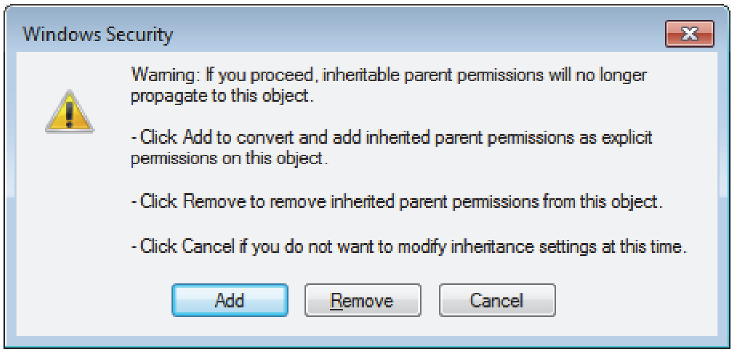
☑ Include inheritable permissions from this object's parent

□ Replace all child object permissions with inheritable permissions from this object

6. Clear the **Include Inheritable Permissions from This Object's Parent** check box.

The Windows Security dialog box opens (Figure 28).

Figure 28. Windows Security dialog box



Warning: If you proceed, inheritable parent permissions will no longer propagate to this object.

- Click Add to convert and add inherited parent permissions as explicit permissions on this object.

- Click Remove to remove inherited parent permissions from this object.

- Click Cancel if you do not want to modify inheritance settings at this time.

7. Click **Add** to copy the inherited parent permissions to the CFR_Database registry key.

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

9. On the Security page of the Permissions 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 your selected group or groups to appear in this box.

   - If your administrator name (or the administrator group) does not appear in the box, add it. (See "Adding Users to Folders" on page 31.)
   - If the group you want to use does not appear in the box, add it. (See "Adding Users to Folders" on page 31.)
   - If other users or groups appear in the box, remove them. (See "Removing Unnecessary Users from Folders" on page 34.)

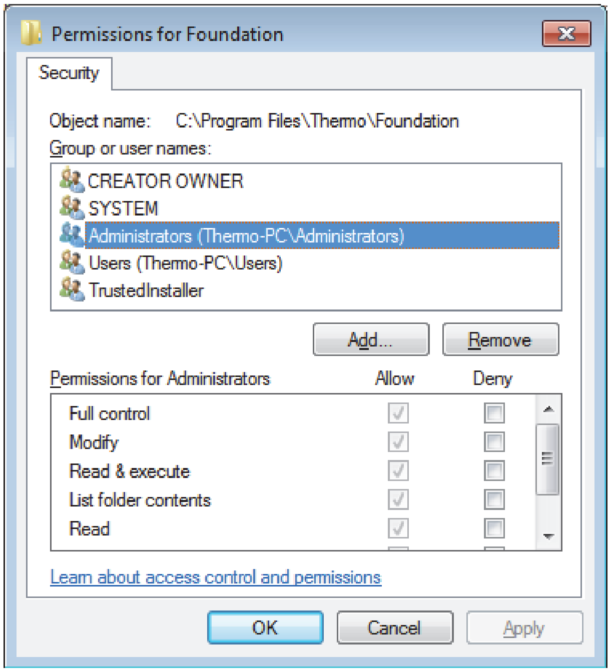
10. Set the permissions for the registry key:

    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 (Figure 29).

Figure 29. Permissions for CFR_Database dialog box



Permissions for Foundation

Security

Object name: C:\Program Files\Thermo\Foundation

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (Thermo-PC\Administrators)
- Users (Thermo-PC\Users)
- TrustedInstaller

Permissions for Administrators	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

    c. In the Group or User Names box, select a group name.

    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 to prevent removal of information.

11. Click **OK**.

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

Specifying the Way Users Log On and Off

To set up the way users log on and log off, follow these procedures:

- Turning Off Fast User Switching for Local Workstations
- Setting the Automatic Logoff Feature

Turning Off Fast User Switching for Local Workstations

To maintain secure file operations, turn off Fast User Switching on all computers that provide this option. The Windows 7 operating system provides Fast User Switching on all computers. Check with your IT group to see if they have applied global settings that cause an unexpected response to turning off this feature.

Starting with Windows 7, 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.

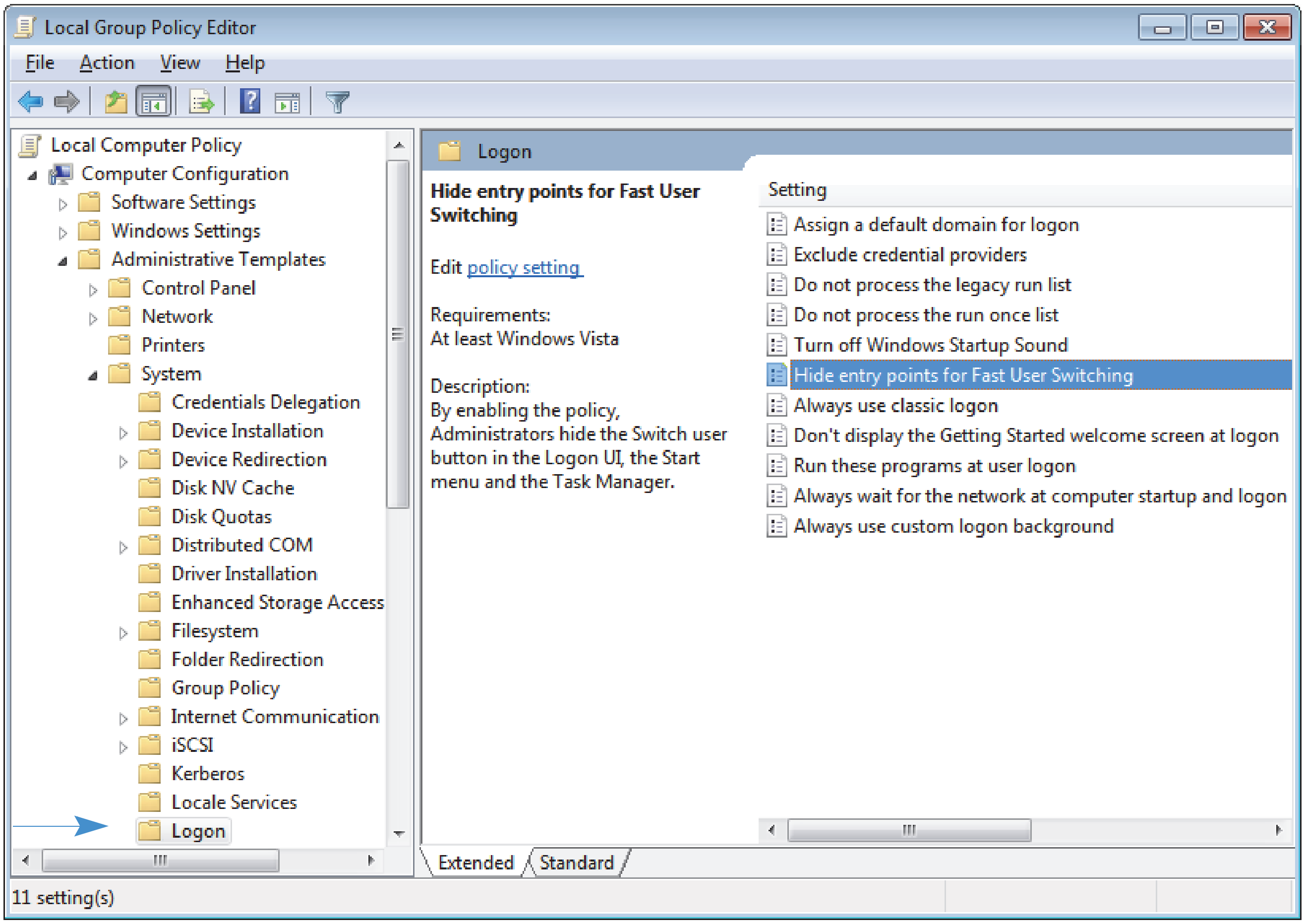
If you do not turn off Fast User Switching when it is allowed, two users could log on at the same time, which can cause strange behavior when they try to control their mass spectrometer. The acquisition service can only handle one user logged in at a time. Thermo Fisher Scientific recommends that all labs turn off Fast User Switching, regardless of whether secure file operations is important to the user or not.

❖ To turn off Fast User Switching

1. From the Windows taskbar, choose **Start**.
2. In the search box, type **gpedit.msc**.
3. Click **gpedit.msc** in the Programs list.

   The Local Group Policy Editor opens.
4. In the Local Computer Policy pane, choose **Computer Configuration** > **Administrative Templates** > **System** > **Logon** to display the Logon options (Figure 30).

Figure 30. Local Group Policy Editor with Logon selected



Logon

Hide entry points for Fast User Switching

Edit policy setting

Requirements:
At least Windows Vista

Description:
By enabling the policy, Administrators hide the Switch user button in the Logon UI, the Start menu and the Task Manager.

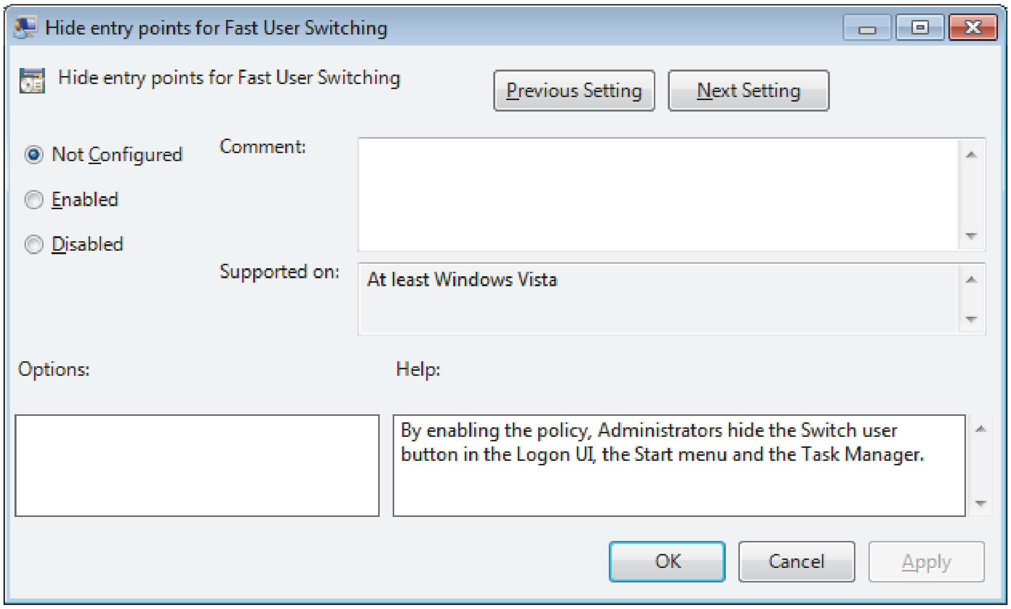
Setting
Assign a default domain for logon
Exclude credential providers
Do not process the legacy run list
Do not process the run once list
Turn off Windows Startup Sound
Hide entry points for Fast User Switching
Always use classic logon
Don't display the Getting Started welcome screen at logon
Run these programs at user logon
Always wait for the network at computer startup and logon
Always use custom logon background

11 setting(s)

5. Under Setting, double-click **Hide Entry Points for Fast User Switching**.

   The Hide Entry Points for Fast User Switching dialog box opens (Figure 31).

Figure 31. Hide Entry Points for Fast User Switching dialog box



Hide entry points for Fast User Switching

Hide entry points for Fast User Switching

● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Help: By enabling the policy, Administrators hide the Switch user button in the Logon UI, the Start menu and the Task Manager.

6. Select the **Enabled** option and click **OK**.

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

Setting the Automatic Logoff Feature

Use the Automatic Logoff feature to allow a user to log on to a workstation, start data acquisition, and then log off while the system continues to acquire the data. A subsequent user can log on to the workstation, queue acquisition sequences, and process data while the acquisition that the first user started continues.

Automatic logoff cannot occur if a password-protected screen saver precedes it. Automatic logoff can occur if the screen saver is not password-protected, but you are not notified when it occurs.

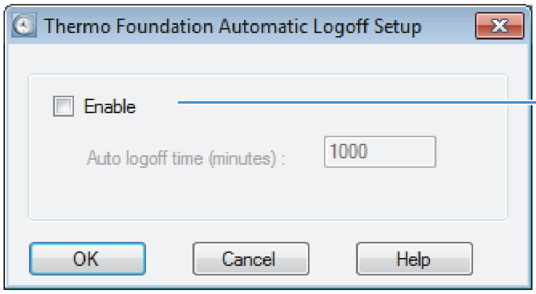
IMPORTANT Thermo Fisher Scientific recommends that you enable automatic logoff to help ensure file integrity and access controls.

❖ To turn the automatic logoff feature on or off

1. Choose **Start** > **Programs** (or **All Programs**) > **Thermo Foundation** ***x.x*** > **AutoLogoff**, where *x.x* is the version.

   The Thermo Foundation Automatic Logoff Setup dialog box opens (Figure 32).

   Figure 32. Automatic Logoff Setup dialog box

   Thermo Foundation Automatic Logoff Setup

   □ Enable

   Auto logoff time (minutes) : 1000

   By default, Automatic Logoff is turned off.

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.

   For the Foundation platform running on the Windows 7 operating system, provide users with the following instruction as part of your standard operating procedure after you turn on AutoLogoff:

   > Each time you log on, the Windows 7 operating system prompts you for permission to run AutoLogoff in the background. Choose **Allow** every time.

3. Click **OK**.

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

Removing and Archiving Files

For data security over a long period of time, it is good to have proper procedures in place for data protection—including raw data, processed data, and metadata.

- Backing up data: Backups should be performed daily, nightly, or weekly (however you set up the system) and protect against a data loss due to computer hardware failure or inadvertent deletion. This might also include developing a procedure for restoring corrupted or lost data from a backup to the server.
- Archiving data: An archive permanently stores data in accordance with data retention requirements. The data is typically no longer needed for regular access and can be locked up in a repository.

  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.
- Retrieving data: Retrieving data from an established archive would generally require a formal request through the IT organization.

  If you have an archive, develop 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.

4

Using the Authorization Manager

To control access to certain features of the Thermo Foundation platform, the Thermo Xcalibur data system, and the LCquan application, define secure user groups and grant these groups appropriate permission levels. By design, every member of a secure user group holds the same rights and permissions. Use the Thermo Foundation Authorization Manager to create new groups and define permission levels.

After you define secure user groups and set permission levels, only those users who are in a secure user group can access the application. All others are prohibited access.

For the Authorization Manager, an application is a functional window or tool in the Foundation platform, Xcalibur data system, or the LCquan application.

IMPORTANT Shut down all applications before running the Authorization Manager. Otherwise, if you make changes to permissions for an application when the application is open, the changes might not take effect until you exit and restart the program.

To use the Thermo Foundation Authorization Manager, follow these procedures.

Contents

Planning User Groups

Before you begin, decide how many user groups you require or, if more appropriate, how many levels of access to grant to your users. For example, consider a laboratory where both scientists and technicians work. The standard operating procedures for this laboratory state that technicians cannot perform certain operations with the software in contrast to scientists who have no restrictions. In this case, if you are the laboratory administrator, you must create at least two user groups—one for technicians and one for scientists.

There is no limit to the number of user groups defined. For simplicity, if all users are to have the same privileges, define a single user group.

IMPORTANT As a precaution, define at least one user group. If no user groups are configured in the Authorization Manager, access to controlled features is unrestricted.

A user group can be either an existing Windows domain logon group or a private group:

- The domain administrator must create and manage Windows domain logon groups. For help with domain logon groups, contact your domain administrator.
- The workstation administrator can create and manage private groups. However, before the administrator can add a user to a private group, the user must be a member of a domain group. If an intended user is not a user on the domain, grant a domain account for that person. Contact your domain administrator for help in completing this task.

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.

IMPORTANT To use Windows Active Directory Domain groups with Authorization Manager, they must be configured as Domain Global groups. Because Domain Local groups are not visible to Authorization Manager, you cannot use them.

Using the Authorization Manager to Set Up Secure User Groups

For information about the parameters in the Authorization Manager window, see the next topic “Authorization Manager Parameters.”

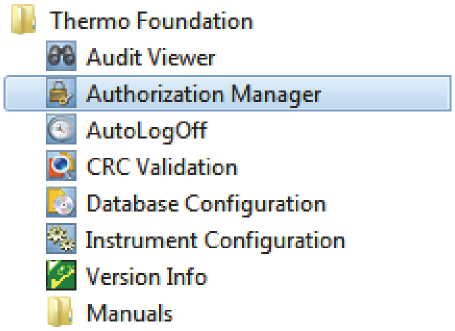
To set up the secure user groups with the Authorization Manager, follow these steps:

- Step 1: Defining Secure User Groups
- Step 2: Setting the Permission Levels
- Step 3: Setting Up a List of Predefined Comments (Optional)
- Step 4: Setting Up Additional Security Features for LCquan
- Step 5: Saving the Security Settings

For information about viewing the History Log, see “Viewing the Authorization Manager History Log” on page 87. For information about printing the security settings, see “Printing the Security Settings” on page 87.

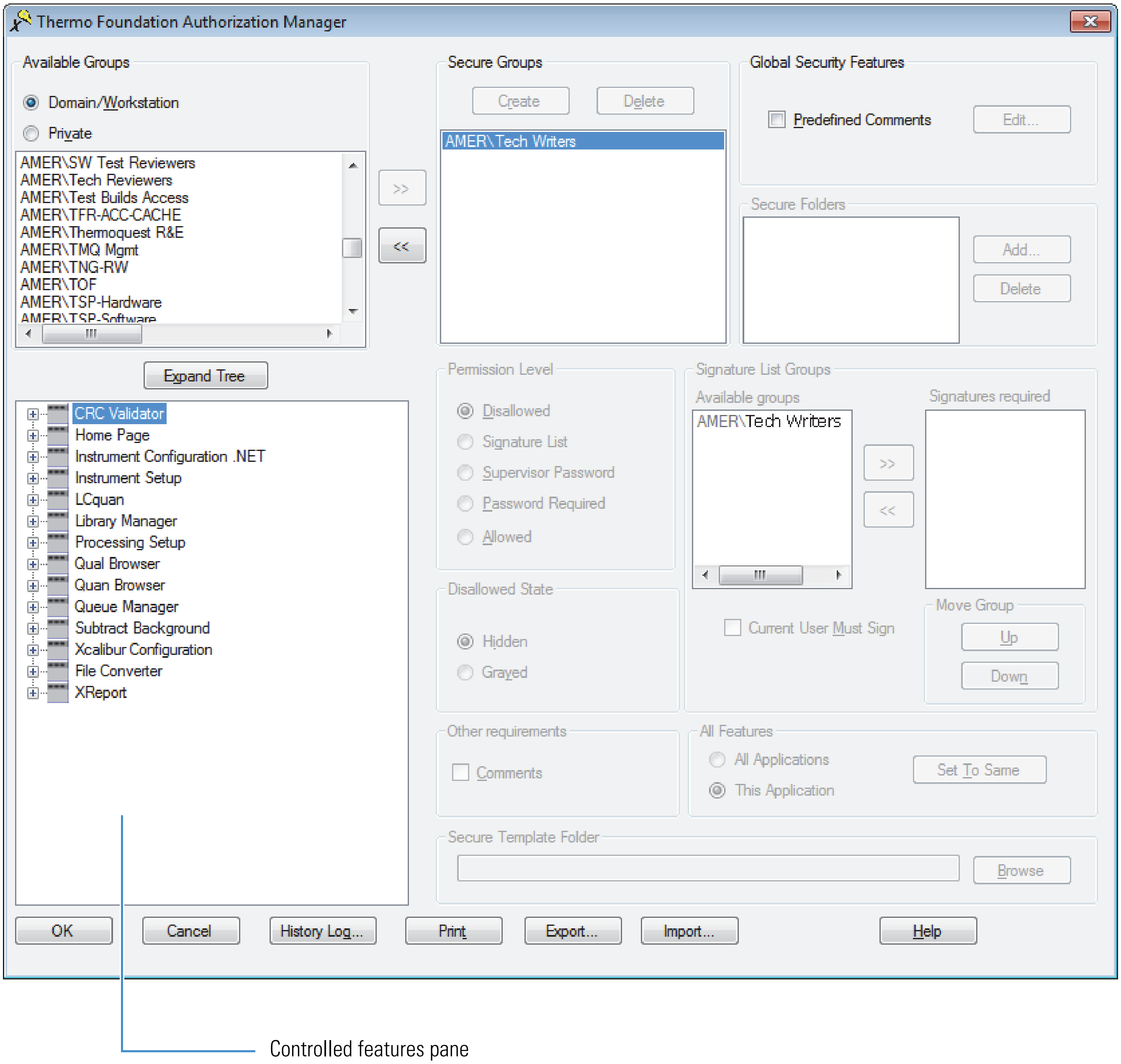
❖ To open the Authorization Manager

From the Windows taskbar, choose **Start > Programs** (or **All Programs**) **> Thermo Foundation *x.x* > Authorization Manager**, where *x.x* is the version.



The Thermo Foundation Authorization Manager window opens (Figure 33).

Figure 33. Thermo Foundation Authorization Manager



Thermo Foundation Authorization Manager

Available Groups

● Domain/Workstation
○ Private

AMER\SW Test Reviewers
AMER\Tech Reviewers
AMER\Test Builds Access
AMER\TFR-ACC-CACHE
AMER\Thermoquest R&E
AMER\TMQ Mgmt
AMER\TNG-RW
AMER\TOF
AMER\TSP-Hardware
AMER\TSP-Software

Secure Groups

AMER\Tech Writers

Global Security Features

□ Predefined Comments

Secure Folders

CRC Validator
Home Page
Instrument Configuration .NET
Instrument Setup
LCquan
Library Manager
Processing Setup
Qual Browser
Quan Browser
Queue Manager
Subtract Background
Xcalibur Configuration
File Converter
XReport

Permission Level

● Disallowed
○ Signature List
○ Supervisor Password
○ Password Required
○ Allowed

Signature List Groups

Available groups: AMER\Tech Writers

Signatures required

Disallowed State

● Hidden
○ Grayed

□ Current User Must Sign

Move Group

Other requirements

□ Comments

All Features

○ All Applications
● This Application

Secure Template Folder

Controlled features pane

Authorization Manager Parameters

In addition to using the security features of your computer operating system, use the Authorization Manager to define user groups and to set permission levels for those groups. Setting permission levels makes sure that only those who are to some degree responsible for electronic records can access the specific applications that generate them. You must be logged on as an administrator to set these permissions.

These tables describe the parameters in the Authorization Manager window and the features that you can configure from this window:

- Table 3 describes the parameters in the Authorization Manager window.
- Table 4 on page 62 describes the application features that you can configure from the Authorization Manager window.

Table 3. Foundation Authorization Manager parameters (Sheet 1 of 7)

Parameter	Description
Available Groups	
Domain/Workstation	Select this option to use the existing Windows logon groups. Contact your network administrator to create or change logon groups.
Private	Select this option to use or create a private (local) user group. The administrator of the workstation can create private groups.
Available Groups	Displays the available Windows logon groups (Domain/Workstation option) or private (local) groups (Private option). To move a group into the Secure Groups box, select the group in the Available Groups list and click >>. To move a group out of the Secure Groups box, select the group in the Secure Groups box and click <<, or double-click the group.
Secure Groups	
Create	Opens the Create Private Group dialog box, where you can create private groups. In the Available Groups area, select the **Private** option to enable the Create button.
Delete	Deletes the selected group from the list of secure groups. Select a private group in the Secure Groups box and click **Delete** to delete the group.

Table 3. Foundation Authorization Manager parameters (Sheet 2 of 7)

Parameter	Description
Secure Groups	Displays the Windows logon groups (Domain/Workstation option) or private (local) groups (Private option) whose permission levels you have set. To move a group into the Secure Groups box, select the group in the Available Groups list and click >>. To move a group out of the Secure Groups box, select the group in the Secure Groups box and click <<, or double-click the group. To delete a secure group, select the group in the Secure Groups box and click **Delete**. Right-click a group in the Secure Groups box to display a shortcut menu with the following commands: **Members**: Opens the Edit User List Of Private Group dialog box (for private groups) or the Users In Group dialog box (for domain groups). **Globally Set To**: Sets all software features in all applications to the same permission level: Disallowed, Signature List, Supervisor Password, Password, or Allowed. **Inherit From**: Opens the Choose Secure Group dialog box. **Create Group**: Opens the Create Private Group dialog box. (Only for private groups)
Global Security Features	
Predefined Comments	Select this check box to require the user to select from a list of predefined comments instead of typing in a comment for features that require comments. When you select this check box, the Edit button becomes active. Click **Edit** to open the Edit Comment List dialog box and define a list of comments.
Edit	Opens the Comments List box, where you can define a list of comments that a user must choose from for certain features.

Table 3. Foundation Authorization Manager parameters (Sheet 3 of 7)

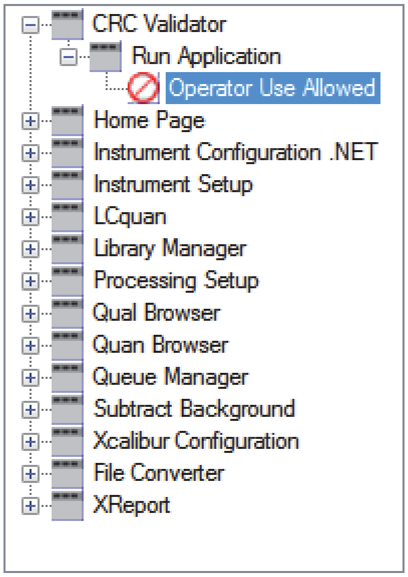
Parameter	Description
Controlled features list	
Controlled features list	 CRC Validator Run Application Operator Use Allowed Home Page Instrument Configuration .NET Instrument Setup LCquan Library Manager Processing Setup Qual Browser Quan Browser Queue Manager Subtract Background Xcalibur Configuration File Converter XReport Displays permission levels for software applications. To display the controlled features list, select a group in the Secure Groups list. To display the group's permission levels for an application, select the application in the controlled features list and click **Expand Tree**. To change a permission level, select a permission for a feature in the controlled features list to activate the Permission Level area. Select the new permission level in the Permission Level area. When you log on after restarting a session, wait a few moments before opening the LCquan application so that the system recognizes your permission levels.
Expand/ Collapse Tree	Displays the permissions for an application after you select the application in the controlled features list.
Secure Folders (LCquan only)	
Secure folders	Displays the folders whose root folder can be changed. In the controlled features list, if you set the feature to Allow Change of Root Folder and choose a permission level other than Disallowed, you must define a list of secure folders. For more information about creating a list of secure folders, see Chapter 3, "Establishing Secure File Operations." Secure folders are used only in the LCquan application. This box is unavailable unless LCquan is selected in the controlled features list.
Add	Opens the Browse for Folder dialog box where you can locate the folder that you want to add to the Secure Folders list. Secure folders are used only in the LCquan application. This button is unavailable unless LCquan is selected in the controlled features list.

Table 3. Foundation Authorization Manager parameters (Sheet 4 of 7)

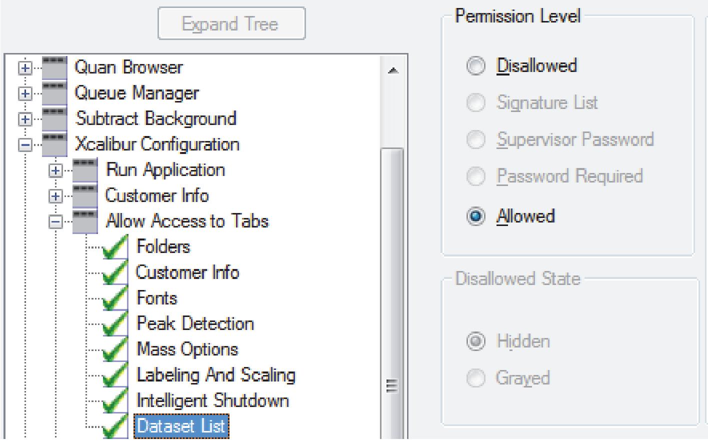
Parameter	Description
Delete	Removes the selected folder from the Secure Folders list. Secure folders are used only in the LCquan application. This button is unavailable unless LCquan is selected in the controlled features list.
Permission Level	
Disallowed	To refuse access to the feature that you selected, set the permission level of the feature in the controlled features list to Disallowed. By default, all new secure user groups have all features set to Disallowed. If Disallowed and Allowed are the only options available (all of the other options are grayed out), then these options do not indicate permission levels, but instead indicate configuration settings. Disallowed means that the selection in the controlled features list is not displayed by the application and Allowed means that the selection is displayed. For example, if you select Xcalibur Configuration > Allow To Access Tabs > Dataset List page in the list of controlled features pane, only the Disallowed and Allowed settings are available. If you select Disallowed, the Dataset List page is not displayed in the Xcalibur Configuration dialog box. If you select Allowed, the Dataset List page is displayed in the Xcalibur Configuration dialog box.  Permission Level: ○ Disallowed ○ Signature List ○ Supervisor Password ○ Password Required ● Allowed Disallowed State: ● Hidden ○ Grayed

Table 3. Foundation Authorization Manager parameters (Sheet 5 of 7)

Parameter	Description
Signature List	Require that the names and passwords of everyone on the signature list be entered to perform the action that you selected in the controlled features list. When an action with a permission level of Signature List is chosen, a series of password dialog boxes appear, one for each signature (name and password of a member of a designated signature group). The order of the groups shown in the Signature List Groups: Signature Required list defines the order in which the password dialog boxes appear.
Supervisor Password	Require that the name and password of the supervisor be entered to perform the action that you selected in the controlled features list. In this context, a supervisor is any person who has permission to do this operation—that is, the person's permission level for this operation is either Allowed or Password Required.
Password Required	Require that the password of the user be entered to perform the action that you selected in the controlled features list.
Allowed	No restrictions. Allows the user to perform the action that you selected in the controlled features list without restriction. If Disallowed and Allowed are the only options available (all of the other options are grayed out), then these options do not indicate permission levels, but instead indicate configuration settings. Disallowed means that the selection in the controlled features list is not displayed by the application and Allowed means that the selection is displayed. For example, if you select Xcalibur Configuration > Allow To Access Tabs > Dataset List page in the controlled features list, only the Disallowed and Allowed settings are available. If you select Disallowed, the Dataset List page is not displayed in the Xcalibur Configuration dialog box. If you select Allowed, the Dataset List page is displayed in the Xcalibur Configuration dialog box.
Disallowed State	
Hidden	Hide the disallowed action that you selected in the controlled features list.
Grayed	Gray out the disallowed action that you selected in the controlled features list.

Table 3. Foundation Authorization Manager parameters (Sheet 6 of 7)

Parameter	Description
Signature List Groups	
Available Groups	Displays the groups whose signatures you can require. To move a group into the Signature Required list, select the group in the Available Groups list and click **>>**. To move a group from the Signature Required list, select the group in the Signature Required list and click **<<** or double-click the group. The only groups that can be in the Signature Required list are those groups that have permission (Allowed or Password Required) to do the operation. Select **Permission Level: Signature List** to activate the Available Groups list.
Signature Required	Requires a signature from a selected group. When an action with a permission level of Signature List is chosen, a series of password dialog boxes appear, one for each signature (name and password of a member of a designated signature group). The order of the groups shown in the Signatures Required list defines the order in which the password dialog boxes appear. To move a group into the Signature Required list, select the group in the Available Groups list and click **>>**. To move a group from the Signature Required list, select the group in the Signature Required list and click **<<**. The only groups that can be in the Signature Required list are those groups that have permission (Allowed or Password Required) to do the operation. Select the **Signature List** option in the Permission Level area to activate the Signatures Required list.
Current User Must Sign	Adds the current user to the Signatures Required list. Select **Signature List** option in the Permission Level area and add one or more groups to the Signatures Required list to activate the Current User Must Sign check box.
Move Group Up	Moves the group that you selected in the Signatures Required list up one spot in the list. Select the S**ignature List** option in the Permission Level area, add more than one group to the Signatures Required list, and select a group that is below another group to activate the Move Group Up button.

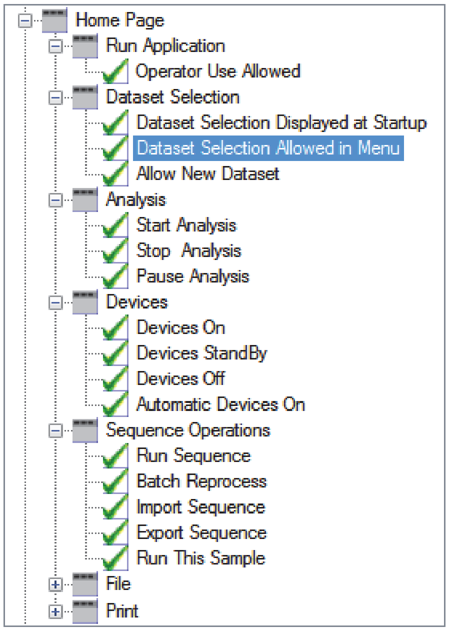
Table 3. Foundation Authorization Manager parameters (Sheet 7 of 7)

Parameter	Description
Move Group Down	Moves the group that you selected in the Signatures Required list down one spot in the list. Select the S**ignature List** option in the Permission Level area, add more than one group to the Signatures Required list, and select a group that is above another group to activate the Move Group Down button.
Other Requirements	
Comments	Requires the user to enter a comment that will appear in the Audit Log when performing an action.
All Features	
All Applications	Select this option to set the software features in all applications to the same permission level that you just set.
This Application	Select this option to set all of the other software features in the selected application to the same permission level that you just set.
Set To Same	Sets all the other software features (for all applications or for just this application) to the same permission level that you just set.
Buttons	
History Log	Opens the Audit Viewer. The Audit Viewer is a record of all changes made to the security settings. The following events are logged: • The creation of a private group • A change in group permissions • A switch between private and domain/workstation groups • Changes to the Signature List
Print	Prints a report of Authorization Manager settings for each secure group. The reports include listings of group members, secure folders, and applications and their permissions.
Export	Saves the Authorization Manager settings in a permissions file (EPERM).
Import	Imports previously saved Authorization Manager settings. You save Authorization Manager settings in a permissions file.

Use the Authorization Manager to set permissions for the Foundation platform and the Xcalibur data system features. You can set them for individuals or for groups. Certain permission level settings override other settings.

Table 4. Authorization Manager application features (Sheet 1 of 7)

Features	Description
CRC Validator	
Run Application	If you set this feature to Disallow, then the user cannot open the CRC Validator window. In this case, the application ignores the permission level settings for other features. If a user whose permission is set to Disallow tries to access the system, an entry is made in the Global Auditing Database history log.
Home Page	
Run Application	If you set this feature to Disallow, then the user cannot open the Xcalibur data system or turn devices on or off from the Information view. In this case, the application ignores the permission level settings for other features. If a user whose permission is set to Disallow tries to access the system, an entry is made in the Global Auditing Database history log.
For the Homepage window, you can allow or disallow the following actions.	
Dataset Selection	• Dataset Selection Displayed at Startup • Dataset Selection Allowed in Menu • Allow New Dataset
Analysis	• Start Analysis • Stop Analysis • Pause Analysis
Devices	• Devices On • Devices Standby • Devices Off • Automatic Devices On
Sequence Operations	• Run Sequence • Batch Reprocess • Import Sequence • Export Sequence • Run This Sample
File	File Save
Print	Print Sequence



- ⊟ Home Page
  - ⊟ Run Application
    - ✓ Operator Use Allowed
  - ⊟ Dataset Selection
    - ✓ Dataset Selection Displayed at Startup
    - ✓ Dataset Selection Allowed in Menu
    - ✓ Allow New Dataset
  - ⊟ Analysis
    - ✓ Start Analysis
    - ✓ Stop Analysis
    - ✓ Pause Analysis
  - ⊟ Devices
    - ✓ Devices On
    - ✓ Devices StandBy
    - ✓ Devices Off
    - ✓ Automatic Devices On
  - ⊟ Sequence Operations
    - ✓ Run Sequence
    - ✓ Batch Reprocess
    - ✓ Import Sequence
    - ✓ Export Sequence
    - ✓ Run This Sample
  - ⊞ File
  - ⊞ Print

Table 4. Authorization Manager application features (Sheet 2 of 7)

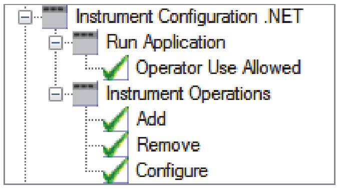
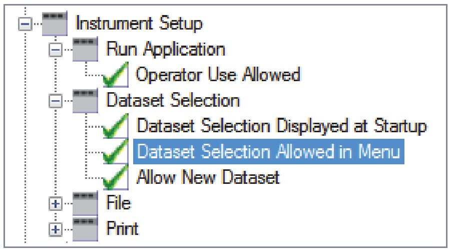
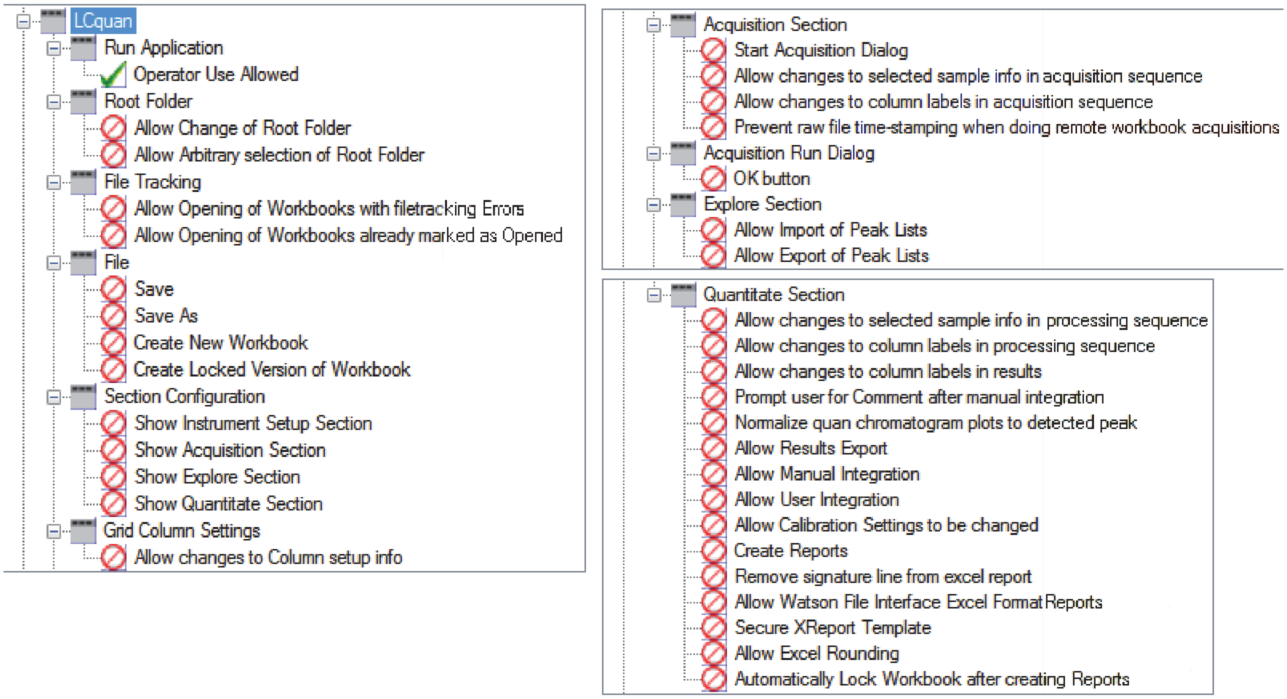
Features	Description
Instrument Configuration	
Run Application	If you set this feature to Disallow, then the user cannot open the Thermo Foundation Instrument Configuration window. In this case, the application ignores the permission level settings for other features. If a user whose permission is set to Disallow tries to access the system, an entry is made in the Global Auditing Database history log.
For the Instrument Configuration window, you can allow or disallow the following actions.	
Instrument Operations	• Add Instrument • Remove Instrument • Configure Instrument  Instrument Configuration .NET Run Application ✓ Operator Use Allowed Instrument Operations ✓ Add ✓ Remove ✓ Configure
Instrument Setup	
Run Application	If you set this feature to Disallow, then the user cannot open the Instrument Setup window. In this case, the application ignores the permission level settings for other features. If a user whose permission is set to Disallow tries to access the system, an entry is made in the Global Auditing Database history log.
For the Instrument Setup window, you can allow or disallow access to the following actions.	
Dataset Application	• Dataset Selection Displayed at Startup • Dataset Selection Allowed in Menu • Allow New Dataset  Instrument Setup Run Application ✓ Operator Use Allowed Dataset Selection ✓ Dataset Selection Displayed at Startup ✓ Dataset Selection Allowed in Menu ✓ Allow New Dataset File Print
File	File Save
Print	Print Instrument Method

Table 4. Authorization Manager application features (Sheet 3 of 7)

Features	Description
LCquan	

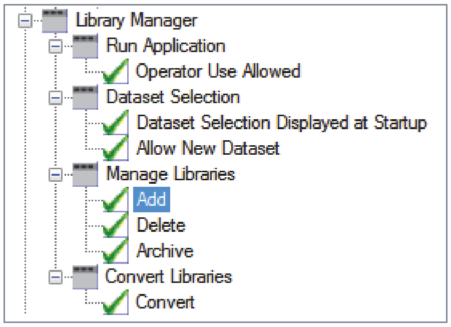


- LCquan
  - Run Application
    - ✓ Operator Use Allowed
  - Root Folder
    - ⊘ Allow Change of Root Folder
    - ⊘ Allow Arbitrary selection of Root Folder
  - File Tracking
    - ⊘ Allow Opening of Workbooks with filetracking Errors
    - ⊘ Allow Opening of Workbooks already marked as Opened
  - File
    - ⊘ Save
    - ⊘ Save As
    - ⊘ Create New Workbook
    - ⊘ Create Locked Version of Workbook
  - Section Configuration
    - ⊘ Show Instrument Setup Section
    - ⊘ Show Acquisition Section
    - ⊘ Show Explore Section
    - ⊘ Show Quantitate Section
  - Grid Column Settings
    - ⊘ Allow changes to Column setup info

- Acquisition Section
  - ⊘ Start Acquisition Dialog
  - ⊘ Allow changes to selected sample info in acquisition sequence
  - ⊘ Allow changes to column labels in acquisition sequence
  - ⊘ Prevent raw file time-stamping when doing remote workbook acquisitions
- Acquisition Run Dialog
  - ⊘ OK button
- Explore Section
  - ⊘ Allow Import of Peak Lists
  - ⊘ Allow Export of Peak Lists

- Quantitate Section
  - ⊘ Allow changes to selected sample info in processing sequence
  - ⊘ Allow changes to column labels in processing sequence
  - ⊘ Allow changes to column labels in results
  - ⊘ Prompt user for Comment after manual integration
  - ⊘ Normalize quan chromatogram plots to detected peak
  - ⊘ Allow Results Export
  - ⊘ Allow Manual Integration
  - ⊘ Allow User Integration
  - ⊘ Allow Calibration Settings to be changed
  - ⊘ Create Reports
  - ⊘ Remove signature line from excel report
  - ⊘ Allow Watson File Interface Excel Format Reports
  - ⊘ Secure XReport Template
  - ⊘ Allow Excel Rounding
  - ⊘ Automatically Lock Workbook after creating Reports

Features	Description
Library Manager	
Run Application	If you set this feature to Disallow, then the user cannot open the Library Manager dialog box. In this case, the application ignores the permission level settings for other features. If a user whose permission is set to Disallow tries to access the system, an entry is made in the Global Auditing Database history log.
For the Library Manager dialog box, you can allow or disallow the following actions.	
Dataset Application	• Dataset Selection Displayed at Startup • Allow New Dataset
Manage Libraries	• Add Library • Delete Library • Archive Library
Convert Libraries	Convert Library



- Library Manager
  - Run Application
    - ✓ Operator Use Allowed
  - Dataset Selection
    - ✓ Dataset Selection Displayed at Startup
    - ✓ Allow New Dataset
  - Manage Libraries
    - ✓ Add
    - ✓ Delete
    - ✓ Archive
  - Convert Libraries
    - ✓ Convert

Table 4. Authorization Manager application features (Sheet 4 of 7)

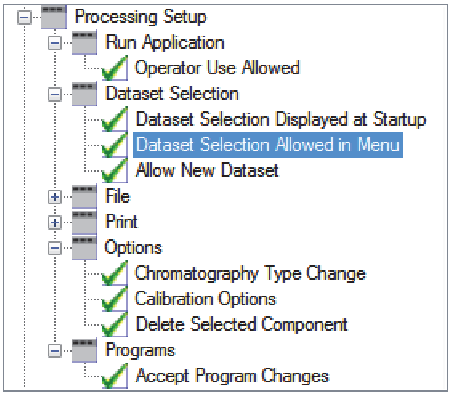
Features	Description
Processing Setup	
Run Application	If you set this feature to Disallow, then the user cannot open the Processing Setup window. In this case, the application ignores the permission level settings for other features. If a user whose permission is set to Disallow tries to access the system, an entry is made in the Global Auditing Database history log.
For the Processing Setup window, you can allow or disallow the following actions.	
Dataset Application	• Dataset Selection Displayed at Startup • Dataset Selection Allowed in Menu • Allow New Dataset  Processing Setup Run Application ✓ Operator Use Allowed Dataset Selection ✓ Dataset Selection Displayed at Startup ✓ Dataset Selection Allowed in Menu ✓ Allow New Dataset File Print Options ✓ Chromatography Type Change ✓ Calibration Options ✓ Delete Selected Component Programs ✓ Accept Program Changes
File	File Save
Print	Print Processing Method
Options	• Chromatography Type Change • Calibration Options • Delete Selected Component
Programs	Accept Program Changes
Qual Browser	
Run Application	If you set this feature to Disallow, then the user cannot open the Qual Browser window. In this case, the application ignores the permission level settings for other features. If a user whose permission is set to Disallow tries to access the system, an entry is made in the Global Auditing Database history log.
For the Qual Browser window, you can allow or disallow the following actions.	

Table 4. Authorization Manager application features (Sheet 5 of 7)

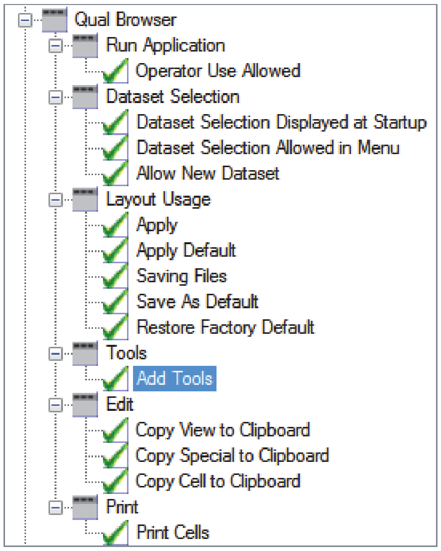
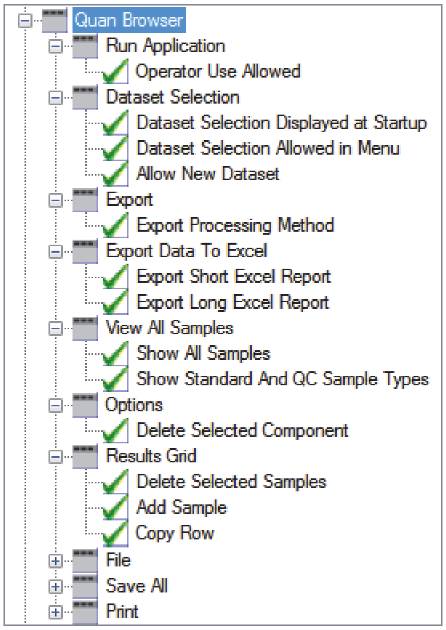
Features	Description	
Dataset Application	- Dataset Selection Displayed at Startup - Dataset Selection Allowed in Menu - Allow New Dataset	 Qual Browser Run Application ✓ Operator Use Allowed Dataset Selection ✓ Dataset Selection Displayed at Startup ✓ Dataset Selection Allowed in Menu ✓ Allow New Dataset Layout Usage ✓ Apply ✓ Apply Default ✓ Saving Files ✓ Save As Default ✓ Restore Factory Default Tools ✓ Add Tools Edit ✓ Copy View to Clipboard ✓ Copy Special to Clipboard ✓ Copy Cell to Clipboard Print ✓ Print Cells
Layout Usage	- Apply Layout - Apply Default Layout - Save Layout - Save Layout as Default - Restore Factory Default	
Tools	Add Tools	
Edit	- Copy View to Clipboard. - Copy Special to Clipboard - Copy Cell to Clipboard	
Print	Print Cells	
Quan Browser		
Run Application	If you set this feature to Disallow, then the user cannot open the Quan Browser window. In this case, the application ignores the permission level settings for other features. If a user whose permission is set to Disallow tries to access the system, an entry is made in the Global Auditing Database history log.	
For the Quan Browser window, you can allow or disallow the following actions.		
Dataset Application	- Dataset Selection Displayed at Startup - Dataset Selection Allowed in Menu - Allow New Dataset	 Quan Browser Run Application ✓ Operator Use Allowed Dataset Selection ✓ Dataset Selection Displayed at Startup ✓ Dataset Selection Allowed in Menu ✓ Allow New Dataset Export ✓ Export Processing Method Export Data To Excel ✓ Export Short Excel Report ✓ Export Long Excel Report View All Samples ✓ Show All Samples ✓ Show Standard And QC Sample Types Options ✓ Delete Selected Component Results Grid ✓ Delete Selected Samples ✓ Add Sample ✓ Copy Row File Save All Print
Export	Export Processing Method	
Export Data to Excel	- Export Short Excel Report - Export Long Excel Report	
View All Samples	- Show All Samples - Show Standard and QC Sample Types	
Options	Delete Selected Component	
Results Grid	- Delete Selected Samples - Add Samples - Copy Row	
File	File Save	
Save All	Save All Result Files	
Print	Print Reports	

Table 4. Authorization Manager application features (Sheet 6 of 7)

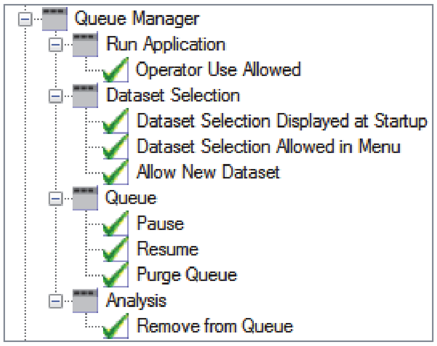
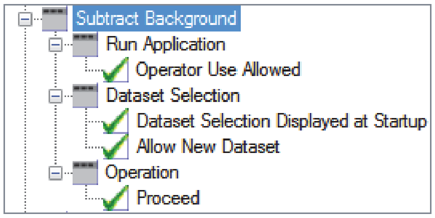
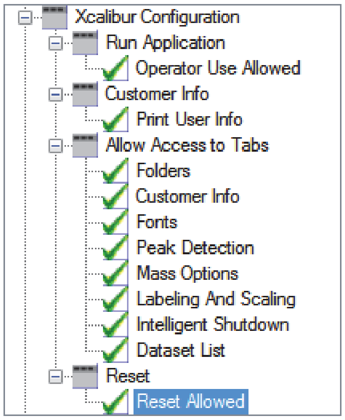
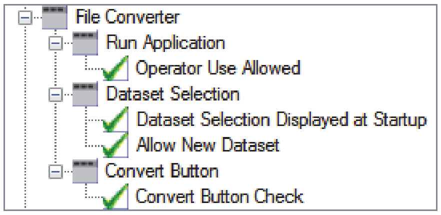
Features	Description
Queue Manager	
Run Application	If you set this feature to Disallow, then the user cannot submit sequences to the acquisition queue. In this case, the application ignores the permission level settings for other features. If a user whose permission is set to Disallow tries to access the system, an entry is made in the Global Auditing Database history log.
Selecting the Disallow check box hides access to the following features.	
Dataset Application	• Dataset Selection Displayed at Startup • Dataset Selection Allowed in Menu • Allow New Dataset Queue Manager Run Application ✓ Operator Use Allowed Dataset Selection ✓ Dataset Selection Displayed at Startup ✓ Dataset Selection Allowed in Menu ✓ Allow New Dataset Queue ✓ Pause ✓ Resume ✓ Purge Queue Analysis ✓ Remove from Queue
Queue	• Pause Queue • Resume Queue • Purge Queue
Analysis	Remove from Queue
Subtract Background	
Run Application	If you set this feature to Disallow, then the user cannot open the software application. In this case, the application ignores the permission level settings for other features. If a user whose permission is set to Disallow tries to access the system, an entry is made in the Global Auditing Database history log.
Selecting the Disallow check box hides access to the following features.	
Dataset Selection	• Dataset Selection Displayed at Startup • Allow New Dataset Subtract Background Run Application ✓ Operator Use Allowed Dataset Selection ✓ Dataset Selection Displayed at Startup ✓ Allow New Dataset Operation ✓ Proceed
Operation	Proceed

Table 4. Authorization Manager application features (Sheet 7 of 7)

Features	Description
Xcalibur Configuration	
Run Application	If you set this feature to Disallow, then the user cannot open the software application. In this case, the application ignores the permission level settings for other features. If a user whose permission is set to Disallow tries to access the system, an entry is made in the Global Auditing Database history log.
Selecting the Disallow check box hides access to the following features:	
Customer Info	Print User Info  Xcalibur Configuration Run Application Operator Use Allowed Customer Info Print User Info Allow Access to Tabs Folders Customer Info Fonts Peak Detection Mass Options Labeling And Scaling Intelligent Shutdown Dataset List Reset Reset Allowed
Allow Access to Tabs	• Folders • Customer Info • Fonts • Peak Detection • Mass Options • Labeling and Scaling • Intelligent Shutdown • Dataset List
Reset	Reset Allowed
File Converter	
Run Application	If you set this feature to Disallow, then the user cannot open the File Converter application. In this case, the application ignores the permission level settings for other features. If a user whose permission is set to Disallow tries to open the File Converter application, an entry is made in the Global Auditing Database history log.
Selecting the Disallow check box hides access to the following features.	
Dataset Selection	• Dataset Selection Displayed at Startup • Allow New Dataset  File Converter Run Application Operator Use Allowed Dataset Selection Dataset Selection Displayed at Startup Allow New Dataset Convert Button Convert Button Check
Convert Button	Convert Button Check
XReport	
Run Application	If you set this feature to Disallow, then the user cannot open the Xreport application. In this case, the application ignores the permission level settings for other features. If a user whose permission is set to Disallow tries to access the system, an entry is made in the Global Auditing Database history log.

Step 1: Defining Secure User Groups

After you plan the user groups, open the Authorization Manager and follow one of these procedures to set up the planned groups.

- Defining Secure Domain or Workstation Groups
- Defining and Editing Secure Private Groups

Defining Secure Domain or Workstation Groups

Follow these procedures to define a secure Domain/Workstation group and to view the names of the group members.

❖ To define secure domain or workstation user groups

1. If it is not already open, open the Authorization Manager (see "Using the Authorization Manager to Set Up Secure User Groups" on page 53).
2. In the Available Groups area, to use the existing Windows logon groups, select the **Domain/Workstation** option.

   Contact your domain administrator to create or change logon groups.
3. To select the secure domain/workstation logon groups, do the following:

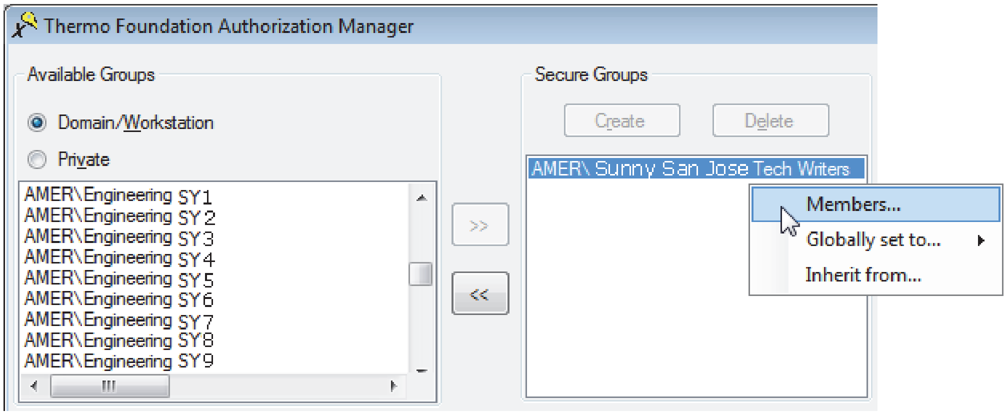
   a. Select a group in the Available Groups list and click >>.

   The group appears in the Secure Groups box.

❖ To view the members of a domain group

Right-click the user group in the Secure Groups box and choose **Members** from the shortcut menu (Figure 34).

Figure 34. Shortcut menu for the Secure Groups that are part of a domain/workstation



AMER\Engineering SY1
AMER\Engineering SY2
AMER\Engineering SY3
AMER\Engineering SY4
AMER\Engineering SY5
AMER\Engineering SY6
AMER\Engineering SY7
AMER\Engineering SY8
AMER\Engineering SY9

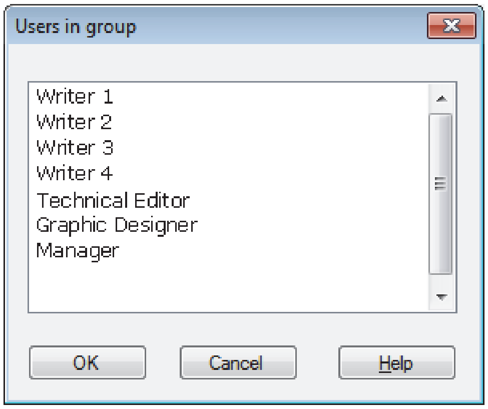
AMER\ Sunny San Jose Tech Writers

The Users in Group dialog box opens (Figure 35). Because membership in these groups is controlled by the domain administrator, the lists in the Users in Group dialog box are read-only.

Users In Group Dialog Box

Use the Users In Group dialog box to view the users in a domain or workstation logon group. Because the domain administrator controls membership in these groups, the lists in this dialog box are read-only. See your domain administrator to make changes to domain or workstation logon groups.

Figure 35. Users In Group dialog box



Users in group

Writer 1
Writer 2
Writer 3
Writer 4
Technical Editor
Graphic Designer
Manager

The Users In Group dialog box has one parameter (Table 5).

Table 5. Users In Group dialog box parameters

Parameter	Description
Users In Group	Users who are currently in the domain logon group.

Defining and Editing Secure Private Groups

Follow these procedures to create and edit secure private groups.

❖ To define secure private groups

1. If it is not already open, open the Authorization Manager (see “Using the Authorization Manager to Set Up Secure User Groups” on page 53).

2. In the Available Groups area, to use (or to create) a local user group, select the **Private** option.

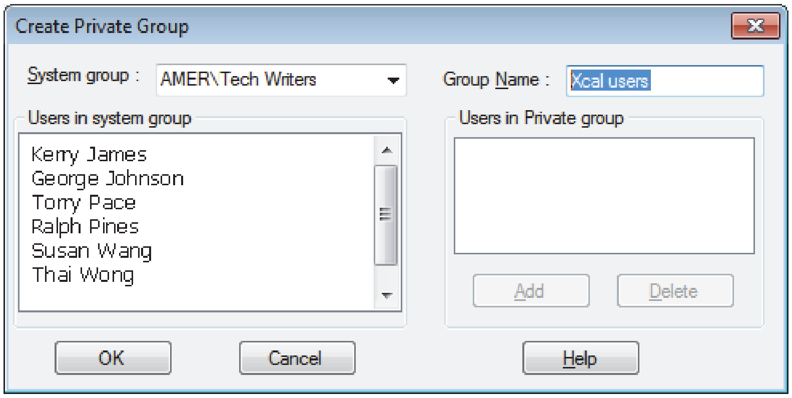
   The administrator of the workstation can create private groups.

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

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

      The Create Private Group dialog box opens (Figure 36).

Figure 36. Create Private Group dialog box



System group : AMER\Tech Writers

Group Name : Xcal users

Users in system group

Kerry James
George Johnson
Torry Pace
Ralph Pines
Susan Wang
Thai Wong

Users in Private group

b. In the Group Name box, type a name for the new private group.

c. For each user that you want to add to the new private group, do the following:

   i. In the System Group list, select a domain.

      The Users in System Group box lists the domain user accounts.

   ii. Select a user account and click **Add** to add it to the new private group.

      The user account appears in the Users in Private group box.

d. When you have added all the planned users, click **OK**.

   The new private group appears in the Secure Groups box.

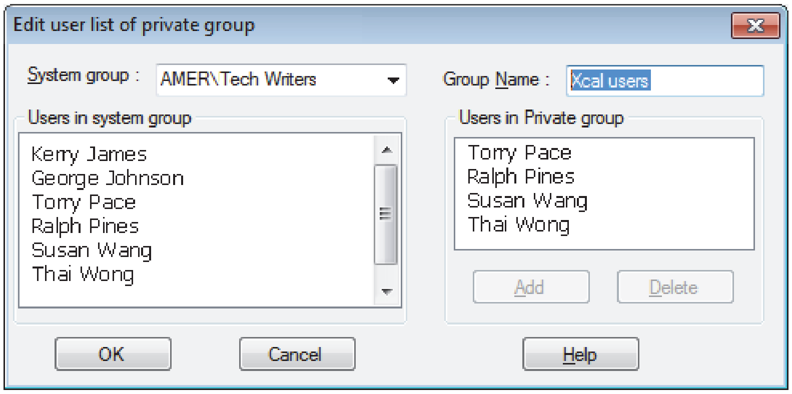
e. To create additional private groups, repeat steps step 3b to step 3d.

❖ To change the members of a secure private group

1. Right-click the user group in the Secure Groups box and choose **Members** from the shortcut menu.

   The Edit User List of Private Group dialog box opens (Figure 37). This dialog box contains the same parameters as the Create Private Group dialog box.

Figure 37. Edit User List of Private Group dialog box



System group : AMER\Tech Writers

Group Name : Xcal users

Users in system group

Kerry James
George Johnson
Torry Pace
Ralph Pines
Susan Wang
Thai Wong

Users in Private group

Torry Pace
Ralph Pines
Susan Wang
Thai Wong

2. For each user that you want to remove from the private group, select the user in the Users in Private Group box, and then click **Delete**.

3. For each user you want to add to the private group, do the following:

   a. In the System Group list, select the group that contains the new user.

      A list of users in the selected group appears in the Users in System Group box.

   b. In the Users in System Group box, select the user you want to add.

   c. Click **Add**.

Create Private Group and Edit User List Of Private Group Dialog Boxes

Use the Create Private Group dialog box to create a new private (local) group and to add users to the group. After you create a private group, use the Edit User List of Private Group dialog box to add or remove users from the group.

Table 6 describes the parameters in the Create Private Group or Edit User List of Private Group dialog box.

Table 6. Create Private Group dialog box parameters

Parameter	Description
System Group	Select a domain name from this list.
Users In System Group	Displays the user accounts in the selected domain.
Group Name	Type the name of the new private group.
Users in Private Group	Lists the users in the private group. You can add or delete users.
Buttons	
Add	Adds the currently selected user in the Users In System Group list to the new private group.
Delete	Removes the selected user in the Users in Private Group list.

Step 2: Setting the Permission Levels

For each secure user group, set the permission levels in the Permission Level area for certain features of the CRC Validator and Instrument Configuration applications, the Xcalibur data system, and the LCquan data system (if installed).

To set the permission levels for secure user groups, follow these procedures:

- "Setting the Permission Levels for a Secure User Group" on page 74
- "Setting All Features to the Same Permission Level" on page 76
- "Inheriting Permissions" on page 76
- "Exporting and Importing Permissions" on page 78

Table 7 describes the permission levels. All new secure user groups, whether domain/workstation groups or private groups, have all features set to Disallowed.

Table 7. Permission levels and descriptions

Permission level	Description
Disallowed	Not permitted. Specify whether the user interface control for the disallowed operation is hidden or grayed out.
Signature List	To perform the desired action, enter the names and passwords of everyone on the signature list. A series of dialog boxes (one for each signature) appear when a user attempts to perform this action in the software application.
Supervisor Password	To perform the desired action, enter the supervisor name and password. A dialog box for the supervisor signature opens when a user attempts to perform this action in the software application.
Password	To perform the desired action, enter the user password. A dialog box for the user password opens when a user attempts to perform this action in the software application.
Allowed	No restrictions.

Setting the Permission Levels for a Secure User Group

You can change the permission levels for a secure user group individually for each feature or you can set all the features to the same permission level. Follow this procedure to set up the permission levels for one feature, and then go to "Setting All Features to the Same Permission Level" on page 76 if you want to set all features to the same permission level.

If you have already set up the permission levels for one secure user group and you want to set the same permission levels for other secure user groups, go to "Inheriting Permissions" on page 76.

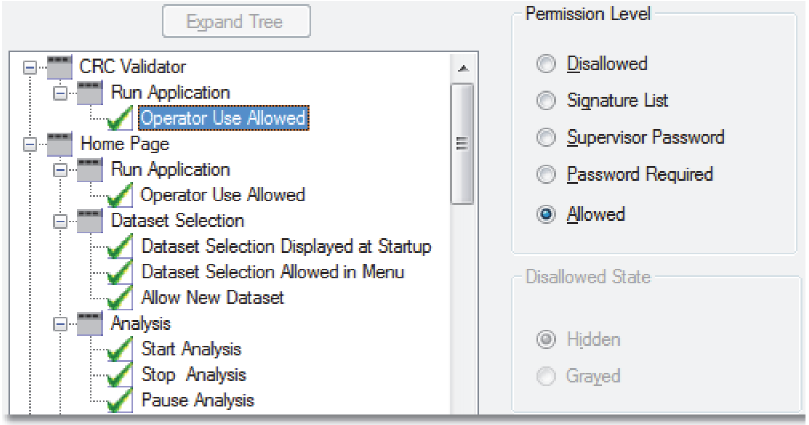
If you have already set up the permissions levels for all your secure user groups and you want to transfer these settings to another workstation, go to "Exporting and Importing Permissions" on page 78.

❖ To change the permission level of an individual feature

1. If you have not already done so, open the Authorization Manager and create the appropriate secure user groups (see "Step 1: Defining Secure User Groups" on page 69).
2. In the Secure Groups box, select a secure user group.
3. Select the application from the list in the lower left of the Authorization Manager.
4. Click **Expand Tree** to show the entire list of controlled features for the application.
5. From the list of controlled features, select the feature whose permission level you want to change (Figure 38).

> **Note** You can set permissions only for individual features, not subgroups. After selecting a feature, the Permission Level options are active. If they are unavailable, you probably selected a subgroup, not a feature.

Figure 38. View of allowed features in the list of features pane



- CRC Validator
  - Run Application
    - ✓ Operator Use Allowed
- Home Page
  - Run Application
    - ✓ Operator Use Allowed
  - Dataset Selection
    - ✓ Dataset Selection Displayed at Startup
    - ✓ Dataset Selection Allowed in Menu
    - ✓ Allow New Dataset
  - Analysis
    - ✓ Start Analysis
    - ✓ Stop Analysis
    - ✓ Pause Analysis

Permission Level

○ Disallowed
○ Signature List
○ Supervisor Password
○ Password Required
● Allowed

Disallowed State

● Hidden
○ Grayed

6. Select one of the Permission Level options:

   - Disallowed
   - Signature List
   - Supervisor Password
   - Password Required
   - Allowed

> **Tip** To define the permission level of a feature, right-click the feature and choose the permission level from the shortcut menu.

7. For Disallowed features, specify the appearance of the user interface control in the Disallowed State area:

   - If you do not want the user interface control to appear at all, select the **Hidden** option.
   - To make the user interface control unavailable, select the **Grayed** option.

8. For Permission Level, if you selected Signature List, use the Signature List Groups area to define the signature list groups:

   a. Select a user group in the Available groups box and click >>.

      The group appears in the Signature required box.

   b. Add other groups to the signature list in the same manner as needed.

   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. If you must rearrange the order of the groups in the signature list, select a group and click **Up** or **Down** in the Move Group area.

> **Note** When you choose a feature in the software application with a permission level of Signature List, a series of password dialog boxes appear, one for each signature (the name and password of every member of the designated group).
>
> The order of the groups shown in the Available groups box defines the order of appearance for the password dialog boxes.

9. To permit the user to enter a comment after performing an action, select the **Comment** check box under Other requirements. (This option is available for all permission settings, except Disallowed.)

   After the user enters a comment, it appears in the audit log for the application.

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

    a. Repeat step 5 through step 9.

    b. Go to "Setting All Features to the Same Permission Level."

> **IMPORTANT** Permission level settings are retained when you move a user group out of the Secure Groups box and into the Available Groups box. When you move the group back into the Secure Groups box, the permission settings remain intact.
>
> When you delete a user group from the Secure Groups box, however, all permission settings are lost.

Setting All Features to the Same Permission Level

After you set up the permissions for one controlled feature, follow this procedure to setup up the permission levels for the remaining controlled features.

❖ To set all of the features to the same permission level

Do one of the following:

- After you set the permission level for one feature as described in "Setting the Permission Levels for a Secure User Group" on page 74, do one of the following:
  - To set all of the other features for this application to the same permission level that you just set, select the **This Application** option in the All Features area and click **Set To Same**.

    The Permission Level setting, the Disallowed state setting (if applicable), and the Comment setting are copied to all of the other features for the currently selected application.
  - To set all other features for all applications to the permission level that you just set, select the **All Applications** option and click **Set To Same**.

    The software copies the Permission Level setting, the Disallowed state setting (if applicable), and the Comment setting to all other features for all applications.
- 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 permission levels from one group to another.

❖ To copy a complete set of permission levels

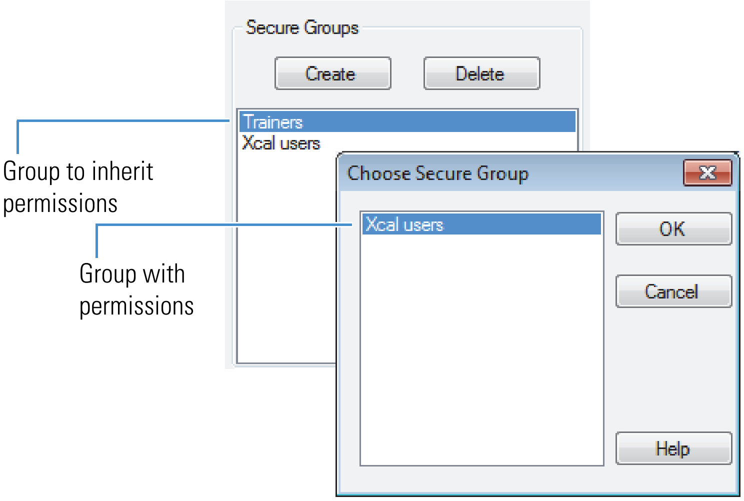
1. Set up the permissions for a secure user group as described in "Setting the Permission Levels for a Secure User Group" on page 74.

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

3. Right-click the selected group and choose **Inherit From** from the shortcut menu.

   The Choose Secure Group dialog box opens (Figure 39) and displays a list of the secure groups (minus the current one).

   Figure 39. Choose Secure Group dialog box

4. Select the group containing the permission levels to copy and click **OK**.

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

Choose Secure Group Dialog Box

Use the Choose Secure Group dialog box to select a secure user group so that you can copy the complete set of permission levels to another group.

Table 8 describes the Secure Group parameter.

Table 8. Choose Secure Group dialog box parameters

Parameter	Description
Secure Group	Displays the list of secure user groups. When you select a group and click OK, the complete set of permission levels for the group is copied to the group selected in the Secure Groups list in the Authorization Manager.

Exporting and Importing Permissions

Importing the permission list that contains the user groups and permissions from a workstation saves time when you have more than one workstation in your lab and plan to provide users access to all stations. Instead of setting up identical user groups on each workstation, copy the permission list from a workstation that has the user groups and access permissions that you require.

IMPORTANT To maintain the security of the permission list, export it to a secure location. The security folder (with proper security settings) on the current workstation is an ideal location.

❖ To export and import the permission list

1. On the workstation where the correct users and permission levels are set, open the Authorization Manager.

2. Click **Export**. (This button is located at the bottom of the window.)

   The Save As dialog box opens.

3. Save the permission list in the security folder as a file with the (.eperm) extension.

   The Windows 7 default location is as follows:

   > *drive*:\Program Data\Thermo Scientific\

   The default file name is permissions.eperm.

4. Copy the file to the security folder on the new workstation.

5. On the new workstation, start the Authorization Manager and click **Import**.

   The Open dialog box opens.

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

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

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

Step 3: Setting Up a List of Predefined Comments

As an option, you can require users to select comments from a predefined list rather than type in comments when they use features that require comment entry.

❖ To require users to select comments from a predefined list

1. If it is not already open, open the Authorization Manager by choosing **Start** > **Programs** or (**All Programs**) > **Thermo Foundation *x.x*** > **Authorization Manager**, where *x.x* is the version.
2. In the Global Security Features area, select the **Predefined Comments** check box.
3. Click **OK** to accept the setting and close the Authorization Manager window.

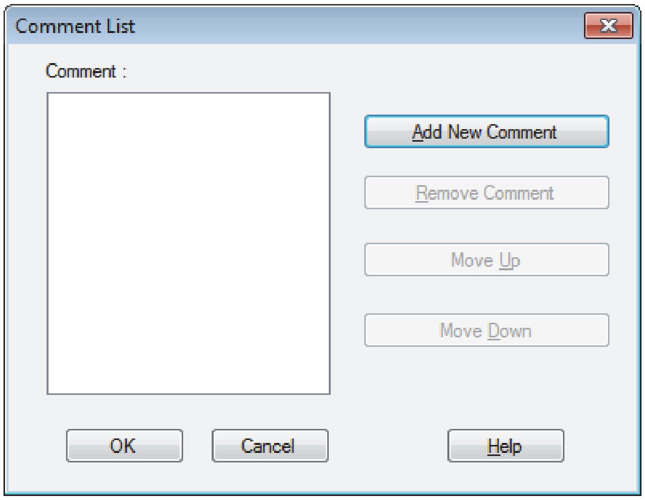
   When predefined comments are active, a dialog box opens whenever a user performs an action that requires a comment. The user must select a comment from a list before proceeding.

❖ To create a list of predefined comments

1. If it is not already open, open the Authorization Manager by choosing **Start** > **Programs** or (**All Programs**) > **Thermo Foundation *x.x*** > **Authorization Manager**, where *x.x* is the version.
2. In the Global Security Features area, select the **Predefined Comments** check box.
3. Click **Edit**.

   The Comment List dialog box opens (Figure 40).

Figure 40. Comment List dialog box

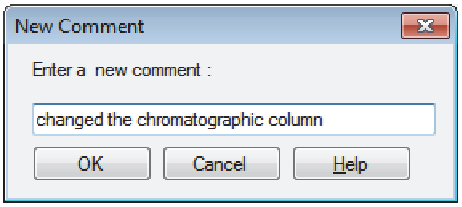


4. For each comment that you want to add to the list, do the following:

   a. Click **Add New Comment**.

      The New Comment dialog box opens (Figure 41).

      Figure 41. New Comment dialog box

      New Comment

      Enter a new comment :

      changed the chromatographic column

   b. Type the comment text and click **OK**.

5. Make any additional changes to the comment list:

   - To delete a comment from the list, select the comment and click **Remove Comment**.
   - To move a comment up or down in the list, select it and click **Move Up** or **Move Down**.

6. Click **OK** to save your changes and close the dialog box.

For more information about the Comment List and New Comments dialog boxes, see these topics:

- Comment List Dialog Box
- New Comment Dialog Box

Comment List Dialog Box

Use the Comment List dialog box to define a list of comments that a user must select from for features that require entering a comment.

Table 9 describes the parameters in the Comment List dialog box.

Table 9. Edit Comment List dialog box parameters

Parameter	Description
Comment	Displays the defined comments in the order that they appear to the user.
Buttons	
Add New Comment	Opens the New Comment dialog box where you can define a new comment.
Remove Comment	Deletes the selected comment in the Comment list.
Move Up	Moves the selected comment up one position in the Comment list.
Move Down	Moves the selected comment down one position in the Comment list.

New Comment Dialog Box

Use the New Comment dialog box to add comments to the list of predefined comments.

❖ To open the New Comment dialog box

1. In the Global Security Features area of the Authorization Manager, select the **Predefined Comments** check box and click **Edit**.
2. In the Comment List dialog box, click **Add New Comment**.

❖ To add a comment

1. Type text in the Enter a New Comment box.
2. Click **OK**.

   The text appears in the Comment area of the Comment List dialog box.

Table 10 describes the parameters in the New Comment dialog box.

Table 10. New Comment dialog box parameters

Parameter	Description
Enter A New Comment	Enter a new comment to be added to the comments list.
OK	Adds the new comment to the comment list in the Comments List dialog box

Step 4: Setting Up Additional Security Features for LCquan

Follow these procedures to set up the secure folders for the LCquan application and the secure template folder for the XReports for LCquan reporting application.

- Setting Up the List of Secure Folders for the LCquan Application
- Setting Up Secure Reports for the LCquan Application

Setting Up the List of Secure Folders for the LCquan Application

For the LCquan application, you can define a set of secure folders. Store all electronic records in protected folders. To ensure the application 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 the application name in the controlled features list and double-click **Root Folder**.

❖ To define the list of secure folders for the LCquan application

1. If it is not already open, open the Authorization Manager by choosing **Start > Programs** or (**All Programs**) **> Thermo Foundation *x.x* > Authorization Manager**, where *x.x* is the version.
2. Select **LCquan** in the features pane.

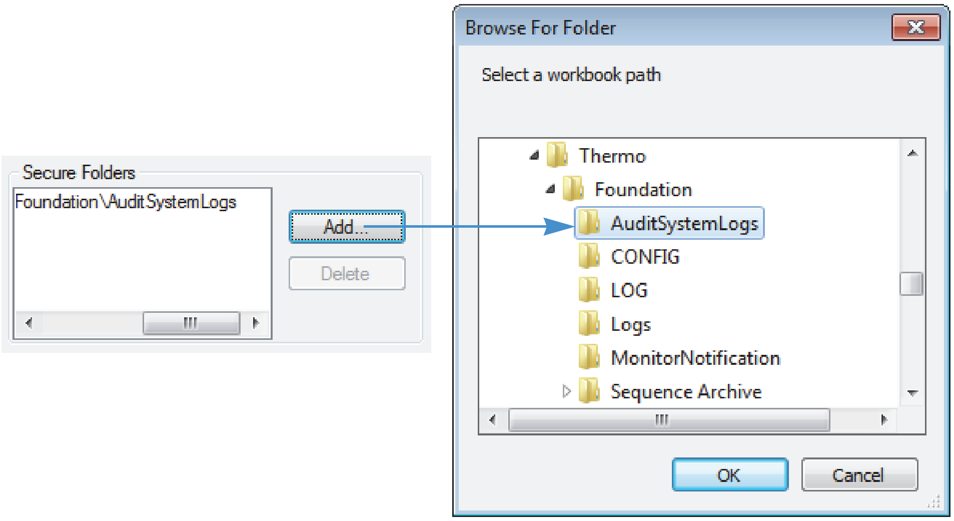
   The Secure Folders area becomes available.
3. For each folder that you want to add, do the following:

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

      The Browse For Folder dialog box opens (Figure 42).

IMPORTANT Define secure folders by using fully qualified path names. Use of mapped drive paths might result in network disconnection upon auto-logoff.

Figure 42. Browse for Folder dialog box



b. 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.

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.

Setting Up Secure Reports for the LCquan Application

You can limit a user group's authorization for creating quantitation reports to the secure XReport templates that you specify. After you configure the secure XReport templates feature in the Foundation Authorization Manager window, 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 Review Reports view, the options to print reports and create new XReport templates are not available.

See the following topics:

- About the Secure Reports
- Setting Up a Secure Template Folder
- Configuring Secure Reports
- Locking the Workbook After Creating Reports

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 application experiment. If user groups with different security privileges create reports from the same experiment, 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

Follow this procedure to restrict access to the XReport templates for the LCquan application.

❖ To configure secure reports

1. If it is not already open, open the Authorization Manager by choosing **Start** > **Programs** or (**All Programs**) > **Thermo Foundation *x.x*** > **Authorization Manager**, where *x.x* is the version.
2. Select a user group from the Secure Groups area.
3. In the list of controlled features (lower left side), select the **LCquan** application name and click **Expand Tree**.
4. In the Quantitate Section, select **Secure XReport Template**.
5. In the Permission Level area, select **Allowed**.

   For the Secure XReport Template feature, Allowed is the most restrictive setting.
6. In the Secure Template Folder area, click **Browse**.
7. In the Browse for Folder dialog box, select the folder that contains the secure templates and click **OK**.

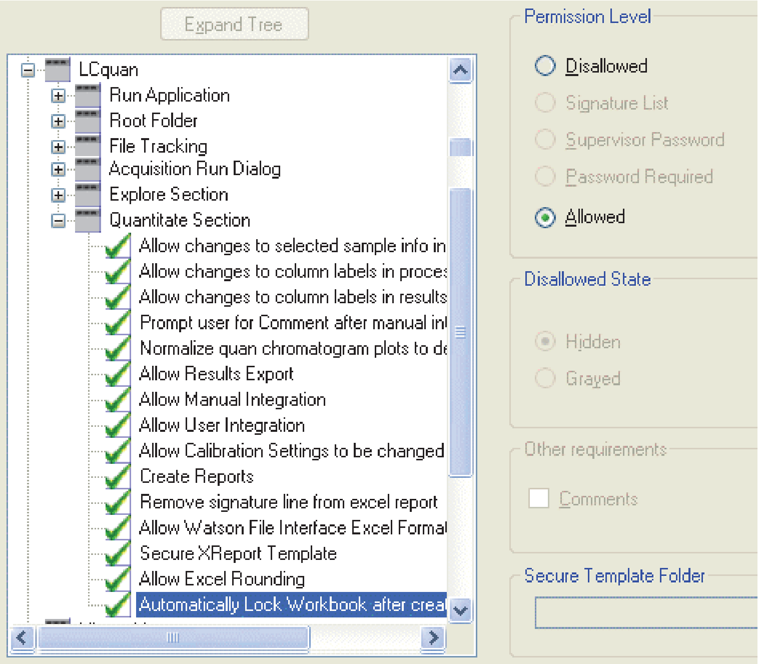
Locking the Workbook After Creating Reports

You can have the application automatically lock the LCquan workbook (not a copy of the workbook) after you create a report. A locked workbook (and its associated files) is a workbook that cannot be overwritten. You cannot save any changes made to a locked workbook, and you cannot acquire data in a locked workbook. You can create new reports, but the application does not save the report selections. When you open a locked workbook, the application displays [Locked] in the title bar next to the workbook name and in the status bar.

❖ To automatically lock the workbook after you create a report

1. If it is not already open, open the Authorization Manager by choosing **Start** > **Programs** or (**All Programs**) > **Thermo Foundation *x.x*** > **Authorization Manager**, where *x.x* is the version.
2. Select a user group in the Secure Groups box.

3. Click **Expand Tree** to show the entire list of controlled features for the application.



4. From the list, click the expand icon before the LCquan folder.

5. Click the expand icon before the Quantitate Section folder.

6. Select **Automatically Lock Workbook after Creating Reports**.

   The Permission Level options become available.

7. Select the **Allowed** option, and click **OK**.

Step 5: Saving the Security Settings

Before you close the Authorization Manager window, you must click OK to save the security settings.

❖ To save the security settings

After defining your user groups, setting the appropriate permission levels, and specifying the type of application auditing, click **OK** to save your settings and exit the Authorization Manager.

The controlled feature information is saved in a configuration file named XCAL.outi.

Prohibit non-administrator access to this folder by properly setting the security for this folder. If you have not already done this, see Chapter 3, “Establishing Secure File Operations.”

Viewing the Authorization Manager History Log

The 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 for the Authorization Manager

1. If it is not already open, open the Authorization Manager by choosing **Start > Programs** or (**All Programs**) > **Thermo Foundation *x.x*** > **Authorization Manager**, where *x.x* is the version.
2. Click **History Log**.

   Each entry in the history log contains the time and date, the user ID and full name, and a description of the event. Sort and filter the entries in the history log by field (for example, sort and filter by date and time) or print the log.

Printing the Security Settings

After you set up the user groups in the Authorization Manager, print a report.

❖ To print a report of the security settings for a secure user group

1. If it is not already open, open the Authorization Manager by choosing **Start > Programs** or (**All Programs**) > **Thermo Foundation *x.x*** > **Authorization Manager**, where *x.x* is the version.
2. In the Secure Groups area, select the secure group, and then click **Print**.

   The Print dialog box opens.
3. Select the appropriate printer and properties. Then click **OK**.

   The report contains a list of the members of the group, the controlled feature information for each application, and the names of any secure folders for each application.

Using the CRC Validator

The Thermo Foundation CRC Validator compares the cyclic redundancy check (CRC) value stored in the database for a file with the CRC value computed from the file stored on the hard disk. If the stored CRC value and the computed CRC value do not match, the file might have been corrupted or altered from the time when a layered application saved it. This chapter describes how to use the Foundation CRC Validator to check your files.

Contents

Note Close any open layered applications before running the Foundation CRC Validator.

Checking Files with the Foundation CRC Validator

This topic describes how to use the Foundation CRC Validator to check your files for changes or deletions.

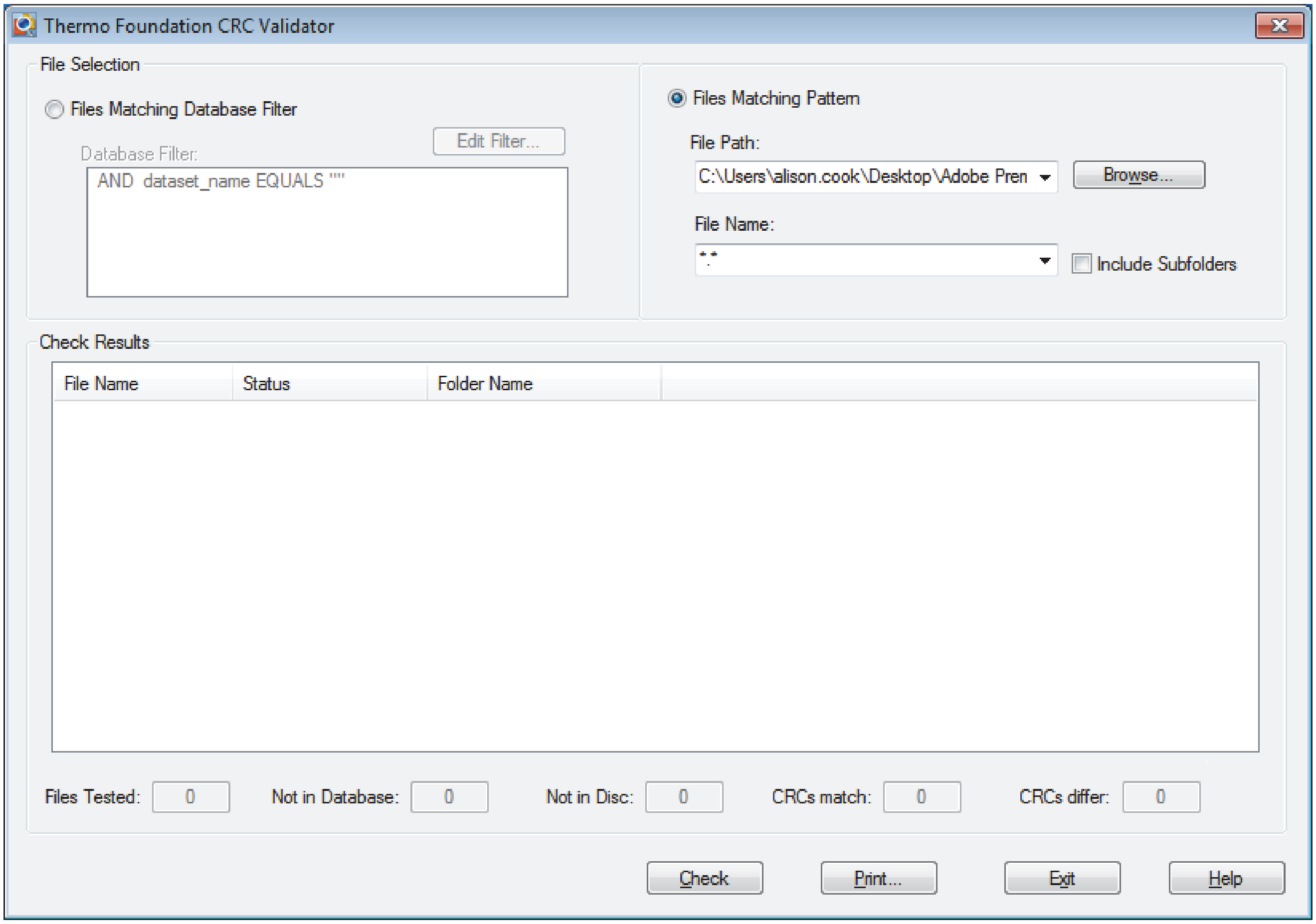
❖ To use the Foundation CRC Validator

1. From the Windows taskbar, choose **Start > Programs** (or **All Programs**) **> Thermo Foundation *x.x* > CRC Validation**, where *x.x* is the version.

   The Foundation CRC Validator window opens (Figure 43).

   For information about the parameters in this window, see "CRC Validator Parameters" on page 95.

   Figure 43. CRC Validator window



Thermo Foundation CRC Validator

File Selection

○ Files Matching Database Filter

Database Filter:

AND dataset_name EQUALS ""

● Files Matching Pattern

File Path: C:\Users\alison.cook\Desktop\Adobe Pren

File Name: *.*

□ Include Subfolders

Check Results

File Name	Status	Folder Name

Files Tested: 0 Not in Database: 0 Not in Disc: 0 CRCs match: 0 CRCs differ: 0

2. In the File Selection area, select a file selection method:

   - To select files that match a database filter, see "Selecting Files Using Database Filters" on page 91.
   - To select files that match a pattern, see "Selecting Files Using a Pattern" on page 94.

3. To check the selected files, do the following:

   a. Click **Check**.

      The validation commences.

   b. Examine the results displayed in the Check Results area.

      The Status column in the file list indicates the status of each file (see Table 11).

4. Click **Exit** to close the CRC Validator window.

Table 11. Status values for CRC Validation

Status	Description
CRCs Match	The CRC stored in the database matches the CRC just calculated for the file.
CRCs Do Not Match	The CRC stored in the database does not match the CRC just calculated for the file. Most likely, the file has been modified since the tracking record was created.
File Not In Database	The file was found on the hard disk, but not in the database. It might not be a tracked file.
File Not On Disk	The file was found in the database, but not on the hard disk. The file might have been archived or deleted.

Selecting Files Using Database Filters

Use the Filter Entries dialog box to specify how you want to filter the entries in the Audit Viewer or in the CRC Validator. By applying a filter, you can display a subset of the entries in the Audit Viewer or a subset of the entries to be validated in the CRC Validator.

When you select files using database filters, select files for validation or viewing on the basis of information about those files that is stored in the auditing database. For example, select files created by a particular layered application or select files created or modified at certain times.

Create two types of filters: non-date filters and date filters. Non-date filters are based on fields from the auditing database. Use them to select files based on characteristics, such as the application used to create the file or the name of the user who created the file. Use date filters to select files on the basis of the date when they were created or last modified.

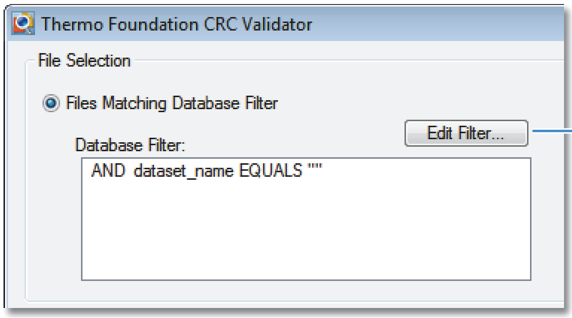
Combine multiple non-date filters using the AND and OR operators. The default filter is the most recently selected dataset name.

❖ To select files using a database filter

1. Depending on the application, open the Filter Entries dialog box as follows:

   - In the CRC Validator, select the **Files Matching Database Filter** option in the File Selection area. Then, click **Edit Filter** (Figure 44).

     Figure 44. Upper-left portion of the CRC Validator window, showing the Edit Filter button

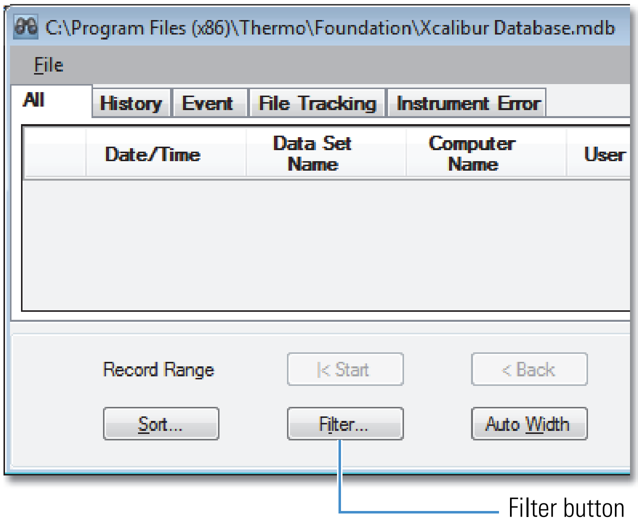
     ● Files Matching Database Filter

     Database Filter:
     AND dataset_name EQUALS ""

     Edit Filter button

   - In the Audit Viewer, click **Filter** (Figure 45).

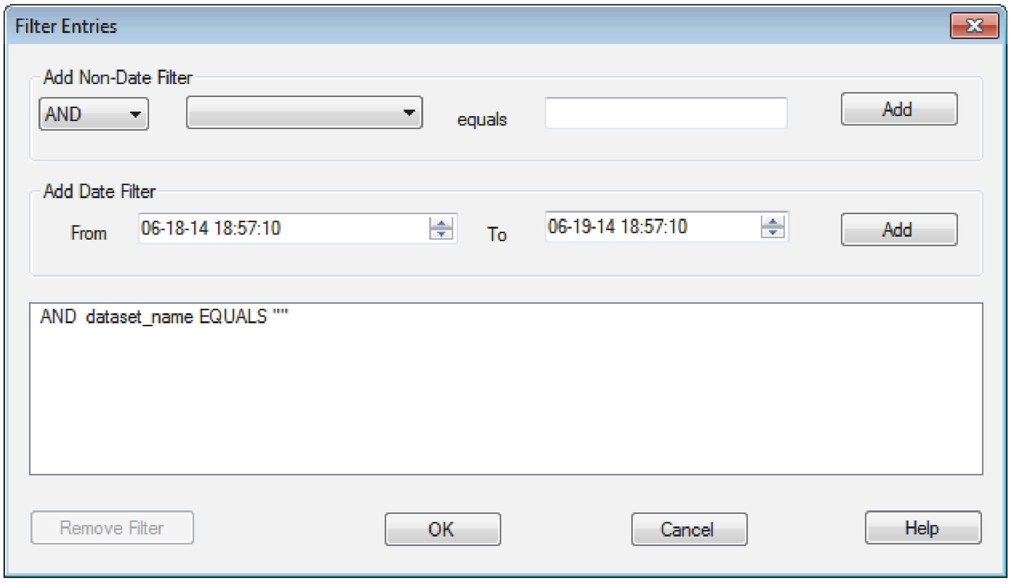
     Figure 45. Left side of the Audit Viewer, showing the Filter button

     Filter button

The Filter Entries dialog box opens (Figure 46). For parameter descriptions, see “Filter Entries Dialog Box” on page 97.

Figure 46. Filter Entries dialog box



AND

06-18-14 18:57:10

06-19-14 18:57:10

AND dataset_name EQUALS ""

2. For each non-date filter that you want to add, do the following in the Add Non-Date Filter area:

    a. In the first list, select **AND** or **OR**.

    b. In the second list, select the database key to filter on.

    c. In the Equals box, type the value for the database key. For example, if you selected Application Name in the second list, you might enter Home Page or Qual Browser in the Equals box.

    d. Click **Add** to add this filter to the list of current filters.

3. For each date filter that you want to add, do the following in the Add Date Filter area:

    a. In the From box, enter the starting date and time for the filter.

    b. In the To box, enter the ending date and time for the filter.

    c. Click **Add** to add this filter to the list of current filters.

4. To remove unwanted filters from the filter list, click the filter name in the list and click **Remove Filter**.

5. When you have made all needed changes, click **OK** to save your changes and close the dialog box.

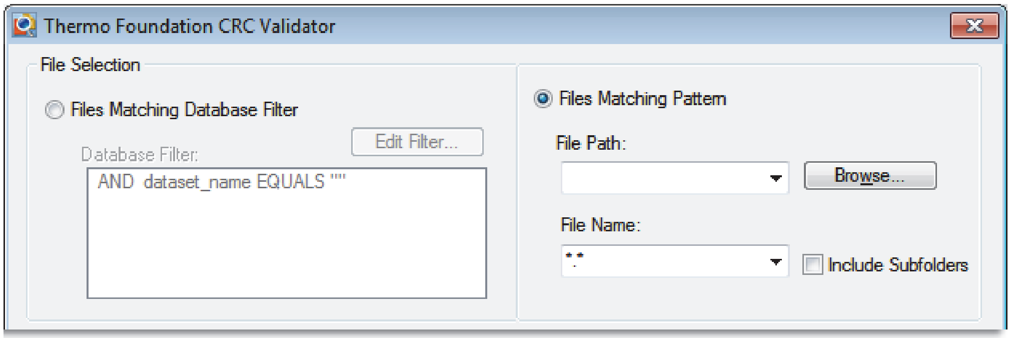
Selecting Files Using a Pattern

When selecting files that use a pattern, specify the folder containing the files and the format type of the files [for example, a raw data file (RAW)].

❖ To select files using a pattern

1. In the File Selection area of the CRC Validator window, select the **Files Matching Pattern** option (Figure 47).

   Figure 47. File Selection area of the CRC Validator window with the Files Matching Pattern option selected



Thermo Foundation CRC Validator

File Selection

○ Files Matching Database Filter

Database Filter:

AND dataset_name EQUALS ""

● Files Matching Pattern

File Path:

File Name: *.*

□ Include Subfolders

2. In the File Path list, select the path to the folder containing the files to check or click **Browse** to find the folder.

3. In the File Name list, select the file extension of the files to check.

4. Select the **Include Subfolders** check box to have the CRC Validator check files in subfolders of the selected folder.

5. Click **OK** to save your changes and close the dialog box.

CRC Validator Parameters

Use the CRC Validator window to compare the cyclic redundancy check (CRC) value stored in the database with the one calculated for the current file or files on the hard disk.

❖ To open the CRC Validator window

From the Windows taskbar, choose **Start** > **Programs** (or **All Programs**) > **Thermo Foundation *x.x*** > **CRC Validator**, where *x.x* is the version.

Table 12 describes the parameters in the CRC Validator window.

Table 12. CRC Validator parameters (Sheet 1 of 2)

Parameter	Description
File Selection	
Files Matching Database Filter	Select files by using the filter shown in the Database Filter box.
Edit Filter button	Opens the Filter Entries dialog box where you specify how you want to filter the entries in the Audit Viewer or in the CRC Validator. For information about the Filter Entries dialog box, see "Filter Entries Dialog Box" on page 97.
Database Filter	Displays the current database filter. This box is read-only. The default filter is the last selected dataset name. To change the filter, click **Edit Filter**.
Files Matching Pattern	Select files matching the file pattern listed in the File Path and File Name lists.
File Path	Specifies the path to files to be checked. You can enter the path manually or click Browse to select the path.
File Name	Specifies the name of the file to check. You can use a wildcard character to represent one or more characters in the file name. Use an asterisk (*) as a substitute for zero or more characters. Use a question mark (?) as a substitute for a single character in the file name. You can also select a common file extension from the list.
Include Subfolders	Selecting this check box includes all subfolders in the search for matching files.

Table 12. CRC Validator parameters (Sheet 2 of 2)

Parameter	Description
Check Results	
Displays the results of the comparison of the CRC value for each selected file. The table includes the name of the file tested, the status of the check, and the full path to the file.	
File Name	Displays the name of the file tested, including the extension.
Status	Displays the status of the check. The status value is one of the following: • CRCs Match: The CRC stored in the database matches the CRC just calculated for the file. • CRCs Do Not Match: The CRC stored in the database does not match the CRC just calculated for the file. Most likely, the file has been modified since the tracking record was created. • File Not In Database: The file was found on the hard disk but was not found in the database. It might not be a tracked file. • File Not On Disk: The file was found in the database but was not found on the hard drive. The file might have been deleted or archived.
Folder Name	Displays the full path to the file.
Files Tested	Displays the total number of files tested.
Not In Database	Displays the number of files that were not found in the database.
Not On Disc	Displays the number of files that are in the database but could not be found on the disk.
CRCs Match	Displays the number of files where the CRC value stored in the database matches the CRC just calculated for the file.
CRCs Differ	Displays the number of files where the CRC value stored in the database does not match the CRC just calculated for the file.
Buttons	
Check	Starts the comparison of the CRC value stored in the database with the one calculated for the specified file or files on the hard disk.
Print	Opens the Print dialog box, where you select the print options and then click OK to print a hard copy of the CRC validation report or to save the report as a PDF file by using a PDF printer. The report contains which filter or file mask was used and the time and date when the report was produced.

Filter Entries Dialog Box

Table 13 describes the parameters in the Filter Entries dialog box.

For information about filtering database entries in the CRC Validator window, see "Selecting Files Using Database Filters" on page 91. For information about filtering data in the Audit Viewer, see "Filtering Audit Viewer Entries" on page 104.

Table 13. Filter Entries dialog box parameters (Sheet 1 of 2)

Parameter	Description
Add Non-Date Filter	
Operator	Specifies the operator (AND or OR) used in the filter.
Field	Specifies the field to filter, for example, Application Name. Selections: • CRC Validator window: Application Name, Comments, Computer Name, Dataset Name, File Status, Filename, Full Name, Path, or User Name. • Audit Viewer – All page: Application Name, Comments, Computer Name, Data Set Name, File Status, Full Name, or User Name • Audit Viewer – History page: Application Name, Change Type, Computer Name, Data Set Name, File Name, Full Name, Item Changed, New Row, New Value, Old Row, Old Value, Path, User Data, or User Name • Audit Viewer – Event page: Application Name, Comments, Computer Name, Data Set Name, Event, Full Name, Response, or User Name • Audit Viewer – File Tracking page: Application Name, Comments, Computer Name, Data Set Name, File Name, File Status, Full Name, Path, or User Name • Audit Viewer – Instrument Error page: Application Name, Computer Name, Data Set Name, Device VI State, Full Name, Instrument Error Code, Instrument Error Severity, Instrument Error String, Time Offset, or User Name
Equals String	Specifies the field value to filter, for example, Authorization Manager. Type an alphanumeric text string in this box.
Add button	Adds the new filter to the Filter Entry box.

Table 13. Filter Entries dialog box parameters (Sheet 2 of 2)

Parameter	Description
Add Date Filter	
From Date/Time	Specifies the earliest date and time for the time/date range for the filter.
To Date/Time	Specifies the latest date and time for the time/date range for the filter.
Add button	Adds the new filter to the Filter Entry box.
Filter Entry box	Specifies the filters that an application uses to filter the audit records. You can click the filters to select them. When a filter is selected, the Remove Filter button becomes available.
Button	
Remove Filter	Deletes the selected filter in the Filter Entry box.

6

Auditing

This chapter describes how to use the Audit Viewer utility for auditing functions. You can perform these auditing functions:

- Display all auditable events and changes made to files created or managed by various Thermo Scientific applications.
- View a history of what has been done during data acquisition and data processing.
- Get information about all auditable events that have occurred within the application.

When you open the Audit Trail from within the Xcalibur data system, you can view the same information that is provided in the Audit Viewer utility; however, you cannot print reports.

Contents

Viewing Audit Viewer Databases

The Foundation platform, Xcalibur data system, or LCquan application writes to the Global Auditing database and maintains the application's local databases. The Global Auditing database stores the application start and stop events. All other application events are stored in the local databases for the application.

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

- The Global Auditing database 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 local application database keeps a log of auditable events associated with the current application, including the entries that have not been saved to the database. Each application database also includes a log about the raw files that are acquired as part of the application. For the LCquan application, the audit database is the LCquan Workbook Audit Trail.

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.

IMPORTANT You must configure the database in the Thermo Foundation Auditing Database Configuration Manager before you can access the Global Auditing database. See "Configuring Your Auditing Database" on page 12.

To access the databases, follow these procedures:

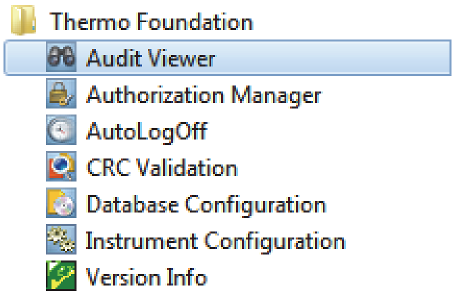
- Accessing the Global Auditing Database
- Accessing the Local Database

Accessing the Global Auditing Database

The Global Auditing database is a log of auditable events for all the application-related data files and applications that it recognizes. You access the Global Auditing database when you start Audit Viewer from the Windows taskbar.

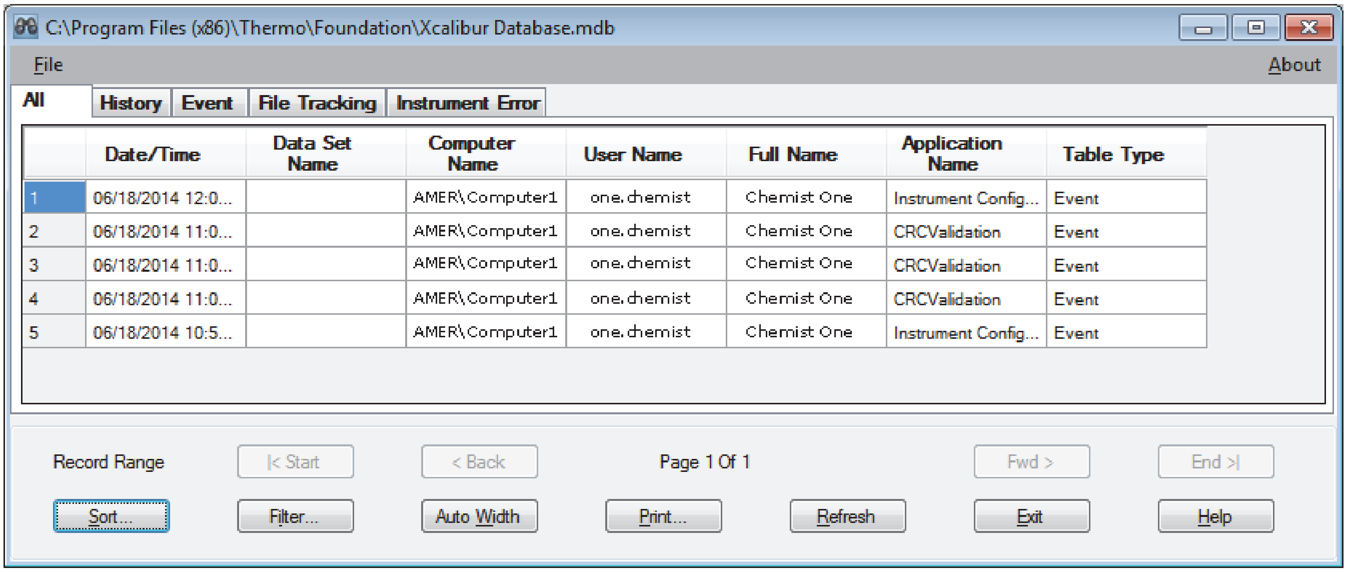
❖ To start Audit Viewer from the Windows taskbar

Choose **Start** > **Programs** (or **All Programs**) > **Thermo Foundation *x.x*** > **Audit Viewer**, where *x.x* is the version.



The Audit Viewer window opens. The window title bar shows the location of the database being viewed (Figure 48).

Figure 48. Audit Viewer – All page



C:\Program Files (x86)\Thermo\Foundation\Xcalibur Database.mdb

	Date/Time	Data Set Name	Computer Name	User Name	Full Name	Application Name	Table Type
1	06/18/2014 12:0...		AMER\Computer1	one.chemist	Chemist One	Instrument Config...	Event
2	06/18/2014 11:0...		AMER\Computer1	one.chemist	Chemist One	CRCValidation	Event
3	06/18/2014 11:0...		AMER\Computer1	one.chemist	Chemist One	CRCValidation	Event
4	06/18/2014 11:0...		AMER\Computer1	one.chemist	Chemist One	CRCValidation	Event
5	06/18/2014 10:5...		AMER\Computer1	one.chemist	Chemist One	Instrument Config...	Event

Accessing the Local Database

The local database for an application is a log of auditable events associated with the current view or window (Xcalibur data system) or workbook (LCquan application), including the entries that have not been saved to the database. Each database also includes a log about the raw files that are acquired as part of the Xcalibur study or LCquan workbook.

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

❖ To access the auditing database for an LCquan workbook or an Xcalibur window or view

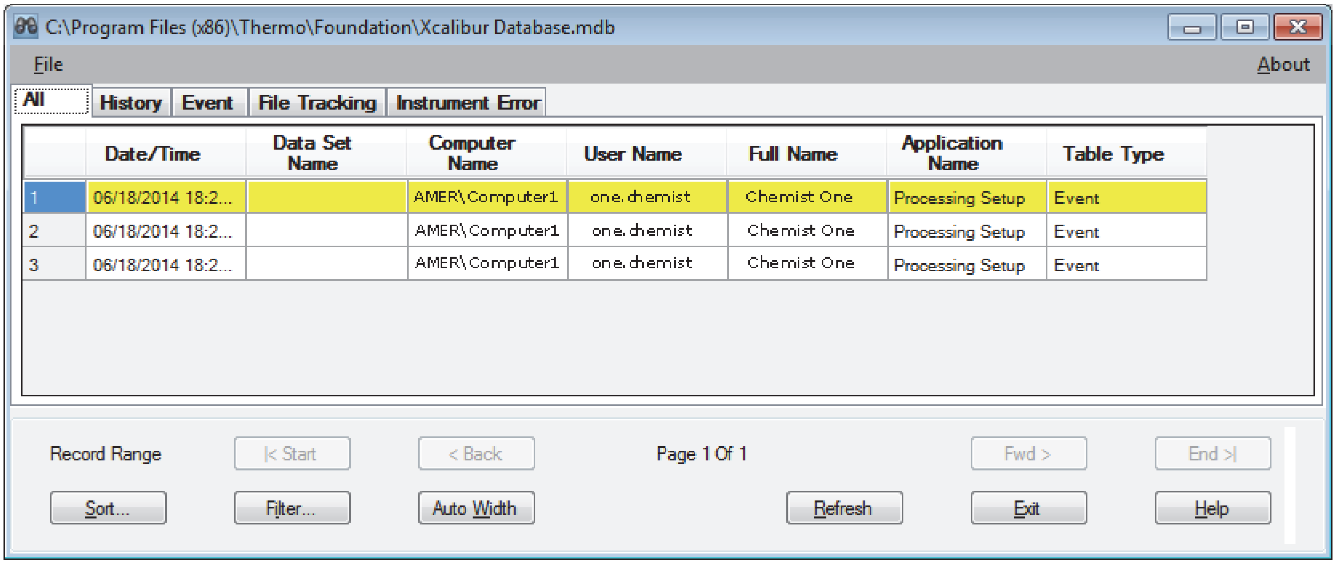
1. Open the LCquan workbook or Xcalibur window or view.

2. In the LCquan Workbook window or the Xcalibur view or window, choose **File > Audit Trail**.

   The Audit Viewer window opens and displays the entries for the open study or workbook. Yellow highlights indicate any unsaved entries. In the LCquan application, you can open more than one workbook at a time.

   Figure 49 shows the audit trail for the Processing Setup window of the Xcalibur data system. You cannot print an audit trail from within the Xcalibur data system. To print the audit trail for a specific application in the Xcalibur data system, you must open the Thermo Foundation Audit Viewer and select the application in the Filter Entries dialog box.

Figure 49. Audit Viewer – All page



C:\Program Files (x86)\Thermo\Foundation\Xcalibur Database.mdb

	Date/Time	Data Set Name	Computer Name	User Name	Full Name	Application Name	Table Type
1	06/18/2014 18:2...		AMER\Computer1	one.chemist	Chemist One	Processing Setup	Event
2	06/18/2014 18:2...		AMER\Computer1	one.chemist	Chemist One	Processing Setup	Event
3	06/18/2014 18:2...		AMER\Computer1	one.chemist	Chemist One	Processing Setup	Event

Record Range

Page 1 Of 1

Viewing Audit Viewer Pages

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

- The All page (see "All Page of the Audit Viewer" on page 110) 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 page (see "History Page of the Audit Viewer" on page 111) provides a chronological listing of all the changes made to method files and result lists.

- The Event page (see "Event Page of the Audit Viewer" on page 113) lists all user-initiated auditable events. All events that are subject to authorization control are auditable.

- The File Tracking page (see "File Tracking Page of the Audit Viewer" on page 114) provides the following type of information:

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

  – Local application database: Lists the changes made within the application or to any application-owned files in the LCquan workbook or Xcalibur window, including the LCquan 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 application that are tracked in the Global Auditing database.

    For any files that are modified outside of the application, the Foundation platform displays a file-tracking error message.

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

- The Instrument Error page (see "Instrument Error Page of the Audit Viewer" on page 116) lists events that occur to instruments that the Xcalibur data system creates or manages.

Filtering Audit Viewer Entries

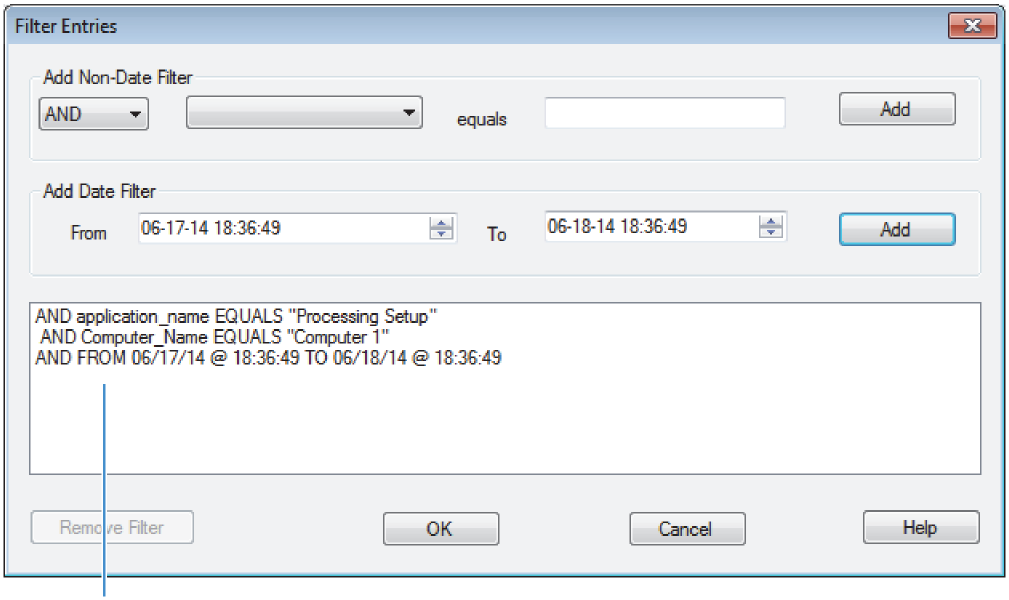
By applying a filter, you can display a subset of the entries in the Audit Viewer window. You can set up two types of filters: filters that are based on dates and filters that are not based on dates (non-date filters). You can use a combination of the two types of filters. For information about the parameters in this dialog box, see "Filter Entries Dialog Box" on page 97.

❖ To set up a non-date filter

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

   The Filter Entries dialog box opens (Figure 50).

Figure 50. Filter Entries dialog box



AND

From 06-17-14 18:36:49 To 06-18-14 18:36:49

```
AND application_name EQUALS "Processing Setup"
 AND Computer_Name EQUALS "Computer 1"
AND FROM 06/17/14 @ 18:36:49 TO 06/18/14 @ 18:36:49
```

Searches for records created by on Computer1 between
6:36 PM on June 17 and 6:36 PM on June 18.

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 drop-down 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** in the Filter Entries dialog box.

The Audit Viewer window displays the results on the All page. For more information about this page, see "All Page of the Audit Viewer" on page 110.

Sorting Audit Viewer Entries

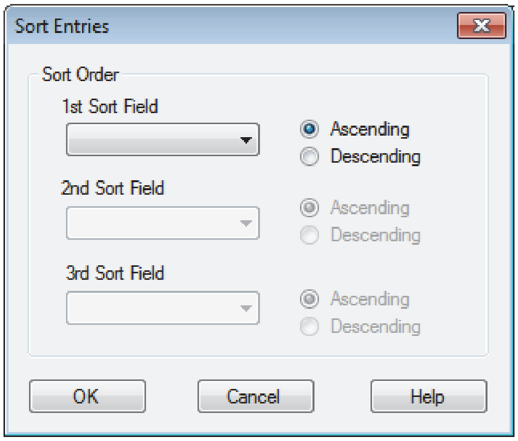
You can sort entries by the column headings on each of the Audit Viewer pages. For more information about these pages, see "Viewing Audit Viewer Pages" on page 103.

❖ 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 (Figure 51).

   Figure 51. Sort Entries dialog box



3. In the 1st Sort Field list, select a column heading and select the **Ascending** or **Descending** option.
4. Repeat this step for the 2nd Sort Field and 3rd Sort Field.
5. Click **OK**.

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

Sort Entries Dialog Box

Use the Sort Entries dialog box to specify how to sort the entries in the Audit Viewer. Each page in the Audit Viewer has a unique set of fields that you can sort.

Table 14. Sort Entries dialog box parameters

Parameter	Description
1st Sort Field	Specifies the first field in the log that is sorted.
2nd Sort Field	Specifies the second field in the log that is sorted. You cannot specify a second sort field if the first sort field is not already defined.

Table 14. Sort Entries dialog box parameters

Parameter	Description
3rd Sort Field	Specifies the third field in the log that is sorted. You cannot specify a third sort field if the second sort field is not already defined.
Ascending	Sorts fields in ascending order.
Descending	Sorts fields in descending (reverse) order.

Printing Audit Viewer Entries

The printing options vary depending on whether you are printing the Audit Trail for the Global Auditing Database (Audit Viewer) or a local database (Audit Trail).

- Printing the Audit Trail for the Global Auditing Database
- Printing the Audit Trail from LCquan

Printing the Audit Trail for the Global Auditing Database

Follow this procedure to print the information on one of the Thermo Foundation Audit Viewer pages.

❖ **To print the Audit Trail for the Global Auditing database**

1. From the Windows taskbar, choose **Start** > **Programs** (or **All Programs**) > **Thermo Foundation *x.x*** > **Audit Viewer**, where *x.x* is the version.

   The Audit Viewer window opens.

2. Click the tab of the page you want to print.

3. Click **Print**.

   The Print Options dialog box opens. For descriptions of these parameters, see Table 15 on page 109.

4. Select the printing options (see Print Options Dialog Box) and then click **OK**.

Printing the Audit Trail from LCquan

You can print the entries from an LCquan application database only when you save all displayed records on the specific page of the Audit Viewer window. Use the Print Options dialog box (see Table 15) to choose document properties for printing the log.

> **Note** In the Xcalibur data system, you cannot print the Audit Trail for an application window.

❖ To print the Audit Trail for an application database

1. In the application study window, choose **File > Audit Trail**.
2. Do one of the following:
   - If the Xcalibur or LCquan study already contains saved entries, go to step 3.
   - If the Xcalibur or LCquan study contains any unsaved entries, the Foundation platform displays a View Audit Trail message prompting you to save the study before continuing.

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

     – Click **Yes** to save the study entries.

     The Foundation platform logs the automatic save in the Audit Trail and starts Audit Viewer.

     – Click **No** to start Audit Viewer without saving the study.

   > **Note** If you select the Don't Tell Me About This Again check box, the Foundation platform automatically applies the last requested behavior (Save or Not Save) each time you start Audit Viewer when the application contains unsaved entries. To restore the message, choose **Options > Enable Warnings**.
3. In the Audit Viewer window, click the tab of the page that you want to print.
4. Make sure the displayed page contains only saved entries. Yellow highlights appear on the rows of any unsaved entries.

   If you have a mix of saved and unsaved entries, you can do one of the following:
   - In the application window, choose **File > Save** to save the application study. 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. See “Filtering Audit Viewer Entries” on page 104 for details.
5. Click **Print**.
6. In the Print Options dialog box, select printing options, and then click **OK**.

Print Options Dialog Box

Use the Print Options dialog box to set up the print options for logs and audit trails.

Table 15. Print Options dialog box parameters

Parameter	Description
Printer Options	
Orientation: Portrait	Print the log vertically.
Orientation: Landscape	Print the log horizontally.
Font Size: Small	Print the log in 8-point font.
Font Size: Medium	Print the log in 10-point font.
Font Size: Large	Print the log in 12-point font.

Audit Viewer Parameters

The Thermo Foundation Audit Viewer displays all auditable events and changes made to files created or managed by an application on the Foundation platform.

Audit Viewer has the following pages:

- All Page of the Audit Viewer
- History Page of the Audit Viewer
- Event Page of the Audit Viewer
- File Tracking Page of the Audit Viewer
- Instrument Error Page of the Audit Viewer

When you double-click a log item on the All page, the Audit Viewer displays the page associated with the log item and highlights the item on that page. The History page provides a chronological listing of all of the changes made to method files, result lists, or both. The Event page lists auditable software application events that the user initiated. The File Tracking page lists all changes made to data files.

The Audit Viewer has slightly different capabilities when run as a stand-alone application than when run from within a Thermo Scientific application.

- When you run the Audit Viewer as a stand-alone application (by choosing **Start > Programs** (or **All Programs**) **> Thermo Foundation *x.x* > Audit Viewer**, where *x.x* is the version), the Audit Viewer displays all items in the database (excluding any uncommitted items or unsaved changes), and you can print the data.
- When you open the Audit Viewer from within most applications (by choosing **File > Audit Trail**), the Audit Viewer displays only the items associated with the current application, including uncommitted items and you cannot print the data.
- When you open Audit Viewer from within the LCquan application (by choosing **File > Audit Trail**), the Audit Viewer window displays both committed and uncommitted items and you can print the committed items.

In addition, you can access these two dialog boxes from the Audit Viewer:

- Sort Entries Dialog Box
- Filter Entries Dialog Box

All Page of the Audit Viewer

The All page of the Audit Viewer displays all auditable events and changes made to files created by or managed by a layered application. When you double-click a log item on the All page, the Audit Viewer displays the page associated with the log item and highlights the item on that page.

Table 16 describes the parameters on the All page of the Audit Viewer.

Table 16. All page parameters (Sheet 1 of 2)

Parameter	Description
Date/Time	Displays when the log entry occurred.
Dataset Name	Displays the dataset that contains the affected files.
Computer Name	Displays the name of the workstation where the item change originated.
User Name	Displays the logon name of the user who changed the item. The administrator of the network assigns logon names for each user.
Full Name	Displays the descriptive name of the user who changed the item. Often, this is the first and last name of the user. The administrator of the network assigns a full name to the logon name for each user.
Application Name	Displays the name of the software application that is associated with the log entry.

Table 16. All page parameters (Sheet 2 of 2)

Parameter	Description
Table Name	Displays the type of record: History, Event, or File Tracking. The log entry is found on this page of the Audit Viewer.
Buttons	
Sort	Opens the Sort Entries dialog box, where you can specify how you want to sort the entries in the Audit Viewer. See "Sorting Audit Viewer Entries" on page 106.
Filter	Opens the Filter Entries dialog box, where you can specify how you want to filter the entries in the Audit Viewer. See "Filtering Audit Viewer Entries" on page 104.
Auto Width	Expands the table columns to display the longest entry in that column.
Print	Prints an active file or document.
Refresh	Updates the log.

History Page of the Audit Viewer

The History page of the Audit Viewer provides a chronological listing of all of the parameter changes made to method files or result lists.

Table 17 describes the parameters on the History page of the Audit Viewer.

Table 17. History page parameters (Sheet 1 of 2)

Parameter	Description
Date/Time	Displays when the log entry occurred.
Dataset Name	Displays the dataset that contains the affected files.
Computer Name	Displays the name of the workstation where the item change originated.
User Name	Displays the logon name of the user who changed the item that is listed in the Item Changed field. The administrator of the network assigns logon names for each user.
Full Name	Displays the full name of the user who changed the item that is listed in the Item Changed field. Often, this is the first and last name of the user. The administrator of the network assigns a full name to the logon name for each user.
Application Name	Displays the name of the software application that is associated with the log entry.

Table 17. History page parameters (Sheet 2 of 2)

Parameter	Description
Filename	Displays the name of the affected file. The file name is not case-sensitive.
Path	Displays the route through the file system to the affected file.
Old Row	Displays the pre-change row number of the item if the change resulted in a change of row number.
New Row	Displays the post-change row number of the item if the change resulted in a change of row number.
Change Type	Displays the type of operation (edit, delete, and so on) that changed the item.
Item Changed	Displays the setting that was changed.
Old Value	Displays the old value of the item that is listed in the Item Changed field (if applicable).
New Value	Displays the new value of the item that is listed in the Item Changed field.
User Data 1	Displays custom user data, if supported by the application. The user data is unique for each application.
User Data 2	Displays custom user data, if supported by the application. The user data is unique for each application.
User Data 3	Displays custom user data, if supported by the application. The user data is unique for each application.
User Data 4	Displays custom user data, if supported by the application. The user data is unique for each application.
User Data 5	Displays custom user data, if supported by the application. The user data is unique for each application.
Buttons	
Sort	Opens the Sort Entries dialog box, where you can specify how you want to sort the entries in the Audit Viewer. See “Sorting Audit Viewer Entries” on page 106.
Filter	Opens the Filter Entries dialog box, where you can specify how you want to filter the entries in the Audit Viewer. See “Filtering Audit Viewer Entries” on page 104.
Auto Width	Expands the table columns to display the longest entry in that column.
Print	Prints an active file or document.
Refresh	Updates the log.

Event Page of the Audit Viewer

The Event page of the Audit Viewer lists auditable application events that were initiated by the user. Events can include starting a Thermo Scientific application, printing a file from within a Thermo Scientific application, and importing a file from within an application.

Table 18 describes the parameters on the Event page of the Audit Viewer.

Table 18. Event page parameters (Sheet 1 of 2)

Parameter	Description
Date/Time	Displays when the event occurred.
Dataset Name	Displays the data set that contains the affected files.
Computer Name	Displays the name of the workstation initiating the event.
User Name	Displays the logon name of the user who initiated the event. The administrator of the network assigns logon names for each user.
Full Name	Displays the descriptive name of the user who initiated the event. Often, this is the first and last name of the user. The administrator of the network assigns a full name to the logon name for each user.
Application Name	Displays the name of the software application that is associated with the event.
Event	Displays what occurred. Typical events include importing and exporting data files, methods, and sequences.
Response	Displays the action taken by the user (if any) in response to the event.
Comment	Displays the comment associated with the event.
Buttons (at the bottom of the window)	
Sort	Opens the Sort Entries dialog box, where you can specify how you want to sort the entries in the Audit Viewer. See “Sorting Audit Viewer Entries” on page 106.
Filter	Opens the Filter Entries dialog box, where you can specify how you want to filter the entries in the Audit Viewer. See “Filtering Audit Viewer Entries” on page 104.
Auto Width	Expands each table column to display the longest entry in that column.

Table 18. Event page parameters (Sheet 2 of 2)

Parameter	Description
Print	Opens the Print Options dialog box, where you can select the page orientation and font size for the report. Clicking OK in the Print Options dialog box opens the Print dialog box, where you can select the printer, print range, and number of copies. Clicking OK in the Print box sends the document to the specified printer. The document to be printed is the current Audit Viewer page.
Refresh	Updates the log.

File Tracking Page of the Audit Viewer

The File Tracking page of the Audit Viewer lists significant events that occur to files that a Thermo Scientific application creates or manages. File tracking helps to make sure the data on the hard disk is not tampered with.

Table 19 describes the parameters on the File Tracking page of the Audit Viewer.

Table 19. File Tracking page parameters (Sheet 1 of 2)

Parameter	Description
Date/Time	Displays when the log entry occurred.
Dataset Name	Displays the data set that contains the affected files.
Computer Name	Displays the name of the workstation performing the file change.
User Name	Displays the logon name of the user who changed the file. The administrator of the network assigns logon names for each user.
Full Name	Displays the descriptive name of the user who changed the file. Often, this is the first and last name of the user. The administrator of the network assigns a full name to the logon name for each user.
Application Name	Displays the name of the software application that was used to change the file.
File name	Displays the name of the affected file. The file name is **not** case-sensitive.
Path	Displays the route through the file system to the affected file.

Table 19. File Tracking page parameters (Sheet 2 of 2)

Parameter	Description
File Status	Displays the operation or action that caused the entry to be made in the log: • File is created • File was copied • File was moved • File was deleted • File was modified • File was renamed • Result of rename • Old folder name • New folder name • Result of file move
Comment	Displays the comment associated with the log entry.
Buttons (at the bottom of the window)	
Sort	Opens the Sort Entries dialog box, where you can specify how you want to sort the entries in the Audit Viewer. See "Sorting Audit Viewer Entries" on page 106.
Filter	Opens the Filter Entries dialog box, where you can specify how you want to filter the entries in the Audit Viewer. See "Filtering Audit Viewer Entries" on page 104.
Auto Width	Expands each table column to the longest entry in that column.
Print	Opens the Print Options dialog box, where you can select the page orientation and font size for the report. Clicking OK in the Print Options dialog box opens the Print dialog box, where you can select the printer, print range, and number of copies. Clicking OK in the Print box sends the document to the specified printer. The document to be printed is the current Audit Viewer page.
Refresh	Updates the log.

Instrument Error Page of the Audit Viewer

The Instrument Error page of the Audit Viewer lists error codes from instruments.

The Audit Viewer has slightly different capabilities when run as a stand-alone application than when run from within a Thermo Scientific application.

- When you run the Audit Viewer as a stand-alone application (by choosing **Start > All Programs > Thermo Foundation *x.x* > Audit Viewer**, where *x.x* is the version), you can view and print all items in the database (excluding any uncommitted items or unsaved changes).
- When you open the Audit Viewer from within an application (by choosing File > Audit Trail), the Audit Viewer window displays only the items associated with the current application, including uncommitted items. However, you cannot print the data.

Table 20 describes the parameters on the Instrument Error page of the Audit Viewer.

Table 20. Instrument Error page parameters (Sheet 1 of 2)

Parameter	Description
Date/Time	Displays when the log entry occurred.
Computer Name	Displays the name of the workstation performing the change.
User Name	Displays the logon name of the user who made the change that caused the error notification. The administrator of the network assigns logon names for each user.
Full Name	Displays the descriptive name of the user who made the change that caused the error notification. Often, this is the first and last name of the user. The administrator of the network assigns a full name to the logon name for each user.
Application Name	Displays the name of the software application that was used to change the instrument.
Dataset Name	Displays the data set that contains the affected instrument.
Instrument Error Code	Displays the code that the application produced when it received information about the instrument error.
Instrument Error Severity	Displays the severity error level for the incident.
Instrument Error String	Displays the instrument error string that was produced.
Device VI State	Displays the status of the device at the time the log event occurred.
Time Offset	If an acquisition was in progress when the log event occurred, view the acquisition time. If no acquisition was in progress, this field reads zero.

Table 20. Instrument Error page parameters (Sheet 2 of 2)

Parameter	Description
Buttons (at the bottom of the window)	
Sort	Opens the Sort Entries dialog box, where you can specify how you want to sort the entries in the Audit Viewer. See "Sorting Audit Viewer Entries" on page 106.
Filter	Opens the Filter Entries dialog box, where you can specify how you want to filter the entries in the Audit Viewer. See "Filtering Audit Viewer Entries" on page 104.
Auto Width	Expands each table column to the longest entry in that column.
Print	Opens the Print Options dialog box, where you can select the page orientation and font size for the report. Clicking OK in the Print Options dialog box opens the Print dialog box, where you can select the printer, print range, and number of copies. Clicking OK in the Print box sends the document to the specified printer. The document to be printed is the current Audit Viewer page.
Refresh	Updates the log.

7

Setting Up the Instrument Configuration

This chapter describes how to set up the instrument configuration for your LC/MS or GC/MS system by using the Thermo Foundation Instrument Configuration window.

Contents

Adding, Removing, and Configuring the Instrument Drivers

To control a Thermo Scientific GC/MS or LC/MS system from the Xcalibur data system or LCquan application, you add the devices that make up the system to the list of configured devices for the system, and then set up the configuration options for each device.

The data system does not automatically recognize some of the hardware options for the configured instrument devices. For example, the data system cannot sense the size of the sample loop installed on the autosampler injection valve or the tray type installed in the autosampler tray compartment. For most Thermo Scientific mass spectrometers, the data system does automatically recognize the ion source.

Use the Thermo Foundation Instrument Configuration window to review all available devices and to add and configure the devices that you want to control from the data system computer.

❖ To open the Thermo Foundation Instrument Configuration window

Choose **Start > Programs > Thermo Foundation *x.x* > Instrument Configuration**, where *x.x* is the version.

❖ To add devices to the instrument configuration

1. To choose the type of hardware devices to add, select a device type in the Device Types list. The selections include the following: All, Autosampler, Gas Chromatograph, Liquid Chromatograph, Mass Spectrometer, Detector, or Other.

   Selecting All displays all of the installed device drivers in the Available Devices list.

> **Note** If you do not see the device you want to add, you might need to install the device driver.

2. For each device that you want to add to the instrument configuration, in the Available Devices list do the following:

   - Select the device icon, and then click **Add**.

   –or–

   - Double-click the device icon.

   A copy of the device icon appears in the Configured Devices list. To specify the configuration options for each configured device, go to “To set up the configuration options for the instrument devices.”

❖ To remove devices from the instrument configuration

For each device that you want to remove from the instrument configuration, in the Configured Devices list do one of the following:

- Select the device icon, and then click **Remove**.

–or–

- Double-click the device icon.

❖ To set up the configuration options for the instrument devices

1. Add the devices that make up the instrument to the instrument configuration (see “Adding, Removing, and Configuring the Instrument Drivers” on page 119).

2. In the Configured Devices list, do the following:

   - Select the device icon for the device that you want to configure and click **Configure**.

   –or–

   - Double-click the device icon.

   The *Device Name* Configuration dialog box opens.

3. Enter all required configuration information for the device. Complete entries and options for all pages.

4. To save settings and close the *Device Name* Configuration dialog box, click **OK**.

   The Thermo Foundation Instrument Configuration window reappears.

5. To save the configuration settings and close the window, click **Done**.

Instrument Configuration Window Parameters

Table 21 describes the parameters in the Instrument Configuration window.

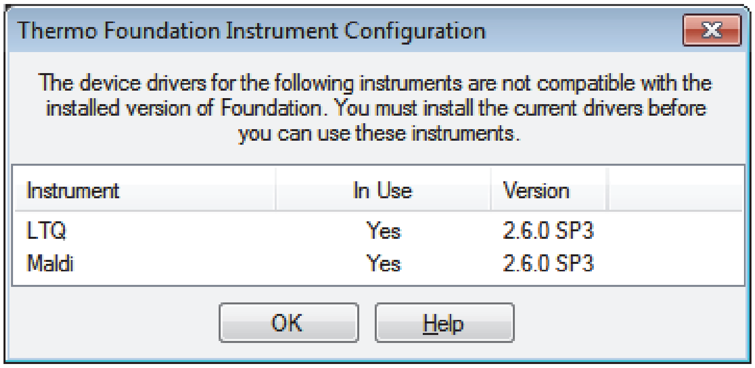
Table 21. Instrument Configuration window parameters

Parameter	Description
Device Types	
This list includes the following selections.	
All	Displays all installed device drivers.
AS	Displays all installed autosampler devices.
Detector	Displays all installed detector devices; for example, this selection displays the installed UV-Vis and photodiode array (PDA) detector devices.
GC	Displays all installed gas chromatography devices.
LC	Displays all installed liquid chromatography devices; for example, displays the liquid chromatography pumps.
MS	Displays all installed Thermo Scientific mass spectrometer devices.
Other	Displays all other installed devices.
Available Devices	
This area displays the installed device drivers that make up the selected category in the Devices list.	
Configured Devices	
This area displays the device drivers that you have added to the instrument configuration.	
Buttons	
Add	Adds the selected device in the Available Devices area to the Configured Devices area.
Remove	Removes the selected devices in the Configured Devices area.
Configure	Opens the Configuration dialog box for the selected devices.
Done	Closes the Instrument Configuration window.
Help	Opens the Foundation Help to this topic.

Out-of-Date Device Drivers Detected

When you open the Thermo Foundation Instrument Configuration window and one or more of the configured device drivers are not compatible with the installed version of the Foundation platform, the application opens a message box that displays the out-of-date drivers it has detected (Figure 52).

Figure 52. Message box that displays a list of incompatible device drivers



The device drivers for the following instruments are not compatible with the installed version of Foundation. You must install the current drivers before you can use these instruments.

Instrument	In Use	Version
LTQ	Yes	2.6.0 SP3
Maldi	Yes	2.6.0 SP3

If this dialog box appears, install the latest software for the instruments listed.

Note Follow the installation instructions provided with the data system and instrument control software DVDs.

Table 22 describes the read-only text in the message box.

Table 22. Out-of-date device drivers detected dialog box parameters

Parameter	Description
Instrument	Displays currently installed instruments with out-of-date software.
In Use	Displays the status of the instrument displayed in the Instrument list: In Use (Yes) or Not In Use (blank). In Use devices appear in the Configured Devices area of the Instrument Configuration window.
Version	Displays the current version of the instrument that is displayed in the same row of the Instrument list. Make sure the version to be installed is more recent than the current version.

8

Viewing and Saving System Version Information

You can check the version information for the installed Thermo Foundation platform, data system, and instrument control device drivers that you added to the Configured Devices list of the Thermo Foundation Instrument Configuration window.

❖ To view the version information

1. From the Windows taskbar, choose **Start** > **Programs** (or **All Programs**) > **Thermo Foundation *x.x*** > **Version Info**, where *x.x* is the version.

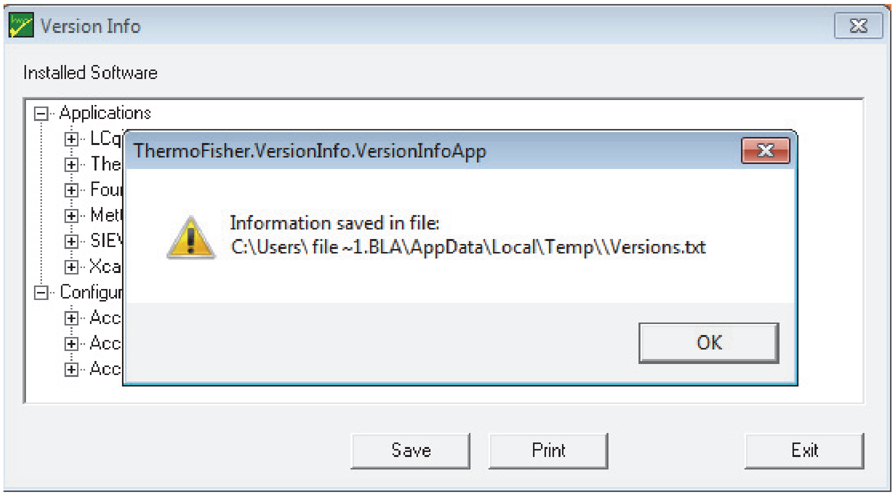
   The Version Info dialog box opens.

2. To view the complete version information for each installed application or instrument, click the **Expand/Collapse** icon.

❖ To save the version information to a text file

1. Click **Save**.

   The following message appears.



ThermoFisher.VersionInfo.VersionInfoApp

Information saved in file:
C:\Users\ file ~1.BLA\AppData\Local\Temp\\Versions.txt

2. Click **OK** to save the version information to a text file and close the box.

Converting Files and Managing Libraries

This chapter provides information about the File Converter and Library Manager applications that you can access from the Home Page Tool menu of the Xcalibur data system.

Contents

Converting Files

Use the Thermo File Converter application to convert one data file type to another data file type.

❖ To convert data files from one file format to another

1. Choose **Tools > File Converter** from the Roadmap view of the Home Page window.

   The Thermo File Converter application opens.

2. To specify the source data type of the files you want to convert, select from the Source Data Type list in the Conversion Source area.

   The selections in the Source Data Type list are RAW, DAT, MS, CDF, and SPA. You can only batch process files with one source data type and one destination data type at a time. You can perform other data type conversions in separate batches.

3. To select the files to be converted, click **Browse** and select the folder that contains the files.

   The files appear in the Conversion Source list. The Xcalibur data system displays the File Name, Type, Size, and Date.

4. Create a list of files to convert using one of the following options:

   - To convert all of the files in the Conversion Source list, click **Select All,** and then click **Add Job(s)**. All of the files appear on the Jobs page in the Conversion Destination area at the bottom.

   - To convert a single file from the Conversion Source list, select the file and then click **Add Job(s)**.

   - To delete a file that appears in the Conversion Source list, select the file and then click **Clear Selection**.

5. To specify the destination data type of the files that you want to convert, select from the Destination Data Type list in the Conversion Destination area.

6. To select a destination folder, click **Browse** to search for a folder to hold the converted files.

   The source files remain in their original directories.

7. To start the file conversion using batch processing of the files on the Jobs page, click **Convert**.

   You can monitor the conversion progress by clicking the Status tab in the Conversion Destination area.

   The Xcalibur data system continues file conversion processing until all files are converted and stored in the specified destination folder.

8. To convert a different source data type, click **Clear Selection** to clear all files displayed in the Conversion Source list. Then repeat step 2 through step 7 for the other source data type.

9. To close the File Converter application, click **Close**.

Note Understand the following:

- The Xcalibur data system does not currently support all interconversion combinations and posts a message whenever an unsupported conversion is requested.

- Not all formats have the same data fields. The data system can only convert matching data fields and does not typically convert instrument method information.

- You can add the XConvert.exe program to a processing method, and then batch reprocess your data files. For instructions about adding the program to a processing method, see the XConvert.exe topic in the Xcalibur Help.

Compatible File Types

Table 23 lists the file types that the Xcalibur data system can convert.

Table 23. File interconversions for data file types

File type	File extension
Xcalibur	*.raw
ICIS	*.dat
GCQ	*.ms
Magnum	*.ms
ANDI	*.cdf
AutoMass	*.spa
MassLab2	*.raw
LaserMAT	*.*

File Converter Parameter Descriptions

Table 24 describes the File Converter parameters.

Table 24. Thermo File Converter parameters (Sheet 1 of 4)

Parameter	Description
Conversion Source	
Source Data Type	Specifies the data type of the file that you want to convert into another data type. All of the files in the Folder list in the Conversion Source area are displayed in the Conversion Source table. You can select the following data types from the Source Data Type list for conversion into another data type: • Xcalibur Files (*.raw) • ICIS Files (*.dat) • GCQ Files (*.ms) • Magnum Files (*.ms) • ANDI Files (*.cdf) • Automass Files (*.spa) • Mass Lab 2 Files (*.raw) • Lasermat Files (*.*) The source data type is selected from the Destination Data Type list.

Table 24. Thermo File Converter parameters (Sheet 2 of 4)

Parameter	Description
Folder	Specifies the path to the source file that you want to convert to another data type. The list contains all the paths that you have recently selected. Click **Browse** in the Conversion Source area to select another path to source files.
Browse button	Opens the Browse For Folder dialog box, where you can select the folder that contains the files that you want to convert to another data type and click **OK**. The data system displays the path to the folder in the Folder list and the previous path remains in the folder list. If the selected folder has no file of the type specified in the Source Data Type list, no entries appear in the Conversion Source table.
Conversion Source table	Displays the file name, type, size, and date of the files located in the directory specified in the Folder list and of the type specified in the Source Data Type list.
Select All button	Selects all of the files that appear in the Conversion Source table. The data system highlights all of the files.
Clear Selection button	Clears the currently selected files. This button is only active when you select one or more files in the Conversion Source table.
Add Job(s) button	Adds the specified conversion job to the Jobs page of the Conversion Destination area. Each file conversion is considered a separate job. The following is an example of a job displayed on the Jobs page for the conversion of an Xcalibur file of type .raw to an ANDI file of type CDF: C:\Xcalibur\examples\data\drugx_06.raw C:\Xcalibur\examples\data\drugx_06.cdf The Add Job(s) button is only active when one or more files have been selected on the Jobs page. You can only add a job if you have selected a valid data type in the Destination Data Type list and have selected a valid destination from the Folder list in the Conversion Destination area.

Table 24. Thermo File Converter parameters (Sheet 3 of 4)

Parameter	Description
Conversion Destination	
Destination Data Type	Specifies the data type that you want the source data files converted to. The following data types can be selected from the Destination Data Type list: • ICIS Files (*.dat) • ANDI Files (*.cdf) • Text Files (*.txt) The software selects the data type that a source data type file can be converted from in the Source Data Type list.
Folder	Specifies the path to the destination folder to hold your converted file. The list contains all the paths that you have recently selected. To select another folder to store your converted files, click **Browse** in the Conversion Destination area.
Browse	Opens the Browse For Folder dialog box, where you can select the folder to hold your converted files and click **OK**. The data system displays the path to the folder and the previous path remains in the Folder list.
Jobs page	This page in the Conversion Destination area displays the jobs that have been selected and added for conversion. The job display format is as follows: C:\Xcalibur\examples\data\drugx_06.raw C:\Xcalibur\examples\data\drugx_06.cdf To remove a job prior to running the conversion, select the job and click **Remove Job(s)**.
Remove Job(s)	Removes jobs that are selected for removal from the Jobs page. You must remove a job prior to converting it. Selecting a job on the Jobs page makes this button available.
Status page	This page in the Conversion Destination area displays the status of jobs that have been converted. The format is as follows: Successfully converted C:\Xcalibur\examples\data\drugx_06.raw to C:\Xcalibur\examples\data\drugx_06.cdf This page also displays the status of unsuccessful conversions.

Table 24. Thermo File Converter parameters (Sheet 4 of 4)

Parameter	Description
Other Buttons	
Convert	Starts the conversion of all jobs displayed on the Jobs page in the Conversion Destination area. The data system stores the converted files in the displayed folder. The status of all converted files appears on the Status page. This page in the Conversion Destination area displays the status of jobs that have been converted. The format is as follows: Successfully converted C:\Xcalibur\examples\data\drugx_06.raw to C:\Xcalibur\examples\data\drugx_06.cdf This page also displays the status of unsuccessful conversions.

Managing Libraries

Use the Thermo Library Manager application to manage NIST libraries used with the NIST search software and to convert libraries between the ICIS/GCQ/ITS 40, MassLab, NIST, and ANDI-MS formats.

The Library Manager supports the following conversions.

From \ To	ICIS/GCQ/ITS 40	MassLab	ANDI-MS	NIST
ICIS/GCQ/ITS 40		X	X	X
MassLab	X		X	X
ANDI-MS	X	X		X
NIST	X	X	X	

Note The Xcalibur data system does not directly support INCOS, LAB-BASE, or JCAMP library conversions. However, MassLab data system users have a conversion program to convert from a LAB-BASE user library to a MassLab user library. In addition, a conversion tool exists in ICIS (a UNIX system) that can convert a LAB-BASE user library to a MassLab user library.

The Library Manager application has the following pages:

- Convert Libraries Page
- Manage Libraries Page

❖ **To open this application**

From the Roadmap view of the Xcalibur Home Page window, choose **Tools > Library Manager**.

Convert Libraries Page

Use the Convert Libraries page of the Library Manager application to convert one type of source library to another type of library at a target location and to copy a library to another location.

Note Library conversion times range from minutes to hours, depending on the number of files and the size of the files.

Table 25 describes the parameters on the Convert Libraries page of the Library Manager application.

Table 25. Convert Libraries page parameters (Sheet 1 of 2)

Parameter	Description
Source Library Details	
Type [Source]	Specifies the source library file type that you want to convert to another file type. Select any of the following file types: ICIS/GCQ/ITS 40 (*.lib, .lbr), MassLab (*.idb), ANDI-MS (*.cdf), NIST, or AutoMass (*.spr, *.prs, *.nam, *.hdr).
Library/Browse [Source]	Specifies the source library that you want to convert. To change the library, click **Browse** and select the path to the source library on your computer or network.
Process Entries [Source]	Specifies the number range of the library entries that you want to convert from the source library. If you leave the box empty, the Xcalibur data system converts all entries. The format is *First Entry-Last Entry.* For example, to convert library entry #100 through library entry #200, type 100-200 in the Process Entries box.
Target library details	
Type [Target]	Specifies the target library file type when converting the source library. • If you select source library file type ICIS/GCQ/ITS 40, MassLab, ANDI-MS, or NIST, you can select from the following target library file types: ICIS/GCQ/ITS 40 (*.lib, .lbr), MassLab (*.idb), NIST, or ANDI-MS (*.cdf). • If you select source library file type AutoMass, you can only select the NIST target library file type. • If you select the library type NIST, the Xcalibur data system displays the path to the NIST library folder in the Library box. You specified this location when you installed NIST.
Library/Browse [Target]	View the file folder to store the converted library file. To change the folder, click **Browse** and select the target folder on your computer or network.
Title [Target]	Specifies the title for the ICIS/GCQ/ITS 40 library or for the Mass Lab library that you create during the conversion. You can add a title to the new library using any format. **Note** This box in the Target library details area only becomes active when you select an ICIS/GCQ/ITS 40 or MassLab library.
Add the library to the NIST software for use with Xcalibur	Select this check box to add the converted library to the NIST software for use with the Xcalibur application.

Table 25. Convert Libraries page parameters (Sheet 2 of 2)

Parameter	Description
Options	
Target library action: Create/Replace	Select this option to create a new library in the target directory or to replace an existing library. You can also append (add) the new (converted) entries to a previously created target library.
Target library action: Append	Select this option to append (adds) the new (converted) entries to a previously created target library. You can also create a new library in the target directory or to replace an existing library.
Include replicate entries from the NIST library in the target library	Select this check box to include replicate entries in the target library. Otherwise, leave the box unchecked. This check box is only active if you are converting from a NIST library to another format.
Replicate library/browse	Specify the location of a replicate library. To change the replicate library, click **Browse** and select the folder for the replicate library on your computer or network. If you specify a replicate library, the Xcalibur data system adds replicate entries into the appropriate replicate library. If you select the library type NIST, the Xcalibur data system displays the path to the NIST replicate library folder in the Library box. You specify this location when you install NIST software.
Button	
Convert	Starts the library conversion you have specified using the Convert Libraries page. The Xcalibur application opens the Library Conversion Status dialog box and displays the Conversion Status progress bar and the Conversion Status box. The Status bar displays messages such as the following: Processed 100% of the entries, continuing on The Conversion Status box displays sequential chronological (top to bottom) messages such as the following: • Started the conversion on SEP 3, 1999 at 10:01, please wait • Finished the conversion on SEP 3, 1999 at 10:02 • Converted 570 entries

Manage Libraries Page

Use the Manage Libraries page of the Library Manager application to add a library to the NIST libraries list or to delete a library from the NIST libraries list. You can also copy a library to another location.

Table 26 describes the parameters on the Manage Libraries page of the Library Manager application.

Table 26. Manage Libraries page parameters (Sheet 1 of 2)

Parameter	Description
NIST Libraries	
NIST Libraries list	Displays all of the NIST libraries currently available on your computer or network. You can add libraries to this list, delete libraries from this list, and copy libraries on the list to another location.
Buttons	
Add	Opens the Add Library dialog box, where you can select a library to add to the NIST Libraries list. The Add Library dialog box has the following parameters: • Source: Specifies the library to be added. • Action: Select one of these options to specify the location of the library that you want to add. – Copy the library to the local computer: Select this option to copy the selected library to your computer. – Link to the library from either a remote location or computer: Select this option to access the library remotely. Because libraries can be large, you might save time by using the Link option rather than the Copy option. Click **OK** when you have selected the library you want to add and selected Action options.

Table 26. Manage Libraries page parameters (Sheet 2 of 2)

Parameter	Description
Delete	Deletes the library that you have previously selected in the NIST Libraries list. Select the library that you want to delete from the NIST Libraries list. Click **Delete**. The Delete Library message box opens with the following message: Are you sure you want to delete the selected NIST library? Click **Yes**. The Xcalibur data system removes the library from the list.
Archive	Copies a selected library to another directory on your computer or network. Select the library that you want to copy to another directory. Click **Archive**. The Archive Library dialog box opens. The Archive Library dialog box has the following parameter: Destination. This parameter specifies the location for the selected library. Click **Browse** to select a destination for the selected file. Click **OK**. The data system makes a copy of the selected NIST library and stores it in the selected directory.

Maintaining Communication with the Instruments

To ensure that both the Xcalibur data system and LCquan application work properly and that the data system computer maintains communication with the LC/MS or GC/MS system, review these IT issues.

Contents

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:\Users\user name\AppData\Local\Temp
- C:\Xcalibur\methods or the directory where the instrument method (METH) and processing method (PMD) files are stored
- C:\Xcalibur\Quanroot or the directory where raw data files (RAW) are stored
- C:\Xcalibur\system\programs\
- C:\Program Files\Thermo\Foundation

Do Not Delete the Xcalibur System Account

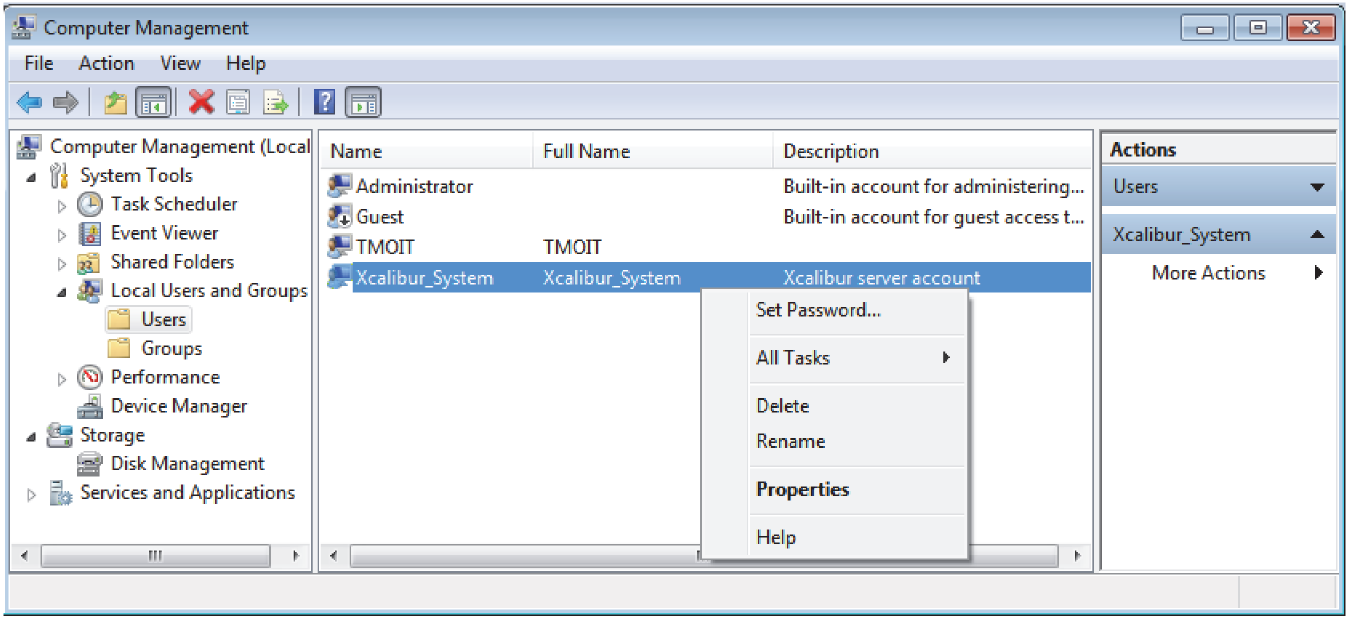
With sequential user logon, a user can log on, start an acquisition, and then log out. When the Foundation platform is installed, a user account—Xcalibur_System—is created under the Administrator's group. This account runs in the background during data acquisition.

To ensure correct system and application functioning, avoid doing the following to the Xcalibur_System account:

- Avoid changing its password.
- Avoid changing its name.
- Avoid deleting it.
- Avoid removing it from the Administrator's group.

Figure 53 shows the shortcut menu for the Xcalibur_System account. If you accidentally delete this account, you must reinstall the Foundation platform.

Figure 53. Shortcut menu for the Xcalibur_System account



Name	Full Name	Description
Administrator		Built-in account for administering...
Guest		Built-in account for guest access t...
TMOIT	TMOIT	
Xcalibur_System	Xcalibur_System	Xcalibur server 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 data system computer is unable to communicate with the instrument. During installation, instrument software now automatically configures the required exception for the Microsoft Windows firewall.

Ensure Your Computer Stays Active

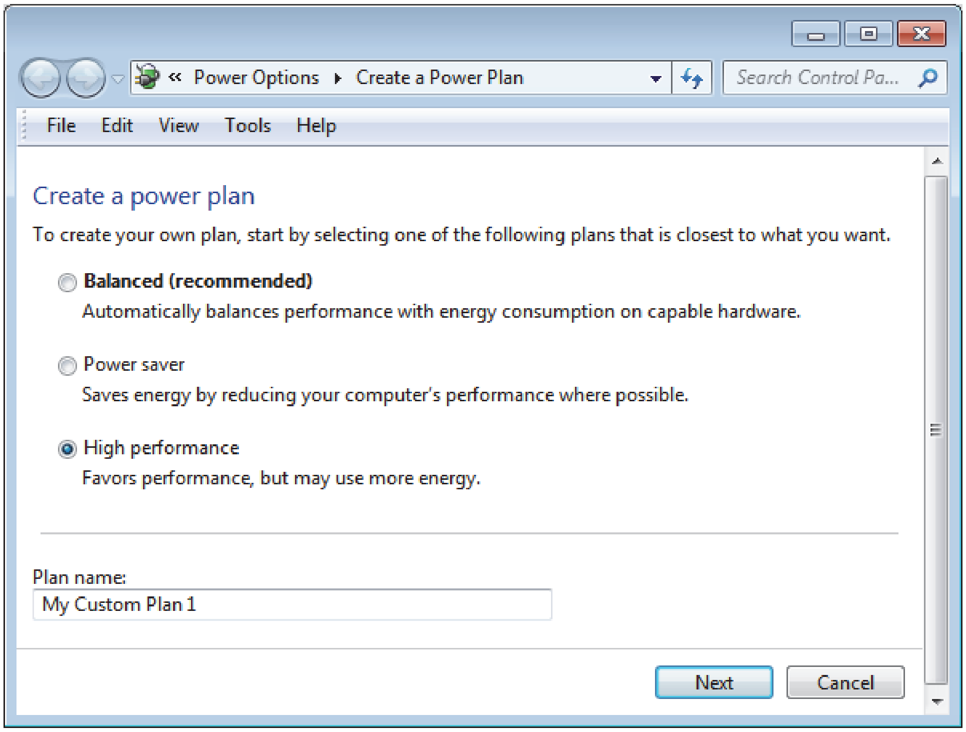
Turn off the sleep and power saver options for your hard drives and network adapters to avoid issues with the Foundation platform when your IT global policy might interfere with software functioning.

❖ To turn off the sleep mode in Windows 7

1. Choose **Start > Control Panel**.
2. In the View by list, select **Category**.
3. Choose **System and Security > Power Options.**
4. On the left side of the window, select **Create a Power Plan**.

   The Create a Power Plan window page (Figure 54).

Figure 54. Create a Power Plan page



Create a power plan

To create your own plan, start by selecting one of the following plans that is closest to what you want.

○ **Balanced (recommended)**
Automatically balances performance with energy consumption on capable hardware.

○ Power saver
Saves energy by reducing your computer's performance where possible.

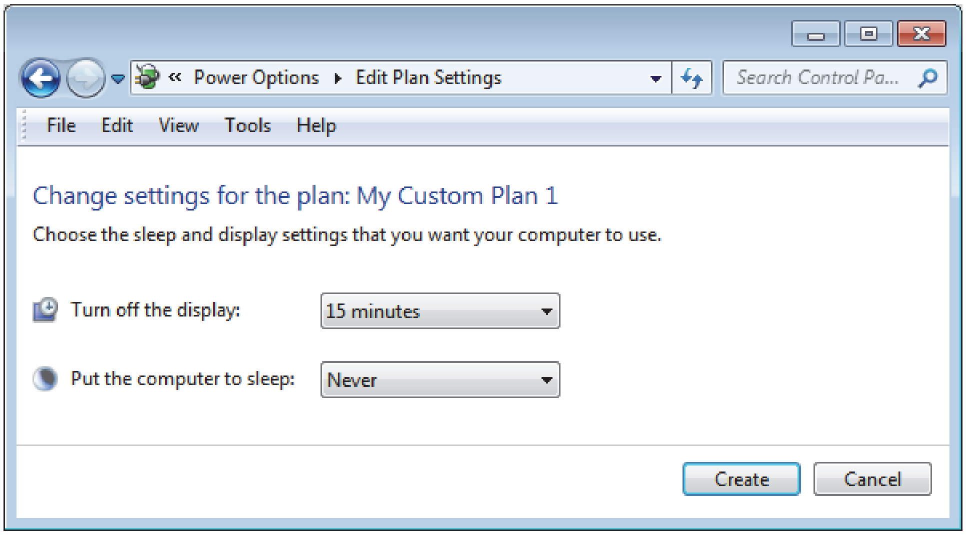
● High performance
Favors performance, but may use more energy.

Plan name:
My Custom Plan 1

5. To keep the computer powered, select the **High Performance** option.
6. In the Plan Name box, type a name for the custom plan.

7. Click **Next** to open the Edit Plan Settings page (Figure 55).

Figure 55. Edit Plan Settings page


« Power Options ▸ Edit Plan Settings
Search Control Pa...
File Edit View Tools Help

Change settings for the plan: My Custom Plan 1

Choose the sleep and display settings that you want your computer to use.

Turn off the display: 15 minutes

Put the computer to sleep: Never

8. For the Put the Computer to Sleep option, select **Never**.

9. Click **Create**.

A

LCquan Folder Structure and Security Features

Use the information in this appendix to understand files and folders for the LCquan application.

Contents

LCquan Folder Structure

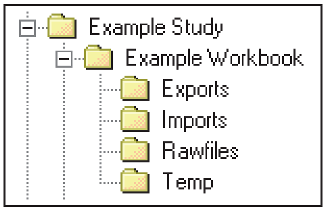
The LCquan folder structure includes the following:

- 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:\ProgramData\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.
  - For storing the acquired data on a network server, you must designate a folder on the network server as the LCquan root folder. Any network folder must be a shared folder accessible through a UNC path: \\*servername**sharename*.

  For each new project, the LCquan application creates the following hierarchical folder structure within the designated root folder.



```
Example Study
  Example Workbook
    Exports
    Imports
    Rawfiles
    Temp
```

- 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) and any imported raw data files.
  - Temp folder—Contains temporary files used by the LCquan application.

Security Features Within LCquan

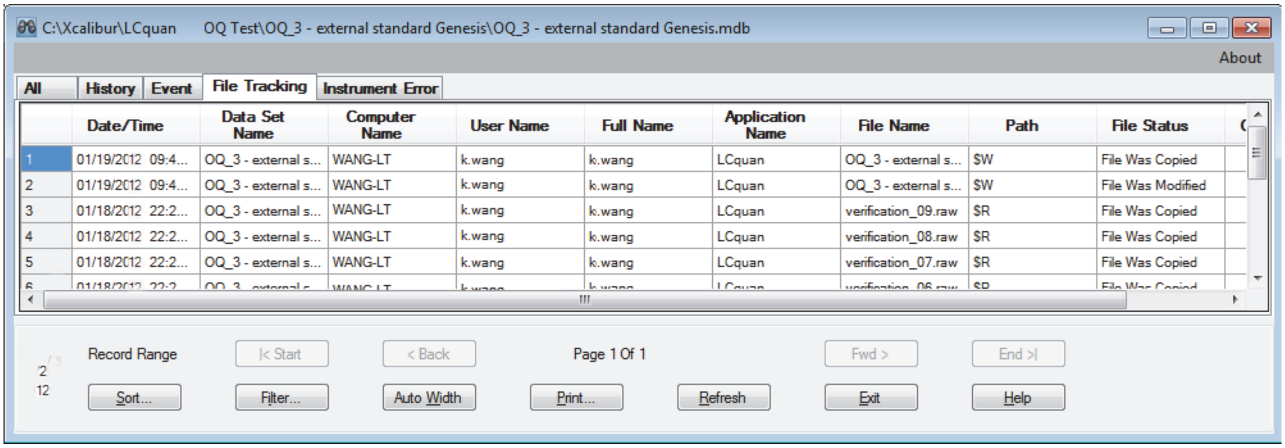
After the appropriate file protections and user access controls are in place, the LCquan application uses several built-in features to ensure the security of the data.

The 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 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 application displays a warning if files within that project have been moved or modified (as determined from the CRC value). The Audit Trail ensures that you can generate all electronic records from the raw data.

❖ To view the audit trail

1. In the workbook, choose **File > Audit Trail**.



C:\Xcalibur\LCquan OQ Test\OQ_3 - external standard Genesis\OQ_3 - external standard Genesis.mdb

	Date/Time	Data Set Name	Computer Name	User Name	Full Name	Application Name	File Name	Path	File Status
1	01/19/2012 09:4...	OQ_3 - external s...	WANG-LT	k.wang	k.wang	LCquan	OQ_3 - external s...	$W	File Was Copied
2	01/19/2012 09:4...	OQ_3 - external s...	WANG-LT	k.wang	k.wang	LCquan	OQ_3 - external s...	$W	File Was Modified
3	01/18/2012 22:2...	OQ_3 - external s...	WANG-LT	k.wang	k.wang	LCquan	verification_09.raw	$R	File Was Copied
4	01/18/2012 22:2...	OQ_3 - external s...	WANG-LT	k.wang	k.wang	LCquan	verification_08.raw	$R	File Was Copied
5	01/18/2012 22:2...	OQ_3 - external s...	WANG-LT	k.wang	k.wang	LCquan	verification_07.raw	$R	File Was Copied

Record Range

Page 1 Of 1

2. Select the type of audit from the tabs at the top of the display.

   The Audit Trail is made up of four parts: the History log, the Event log, the File Tracking log, and the Instrument Error log. The History log contains information about every parameter change a user has made within an application experiment. The Event log contains information about all the events that have occurred within the application and the File Tracking log tracks changes made to files contained within an application. The Instrument Error log lists instrument errors.

Watson Interface

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

Note To use the digital gateways, you must install the Xcalibur and Foundation XDK components.

Contents

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 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 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 (see Setting the Excel Features). Before the Excel rounding feature takes effect for the Watson digital interface, you must start and exit the application.

Setting the Excel Features

Follow this procedure to set up the Excel reporting permissions.

❖ To set the Excel features for reports

1. From the Windows taskbar, choose **Start > All Programs >Thermo Foundation *x.x* > Authorization Manager**.

   Thermo Foundation Authorization Manager opens.

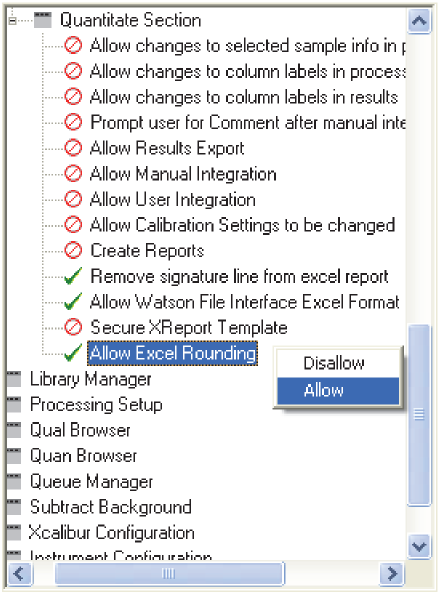
2. In the Secure Groups area, select the group.

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

   The list of controlled features appears.

4. In the LCquan > 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



Quantitate Section
- ⊘ Allow changes to selected sample info in p
- ⊘ Allow changes to column labels in process
- ⊘ Allow changes to column labels in results
- ⊘ Prompt user for Comment after manual inte
- ⊘ Allow Results Export
- ⊘ Allow Manual Integration
- ⊘ Allow User Integration
- ⊘ Allow Calibration Settings to be changed
- ⊘ Create Reports
- ✓ Remove signature line from excel report
- ✓ Allow Watson File Interface Excel Format
- ⊘ Secure XReport Template
- ✓ Allow Excel Rounding

Library Manager
Processing Setup
Qual Browser
Quan Browser
Queue Manager
Subtract Background
Xcalibur Configuration
Instrument Configuration

   A green 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 145.

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

Index