

# MassLynx 4.1

## Security Guide

71500113302/Revision A



Copyright © Waters Corporation 2005.  
All rights reserved.

## Copyright notice

---

© 2005 WATERS CORPORATION. PRINTED IN THE UNITED STATES OF AMERICA AND IRELAND. ALL RIGHTS RESERVED. THIS DOCUMENT OR PARTS THEREOF MAY NOT BE REPRODUCED IN ANY FORM WITHOUT THE WRITTEN PERMISSION OF THE PUBLISHER.

The information in this document is subject to change without notice and should not be construed as a commitment by Waters Corporation. Waters Corporation assumes no responsibility for any errors that may appear in this document. This document is believed to be complete and accurate at the time of publication. In no event shall Waters Corporation be liable for incidental or consequential damages in connection with, or arising from, its use.

Waters Corporation  
34 Maple Street  
Milford, MA 01757  
USA

## Trademarks

Micromass and Waters are registered trademarks, MassLynx is a trademark of Waters Corporation.

Other trademarks or registered trademarks are the sole property of their respective owners.

## Customer comments

Please contact us if you have questions, suggestions for improvements, or find errors in this document. Your comments will help us improve the quality, accuracy, and organization of our documentation.

You can reach us at [tech\\_comm@waters.com](mailto:tech_comm@waters.com).

## Contacting Waters

You will be able to resolve most MassLynx issues yourself. However, if this is not the case, you must contact Waters.

Customers in the USA and Canada should report maintenance problems they cannot resolve to Waters Technical Service (800 252 4572). All others should visit <http://www.waters.com> and click Offices, or phone their local Waters

subsidiary or Water corporate headquarters at 34 Maple Street, Milford, MA 01757, USA.

When contacting Waters, have the following information available:

- The nature of the problem
- Your instrument serial number(s)
- Your software version (click Help > About in the main MassLynx window)
- Any error messages received





# Table of Contents

---

Copyright notice .....	ii
Trademarks .....	ii
Customer comments .....	ii
Contacting Waters .....	ii
<b>1 Introduction .....</b>	<b>1-1</b>
Regulated environments .....	1-2
Support for application managers .....	1-2
<b>2 Before You Start .....</b>	<b>2-1</b>
Creating Operating System users .....	2-2
Installing MassLynx Security .....	2-3
Creating checksums .....	2-5
<b>3 Starting Security Manager .....</b>	<b>3-1</b>
What is Security Manager? .....	3-2
Starting Security Manager .....	3-3
The Security Manager window .....	3-3
<b>4 Creating and Modifying Groups .....</b>	<b>4-1</b>
Understanding MassLynx groups .....	4-2
Built-in Groups .....	4-2
Regulated and Non-Regulated groups .....	4-3
Creating or modifying a group .....	4-4
Adding users to groups .....	4-6
Assigning rights to groups .....	4-7
<b>5 Creating and Modifying Users .....</b>	<b>5-1</b>

Understanding MassLynx users .....	5-2
Creating or modifying a user .....	5-3
<b>6 Configuring Directory Policies .....</b>	<b>6-1</b>
What are directory policies? .....	6-2
Setting directory policies .....	6-3
<b>7 Setting Security Policies .....</b>	<b>7-1</b>
What are security policies? .....	7-2
MassLynx Security enabled .....	7-3
Critical error protection .....	7-4
Use individual INI files .....	7-5
Forget last username .....	7-6
Tamper detection .....	7-7
Audit policy .....	7-8
Audit – Turning event logging on and off.....	7-9
Auditable events – Selecting event types to log.....	7-9
Remote Logging – Using a remote computer as a log server .....	7-10
Remote Alerts.....	7-10
Dual authorization .....	7-11
Timeout .....	7-12
LIMS policy .....	7-13
<b>8 Configuring Signature and Reason Policies .....</b>	<b>8-1</b>
What are signatures and reasons? .....	8-2
Basic Security and Full Security .....	8-2
Deciding whether signatures and reasons are required .....	8-3
Forcing users to enter full signature information.....	8-4

Choosing the actions that require a signature or reason .....	8-6
Setting the available reasons .....	8-7
Entering signatures and reasons .....	8-11
Viewing file signatures and reasons .....	8-12
Adding signatures or reasons to existing files .....	8-13
<b>9 Saving, Printing, and Sharing Security Settings .....</b>	<b>9-1</b>
Saving security settings .....	9-2
Printing security settings .....	9-3
Exporting and importing security settings .....	9-4
<b>10 Viewing, Exporting, and Printing Audit Logs .....</b>	<b>10-1</b>
What are the audit logs? .....	10-2
Starting LogLynx .....	10-3
Viewing the LogLynx log .....	10-5
Importing audit logs .....	10-6
Filtering the LogLynx log .....	10-7
Creating a date/time range query .....	10-7
Creating an event origin query .....	10-11
Creating event type queries .....	10-13
Backing up, exporting, and clearing the LogLynx log .....	10-28
Backing up the LogLynx log.....	10-28
Exporting log file entries .....	10-29
Clearing the LogLynx log .....	10-31
Printing the LogLynx log .....	10-32
<b>11 Using MassLynx in Regulated Environments .....</b>	<b>11-1</b>

Recommendations .....	11-2
Common regulatory requirements .....	11-3
Discern invalid or altered records .....	11-4
View, copy, and print electronic records .....	11-5
Viewing, copying, and printing MassLynx files .....	11-5
Viewing, copying, and printing audit log entries .....	11-5
Protect and back up records .....	11-7
Using BackLynx.....	11-7
Copying files using another method .....	11-7
Backing up the audit log .....	11-7
Limit system access to authorized individuals .....	11-9
Generate time-stamped audit trails .....	11-10
Allow only specified individuals to perform actions .....	11-11
Assure the validity of source data .....	11-12
Hold individuals accountable for actions performed under their electronic signature .....	11-13
Include the name, date, time, and meaning with electronic signatures .....	11-14
Ensure that electronic signatures are associated with the correct record .....	11-15
Ensure electronic signatures are unique to one individual .....	11-16
Confirm that at least two distinct identification components exist for an electronic signature .....	11-17
Force all signature components to be used whenever a signature is performed .....	11-18
Maintain the uniqueness of the identification, and ensure periodic revision of passwords .....	11-19
Notify management of any attempted unauthorized use of the system .....	11-20
<b>A MassLynx Group Rights .....</b>	<b>A-1</b>



Table of rights .....	A-2
<b>B MassLynx Checksums .....</b>	<b>B-1</b>
<b>Outline of checksum operation .....</b>	<b>B-2</b>
Raw data checksum .....	B-2
Other file checksums .....	B-2
Copying files.....	B-2
<b>Index .....</b>	<b>Index-1</b>



# 1 Introduction

MassLynx™ can be installed with one of two levels of security – Basic or Full. The following table outlines the differences between the two.

## MassLynx Security levels:

Feature	Basic	Full
Limit system access to specific users	●	●
Configure restricted access to certain functions or areas	●	●
Record all events in audit logs	●	●
Control the directories the user can access through MassLynx		●
Detect any files that have been modified outside MassLynx		●
Record signatures or reasons when data created, modified, or processed		●

**Exception:** Signatures can be recorded for QuanLynx actions in Basic Security mode.

Basic Security is ideal for situations where you need to control who uses MassLynx, and what they can use it for.

Full Security is appropriate for situations where it is important for you to have absolute confidence that your settings and data have not been tampered with, and where a complete audit log is needed to record the changes that are made.

This guide explains the features available when using security for your system. Most of these features apply both to Basic and Full Security – it is clearly indicated when a feature applies only to one or the other.

## Regulated environments

---

If you operate in a regulated environment you will probably wish to use Full Security.

If there are specific regulatory requirements that you would like MassLynx to help you fulfil, [Using MassLynx in Regulated Environments on page 11-1](#) highlights features that can be used to assist with achieving compliance in some of the most common areas.

**Caution:** MassLynx cannot satisfy regulatory requirements by itself: it is only a component of the processes and procedures you need to have in place. You must consider carefully what the regulations require of you, and configure and operate MassLynx in a manner compatible with your understanding.

## Support for application managers

---

Application Managers are additional software components that can optionally be installed to extend the functionality of MassLynx.

Basic Security provides control over whether users can access the various application managers you may have installed.

The additional features (as shown on [page 1-1](#)) provided in Full Security mode are only available for the QuanLynx and TargetLynx application managers.

# 2

## Before You Start

This chapter outlines what needs to be done before you can begin using MassLynx security, including creating the appropriate users in the Operating System and installing the software.

### Contents:

Topic	Page
<a href="#">Creating Operating System users</a>	2-2
<a href="#">Installing MassLynx Security</a>	2-3
<a href="#">Creating checksums</a>	2-5

## Creating Operating System users

---

To install MassLynx Security, two Windows user accounts will be required:

- A normal user account without administrative permissions, called 'Micromass'.
- The default administrator account (usually called 'Administrator').

These accounts will normally have been set up for you if your instrument has been installed by a Waters engineer.

# Installing MassLynx Security

---

MassLynx Security is installed at the same time as other MassLynx software.

**Tip:** It is possible to install MassLynx security on a PC that you want to use as an audit log server, then log to this PC from one or more other computers that control instruments. You can also install MassLynx security on a PC solely to view log information.

## To install MassLynx security:

1. Log on to the PC using a user account with permission to install software – usually an administrator account.
2. If MassLynx has been supplied on a CD, or other removable media, insert it into the appropriate drive.
3. After a few moments the installer should appear automatically. If it does not, use Windows Explorer to navigate to the directory containing the file setup.exe, and double-click the file; the MassLynx installer is displayed.
4. Follow the on-screen instructions, selecting ‘MassLynx Basic Security’ or ‘MassLynx Full Security’ as appropriate.
5. If this PC will be used to view audit log information, choose to install ‘Audit Event and Audit Trail Viewer’.
6. Choose from where you want to obtain your security settings. The options are:
  - Default Settings – this will install standard MassLynx security settings. Select this option if MassLynx security has not previously been installed, or if you do not want to keep your previous setup.
  - Retain Settings – this will keep the settings from your previous MassLynx installation. Select this option if MassLynx security has previously been installed on this PC and you want to keep that configuration.

- Import Settings – this will allow you to specify a security rollout file, from which MassLynx security settings will be imported. Choose this option if MassLynx security has previously been configured and you want to use those settings for this installation. You will need to have created a security rollout file from the other installation.
7. If you are installing with the default settings, specify a computer for the audit log to be written to.

**Requirement:** If you choose to log to a computer other than the one on which you are currently installing MassLynx, you must have already installed MassLynx on the computer specified.

**Tip:** The machine to log to can be changed after the software has been installed.

8. Unless you have chosen to write the log to a remote computer, specify a location for the audit log database. If you do not specify a location, the audit log will be created in the default location – an MMAuditLog directory in the Windows directory.

**Requirement:** The location specified must be on a local hard drive. A mapped network drive cannot be specified.

9. Proceed with the installation, following the on-screen instructions and choosing the features you wish to install.



## Creating checksums

---

**Full Security only:** This section only applies to Full Security systems.

When the installation has completed, the wizard will inform you that checksums need to be created. Checksums ensure that any files that have been changed outside of MassLynx will be detected, and cannot be opened. For a brief discussion of how MassLynx uses checksums, see [MassLynx Checksums on page B-1](#).

### To create checksums:

1. Click Create Checksums.
2. In the MassLynx User column, type the password for the Micromass Windows user. Check that the domain is set to the name of the PC on which you are installing MassLynx.  
**Exception:** If you are importing security settings from a previous configuration, enter the user name, password, and domain of a non-administrator user.
3. In the MassLynx Administrator column, type the password for the Administrator Windows user. Check that the domain is set to the name of the PC on which you are installing MassLynx.  
**Exception:** If you are importing security settings from a previous configuration, enter the user name, password, and domain of an administrator user.
4. Click OK.  
**Result:** MassLynx will create checksums for the files included in the installation.
5. When the checksum creation process has completed, click Close in the Importing Files dialog box to finish the installation.



# 3

## Starting Security Manager

This chapter will provide a brief overview of Security Manager and show you how to start the application.

### Contents:

Topic	Page
<a href="#">What is Security Manager?</a>	3-2
<a href="#">Starting Security Manager</a>	3-3

## What is Security Manager?

---

Security Manager is an application that enables the MassLynx administrator to perform security-related tasks, including creating and managing users and groups, controlling access to various parts of the MassLynx system, and configuring signature and reason policies.

# Starting Security Manager

---

## To start Security Manager:

1. Close any MassLynx applications that are running.
2. Click Start > All Programs > MassLynx > MassLynx Security Manager.
3. Type the Windows user name of a MassLynx administrator in the Logon Name box.

**Tip:** If MassLynx security was installed with the default settings, the first time you run Security Manager you will need to use the local PC Administrator user name – normally ‘Administrator’.

4. Type the Windows password for the user in the Password box.
5. In the Domain list, click the domain for which the user name is valid.
6. If there is a Role list, click Regulated.
7. Click OK.
8. If a warning message appears, read the message. If you do not understand the message or are not happy to continue, close the Security Manager window as soon as it appears and consult your system administrator. Click OK.

## Tips:

- To log in to MassLynx, the user must always be both a valid Windows user and a MassLynx user.
- The domain, user name, and password are authenticated against the Operating System. If a user’s password is changed in the Operating System, the new password will also be required to access MassLynx.
- To log on to Security Manager, the user must be specified as a MassLynx administrator. They do not need to be a Windows administrator.

## The Security Manager window

When you have successfully logged in to Security Manager, the Security Manager window will be displayed.

## Security Manager window:

The screenshot shows the MassLynx Security Manager window. It features a menu bar with 'File', 'Create', 'Policies', 'Tools', 'View', and 'Help'. Below the menu bar is a toolbar with icons for file operations and user management. The main area is divided into two sections: a 'User list' table at the top and a 'Group list' table at the bottom. The 'User list' table has columns for Username, Domain, Full Name, and Description. The 'Group list' table has columns for Group and Description. Labels with arrows point to the Menu bar, Tool bar, User list, and Group list.

Username	Domain	Full Name	Description
Administrator	MM2888	Default Local Administrator	Local Administrator Account
Micromass	MM2888	Mass Spectrometer Instrument	Micromass User Account

Group	Description
Administrators	Members can fully administer MassLynx
Analysts	Users can start and stop acquisitions and use quantification
Disabled	Users in this group will not be allowed any access to MassLynx
Maintenance	Users in this group will be able to log in at any time with full inst...
Method Developers	Members can alter method files and acquire data
Reviewers	Users have read only access to data and no access to hardwar...

# 4 Creating and Modifying Groups

This chapter will:

- explain what MassLynx groups are
- outline the different types of group
- describe how to add users to groups
- explain how to assign rights to groups

## Contents:

Topic	Page
<a href="#">Understanding MassLynx groups</a>	4-2
<a href="#">Creating or modifying a group</a>	4-4
<a href="#">Adding users to groups</a>	4-6
<a href="#">Assigning rights to groups</a>	4-7

# Understanding MassLynx groups

---

Groups are the building blocks of MassLynx Security – groups are assigned rights to access areas of MassLynx and perform operations. Users derive their rights from the group they belong to.

The groups you will need for your system will depend on the type of users you have. Take some time to consider the roles of different people within your organization, and create a group for each set of users with similar needs.

## Built-in Groups

Some groups are supplied with the MassLynx installation. Two of these are permanent groups that cannot be deleted; the others are example groups to give you an idea of how MassLynx groups can be used.

The example groups may not be present if you retained or imported security settings during the install.

### Permanent groups

**Administrators** – Members can access and fully administer MassLynx and Security Manager.

**Disabled** – Members have no access to MassLynx. New users are assigned by default to this group.

### Example groups

The example groups illustrate some of the possible roles that users might have. You can review the rights that these groups have been assigned and modify them to fit your needs – creating new groups for additional roles – or delete these groups and start afresh.

**Caution:** You should not begin adding users to these groups without thoroughly reviewing the rights assigned to them and confirming that they are appropriate for your needs.

Example groups
Analysts
Maintenance
Method Developers



<b>Example groups</b>
Reviewers

## Regulated and Non-Regulated groups

**Full Security only:** This section only applies to Full Security systems.

When MassLynx is installed with Full Security, the option to make groups Regulated or Non-Regulated is available.

Regulated groups operate under the normal Full Security model, including file modification detection, signatures, and reasons.

Non-regulated groups are not prompted for signatures or reasons, and do not have checksums checked or created for the files they use.

### Why would Non-Regulated groups be used?

Some systems operate in environments where the instrument is being used for regulated work some of the time and for non-regulated, experimental, work at other times. It may be that different people perform different types of work on the machine, or perhaps a single person has a variety of goals to achieve.

Operating under the Full Security system can be time-consuming for users whose work is not subject to official review.

Allowing this type of user to be a member of a Non-Regulated group – or allowing the user to choose whether they should login using their Regulated or Non-Regulated group – enables your system to be used as efficiently as possible without compromising your ability to enforce the strictest security where appropriate.

## Creating or modifying a group

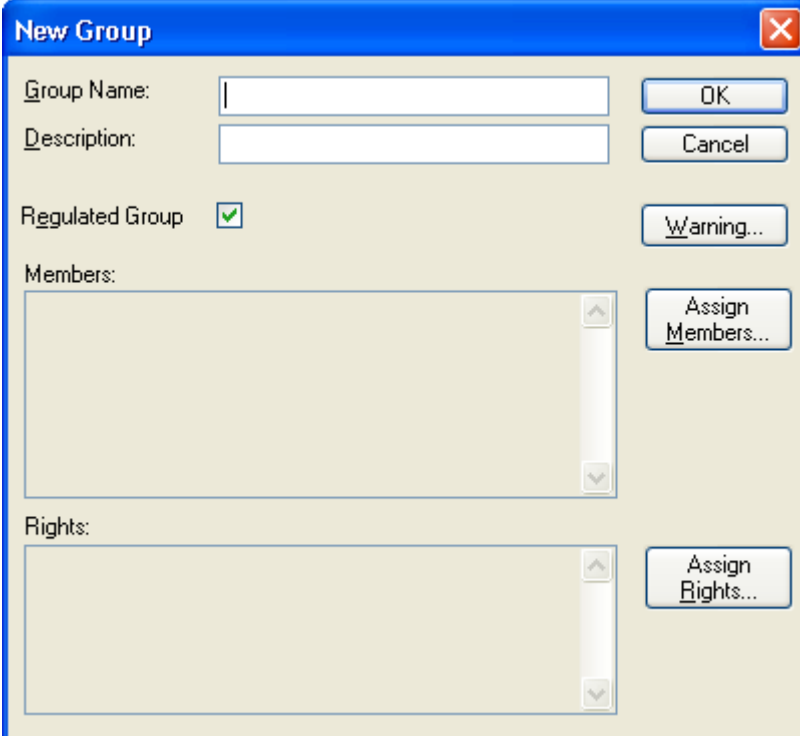
---

### To create a group:

1. Click Create > New Group.

**Alternative:** Click .

The New Group dialog box is displayed:



The screenshot shows the 'New Group' dialog box with the following elements:

- Group Name:** A text input field.
- Description:** A text input field.
- Regulated Group:** A checkbox that is checked.
- Members:** A list box with an 'Assign Members...' button to its right.
- Rights:** A list box with an 'Assign Rights...' button to its right.
- Buttons:** 'OK', 'Cancel', and 'Warning...' buttons are located on the right side of the dialog.


2. Type a name for the group.
3. Type a short description of the role of the users who will be in this group.
4. **Full Security only:** Select whether the group will be Regulated.
5. A warning can be displayed when a member of this group logs on. Click Warning to view or modify the warning given.
6. Click OK.

### To modify a group:

1. In the group list, double-click the group you wish to modify.  
**Alternative:** Right-click the group, then click Edit.  
**Result:** The Manage Group dialog box is displayed.
2. Modify the settings as required.
3. Click OK.

### To delete a group:

**Caution:** If you delete a group, its members will not be able to log in to MassLynx unless they are already a member of another group with rights assigned, or until they are added to another group. As all the settings, rights, and policies configured for the group will be lost, deletion should only be performed after careful consideration.

1. In the group list, click the group you wish to delete.
2. Click Create > Delete.  
**Alternative:** Click .
3. Click Yes to confirm that you want to delete the group.

## Adding users to groups

---

Users inherit rights from the group of which they are a member. MassLynx will only allow a user to be a member of one group.

**Exception:** If Full Security is being used, a user may be a member of one Regulated and one Non-Regulated group.

Users can be added to groups either through the Manage User dialog box or through the Manage Group dialog box.

### To add a single user to a group:

1. In the user list, double-click the user you wish to add.  
**Alternative:** Right-click the user, then click Edit.  
**Result:** The Manage User dialog box is displayed.
2. In the Group Membership frame, select the group you want the user to be a member of.  
**Full security only:** You can select a Regulated group and a Non-Regulated group.
3. Click OK.

### To add users to a group:

1. In the group list, double-click the group you wish to add users to.  
**Alternative:** Right-click the group, then click Edit.  
**Result:** The Manage Group dialog box is displayed.
2. Click Assign Members.  
**Result:** The Group Members dialog box is displayed.
3. Select the check box beside each user you wish to add. Clear the check boxes beside any users you wish to remove.  
**Tip:** If a user is already a member of another group, you will not be able to select them in the list. Remove them from the group they are currently a member of before trying to add them to this group.
4. Click OK to return to the Manage Group dialog box.
5. Click OK.

## Assigning rights to groups

---

Groups need to have rights assigned to them before their members are able to perform actions in MassLynx.

Definitions of the rights available can be found in [MassLynx Group Rights on page A-1](#).

**Recommendation:** It is often important, especially in regulated environments, that when any new data or support files – such as method files, tuning files, calibration files and so on (collectively known as metadata) – are created, all the old information is retained rather than being overwritten.

To ensure that this is the case, grant rights to create new files, but not to alter or overwrite files.

### To assign rights to groups:

1. In the group list, double-click the group you wish to assign rights to.

**Alternative:** Right-click the group, then click Edit.

**Result:** The Manage Group dialog box is displayed.

2. Click Assign Rights.

**Result:** The Group Rights dialog box is displayed.

3. Select the check box beside each right you wish to add. Clear the check boxes beside any rights you wish to remove.

**Tip:** Select multiple rights by clicking a right, then holding the Ctrl key while clicking other rights. Select blocks of rights by clicking the first right in the block, holding the Shift key, then click the last right in the block. Press the space bar to select or clear the check boxes of the selected rights.

4. Click OK to return to the Manage Group dialog box.
5. Click OK.



# 5

## Creating and Modifying Users

This chapter will explain what MassLynx users are, and describe how to create and modify them.

### Contents:

Topic	Page
<a href="#">Understanding MassLynx users</a>	5-2
<a href="#">Creating or modifying a user</a>	5-3

## Understanding MassLynx users

---

Every user who wishes to use MassLynx must have their own MassLynx user created.

It is only possible to create a MassLynx user if an Operating System user account already exists for that user name as, when a login is attempted, MassLynx authenticates the user's domain, user name, and password with the Operating System.

Users are not themselves allocated rights, but inherit them from the group of which they are made a member. Rights can easily be configured for a group – sample analysts, for example – and users added or removed from that group. This simplifies administration by removing the need to allocate rights to individual users.

### Recommendations:

- Standard MassLynx users are created automatically when MassLynx security is installed with default settings. Once other users have been created, these users should be disabled by adding them to the Disabled group. Information on adding users to groups can be found in [Adding users to groups on page 4-6](#).

**Caution:** It is essential that the 'Micromass' Operating System user account is not deleted on the PC controlling the instrument. If the user is deleted from the Operating System, your instrument will no longer operate.

It is always safe to disable the 'Micromass' MassLynx user account. On PCs other than the PC controlling the instrument, it is also safe to delete the 'Micromass' Operating System account.

- One of the new users you create will need to be made a member of the MassLynx Administrators group in order to log on to Security Manager. Adding users to groups is discussed in [Adding users to groups on page 4-6](#).



## Creating or modifying a user

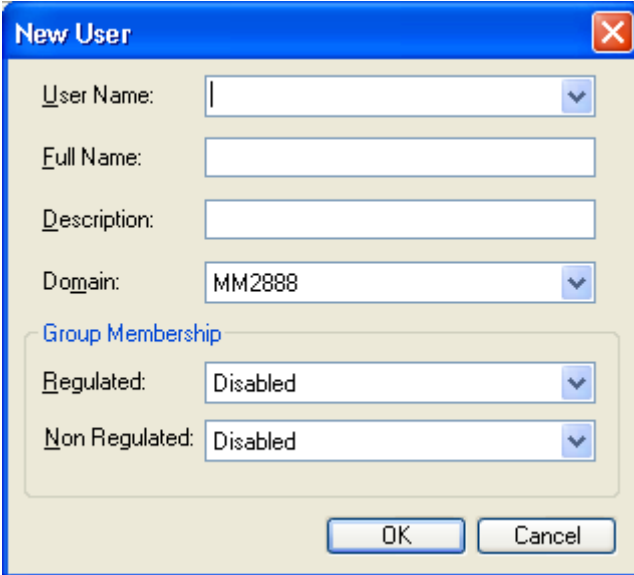
---

To create a new user:

1. Click Create > New User.

**Alternative:** Click .

The New User dialog box is displayed:



The screenshot shows a 'New User' dialog box with the following fields and options:

- User Name:** A dropdown menu.
- Full Name:** A text input field.
- Description:** A text input field.
- Domain:** A dropdown menu with 'MM2888' selected.
- Group Membership:** A section containing two dropdown menus:
  - Regulated:** Set to 'Disabled'.
  - Non Regulated:** Set to 'Disabled'.

Buttons for 'OK' and 'Cancel' are located at the bottom of the dialog.

2. In the Domain list, select the domain for which the user is valid.
3. In the User Name list, select the user name. If you cannot see the user's name in the list, but you are sure that the domain is set correctly, type the name into the User Name box.

**Tip:** The list of user names will usually be available if the user logged in to Security Manager is a member of the relevant domain.

4. In the Full Name box, type the user's full real name

**Tip:** This field is used by MassLynx to annotate security events. It does not have to be the same as the user's Windows Full Name.

5. In the Description box, type a description of the user – their role, for example.
6. Click OK.


### To modify a user:

1. In the user list, double-click the user you wish to modify.  
**Alternative:** Right-click the user, then click Edit.  
**Result:** The Manage User dialog box is displayed.
2. Modify the available settings as desired. Some of the settings for a user cannot be changed once the user has been created.
3. Click OK.

### To delete a user:

**Caution:** Users should never be deleted in regulated environments, and it is inadvisable whatever your situation. As MassLynx actions are recorded in the audit log with the name of the user who performed them, it is beneficial for all users to be retained in the system for future reference.

Users should be added to the Disabled group (see [Adding users to groups on page 4-6](#)) rather than be deleted.

1. In the user list, click the user you wish to delete.
2. Click Create > Delete.  
**Alternative:** Click .
3. Click Yes to confirm that you want to delete the user.

# 6

## Configuring Directory Policies

**Full Security only:** This chapter only applies to Full Security systems.

This chapter will explain what directory policies are, offer advice on how they might be used, and describe how to set them up.

### Contents:

Topic	Page
<a href="#">What are directory policies?</a>	6-2
<a href="#">Setting directory policies</a>	6-3

## What are directory policies?

---

Directory policies are used to control which directories users can access through MassLynx.

Configuring directory policies correctly ensures that different types of work are kept separate, that users do not access inappropriate information, and that there is no chance of Non-Regulated work accidentally crossing into Regulated areas.

Directory policies are configured by specifying the directories that a particular group can access. The users who are members of that group will then be able to use MassLynx to open and save files in those directories, subject to them having rights to do so.

There are two rights that can be granted for a directory:

- Allowed – Members of a group with this right will be able to access this directory and its subdirectories through MassLynx, and load files from and save files to them.
- Import – Members of a Regulated group with this right will be able to import files from this directory and its subdirectories.

### Tips:

- All users have access to the installation directory and its subdirectories. For this reason, these directories should never be used as locations for saving projects.
- Regulated and Non-Regulated groups should not be able to access the same directories through MassLynx.
- If Imported is checked and Allowed is not, then users in the group will not be able to load or save files to that directory, but will be able to import files into one of their allowed directories and modify them.

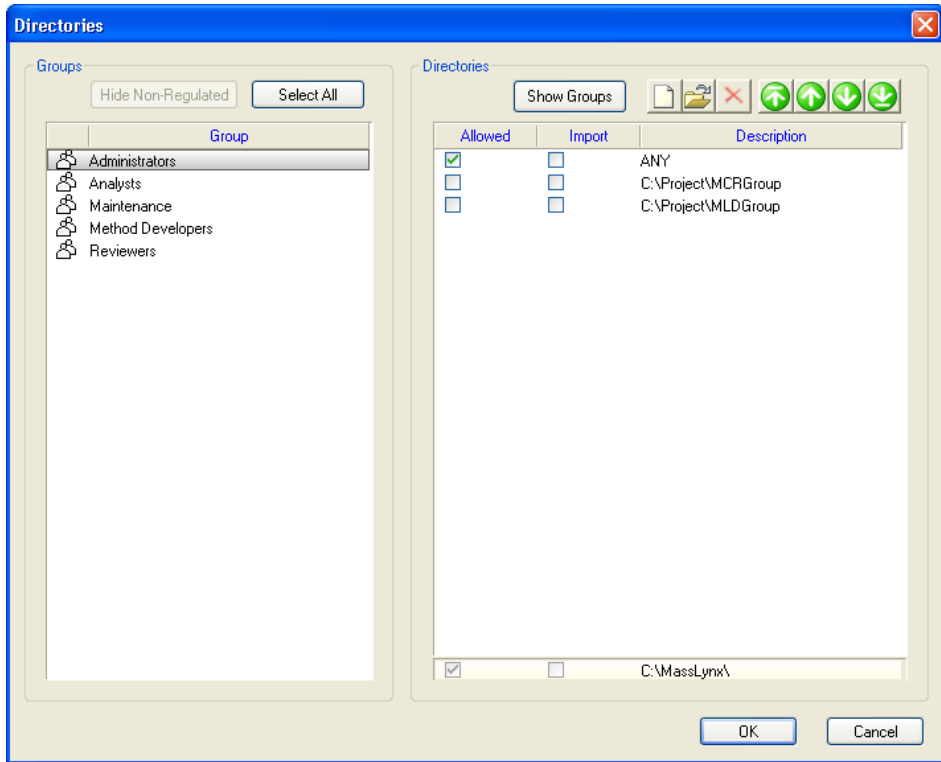
This is ideal for Regulated groups who need to utilize information, such as method files, created by Non-Regulated groups.

# Setting directory policies

To set directory policies:


1. Click Policies > Directory Policy.

**Result:** The Directories window is displayed.



2. Select a group in the left side of the window.

**Result:** In the right side of the window, the check boxes indicate which directories the group has access to.

3. To add a directory, click the  button.
4. In the Add Directory dialog box, enter the directory you wish to grant access to.

5. Click OK.

**Result:** The directory you have added is displayed in the right side of the window.



6. Select the Allowed check box on the line for the directory you have added.

7. Repeat steps 3 to 6 for other directories you want to allow access to.

8. Click OK.

The Directories window provides a number of additional features to help you administer directory policies.

**Directories window features:**

<b>To do this</b>	<b>Do this</b>
Edit a directory	<ol style="list-style-type: none"><li>1. In the right side of the window, click the directory you want to edit.</li><li>2. Click the  button.</li><li>3. Edit the directory, then click OK.</li></ol>
Delete a directory	<ol style="list-style-type: none"><li>1. In the right side of the window, click the directory you want to delete.</li><li>2. Click the  button.</li></ol>
Apply actions to more than one group	<ol style="list-style-type: none"><li>1. Select all the groups you want the action to apply to. To select a number of adjacent groups, click the first group, hold the Shift key, then click the last group. To select a number of non-adjacent groups, click the first group, hold the Ctrl key, then click each of the other groups.</li><li>2. Perform the action – selecting the Allowed check box, for example – that you wish to apply to the groups.</li></ol>

## Directories window features: (Continued)

To do this	Do this
Allow files to be imported from a directory	<ol style="list-style-type: none"><li data-bbox="787 253 1303 357">1. In the left side of the window, click the group you want to apply the policy to.</li><li data-bbox="787 357 1303 510">2. In the right side of the window, select the Imported check box for the directory you want to allow files to be imported from.</li></ol>
Show the groups that can access a directory	<ol style="list-style-type: none"><li data-bbox="787 519 1303 623">1. In the right side of the window, click the directory you are interested in.</li><li data-bbox="787 623 1303 666">2. Click Show Groups.</li></ol> <p data-bbox="787 666 1303 812"><b>Result:</b> The groups that are allowed to access or import from that directory are highlighted in the left side of the window.</p>





# 7

## Setting Security Policies

This chapter outlines the MassLynx Security policies available, and explains when you might wish to use them,

The chapter describes the policies in the same order as they appear in Security Manager.

### Contents:

Topic	Page
<a href="#">What are security policies?</a>	7-2
<a href="#">MassLynx Security enabled</a>	7-3
<a href="#">Critical error protection</a>	7-4
<a href="#">Use individual INI files</a>	7-5
<a href="#">Forget last username</a>	7-6
<a href="#">Tamper detection</a>	7-7
<a href="#">Audit policy</a>	7-8
<a href="#">Dual authorization</a>	7-11
<a href="#">Timeout</a>	7-12
<a href="#">LIMS policy</a>	7-13

## What are security policies?

---

Security policies affect the way in which security-enabled MassLynx runs. There are a number of settings that control:

- which information a user must enter to access and use MassLynx.
- how long a user must be inactive for before MassLynx locks automatically.
- whether users' personal preferences will be remembered.
- how attempts to tamper with files are reported.
- what MassLynx should do in the event of unexpected termination.
- which information should be stored in the audit log, and where the log should be stored.
- how users can export data to LIMS systems.

When configuring the security for a MassLynx system, go through each of the policies in turn, deciding which settings best meet the needs of your organization.

MassLynx security policy settings can be accessed by clicking Policies on the Security Manager menu bar.

# MassLynx Security enabled

---

**Basic Security only:** This section only applies to Basic Security systems.

**Security enabled settings:**

Setting	Implication
Enabled	Users are only able to log on if they are set up as MassLynx users and supply the correct user name and password details. Rights control, and all other Security Manager settings, will be enforced.
Not enabled	MassLynx users can access the system without supplying their credentials. No rights control will be exercised.

To toggle the option, click Policies > MassLynx Security Enabled. A tick will appear alongside MassLynx Security Enabled if security is currently enabled.

## Critical error protection

---

Critical error protection closes all MassLynx applications if a critical error – an abnormal program termination – occurs in any MassLynx component.

This ensures that no inconsistencies can be caused by parts of the program continuing to run, and that there is no chance that security can be compromised.

To toggle the option, click Policies > Critical Error Protection. A tick will appear alongside Critical Error Protection if it is currently enabled.

**Recommendation:** For Full Security systems, critical error protection should always be turned on.

## Use individual INI files

---

If you choose to use individual INI files, many of the user's preferences – such as the current project and location and size of application windows – will be retained.

Enabling this option is likely to enhance the user's experience, but if you want to apply any changes made to every user who logs on – regardless of who they are – choose to disable this feature.

**Recommendation:** Use individual INI files should usually be enabled for Full Security systems.

To toggle the option, click Policies > Use Individual INI files. A tick will appear alongside Use Individual INI files if it is currently enabled.

## Forget last username

---

This option allows you to specify whether a user should have to enter their domain and username every time they access the software.

If this option is selected, the details of the last user to log on will be cleared from the login dialog box, and all the details will need to be re-entered.

If the option is not selected, the username and domain of the last user to log on will be automatically filled in when the login dialog box is displayed – only the password will need to be entered.

**Recommendation:** Forget last username should usually be enabled for Full Security systems.

To toggle the option, click Policies > Forget Last Username. A tick will appear alongside Forget Last Username if it is currently enabled.

## Tamper detection

---

**Full Security only:** This section only applies to Full Security systems.

In Full Security mode, MassLynx will always ensure file integrity by detecting that files have been tampered with if an attempt is made to open them.

This option determines whether attempts to open files that have been tampered with will generate warning messages on the local machine, in the audit log, and (optionally) on a remote machine.

**Requirements:** For alerts to be sent to a remote machine, the Remote Alert settings must be configured in the Audit policy (see [page 7-8](#)), and the Windows Alerter and Messenger services must be running on both the local and remote machines. For assistance on setting up Alerter and Messenger, refer to Microsoft Windows help.

**Recommendation:** Tamper detection should usually be enabled for Full Security systems.

To toggle the option, click Policies > Tamper Detection. A tick will appear alongside Tamper Detection if it is currently enabled.

## Audit policy

---

The Audit Policy determines what type of events (such as users logging on or off, or accessing certain parts of MassLynx) should be recorded in the audit log, and where audit log information and alerts should be sent.

In Full Security mode, only the Remote Logging and Remote Alert settings are available – all events will be always be recorded.

In Basic Security mode, both the events to be recorded and the Remote Logging and Remote Alerts settings can be configured.

To set your Audit Policy, click Policies > Audit. The Audit Policy dialog box is displayed.

### Audit Policy dialog box:

The screenshot shows the 'Audit Policy' dialog box with the following settings:

- Audit:**  Enabled,  Failures Only,  Disabled
- Auditable events:**  Logon and Logoff,  Policy changes,  Object access,  Other event
- Remote Logging:** Enabled ; Store On: [ ]
- Remote Alerts:** Enabled ; Send To: [ ]



## Audit – Turning event logging on and off

**Basic Security only:** This section only applies to Basic Security systems.

To turn logging on for the selected event types, select Enabled in the Audit group box.

To turn logging off for the selected event types, select Disabled in the Audit group box.

To only log failed events, select Failures Only in the Audit group box.

## Auditable events – Selecting event types to log

**Basic Security only:** This section only applies to Basic Security systems.

To choose event types to log, select or clear the Auditable events check boxes.

### Logon and Logoff

Users logging on to and off from MassLynx applications on each workstation in a secure MassLynx system.

### Policy changes

Changes to Security Manager settings.

### Object access

Permissions checks to verify that users have the relevant group rights to perform a particular operation. Includes dual authorizations.

### Other events

#### Security events

- Attempts to compromise MassLynx security.
- LogLynx delete, import, and export & delete operations.
- Changes made within QuanLynx.

#### Audit events

- File signing operations.
- Starting and completing data acquisitions.
- Creating and altering metadata or results files.

## Remote Logging – Using a remote computer as a log server

### To use a remote computer as a log server:

1. Select the Remote Logging Enabled check box.
2. Type the NetBIOS name, DNS name, or IP address of a reachable remote computer in the Store On box.

### Requirements:

- The remote computer must have MassLynx installed, with security, if it is to be used as a log server.
- Some firewall configurations, such as the default settings for Windows XP Service Pack 2, may require alteration for remote logging to work successfully. For further information, see the Release Notes.

## Remote Alerts

Immediate alerts of serious security problems (file tampering, attempts to log on using a disabled account, and so on) can be sent to a remote computer or user.

### To enable remote alerts:

1. Select the Remote Alerts Enabled check box.
2. In the Send To box, do one of the following:
  - Type the name of a remote computer.
  - Type the NetBIOS name, DNS name, or IP address of a remote computer.
  - Type a user name.

**Tip:** Alerts will appear on the remote computer's screen, so they should not be sent to a computer that normally runs without a logged-on user.

**Requirement.** For remote alerts to work, the Windows Alerter and Messenger services must be running on both the local and remote machines. For assistance on setting up Alerter and Messenger, refer to Microsoft Windows help.

## Dual authorization

---

**Full Security only:** This section only applies to Full Security systems.

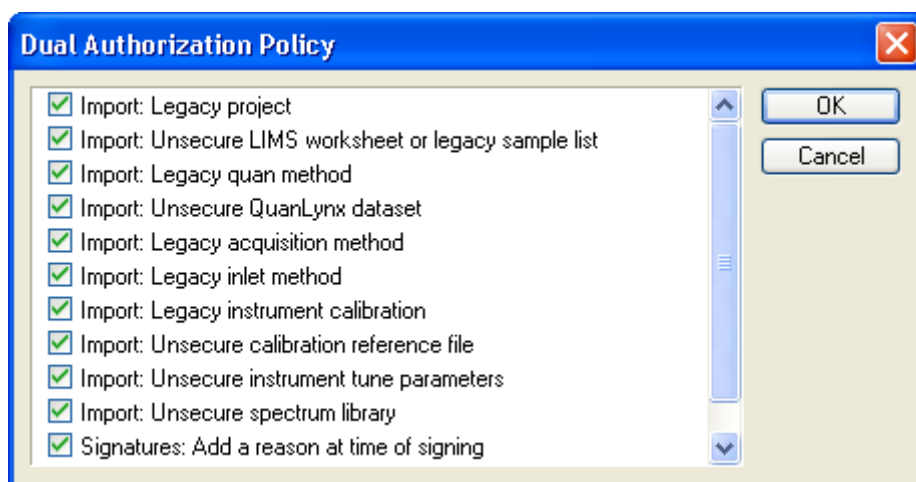
There are certain actions in MassLynx that have the potential to jeopardize the security of the system, but which need to be allowed in some circumstances.

To protect MassLynx security you can require both a MassLynx user and a MassLynx administrator to enter their passwords to authorize these actions. This is known as dual authorization.

### To configure the dual authorization settings:

1. Select Policies > Dual Authorization.

**Result:** The Dual Authorization Policy dialog box appears.



2. Select or clear the check boxes for the actions for which dual authorization will be required.
3. Click OK.

**Requirement:** When MassLynx prompts for dual authorization of an action, it must be the currently logged-in, non-administrator user and an administrator user who perform the authorization. Two administrator users cannot authorize an action.

## Timeout

---

If a user is inactive for a certain period of time they will have to re-enter their password before they can continue using MassLynx. You can specify how long they can be inactive for without needing to re-authenticate themselves.

### To set the timeout:

1. Click Policies > Timeout.
2. Type the length of inactivity after which the login dialog box should be displayed. The value should be between 0.5 and 60 minutes.

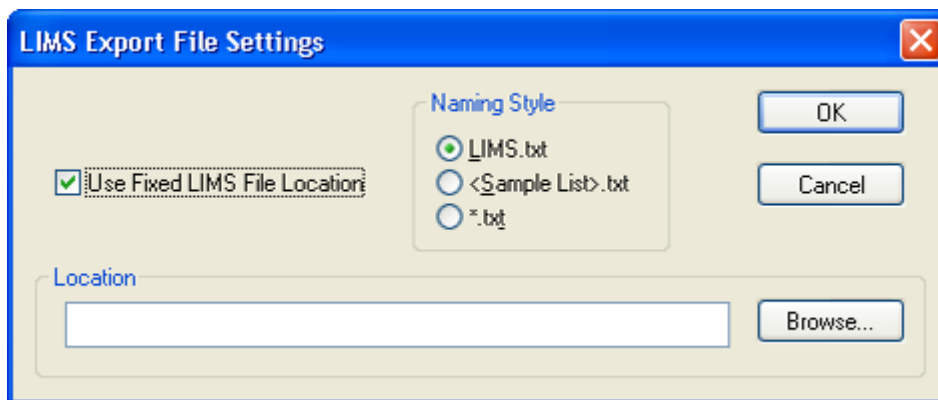
**Tip:** A user is deemed to be inactive if they are not performing any activity on the computer. The activity does not need to be in MassLynx applications.

3. Click OK.

## LIMS policy

You can configure the settings used when exporting LIMS (Laboratory Information Management System) files from QuanLynx, TargetLynx, or other MassLynx applications:

To configure LIMS export file settings, click Policies > LIMS Policy. The LIMS Export File Settings dialog box appears:



You can set values for the following properties:

### LIMS export file settings:

Setting	Description
Use Fixed LIMS File Location	Only export LIMS files to the folder specified in the Location field. This can be useful for integration into third-party LIMS systems which monitor a specific folder.
Location	When Use Fixed LIMS File Location is selected, this is the location that LIMS files are exported to.
Naming Style	
Naming Style - LIMS.txt	Exported LIMS files are always named LIMS.txt.
Naming Style - <SampleList>.txt	Exported LIMS files always use the name of the Sample List used to create the dataset.

### LIMS export file settings: (Continued)

<b>Setting</b>	<b>Description</b>
Naming Style - *.txt	The user will be able to specify the name of the exported LIMS file (but not the folder or the file extension).

# 8 Configuring Signature and Reason Policies

This chapter will outline what electronic signatures and reasons are, and explain how you might configure and use them on your system.

## Contents:

Topic	Page
What are signatures and reasons?	8-2
Deciding whether signatures and reasons are required	8-3
Choosing the actions that require a signature or reason	8-6
Setting the available reasons	8-7
Entering signatures and reasons	8-11
Viewing file signatures and reasons	8-12
Adding signatures or reasons to existing files	8-13

## What are signatures and reasons?

---

MassLynx provides an audit log to electronically record who performed actions – acquiring data, creating MS methods, altering quantitation curves, and so on – and when they were carried out.

In addition to this, however, you can specify certain actions that request or require the user to “sign” what they have done by supplying their authentication credentials, to enter a reason explaining why they have done it, or both.

Signatures and reasons are normally used in situations where it is important to be able to step through the entire process that led to a set of results. This may be part of an internal audit process, or it may be required by a regulatory authority which is reviewing your work.

While it might be essential to require signatures or reasons at some times, it may be unnecessarily time-consuming at others. MassLynx lets you choose the type of actions to apply the check to, and allows you to set whether signatures or reasons should be requested or required.

### Basic Security and Full Security

With Basic Security, signatures and reasons can only be applied to internal modifications. Internal modifications are actions within QuanLynx and TargetLynx that do not result in a file (whether new or modified) being saved to disk.

With Full Security, signatures and reasons can be applied to a wide range of actions that save or change a file on disk, as well as to internal modifications.



## Deciding whether signatures and reasons are required

There are two different types of actions which can have signature and reason policies applied:

- **Electronic Records** – These actions result in files being saved to disk (or files on disk being modified). Signature and reason policies can only be specified for these actions on Full Security systems.
- **Intermediate Modifications** – These actions are operations performed within QuanLynx or TargetLynx that do not result in a file being saved to disk.

The policies are set in the Signature and Reason Policy dialog box, accessed by clicking Policies > Signatures and Reasons.

**Signature and Reason Policy dialog box:**

**Signature and Reason Policy**

**Electronic Records Policy**

Electronic Signatures: None [v] [Actions...]

Reasons for Change: None [v] [Reasons...]

**Intermediate Modifications Policy**

Electronic Signatures: None [v] [Actions...]

Reasons for Change: None [v] [Reasons...]

Default to use of current username when signing

[OK] [Cancel]

For each of these types of action (Electronic Records and Intermediate Modifications), a policy can be set for signatures and a policy set for reasons using the drop-down lists.

### Signature and reason policy options:

Policy	Description
None	The user will not be asked to provide a signature or reason (as applicable).
Don't Force	The user will be asked to provide a signature or reason, but they are free not to do so.
Warn	The user will be asked to provide a signature or reason, and they will be warned if they choose not to.
Force	The user must provide a signature or reason before being able to continue with the action.

Give careful consideration to the needs of your organization before deciding what the signature and reason policy should be. Consider the use that the system will be put to, what will be done with the results, and who might examine your processes.

**Tip:** In most situations it is not normally very useful to have signatures without reasons, as only the person who performed the action will be recorded, not why they did it.

Click Actions to select the actions that will result in your signatures and reasons policy being applied. For details, see [Choosing the actions that require a signature or reason on page 8-6](#).

Click Reasons to set the reasons that will be available for the actions you have chosen. For details, see [Setting the available reasons on page 8-7](#).

Signatures and reasons entered by users will be recorded in the audit logs. For file modifications this is the LogLynx log. For QuanLynx modifications it is the QuanLynx log; for TargetLynx modifications it is the TargetLynx log. See [What are the audit logs? on page 10-2](#) for more information.

## Forcing users to enter full signature information

When a signature is prompted for, MassLynx can automatically fill in the user name and domain of the currently logged-in user. While this is a useful

feature for many, you may wish to require users to enter all their signature information each time they perform a signature.

**To force all signature components to be used:**

1. Click Policies > Signatures and Reasons.
2. Clear the Default to use of current user name when signing check box.
3. Click OK.

## Choosing the actions that require a signature or reason

Once you have decided that signatures or reasons are required, you need to select the actions that will need a signature or reason.

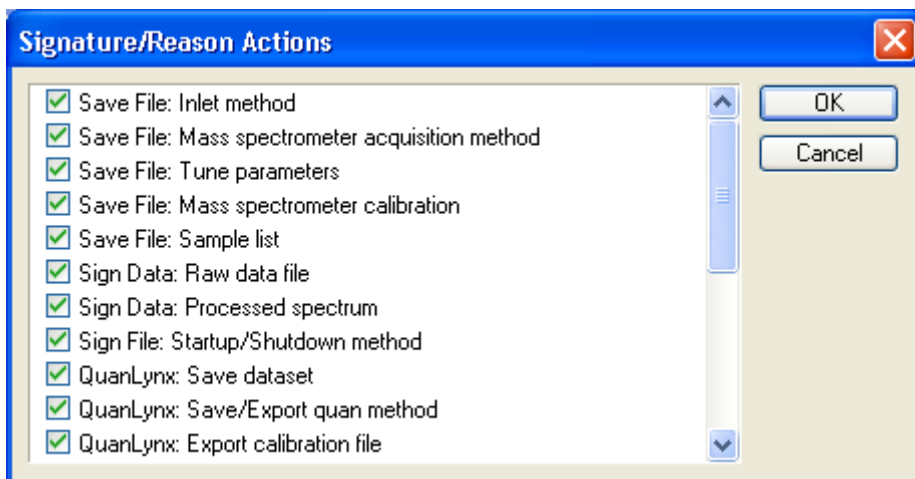
### To select the actions requiring a signature or reason:

1. Click Policies > Signatures and Reasons.

**Result:** The Signature and Reason Policy dialog box is displayed.

2. If you want any Electronic Record actions to prompt for a signature or reason, click the Actions button in the Electronic Records Policy frame.

**Result.** The Signatures/Reasons Actions dialog box is displayed.



3. Select or clear the check boxes for the actions for which signatures or reasons will be required.
4. Click OK.
5. If you want any Intermediate Modification actions to prompt for a signature or reason, click the Actions button in the Intermediate Modifications Policy frame, then repeat steps 3 and 4.

**Tip:** A signature indicates that the user approves that the item they are signing is correct. When deciding which actions need signatures, you should determine the stages of your process that require this type of confirmation.

## Setting the available reasons

---

For each action that you have decided should have a reason associated with it, the list that user can choose from can be configured. You can also allow the user to type their own reason – this is known as freeform entry.

**Tip:** Additional reasons can be added at the point of signature/reason entry if the user is a member of a group with the right - Administrative – Allow reasons to be added at the point of sign. A dual authorization may be required, depending on your dual authorization policy settings.

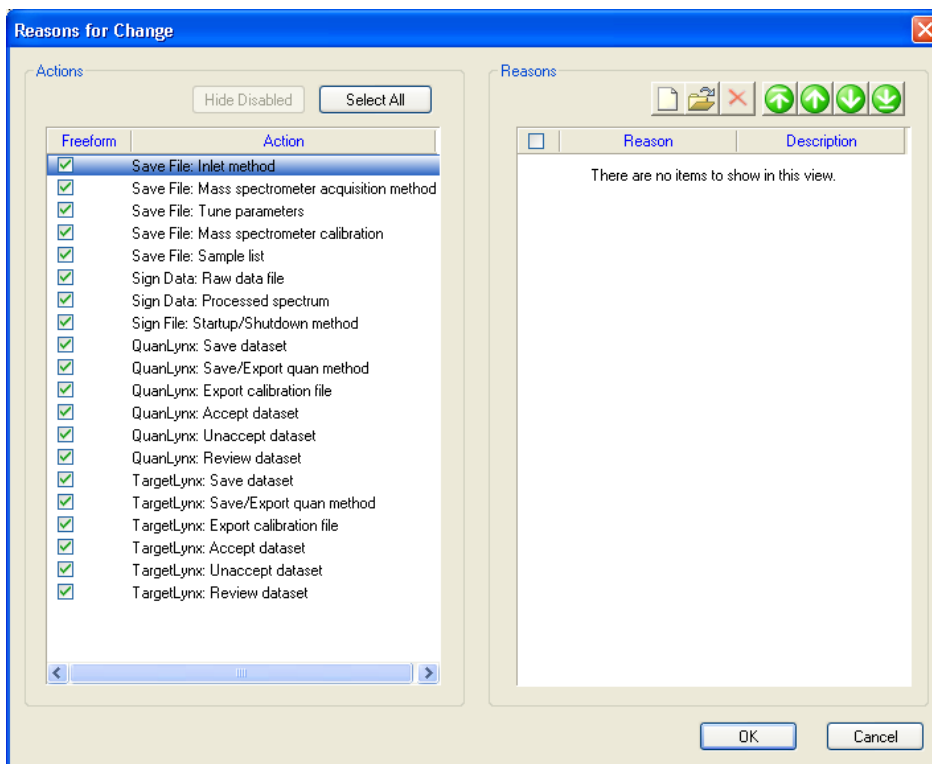
## To configure the reasons:


1. Click Policies > Signatures and Reasons.

**Result:** The Signature and Reason Policy dialog box is displayed.

2. To configure the list of reasons for Electronic Record actions, click the Reasons button on the Electronic Records Policy frame.

**Result:** The Reasons for Change window is displayed, with actions on the left side of the window and possible reasons on the right side.





3. To add a new reason, click .

**Result:** The Add Reason dialog box is displayed



4. Enter the reason you wish to add, and a description.
5. Click OK.  
**Result:** The reason you have added is displayed in the right side of the window.
6. Click an action in the left side of the window that you want the reason to be available for.
7. Select the check box next to the reason.
8. Repeat steps 3 to 7 for other reasons you want to add.
9. Click OK.
10. To configure the list of reasons for Intermediate Modification actions, click the Reasons button on the Intermediate Modifications Policy frame, then repeat steps 3 to 9.

The Reasons for Change window provides a number of additional features to help you configure reasons.

#### Reasons for Change window features:

To do this	Do this
Allow freeform entry of reasons	<ol style="list-style-type: none"> <li>1. In the left side of the window, click the action you want to allow freeform reason entry for.</li> <li>2. Ensure that the Freeform check box is selected.</li> </ol>
Edit a reason	<ol style="list-style-type: none"> <li>1. In the right side of the window, click the reason that you want to edit.</li> <li>2. Click the  button.</li> <li>3. Edit the reason, then click OK.</li> </ol>
Delete a reason	<ol style="list-style-type: none"> <li>1. In the right side of the window, click the reason that you want to delete.</li> <li>2. Click the  button.</li> </ol>

## Reasons for Change window features: (Continued)

To do this	Do this
Apply reasons to more than one action at once	<ol style="list-style-type: none"><li data-bbox="794 253 1300 644">1. Select all the actions you want the reason to be available for. To select a number of adjacent actions, click the first action, hold the Shift key, then click the last action. To select a number of non-adjacent actions, click the first action, hold the Ctrl key, then click each of the other actions.</li><li data-bbox="794 644 1300 722">2. Select or clear the reason check boxes as required.</li></ol>
Change the order of reasons	<ol style="list-style-type: none"><li data-bbox="794 743 1300 803">1. Click the reason you wish to move.</li><li data-bbox="794 803 1300 986">2. Click the  or  buttons to move the reason higher or lower in the list. You can also move the reason to the top or bottom of the list.</li></ol> <p data-bbox="794 1003 1300 1164"><b>Tip:</b> You can highlight and move multiple reasons at the same time by holding down the Ctrl or Shift keys while clicking the reasons you want to move.</p>



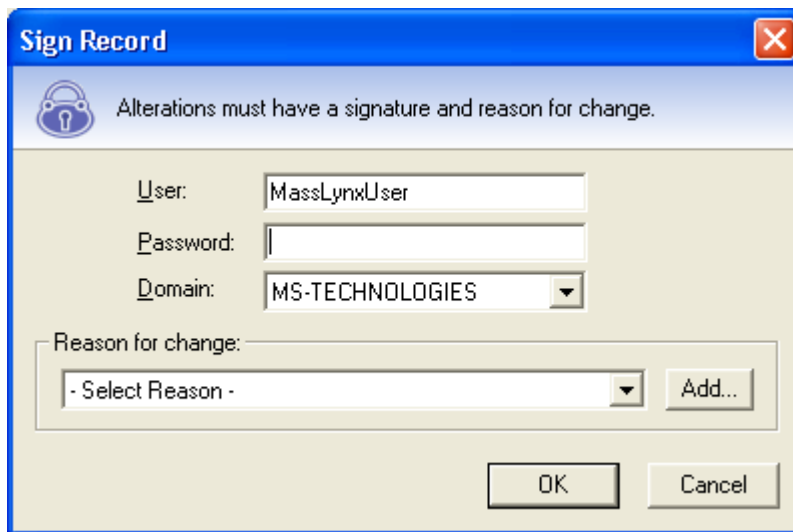
## Entering signatures and reasons

---

If actions have been specified as requiring signatures or reasons, MassLynx will prompt you to enter the appropriate information when you try to perform the action.

Enter the information in the Sign Record dialog box.

### Sign Record dialog box:



The dialog box is titled "Sign Record" and features a blue header bar with a close button. Below the header, a padlock icon is followed by the text "Alterations must have a signature and reason for change." The main content area includes three input fields: "User:" containing "MassLynxUser", "Password:" which is empty, and "Domain:" with a dropdown menu set to "MS-TECHNOLOGIES". Below these is a "Reason for change:" section with a dropdown menu showing "- Select Reason -" and an "Add..." button. At the bottom of the dialog are "OK" and "Cancel" buttons.

The dialog box consists of several parts. The signature and reason sections will only appear if a signature or reason is required for this action.

- The header, containing the padlock image, tells you what you need to do. What is required may change between systems, or between different parts of the same system.
- The signature section contains boxes in which you need to enter your user name (it may already have been filled in for you), your password, and your domain. By signing a change you are confirming that you accept responsibility for it. If you do not want to do this, click Cancel.
- The reason section contains a list from which you can choose a reason that explains why you are performing the action. Depending on how the system is configured, you may be able to type a reason of your own. You may also be able to enter new reasons to be added to the list if you have permissions to do so.

## Viewing file signatures and reasons

---

Signatures and reasons associated with an open file can be viewed in the main MassLynx interface. The option to do so will only be available if your system has been configured to request or require signatures or reasons.

### To view the signatures and reasons for a file:

1. Open the window associated with the file.

**Example:** To view the signatures and reasons for a Sample List, open the main MassLynx window. To view the signatures and reasons for MS Method files, open the Experiment Setup (MS Method) window.

2. Click File > Properties.

**Result:** A Properties dialog for the file is displayed, containing information on the signatures associated with the file (if the file is signed) and the reason (if present).

## Adding signatures or reasons to existing files

---

If MassLynx has been configured to request (but not require) signatures or reasons for certain actions, you can add signatures or reasons to files at any time through the MassLynx interface.

### To add signatures or reasons to a file:

1. Open the window associated with the file.

**Example:** To add a signature or reason to a Sample List, open the main MassLynx window. To add a signature or reason to MS Method files, open the Experiment Setup (MS Method) window.

2. Click File > Sign *<type of file>*

**Rule:** If a file has been modified, it must be saved before it can be signed.

3. Add your signature or reason as required.
4. Click OK.

### To add signatures or reasons to a raw data file:

1. In the main MassLynx window, click File > Open Data File.
2. Browse to the directory containing the file you wish to sign.
3. Click the file you wish to sign.
4. Click Sign.
5. Add your signature or reason as required.
6. Click OK.

**Caution:** By adding a signature or reason, you will replace any existing signature or reason associated with the file. For instance, if a reason is added to a file that already has a signature, the file will not then be signed unless a signature is provided at the same time as the reason. All the signatures and reasons will be recorded in the audit log.



# 9 Saving, Printing, and Sharing Security Settings

This topic will outline how to save your security settings, print them for future reference, and use rollout files to share security settings between MassLynx systems.

## Contents:

Topic	Page
<a href="#">Saving security settings</a>	9-2
<a href="#">Printing security settings</a>	9-3
<a href="#">Exporting and importing security settings</a>	9-4

## Saving security settings

---

Once your security settings have been configured in Security Manager, they must be saved. Your settings will not take effect until they have been saved.

### To save your settings:

Click File > Save.

**Alternative:** Click .

## Printing security settings

---

You can print the Security Manager settings as a record of the site policy implemented on a MassLynx machine, either to allow other machines to be set up appropriately or to provide a record for inspection by an auditor.

### To print your settings:

1. Click File > Print.

**Alternative:** Click .

2. In the Print dialog box, click OK.

### Tips:

- Security settings can only be printed once they have been saved. If the settings have recently been changed, save them before you try to print.
- As security settings are also recorded in the audit log whenever an alteration is made, it is possible to print them by viewing the event in LogLynx. For information on using LogLynx, see [Viewing, Exporting, and Printing Audit Logs on page 10-1](#).

## Exporting and importing security settings

---

So that you do not have to configure all the security settings on every system, MassLynx enables you to export your security settings – and import security settings from elsewhere – by using Security Rollout files.

**Tip:** If you want to replicate the security settings from another MassLynx system, select a Security Rollout file during installation to import the settings automatically.

### To export the current Security Manager settings:

1. Click File > Export.
2. In the Save As dialog box, choose a directory to save the rollout file into, and enter a name.
3. Click Save.

**Result:** A Security Rollout file, with the name you specified and the extension .srf, will be created.

### To import a Security Rollout file:

1. Select File > Import.
2. In the Open dialog box, browse to the Security Rollout file (\*.srf) that you want to import.
3. Click Open.

**Result:** The Security Manager settings are imported. They will only be applied when the security settings are saved.

**Caution:** When security settings are imported, the current MassLynx users will be replaced by the users defined in the Security Rollout file.

Before importing a Security Rollout File, you should check that both the user and administrator accounts defined in the file, and any log server specified, are on accessible domains. If you are not sure how to do this, contact your system administrator.



# 10 Viewing, Exporting, and Printing Audit Logs

This chapter will outline what the audit logs are, explain how to view the information they contain, and describe how to extract the information you need for your records.

## Contents:

Topic	Page
<a href="#">What are the audit logs?</a>	10-2
<a href="#">Starting LogLynx</a>	10-3
<a href="#">Viewing the LogLynx log</a>	10-5
<a href="#">Filtering the LogLynx log</a>	10-7
<a href="#">Backing up, exporting, and clearing the LogLynx log</a>	10-28
<a href="#">Printing the LogLynx log</a>	10-32

## What are the audit logs?

---

Audit logs are created by MassLynx to record system operations. Items recorded in the logs include users logging on, failed login attempts, access to various parts of the interface, and files being saved, among many others.

If you are using Basic Security, the contents of the audit log will depend on your Audit policy (see [Audit policy on page 7-8](#) for details). If you are using Full Security, all information will always be logged.

Most operations are recorded in the main audit log, accessed through a dedicated viewer called LogLynx. Intermediate Modifications – operations which do not result in a file being saved to disk – performed in QuanLynx or TargetLynx are stored in their own audit logs, accessed through the QuanLynx and TargetLynx viewers.

LogLynx – which is only accessible to users with appropriate rights – enables you to view the log, filter the log (so that only the items you are interested in are displayed), print the log, and export it to file.

**See also:** For information on accessing and using audit logs in QuanLynx and TargetLynx, refer to the online Help for those application managers.

# Starting LogLynx

---

## To start LogLynx:

1. Click Start > All Programs > MassLynx > LogLynx.

**Result:** If you are not already logged in to MassLynx, the MassLynx Login dialog appears.

1. Type your Windows user name in the Logon Name field.
2. Type your Windows password in the Password field.
3. From the Domain list, select the domain for which your Windows user name is valid.
4. Click OK.

**Tip:** You will need to be a member of a group with rights to access LogLynx in order to log in.

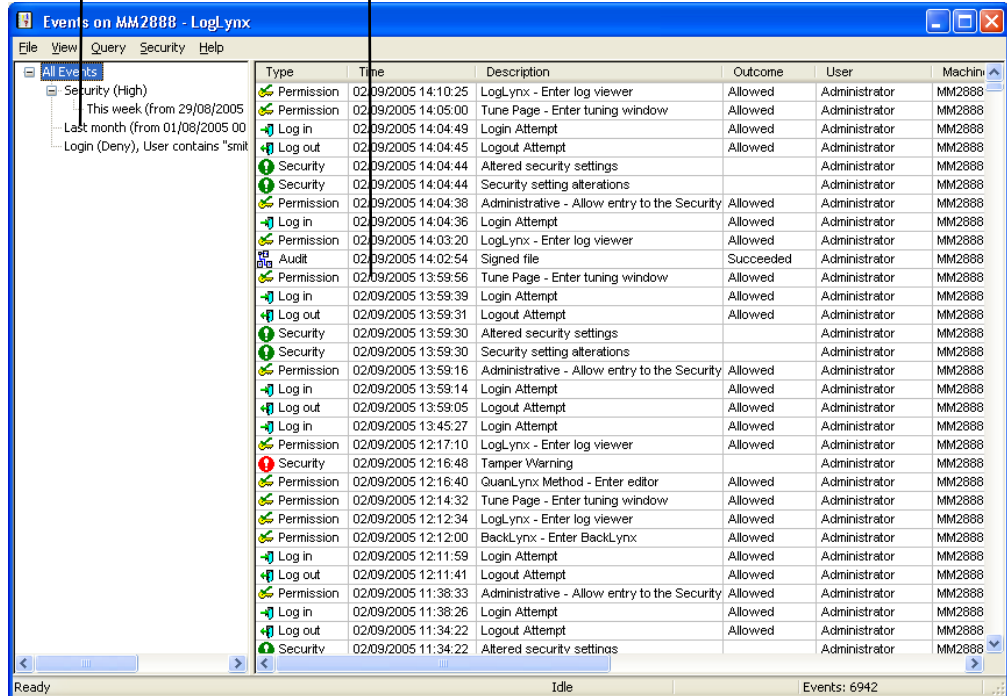
2. If a warning message appears, read the message. If you do not understand the message or are not happy to continue, close the LogLynx window as soon as it appears and consult your system administrator. Click OK.

When you have successfully logged in, the LogLynx window will be displayed.

## LogLynx window:

Tree pane

Events pane



The screenshot shows the LogLynx application window titled "Events on MM2888 - LogLynx". The window has a menu bar with "File", "View", "Query", "Security", and "Help". On the left is a tree pane showing a hierarchy of filters: "All Events", "Security (High)", "This week (from 29/08/2005)", "Last month (from 01/08/2005 00)", and "Login (Deny), User contains 'smit'". On the right is an events pane displaying a table of log events. The table has columns for Type, Time, Description, Outcome, User, and Machine. The events are sorted by time, showing various activities like logins, logouts, security settings changes, and administrative actions. The status bar at the bottom indicates "Ready", "Idle", and "Events: 6942".

Type	Time	Description	Outcome	User	Machine
Permission	02/09/2005 14:10:25	LogLynx - Enter log viewer	Allowed	Administrator	MM2888
Permission	02/09/2005 14:05:00	Tune Page - Enter tuning window	Allowed	Administrator	MM2888
Log in	02/09/2005 14:04:49	Login Attempt	Allowed	Administrator	MM2888
Log out	02/09/2005 14:04:45	Logout Attempt	Allowed	Administrator	MM2888
Security	02/09/2005 14:04:44	Altered security settings		Administrator	MM2888
Security	02/09/2005 14:04:44	Security setting alterations		Administrator	MM2888
Administrative - Allow entry to the Security	02/09/2005 14:04:38	Administrative - Allow entry to the Security	Allowed	Administrator	MM2888
Log in	02/09/2005 14:04:36	Login Attempt	Allowed	Administrator	MM2888
Permission	02/09/2005 14:03:20	LogLynx - Enter log viewer	Allowed	Administrator	MM2888
Audit	02/09/2005 14:02:54	Signed file	Succeeded	Administrator	MM2888
Permission	02/09/2005 13:59:56	Tune Page - Enter tuning window	Allowed	Administrator	MM2888
Log in	02/09/2005 13:59:39	Login Attempt	Allowed	Administrator	MM2888
Log out	02/09/2005 13:59:31	Logout Attempt	Allowed	Administrator	MM2888
Security	02/09/2005 13:59:30	Altered security settings		Administrator	MM2888
Security	02/09/2005 13:59:30	Security setting alterations		Administrator	MM2888
Permission	02/09/2005 13:59:16	Administrative - Allow entry to the Security	Allowed	Administrator	MM2888
Log in	02/09/2005 13:59:14	Login Attempt	Allowed	Administrator	MM2888
Log out	02/09/2005 13:59:05	Logout Attempt	Allowed	Administrator	MM2888
Log in	02/09/2005 13:45:27	Login Attempt	Allowed	Administrator	MM2888
Permission	02/09/2005 12:17:10	LogLynx - Enter log viewer	Allowed	Administrator	MM2888
Security	02/09/2005 12:16:48	Tamper Warning		Administrator	MM2888
Permission	02/09/2005 12:16:40	QuanLynx Method - Enter editor	Allowed	Administrator	MM2888
Permission	02/09/2005 12:14:32	Tune Page - Enter tuning window	Allowed	Administrator	MM2888
Permission	02/09/2005 12:12:34	LogLynx - Enter log viewer	Allowed	Administrator	MM2888
Permission	02/09/2005 12:12:00	BackLynx - Enter BackLynx	Allowed	Administrator	MM2888
Log in	02/09/2005 12:11:59	Login Attempt	Allowed	Administrator	MM2888
Log out	02/09/2005 12:11:41	Logout Attempt	Allowed	Administrator	MM2888
Permission	02/09/2005 11:38:33	Administrative - Allow entry to the Security	Allowed	Administrator	MM2888
Log in	02/09/2005 11:38:26	Login Attempt	Allowed	Administrator	MM2888
Log out	02/09/2005 11:34:22	Logout Attempt	Allowed	Administrator	MM2888
Security	02/09/2005 11:34:22	Altered security settings		Administrator	MM2888

The tree pane shows the filters that are being, or can be, applied to the log. More information on this can be found in [Filtering the LogLynx log on page 10-7](#).

The events pane contains a list of events with a row of details for each event.

## Viewing the LogLynx log

---

The audit log is displayed when LogLynx is opened. The events are listed in date and time order, with the most recent at the top.

When you first open LogLynx, all the events are shown. If you have created filters (see [Filtering the LogLynx log on page 10-7](#)), click All Events in the tree pane to revert to seeing all the events.

### To view details of a specific event:

1. Double-click the event in the events pane.

**Result:** The Event Details are displayed.

2. When you have finished with the details, click File > Exit.

**Tip:** If you need a hard copy, you can print the details from the Event Details dialog box by clicking File > Print.

### To modify the columns displayed:

1. Click View > Choose Columns.
2. Select the check boxes beside the columns you want to display.
3. Clear the check boxes beside the columns you want to hide.
4. Click OK.

### To modify the column order:

Drag the column to the desired location.

### To reset the column display to the defaults:

1. Click View > Choose Columns.
2. Select the Select Default Columns check box.
3. Click OK.

### To change column widths:

Drag the edges of a column headings until the column is the desired width.

**To reset the column widths to the defaults:**

1. Click View > Choose Columns.
2. Select Reset Column Widths.
3. Click OK.

## Importing audit logs

If audit log information has previously been exported from LogLynx (see [Backing up, exporting, and clearing the LogLynx log on page 10-28](#) for details) you can view the information in LogLynx by importing the file.

**To import an audit log:**

1. Click File > Import.
2. Browse for the file you want to import.
3. Click Open.
4. In the File Import dialog box, click OK.

**Result:** The selected audit log will be imported and integrated into the audit log information displayed.

## Filtering the LogLynx log

---

There may be many thousands, perhaps millions, of events in an audit log. You can reduce the number of events displayed, making it easier to find the information you need, by creating a filter – also known as an event query.

Event queries are based on one or more of the following:

- A date/time range (see [Creating a date/time range query on page 10-7](#)).
- The user or machine that caused the event (see [Creating an event origin query on page 10-11](#)).
- The event type (see [Creating event type queries on page 10-13](#)).

**Tip:** Queries are not saved if LogLynx is closed down and re-opened. If you want to keep the results of a query, you can print them from LogLynx. See [Printing the LogLynx log on page 10-32](#) for more information.

### To delete an event query:

1. Click the event query in the tree pane.
2. Right-click, then click Close List.

## Creating a date/time range query

You can filter the audit log so that only events written during specified periods are displayed. To do this, create a date/time range query.

### To create a date/time range query:

1. In the tree pane, click the list you want to filter by date and time.

**Tip:** If this is the first query you have created, click All Events.

2. Click Query > Date/Time Range.

**Result:** The Date/Time Event Query dialog box is displayed.

3. Select the settings to apply to your query. Information on the individual parameters available is given below.

4. Click OK.

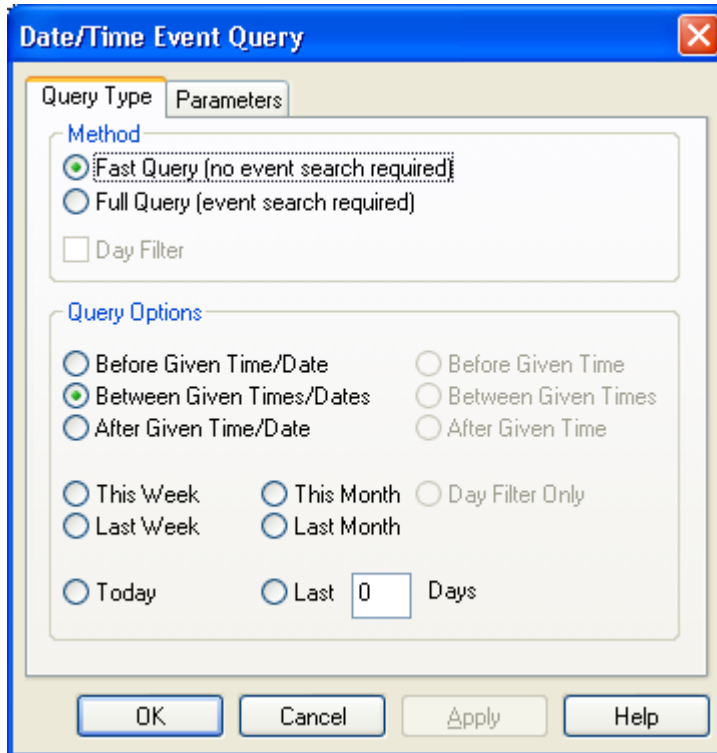
**Result:** The query will be added to the tree pane. Click the query to see the filtered results.

## The Date/Time Event Query dialog box

The dialog box has two tabs:

- Query Type – Defines the query.
- Parameters – Specifies the dates and/or times that the query applies to.

### Query Type tab:





The options available on this tab are described below:

**Query Type tab:**

Name	Description
Method	
Fast Query (no event search required)	<p>Performs a fast search; only Event indexing information is referenced, giving virtually instantaneous results.</p> <p><b>Tip.</b> Where possible, perform a Fast query first on large databases before performing subsequent queries on the restricted dataset; this should speed up the search.</p>
Full Query (event search required)	<p>Performs a full search; every Event between the specified times is read and passed through the filter. This may take several minutes for large databases.</p>
Day Filter	<p>Enables the Weekday options in the Parameters tab, and some additional options on the Query Type tab. This option is only available when the Full Query option is selected.</p>
Query Options	
Before given time and date	<p>Specifies that the query will filter by events before the time and date set on the Parameters tab.</p>
Between given Times/dates	<p>Specifies that the query will filter by events between the times and dates set on the Parameters tab.</p>
After given time/date	<p>Specifies that the query will filter by events after the time and date set on the Parameters tab.</p>
Before given time	<p>Specifies that the query will filter by events before a given time of day, set on the Parameters tab.</p>
Between given times	<p>Specifies that the query will filter by events between the times of day set on the Parameters tab.</p>
After given time	<p>Specifies that the query will filter by events after a given time of day, set on the Parameters tab.</p>
This week	<p>Confines the search to the current week.</p>
Last week	<p>Confines the search to the previous week.</p>
This month	<p>Confines the search to the current month.</p>

### Query Type tab: (Continued)

Name	Description
Last month	Confines the search to the previous month.
Day Filter Only	Confines the search to the days of the week selected on the Parameters tab.
Today	Confines the search to the current day.
Last...days	Confines the search to the specified number of most recent days.

## Parameters tab:

The screenshot shows a dialog box titled "Date/Time Event Query" with a close button (X) in the top right corner. It has two tabs: "Query Type" and "Parameters". The "Parameters" tab is active. Under the "Range and Limits" section, there are two rows. The first row is labeled "From:" and contains a time input field with "16:33:46" and a date dropdown menu showing "28 June 2005". The second row is labeled "To:" and contains a time input field with "16:33:46" and a date dropdown menu showing "28 June 2005". Under the "Weekday" section, there are seven checkboxes for the days of the week: Mon, Tue, Wed, Thu, Fri, Sat, and Sun. At the bottom of the dialog, there are four buttons: "OK", "Cancel", "Apply", and "Help".

The options available on the Parameters tab will vary, depending on the options selected on the Query Type tab.

## Parameters tab:

Name	Description
From....To	The query will filter by events between the times and dates specified.
Weekday	The search will be confined to the days of the week selected.

## Creating an event origin query

You can filter the audit log so that only events that originated with specified users or machines are displayed. To do this, create an event origin query.

### To create an event origin query:

1. In the tree pane, click the list you want to filter by event origin.

**Tip:** If this is the first query you have created, click All Events.

2. Click Query > Origin.

**Result:** The Query: Event Origin dialog box is displayed.

3. Select the settings to apply to your query. Information on the individual parameters available is given below.

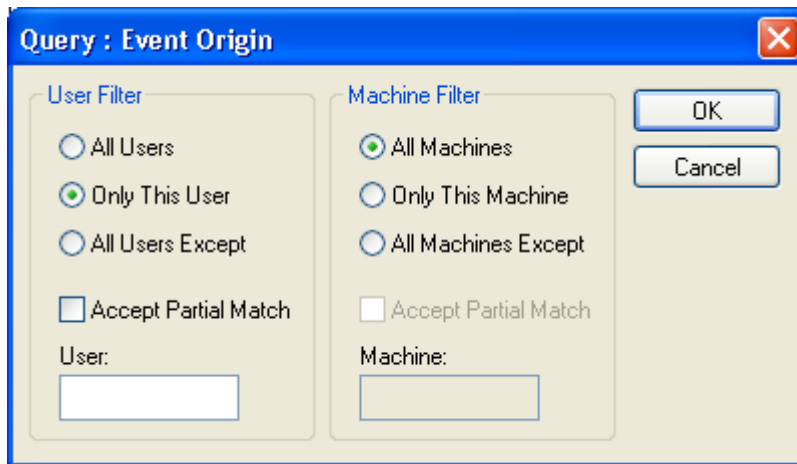
4. Click OK.

**Result:** The query will be added to the tree pane. Click the query to see the filtered results.

### The Query : Event Origin dialog box

Use the Query : Event Origin dialog box to create queries that filter the audit log by the user or machine that originated the events.

#### Query : Event Origin dialog box:



#### Query : Event Origin:

Name	Description
User Filter	
All Users	Searches for events generated by any user.

## Query : Event Origin: (Continued)

Name	Description
Only this user	Searches for events generated by the user specified in the User box.
All users except	Searches for events generated by any user except the user specified in the User box.
Accept partial match	User names that contain the text specified in the User box will be included in the results of the query. If this option is not selected, only user names that are exactly the same as the specified text will be included. <b>Tip.</b> This option can be used to search for a number of users with similar user names.
Machine Filter	
All machines	Searches for events generated by any machine.
Only this machine	Searches for events generated by the machine specified in the Machine box.
All Machines except	Searches for events generated by any machine except the machine specified in the Machine box.
Accept partial match	Machine names that contain the text specified in the Machine box will be included in the results of the query. If this option is not selected, only machine names that are exactly the same as the specified text will be included. <b>Tip.</b> This option can be used to search for a number of machines with similar names.

## Creating event type queries

You can filter the audit log so that only events of a specified type are displayed. You do this by creating event type queries. A number of different event type queries are available:

- Permission check – whether actions were allowed or denied. See [page 10-14](#) for details.
- Log In/Out – successful or unsuccessful logins or logouts. See [page 10-16](#) for details.

- Security – modifications to MassLynx security settings. See [page 10-18](#) for details.
- Audit path – events relating to a specified path on disk and/or limited to certain types of event. See [page 10-20](#) for details.
- Information event – events giving information that does not fall into other categories. See [page 10-23](#) for details.
- Verification event – actions that required dual authorization, either successful or unsuccessful. See [page 10-25](#) for details.

## Permission Check event

A Permission Check event query enables you to filter the audit log to show only actions that were allowed or denied.

### To create a permission check event query:

1. In the tree pane, click the list you want to filter.  
**Tip:** If this is the first query you have created, click All Events.
2. Click Query > Event Type > Permission Check.  
**Result:** The Query: Permission Check Event dialog box is displayed.
3. Select the settings to apply to your query. Information on the individual parameters available is given below.
4. Click OK.  
**Result:** The query will be added to the tree pane. Click the query to see the filtered results.

## Query: Permission Check Event dialog box:

## Query: Permission Check Event dialog options:

Name	Description
Outcome	
Show ALLOWED operations	Searches for Allowed operations (shown as Allowed in the audit log Outcome column).
Show DENIED operations	Searches for Denied operations (shown as Denied in the audit log Outcome column).
User Filter	
Only this user	Searches for events generated by the user specified in the adjacent text box.
Allow partial match	User names that contain the text specified in the adjacent box will be included in the results of the query. If this option is not selected, only user names that are exactly the same as the specified text will be included. <b>Tip.</b> This option can be used to search for a number of users with similar user names.

## Query: Permission Check Event dialog options: (Continued)

Name	Description
Machine Filter	
Only this machine	Searches for events generated by the machine specified in the adjacent text box.
Allow partial match	Machine names that contain the text specified in the adjacent box will be included in the results of the query. If this option is not selected, only machine names that are exactly the same as the specified text will be included. <b>Tip.</b> This option can be used to search for a number of machines with similar names.

### Log In/Out event

A Log In/Out event query enables you to filter the audit log to show only login and logout events.

#### To create an log in/out event query:

1. In the tree pane, click the list you want to filter.

**Tip:** If this is the first query you have created, click All Events.

2. Click Query > Event Type > Log In/Out.

**Result:** The Query: Log In/Out Event dialog box is displayed.

3. Select the settings to apply to your query. Information on the individual parameters available is given below.

4. Click OK.

**Result:** The query will be added to the tree pane. Click the query to see the filtered results.



## Query: Log In/Out Event dialog box:

## Query: Log In/Out Event dialog box options:

Name	Description
Outcome	
Log in ALLOWED	Searches for allowed logins.
Log in DENIED	Searches for login attempts that were denied.
Log Out	Searches for logouts.
User Filter	
Only this user:	Searches for logins and logouts by the user specified in the adjacent text box.
Allow partial match	User names that contain the text specified in the adjacent box will be included in the results of the query. If this option is not selected, only user names that are exactly the same as the specified text will be included. <b>Tip.</b> This option can be used to search for a number of users with similar user names.

## Query: Log In/Out Event dialog box options: (Continued)

Name	Description
Machine Filter	
Only this machine:	Searches for logins and logouts originating on the machine specified in the adjacent text box.
Allow partial match	Machine names that contain the text specified in the adjacent box will be included in the results of the query. If this option is not selected, only machine names that are exactly the same as the specified text will be included. <b>Tip.</b> This option can be used to search for a number of machines with similar names.

## Security event

A Security event query enables you to filter the audit log to show only security-related events.

### To create a security event query:

1. In the tree pane, click the list you want to filter.  
**Tip:** If this is the first query you have created, click All Events.
2. Click Query > Event Type > Security.  
**Result:** The Query: Security Event dialog box is displayed.
3. Select the settings to apply to your query. Information on the individual parameters available is given below.
4. Click OK.  
**Result:** The query will be added to the tree pane. Click the query to see the filtered results.

## Query: Security Event dialog box:

The dialog box titled "Query: Security Event" features a blue title bar with a close button. It is organized into three main sections:

- Severity:** Contains two checked checkboxes: "Show LOW Severity Actions (green)" and "Show HIGH Severity Actions (red)".
- User Filter:** Contains a checked checkbox "Only This User:" followed by an empty text input box, and an unchecked checkbox "Allow Partial Match".
- Machine Filter:** Contains a checked checkbox "Only This Machine:" followed by an empty text input box, and an unchecked checkbox "Allow Partial Match".

On the right side of the dialog, there are "OK" and "Cancel" buttons.

## Query: Security Event dialog box options:

Name	Description
Severity	
Show LOW severity actions (green)	Searches for low severity security events – events that indicate changes occurring during normal operation, such a setting adjustment in Security Manager.
Show HIGH severity actions (red)	Searches for high severity security events – events that indicate critical items such as tamper detection or the deletion of event log data.
User Filter	
Only this user:	Searches for security events generated by the user specified in the adjacent text box.

## Query: Security Event dialog box options: (Continued)

Name	Description
Allow partial match	User names that contain the text specified in the adjacent box will be included in the results of the query. If this option is not selected, only user names that are exactly the same as the specified text will be included. <b>Tip.</b> This option can be used to search for a number of users with similar user names.
Machine Filter	
Only this machine:	Searches for security events originating on the machine specified in the adjacent text box.
Allow partial match	Machine names that contain the text specified in the adjacent box will be included in the results of the query. If this option is not selected, only machine names that are exactly the same as the specified text will be included. <b>Tip.</b> This option can be used to search for a number of machines with similar names.

### Audit Path query

An audit path query enables you to filter the audit log to show only events relating to a specified path on disk and/or limited to certain types of event.

#### To create an audit path query:

1. In the tree pane, click the list you want to filter.

**Tip:** If this is the first query you have created, click All Events.

2. Click Query > Event Type > Audit.

**Result:** The Query: Audit Path dialog box is displayed.

3. Select the settings to apply to your query. Information on the individual parameters available is given below.

4. Click OK.

**Result:** The query will be added to the tree pane. Click the query to see the filtered results.

## Query: Audit Path dialog box:

## Query: Audit Path dialog box options:

Name	Description
Partial Path	
Filter Path	Searches for events that relate to a file on this path. This is a partial match search, so any event relating to a file whose path contains the text entered in this box will be included in the results. <b>Example.</b> If the Filter Path was set to “default”, events relating “c:\myfiles\defaults\projects...” and “c:\masslynx\quantify.pro\default.exp” would both be returned.
Except	Only events that relate to files whose path does not contain the Filter Path will be included.
User	
Filter User	Searches for events generated by the user specified in the adjacent text box.

## Query: Audit Path dialog box options: (Continued)

Name	Description
Partial Match	User names that contain the text specified in the adjacent box will be included in the results of the query. If this option is not selected, only user names that are exactly the same as the specified text will be included. <b>Tip.</b> This option can be used to search for a number of users with similar user names, or (in combination with the Except option) to exclude users with similar user names.
Except	Events for all users except the user specified in the adjacent box will be included.
Machine	
Filter Machine	Searches for events generated by the machine specified in the adjacent text box.
Partial Match	Machine names that contain the text specified in the adjacent box will be included in the results of the query. If this option is not selected, only machine names that are exactly the same as the specified text will be included. <b>Tip.</b> This option can be used to search for a number of machines with similar names, or (in combination with the Except option) to exclude machines with similar names.
Except	Events for all machines except the machine specified in the adjacent box will be included.
Date and Time	
Filter before	The query will only include events that occurred before the time and date specified.
Filter after	The query will only include events that occurred after the time and date specified.
Ignore filter	Disables the date and time filter.

## Query: Audit Path dialog box options: (Continued)

Name	Description
Auditable Operation Type	
Filter	Only events of the types selected in the adjacent list will be included in the results. Event types indicated as legacy can only be created by MassLynx versions prior to 4.1.

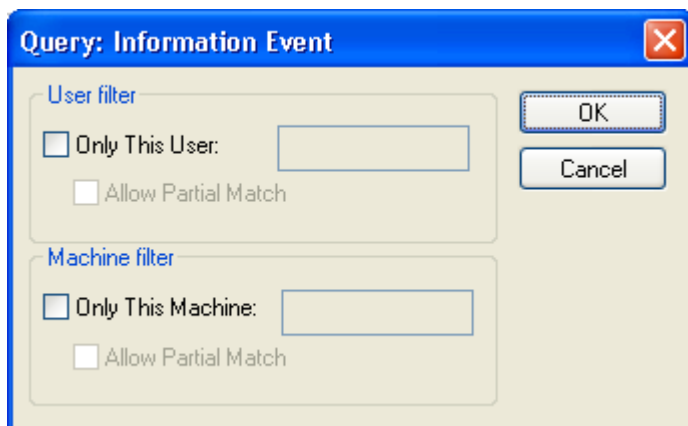
### Information event

An Information event query enables you to filter the audit log to show only entries that give information not falling into other categories.

#### To create an information event query:

1. In the tree pane, click the list you want to filter.  
**Tip.** If this is the first query you have created, click All Events.
2. Click Query > Event Type > Information.  
**Result.** The Query: Information Event dialog box is displayed.
3. Select the settings to apply to your query. Information on the individual parameters available is given below.  
**Tip.** To create an information event query that contains the events for all users and machines, do not select any settings.
4. Click OK.  
**Result.** The query will be added to the tree pane. Click the query to see the filtered results.

## Query: Information Event dialog box:



## Query: Information Event dialog box:

Name	Description
User filter	
Only this user:	Searches for information events generated by the user specified in the adjacent text box.
Allow partial match	User names that contain the text specified in the adjacent box will be included in the results of the query. If this option is not selected, only user names that are exactly the same as the specified text will be included. <b>Tip.</b> This option can be used to search for a number of users with similar user names.
Machine filter	
Only this machine:	Searches for information events originating on the machine specified in the adjacent text box.
Allow partial match	Machine names that contain the text specified in the adjacent box will be included in the results of the query. If this option is not selected, only machine names that are exactly the same as the specified text will be included. <b>Tip.</b> This option can be used to search for a number of machines with similar names.



## Verification event

A Verification event query enables you to filter the audit log to show only events that required dual authorization, whether they were successful or unsuccessful.

### To create a verification event query:

1. In the tree pane, click the list you want to filter.

**Tip:** If this is the first query you have created, click All Events.

2. Click Query > Event Type > Verification.

**Result:** The Query: Verification Event dialog box is displayed.

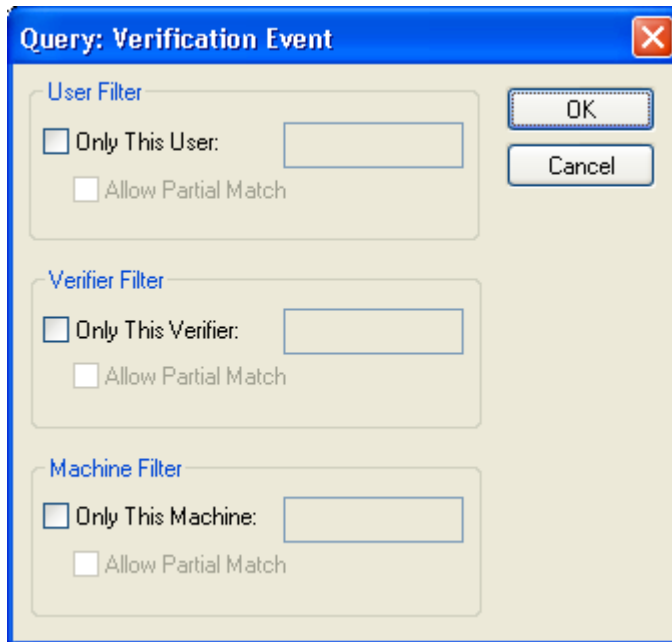
3. Select the settings to apply to your query. Information on the individual parameters available is given below.

**Tip:** To create a verification event query that contains the events for all users and machines, do not select any settings.

4. Click OK.

**Result:** The query will be added to the tree pane. Click the query to see the filtered results.

## Query: Verification Event dialog box:



## Query: Verification Event dialog box:

Name	Description
User Filter	
Only this user:	Searches for verification events generated by the user specified in the adjacent text box.
Allow partial match	User names that contain the text specified in the adjacent box will be included in the results of the query. If this option is not selected, only user names that are exactly the same as the specified text will be included. <b>Tip.</b> This option can be used to search for a number of users with similar user names.
Verifier Filter	
Only this verifier:	Searches for verification events where the second user involved (the verifier) had the user name specified in the adjacent text box.

### Query: Verification Event dialog box: (Continued)

Name	Description
Allow partial match	User names that contain the text specified in the adjacent box will be included in the results of the query. If this option is not selected, only user names that are exactly the same as the specified text will be included.
Machine Filter	
Only this machine:	Searches for information events originating on the machine specified in the adjacent text box.
Allow partial match	Machine names that contain the text specified in the adjacent box will be included in the results of the query. If this option is not selected, only machine names that are exactly the same as the specified text will be included. <b>Tip.</b> This option can be used to search for a number of machines with similar names.

## Backing up, exporting, and clearing the LogLynx log

---

You will want to perform some administrative tasks on the audit log, to ensure that nothing is lost if hardware errors occur on the machines running the software. You may also want to archive some events, or to remove events altogether.

### Backing up the LogLynx log

**Recommendation:** You are strongly advised to make regular backups of the complete audit log in case of disaster.

The audit log can be difficult to back up using normal archiving utilities due to its large size – it may contain gigabytes of data – and the fact that it is a “live” file.

MassLynx is supplied with a utility called `sectiontool` which you can use to divide the audit log into manageable sections.

**Restriction:** `Sectiontool` can only be run on the machine on which the log is actually stored. If the log is stored on a remote machine, `sectiontool` must be run on that machine.

#### To divide the audit log into sections:

1. Open a command prompt.
2. Type `sectiontool -d [UNC path to the directory to write the sections to]`

**Example:** If the machine is called `logserverPC`, you could type

```
sectiontool -d \\logserverPC\c$\log\section\
```

The sections would be written to the `c:\log\section\` directory.

The sections will be written with numbered filenames, beginning at 00001. If you type text after the final slash of UNC path, that text will be used as a base for the filenames.

**Example:** If the machine is called `logserverPC`, you could type

```
sectiontool -d \\logserverPC\c$\log\section\log
```

Output files, named `log00001`, `log00002`, and so on, would be written to the `c:\log\section\` directory.

The sectiontool utility has a number of additional features. For information on the options available and the syntax to use, open a command prompt and type:

```
sectiontool -h
```

### To join the event log sections:

As sectiontool divides the audit log into binary chunks, all that is required is that the binary chunks are combined together in the correct order.

**Requirement:** Ensure that binary mode is used when the chunks are combined.

The “copy” utility provided with Windows, and accessible from the command prompt, is one method that might be used to join the sections.

For information on how to use the copy command, open a command prompt and type:

```
copy /?
```

**Tip:** If you have a large number of sections, it may be easier to combine them if they share a common base to their filename.

## Exporting log file entries

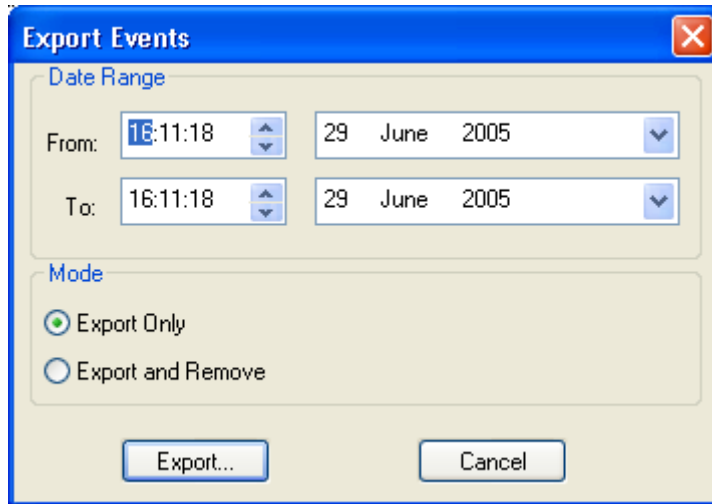
You can archive log file entries by exporting them to a file. The entries can be merged in to the log file again at a later date (see [Importing audit logs on page 10-6](#)).

A permanent entry in the audit log (which cannot be removed by subsequently exporting or clearing the audit log) will be generated by an export or import event. Therefore, it will always be clear that an export/import has taken place, even if the same events are merged back into the log at a later date.

## To archive events from the event log:

1. Click File > Export.

**Result:** The Export Events dialog box is displayed:



2. Enter the time and date range of the events you want to archive.
3. Select one of:
  - Export Only, to archive the events and leave them in the audit log.
  - Export and Remove, to archive the events and remove them from the audit log after archiving.

**Caution:** Before removing events from the audit log, you should ensure that you have appropriate policies to store and protect the event archive files produced. Failure to do this may result in the permanent loss of audit log information.

4. Click Export.
5. Read the Event Export message, then click Yes if you want to continue.
6. Click OK.

**Result:** The Save As dialog box is displayed.

7. Enter a name for the file to export the entries to.
8. Click Save.

## Clearing the LogLynx log

**Caution:** You should only clear entries from the LogLynx log if you are confident that they have been successfully archived, or if you are certain that the information will not be required in the future.

You can clear all the events from the audit log, except for audit events that indicate actions on the audit log itself.

A permanent entry in the audit log (which cannot be removed by subsequently exporting or clearing the audit log) will be generated by a clearing event.

### To clear the log:

1. Click File > Delete All.
2. Read the warning message, then click Yes if you want to continue.
3. Click OK.

## Printing the LogLynx log

---

You can print out audit log information if you need a hard copy.

You can print:

- All of the audit log
- Audit log entries resulting from a query
- Details of a single event

**Tip:** You may wish to examine the Print Setup options to make sure that your print-outs are as good as possible. To do this, click File > Print Setup. Selecting Landscape rather than Portrait orientation can often help improve clarity.

### To print all of the audit log:

1. In the tree pane on the left of the screen, click All Events.
2. Click File > Print.
3. Check the settings in the Print dialog box.
4. Click OK.

**Tip:** The audit log may contain many thousands, or even millions, of events. Only print out the whole audit log if you are sure that it is what you need – often it will be more useful to create a query to filter your results first (see [Filtering the LogLynx log on page 10-7](#)).

### To print audit log entries resulting from a query:

1. In the tree pane on the left of the screen, click the appropriate query.
2. Click File > Print.
3. Check the settings in the Print dialog box.
4. Click OK.

### To print the details of a single event:

1. In the events pane on the right of the screen, double-click the appropriate event.
2. In the Event Details window, click File > Print.



3. Check the settings in the Print dialog box.
4. Click OK.



# 11 Using MassLynx in Regulated Environments

MassLynx Security has been designed with regulatory requirements in mind, and provides many features that help you operate successfully in regulated environments.

This chapter begins with some important recommendations, then continues with a number of sections: each one addresses a common regulatory requirement and provides information on the MassLynx features available to help you fulfil it.

**Caution:** MassLynx cannot satisfy regulatory requirements by itself: it is only a component of the processes and procedures you need to have in place. You must consider carefully what the regulations require of you, and configure and operate MassLynx in a manner compatible with your understanding.

## Contents:

---

Topic	
<a href="#">Recommendations</a>	11-2
<a href="#">Common regulatory requirements</a>	11-3

---

## Recommendations

---

- You should evaluate and test your review and disaster recovery procedures at an early stage, and at regular intervals afterwards. Failure to do so could result in irrevocable loss of data or audit information.
- When archived data and log information is being audited, it is advisable to use a forensic PC – a dedicated machine that is separate from the PC used to operate the instrument or process data.

Using a forensic PC avoids events that are caused by the audit process and are unrelated to your work (such as the importing and exporting of log entries, for example) being generated in your live audit log.

If the data and log information being audited is still actively being used in your MassLynx system, it will not be possible to use a forensic PC.

## Common regulatory requirements

---

The following table lists some common regulatory requirements. Refer to the pages specified to learn more.

### Common regulatory requirements:

Requirement	See
Discern invalid or altered records	page 11-4
View, copy, and print electronic records	page 11-5
Protect and back up records	page 11-7
Limit system access to authorized individuals	page 11-9
Generate time-stamped audit trails	page 11-10
Allow only specified individuals to perform actions	page 11-11
Assure the validity of source data	page 11-12
Hold individuals accountable for actions performed under their electronic signature	page 11-13
Include the name, date, time, and meaning with electronic signatures	page 11-14
Ensure that electronic signatures are associated with the correct record	page 11-15
Ensure electronic signatures are unique to one individual	page 11-16
Confirm that at least two distinct identification components exist for an electronic signature	page 11-17
Force all signature components to be used whenever a signature is performed	page 11-18
Maintain the uniqueness of the identification, and ensure periodic revision of passwords	page 11-19
Notify management of any attempted unauthorized use of the system	page 11-20

## Discern invalid or altered records

---

MassLynx is designed to ensure that the data produced is accurate and reliable, and is tested thoroughly to confirm that this is the case.

If you install MassLynx with Full Security, checksums are applied to:

- All the data files acquired.
- All the metadata files (that is, files that control how data is acquired, such as inlet or MS methods).
- Data processed using QuanLynx or TargetLynx.

If records are altered or renamed, the checksums ensure that MassLynx detects the unauthorized changes. Users will not be permitted to open the invalid or altered records, appropriate warnings will be displayed, and information will be written to the audit log.

Only authorized alterations that take place within MassLynx result in valid records.

### See also:

- [Introduction on page 1-1](#)
- [MassLynx Checksums on page B-1](#)
- [Viewing, Exporting, and Printing Audit Logs on page 10-1](#)

## View, copy, and print electronic records

---

### Viewing, copying, and printing MassLynx files

Data acquired can be viewed in MassLynx – most commonly by using the Chromatogram and Spectrum windows – from where it can also be printed if necessary. The signatures or reasons associated with data can be displayed within the Chromatogram and Spectrum windows by adding the information to the display header. For more information, refer to the MassLynx online Help.

Results from QuanLynx and TargetLynx can be viewed in the browsers within those application managers. In both cases it is possible to print the data, or to export it in LIMS or XML format.

If electronic distribution is required, data can be printed to third-party print drivers that produce files in electronic formats, such as PDF.

Metadata (such as inlet methods, tune files, and MS methods) can also be viewed and printed by opening the appropriate window from the main MassLynx window.

MassLynx checksums (which secure files when Full Security is being used) allow files to be copied to other locations so long as neither the filename nor the contents of the file are altered.

#### See also:

- MassLynx online Help
- [MassLynx Checksums on page B-1](#)

### Viewing, copying, and printing audit log entries

Most operations are recorded in the main audit log, accessed through a dedicated viewer called LogLynx. Internal Modifications – operations which do not result in a file being saved to disk – performed in QuanLynx or TargetLynx are stored in their own audit logs, accessed through the QuanLynx and TargetLynx viewers.

Individual events, the whole log, or part of the log, can be printed from LogLynx. Log files can be copied to other locations so long as they are not changed.

**See also:**

- [Viewing, Exporting, and Printing Audit Logs on page 10-1](#)
- [Generate time-stamped audit trails on page 11-10](#)
- [QuanLynx online Help](#)
- [TargetLynx online Help](#)



## Protect and back up records

---

It is important that your data, metadata, and audit log information are regularly backed up. You will need to consider your needs carefully, and implement appropriate procedures.

**Recommendation:** You should evaluate and test your disaster recovery procedures at an early stage, and at regular intervals afterwards. Failure to do so could result in irrevocable loss of data.

### Using BackLynx

MassLynx is supplied with BackLynx – a utility that provides one possible method you may wish to use to backup MassLynx files. BackLynx is specially designed for copying MassLynx files, but you should evaluate whether it fits your needs before deciding to use it.

**See also:** BackLynx online Help

### Copying files using another method

When Full Security is being used, MassLynx checksums ensure that files that have been tampered with cannot be opened, and that they can only be changed within MassLynx. The way in which checksums work, however, means that files can be copied to other locations as long as you make sure that:

- The associated checksum file is also copied.
- Neither the filename nor contents are changed.

**See also:** [MassLynx Checksums on page B-1](#)

### Backing up the audit log

When you are deciding how to back up the audit log, bear in mind both that the file may be extremely large and that it is live (that is, it is held open by MassLynx).

A utility called sectiontool is provided with MassLynx to help break the audit log into smaller pieces without affecting the integrity of the event entries contained in the file. This utility, or a similar alternative, is ideal for regular backups for disaster recovery purposes.

Groups of audit log entries, or the entire log, can be archived to separate files from within the LogLynx interface. These exported audit log entries can then be imported into LogLynx on other PCs for viewing.

**See also:** [Backing up, exporting, and clearing the LogLynx log on page 10-28](#)

## Limit system access to authorized individuals

---

Only users who have valid Operating System accounts and have been designated as MassLynx users by the system administrator are permitted to login to MassLynx.

When a user attempts to login, MassLynx authenticates the details supplied with the Operating System, thereby ensuring that the user has a currently valid user account on the domain indicated and that their password is correct.

Valid Operating System users who have not had a MassLynx user account created for them in Security Manager will not be able to access the system, regardless of their Operating System privileges.

**See also:** [Understanding MassLynx users on page 5-2](#)

## Generate time-stamped audit trails

---

When MassLynx is installed with Full Security, all events – including logins, logouts, data acquisition, saving and signing files, and accessing parts of the interface – are recorded in the audit log.

The details of each action are recorded, along with the date, the time, the user who performed the action, and the machine the action was performed on. This information can be viewed, printed, and exported using the LogLynx log viewer.

Information on internal modifications in QuanLynx and TargetLynx (which do not result in a file being saved to disk) is recorded in the QuanLynx and TargetLynx audit logs.

In addition to being able to see what was done and when, you can prevent old files from being overwritten by setting appropriate rights for user groups (allowing them to create new files but not to amend existing ones). This ensures that the previous versions of files – tuning parameters, for example – are always available for inspection, and can be compared with newer versions.

### See also:

- [Viewing, Exporting, and Printing Audit Logs on page 10-1](#)
- [QuanLynx online help](#)
- [TargetLynx online help](#)
- [Assigning rights to groups on page 4-7](#)

## Allow only specified individuals to perform actions

---

Only users who have valid Operating System accounts and have been designated as MassLynx users by the system administrator are permitted to login to MassLynx.

Once a user has logged in, the parts of MassLynx that they have access to and the actions they can perform can be closely controlled. This is done through assigning rights to the groups that they are a member of.

### See also:

- [Understanding MassLynx users on page 5-2](#)
- [Understanding MassLynx groups on page 4-2](#)
- [Assigning rights to groups on page 4-7](#)
- [MassLynx Group Rights on page A-1](#)

## Assure the validity of source data

---

Data is acquired into MassLynx directly from the instruments to which it is connected, and over which it has control.

MassLynx communicates with the instruments using a proprietary, binary format – over a dedicated link – helping to provide a high level of confidence in the validity of source data.

## Hold individuals accountable for actions performed under their electronic signature

---

It is the responsibility of your organization to implement appropriate policies to ensure that individuals are accountable for the actions they perform, and procedures to make sure that the policies are adhered to.

MassLynx can assist you by presenting a warning message when a user logs on, reminding them of their responsibilities. The user must OK this message before they can proceed to any part of the MassLynx, LogLynx, or Security Manager interface.

The message can be configured to contain any text you wish, and can be varied from group to group depending on your requirements.

**Recommendation:** Displaying a warning message is highly unlikely, in isolation, to be deemed sufficient to meet regulatory requirements; you should consider carefully the policies and procedures required.

**See also:** [Creating or modifying a group on page 4-4](#)

## Include the name, date, time, and meaning with electronic signatures

---

It is possible to configure a policy so that an electronic signature associated can be prompted for, or required, for a range of different actions that the user might perform.

When an electronic signature or reason (explaining why the change has been made) is entered by the user, the following details are recorded:

- Full name of the user
- Domain and user name of the user
- Date of signature or reason
- Time of signature or reason
- Action performed (the meaning)
- Reason for the change (if appropriate)

If the action has resulted in a file being saved to disk, these details are stored with the file. The same information (with the exception of the full name) is also recorded in the audit log.

If a user has appropriate permissions, a file can be re-signed and a new reason specified. The original information will always be retained in the audit log.

### See also:

- [Configuring Signature and Reason Policies on page 8-1](#)
- [Viewing file signatures and reasons on page 8-12](#)
- [What are the audit logs? on page 10-2](#)



## Ensure that electronic signatures are associated with the correct record

---

If configured, MassLynx automatically prompts for an electronic signature at the time that an action is performed on a record, thereby forcing a signature for the creation or modification of each record.

The signature is stored with the relevant record, and cannot be transferred to any other record. Any modification of the record will result in the signature being removed.

The signature is also recorded in the audit log. Subsequent signatures on the same file do not obscure previous signatures in the log, providing a clear audit trail that identifies the files that have been signed along with the identity of the signatory and the time and date of the signature.

### See also:

- [Configuring Signature and Reason Policies on page 8-1](#)
- [Entering signatures and reasons on page 8-11](#)
- [Viewing file signatures and reasons on page 8-12](#)
- [What are the audit logs? on page 10-2](#)

## **Ensure electronic signatures are unique to one individual**

When electronic signatures are configured for an action, MassLynx prompts the user for a signature when they perform the action. In order to sign the action the user must, as a minimum, provide their password in order to confirm their identity.

MassLynx can also be configured to require the user to enter their user name, the domain on which their user name is valid, and their password every time they are prompted for a signature.

Whichever method is used, if you are to be certain that each signature is unique to a single individual, your organization will need appropriate policies to ensure that only one individual can use each Operating System account which has access to MassLynx.

### **See also:**

- [Configuring Signature and Reason Policies on page 8-1](#)
- [Entering signatures and reasons on page 8-11](#)

## Confirm that at least two distinct identification components exist for an electronic signature

---

When an electronic signature is made in MassLynx, three identification components are required:

- User name
- Domain on which the user name is valid
- Password

This information is authenticated with the Operating System every time that a signature is attempted.

Depending on your MassLynx configuration, some of this information may be automatically filled in for the user. If you not want this to happen, MassLynx must be configured to force all the signature components to be entered on every occasion.

### See also:

- [Configuring Signature and Reason Policies on page 8-1](#)
- [Entering signatures and reasons on page 8-11](#)
- [Force all signature components to be used whenever a signature is performed on page 11-18](#)

## Force all signature components to be used whenever a signature is performed

---

MassLynx can be configured so that the user name and domain last used for a signature are automatically completed when a user attempts a signature, requiring them only to enter their password.

Alternatively, all the signature components (user name, domain, and password) can be cleared every time the user is prompted for a signature, forcing them to enter all the information on every occasion.

**Requirement:** You will need to set up appropriate Signature and Reason policies before any users will be prompted to perform signatures.

### See also:

- [Configuring Signature and Reason Policies on page 8-1](#)
- [Forcing users to enter full signature information on page 8-4](#)
- [Entering signatures and reasons on page 8-11](#)

## Maintain the uniqueness of the identification, and ensure periodic revision of passwords

---

Your organization will need to put appropriate policies in place to ensure that user names and passwords remain unique to one individual, and to ensure that revisions are made as required.

MassLynx simplifies the process for you, however, by authenticating using Operating System user names and passwords. By doing this, MassLynx authentication automatically benefits from policies put in place to ensure the uniqueness of Operating System user accounts and the periodic revision of Operating System passwords.

**See also:** [Understanding MassLynx users on page 5-2](#)

## Notify management of any attempted unauthorized use of the system

---

When MassLynx is installed with Full Security all events, including attempts to access restricted areas of the system, login with disabled user accounts, or open invalid files, are recorded in MassLynx's audit log.

The log – which can be viewed using LogLynx – can be stored either on the MassLynx PC or on a remote machine, and can be accessed by any user with appropriate permissions. Events where access was denied are highlighted, and queries can be run that restrict the display to only these events.

In addition, MassLynx can be configured to send messages to a remote machine (that of an authorized manager, for example) if any serious security problems – such as file tampering or unauthorized attempts to log on – are detected. Whether messages are sent, and where to, depends on your tamper detection and audit policy settings.

### See also:

- [Tamper detection on page 7-7](#)
- [Audit policy on page 7-8](#)
- [What are the audit logs? on page 10-2](#)

# A MassLynx Group Rights

This appendix contains all the rights that can be allocated to MassLynx groups, and descriptions of what these rights control.

**Contents:**

<b>Topic</b>	<b>Page</b>
<a href="#">Table of rights</a>	<a href="#">A-2</a>

## Table of rights

---

The following table lists the rights that can be assigned to groups, in the same order as they appear in Security Manager.

**Tip:** It is often important, especially in regulated environments, that when any new data or support files – such as method files, tuning files, calibration files and so on (collectively known as ‘metadata’) – are created, all the old information is retained rather than being overwritten.

To ensure that this is the case, grant rights to create new files, but not to alter or overwrite files.

### MassLynx rights:

Right	Allows the user to
ACE Inlet Editor – Enter editor	Enter the Acquisition Control Editor (ACE) inlet control and method editor window.
ACE Inlet Editor – Create new file on disk	Create new ACE inlet method files.
ACE Inlet Editor – Alter existing file on disk	Overwrite existing ACE inlet method files.
ACE Inlet Editor – Allow instrument configuration	Access the Tools > Configuration settings in the inlet editor window.
Acquisition – Start from tune page	Acquire data from the Tune window.
Acquisition – Start from sample list	Start data acquisitions from the Sample List within the main MassLynx window.
Acquisition – Start calibration acquisitions	Start the calibration process to create new calibration acquisitions from the tune calibration window.
Acquisition – Overwrite raw data	Acquire raw data to a filename which already exists.
Acquisition – Access the sample queue	Access the MassLynx sample queue.
Acquisition – Access another person’s sample queue items	Access and delete currently scheduled sample batches belonging to another user.



## MassLynx rights: (Continued)

Right	Allows the user to
Acquisition – Allow priority samples	Alter the priority of sample batches.
Administrative – Administer user accounts and groups	Create, modify and delete MassLynx users and groups and assign MassLynx rights to groups. <b>Restriction.</b> This right cannot be assigned to any group except Administrators.
Administrative – Override current MassLynx login	Log on to a locked MassLynx session in place of the current user.
Administrative – Validate import options	Act as second signatory on import operations requiring dual authorization. <b>Restriction.</b> This right cannot be assigned to any group except Administrators.
Administrative – Allow reasons to be added at the point of signing	Add new reasons to the list of available reasons at the point where a reason is requested.
Administrative – Allow entry to the Security Manager	Access Security Manager. <b>Restriction.</b> This right cannot be assigned to any group except Administrators.
BackLynx – Enter BackLynx	Access the BackLynx window.
BackLynx – Overwrite old target	Overwrite destination files which are older than the source files.
BackLynx – Overwrite any target	Overwrite all target files.
BackLynx – Delete source	Delete source files.
BackLynx – Remove task from queue	Delete BackLynx tasks.
BioLynx – Use BioLynx	Access BioLynx features.
ChromaLynx – Use ChromaLynx	Access ChromaLynx features.
File Browser – Delete file	Delete raw data on disk from within MassLynx.

## MassLynx rights: (Continued)

Right	Allows the user to
FractionLynx – Use FractionLynx	Access FractionLynx features.
General – Import legacy projects	Import data or metadata into MassLynx in Full Security mode.
General – Modify fonts and colors	Change the fonts and colors used by MassLynx.
General – Modify sample list format	Change the columns displayed in the sample list within the main MassLynx window.
General – Customize MassLynx system globals	Change MassLynx global settings in the main MassLynx window.
Library – Use Library functions	Access the Library features.
LogLynx – Enter log viewer	Open the LogLynx audit log viewer.
LogLynx – Delete log	Delete sections of the MassLynx event log. After deletion, the log will contain an entry noting when the contents were deleted and by whom.
LogLynx – Import log	Import sections of a MassLynx event log from a file.
LogLynx – Export log	Export sections of the MassLynx event log to a file.
MS Calibration – Enter instrument calibration window	Enter the Calibration window for the mass spectrometer.
MS Calibration – Create new file on disk	Create new MS Calibration files.
MS Calibration – Alter existing file on disk	Overwrite existing MS Calibration files.
MS Calibration – Recalibrate a raw file	Apply a calibration file to a raw data file, in either the Spectrum window or the Calibration window.
MS Method – Enter editor	Enter the MS Method/Experiment Setup window.
MS Method – Create new file on disk	Create new MS acquisition method files.

## MassLynx rights: (Continued)

Right	Allows the user to
MS Method – Alter existing file on disk	Overwrite existing MS acquisition method files.
MarkerLynx – Use MarkerLynx	Access MarkerLynx features.
MetaboLynx – Use MetaboLynx	Access MetaboLynx features.
MicrobeLynx – Use MicrobeLynx	Access MicrobeLynx features.
NeoLynx – Use NeoLynx	Access NeoLynx features.
NeoLynx – Modify test tables	Modify NeoLynx test tables.
NeoLynx – Modify browser schemes	Modify NeoLynx browser schemes.
OpenLynx – Use OpenLynx functions	Use OpenLynx functions.
Post Source Decay – Use PSD MX functions	Access the Post Source Decay option.
ProfileLynx – Use ProfileLynx	Access ProfileLynx features.
ProteinLynx – Use ProteinLynx	Access ProteinLynx features.
Quan Optimize – Use QuanOptimize	Access QuanOptimize features. In Full Security mode, this option will only be available for Non-Regulated groups.
QuanLynx – Enter QuanLynx	Access QuanLynx features.
QuanLynx – Save new calibration curves to disk	Create new quantitation calibration curves.
QuanLynx – Alter existing calibration curves on disk	Manually alter points on quantitation calibration curves.
QuanLynx – Re/Integrate samples	Create integrated peaks.
QuanLynx – Add/Modify/Delete peaks	Add new peaks and modify or delete existing peaks.
QuanLynx – Quantify samples	Apply the quantitation step in processing to form concentrations.
QuanLynx – Use calculated calibration	Calculate a calibration curve from the data and perform the calibration step in processing.

## MassLynx rights: (Continued)

Right	Allows the user to
QuanLynx – Include/Exclude calibration points	Include or exclude points in the calibration curve in QuanLynx or TargetLynx.
QuanLynx – Change individual curve fitting	Change the fit for a calibration curve in QuanLynx or TargetLynx.
QuanLynx – Export LIMS file	Export LIMS-format files.
QuanLynx – Export XML file	Export XML-format files.
QuanLynx – Export current summary	Export the summary information for the currently selected sample or compound.
QuanLynx – Export complete summary	Export complete QuanLynx Summary Reports.
QuanLynx – Export all groups summary	Export the All Groups summary from the QuanLynx Summary Report.
QuanLynx – Print report	Print reports from QuanLynx.
QuanLynx – Modify layout	Save a QuanLynx layout.
QuanLynx – Modify report format	Modify the format of the printed quantitation report.
QuanLynx Dataset – Save new dataset to disk	Create a new QuanLynx or TargetLynx Dataset.
QuanLynx Dataset – Alter existing dataset on disk	Overwrite an existing QuanLynx or TargetLynx Dataset on disk.
QuanLynx Dataset – Accept a dataset	“Accept” a QuanLynx or TargetLynx Dataset.
QuanLynx Dataset – Review a dataset	“Review” a QuanLynx or TargetLynx Dataset.
QuanLynx Dataset – Unaccept a dataset	“Unaccept” a QuanLynx or TargetLynx Dataset.
QuanLynx Method – Enter editor	Enter the QuanLynx method editor window.
QuanLynx Method – Create new file on disk	Create new quantitation method files.

## MassLynx rights: (Continued)

Right	Allows the user to
QuanLynx Method – Alter existing file on disk	Overwrite existing quantitation method files.
QuanLynx Method – Internal alteration	Alter the quantitation method within a QuanLynx dataset (but not save the method to disk).
QuanLynx Method – Internal RT auto adjustment	Automatically alter retention times in the quantitation method in a QuanLynx dataset.
QuanLynx Method – Alter format of editor	Configure which fields are visible in the QuanLynx or TargetLynx quantitation method editor.
SDMS – Configure SDMS options	Set or change the SDMS configuration options.
SDMS – Use Send Tool	Use the facility to send files to SDMS.
SDMS – Allow file removal when using Send Tool	Remove files when they have been sent to SDMS.
SDMS – Use Retrieve Tool	Use the facility to retrieve files from SDMS.
Sample List – Create new file on disk	Create new sample list files.
Sample List – Alter existing file on disk	Overwrite sample list files.
Setup – Modify lab and user info	Adjust the MassLynx lab and user information to be stored with acquired or quantified data.
Shutdown Method – Enter startup/shutdown editor	Enter the startup/shutdown editor window.
Shutdown Method – Create new file on disk	Create new startup/shutdown files.
Shutdown Method – Alter existing file on disk	Overwrite startup/shutdown files.
TargetLynx – Enter TargetLynx	Access TargetLynx features.

## MassLynx rights: (Continued)

Right	Allows the user to
Tools – Enter ChroTool	Access the ChroTool feature in the Chromatogram window.
Tools – Enter DDATool	Access the DDATool feature in the Chromatogram window.
Tools – Enter Strip Datafile	Access the Strip Datafile feature.
Tools – Enter Accurate Mass Measure	Access the All File Accurate Mass Measure (AFAMM) feature.
Tools – Enter Combine Functions	Access the Combine Functions feature.
Tools – Enter Combine All Files	Access the Combine All Files feature.
Tools – Enter Molecular Weight Calculator	Access the Molecular Weight Calculator feature.
Tools – Enter Molecule Viewer	Access the Molecule Viewer feature.
Tune Page – Edit lock masses	Add or alter Lock Mass mass entries. <b>Restriction:</b> This feature is not available for all instruments.
Tune Page – Enter tuning window	Enter the Tune window.
Tune Page – Enable tune page during acquisitions	Access the Tune window while an Tune window acquisition is in progress.
Tune Page – Access engineering settings	Access the engineering pages in Tune window. <b>Restriction:</b> Engineering pages are not available for all instruments.
Tune Page – Create tune file	Create a tune parameter file.
Tune Page – Alter tune file	Overwrite the contents of a tune parameter file.
Tune Page – Enter Autotune	Use the Autotune wizard. <b>Restriction:</b> The Autotune wizard is not available for all instruments.

### MassLynx rights: (Continued)

<b>Right</b>	<b>Allows the user to</b>
Tune Page – Alter Machine Name	Change the instrument name from the Tune window.





# B MassLynx Checksums

This appendix describes how MassLynx checksums work, and how MassLynx files with checksums can be copied.

## Contents:

Topic	Page
<a href="#">Outline of checksum operation</a>	B-2

## Outline of checksum operation

---

In Full Security mode, MassLynx applies checksums to all data and metadata files. This ensures that the files created in MassLynx cannot be modified or renamed except through security-controlled and audit logged actions within MassLynx itself.

The checksum ensures that the following properties of the file have not been altered:

- Filename
- Size
- Contents

It will not be possible to open the file in MassLynx if any of these properties have been changed. A warning can be displayed and an entry will be made in the log file.

In addition, MassLynx can be configured to send messages advising of file tampering to another machine, such as that of a senior manager who wishes to be notified of attempts to breach security.

### Raw data checksum

For raw data, a checksum file called `protected` is created in each raw data directory.

### Other file checksums

For each file, a `.csm` file is created.

**Example:** For a Sample List called `acquisition1.spl` a checksum file called `acquisition1.spl.csm` is created.

### Copying files

MassLynx checksums have been designed so that MassLynx files can easily be copied (for backup purposes, for instance) without becoming invalid. As long as neither the filename nor the file contents are changed, files can be copied to another location – along with their checksums – and successfully opened in MassLynx. Raw data can be copied so long as the whole raw data directory – including the `protected` file – is copied.

# Index

---

## A

- Abnormal program termination [7-4](#)
- Accessing directories [6-2](#)
- Actions requiring signatures or reasons [8-6](#)
- Adding reasons [8-9](#)
- Adding users to groups [4-6](#)
- Administrator user [2-2](#), [7-11](#)
- Administrators group [4-2](#), [5-2](#)
- Alert on file tamper detect [7-7](#)
- Alerts
  - remote [7-8](#), [7-10](#), [11-20](#)
- Analysts group [4-2](#)
- Application managers
  - support for [1-2](#)
- Applying security settings [9-2](#)
- Assigning rights to groups [4-7](#)
- Audit events [7-9](#)
- Audit log [7-8](#), [8-2](#), [9-3](#), [11-4](#)
  - backing up [10-28](#), [11-7](#)
  - clearing [10-31](#)
  - exporting [10-29](#)
  - filtering [10-7](#)
  - generating [11-10](#)
  - importing [10-6](#)
  - location [2-4](#)
  - overview [10-2](#)
  - printing [10-32](#)
  - reviewing [11-2](#)
  - server [2-3](#)
  - signatures [11-15](#)
  - signatures and reasons [11-14](#)
  - tamper detection [B-1](#)
  - viewing [10-5](#)
- Audit logs
  - exporting [10-6](#)

- Audit path query [10-20](#)
- Audit policy [7-8](#), [11-20](#)
- Audit trail [4-7](#), [11-10](#)
- Auditable events [7-8](#), [7-9](#)
- Authorization
  - dual [7-11](#)
- Automatic logout [7-12](#)

## B

- Backing up [11-2](#), [11-7](#)
- Backing up the audit log [10-28](#)
- BackLynx [11-7](#)
- Basic Security [1-1](#), [8-2](#)
- Built-in groups [4-2](#)

## C

- Changing column order in LogLynx [10-5](#)
- Checksums [2-5](#), [11-4](#), [11-5](#), [11-7](#), [B-1](#)
- Clearing the audit log [10-31](#)
- Columns
  - modifying in LogLynx [10-5](#)
- Copying data [11-5](#), [B-1](#)
- Creating a user [5-3](#)
- Creating groups [4-4](#)
- Critical error protection [7-4](#)

## D

- Data
  - copying [B-1](#)
- Date/Time range query [10-7](#)
- Default settings [2-3](#)
- Deleting
  - event query in LogLynx [10-7](#)
- Deleting a user [5-4](#)
- Deleting groups [4-5](#)
- Deleting reasons [8-9](#)

- Detect file tampering [7-7](#)
- Dialogs
  - Dual Authorization Policy [7-11](#)
  - Export Events [10-30](#)
  - LIMS Export File Settings [7-13](#)
  - MassLynx Login [3-3](#)
  - Query: Event Origin [10-12](#)
- Directories window [6-3](#)
- Directory policies [6-2](#)
  - setting [6-3](#)
- Disabled group [4-2](#), [5-2](#)
- Disabling audit log [7-8](#)
- Disabling security [7-3](#)
- Disaster recovery [11-2](#)
- Dividing event logs into sections [10-28](#)
- Dual authorization [7-11](#), [8-7](#)
- Dual Authorization Policy dialog [7-11](#)

## E

- Editing a user [5-3](#)
- Editing groups [4-4](#)
- Editing reasons [8-9](#)
- Electronic records
  - signature and reason policy [8-3](#)
- Electronic signatures [11-14](#), [11-15](#),  
[11-16](#)
- Enabling
  - audit log [7-8](#)
  - remote alerts [7-10](#)
  - security [7-3](#)
- Entering signatures and reasons [8-11](#)
- Event archive file [10-29](#)
- Event logging
  - setting up [7-9](#)
  - turning on and off [7-9](#)
- Event logs
  - dividing into sections [10-28](#)
- Event Origin query [10-11](#)
- Event query

- deleting [10-7](#)
- Event query in LogLynx [10-7](#)
- Event type query [10-13](#)
- Event types
  - Audit [7-9](#)
  - Logoff [7-9](#)
  - Logon [7-9](#)
  - Object Access [7-9](#)
  - Policy Changes [7-9](#)
  - Security [7-9](#)
  - selecting [7-9](#)
- Events
  - removing from the audit log [10-31](#)
  - viewing log of [10-5](#)
- Example groups [4-2](#)
- Export Events dialog [10-30](#)
- Exporting
  - audit logs [10-6](#), [10-29](#)
  - data [11-5](#)
  - LIMS policy [7-13](#)
  - security settings [9-4](#)

## F

- File tampering
  - detect [7-7](#)
- Force identification components to be used [11-17](#), [11-18](#)
- Force username entry [7-6](#)
- Forensic PC [11-2](#)
- Forget last username [7-6](#)
- Freeform reasons [8-7](#)
- Full Security [1-1](#), [8-2](#), [11-4](#), [11-7](#),  
[11-10](#), [11-20](#)
  - support for application managers  
[1-2](#)

## G

- Group Rights [A-1](#)
- Group Rights dialog box [4-7](#)
- Groups [4-2](#)

- adding users 4-6
- assigning rights to 4-7
- built-in 4-2
- creating 4-4
- deleting 4-5
- modifying 4-4
- Non-Regulated 4-3
- Regulated 4-3

## I

- Identification components 11-17
  - force use of 7-6
- Import settings 2-3
- Importing audit logs 10-6
- Importing from directories 6-2
- Importing security settings 9-4
- Inactive logout 7-12
- Information event 10-23
- Installing security 2-3
- Intermediate modifications
  - signature and reason policy 8-3
- Invalid records 11-4
- IP addresses, using 7-10

## L

- Laboratory Information Management System 7-13
- LIMS export
  - fixed file location 7-13
- LIMS Export File Settings dialog 7-13
- LIMS policy 7-13
  - naming style 7-13
- Location
  - LIMS 7-13
- Log In/Out event 10-16
- Log location 2-4
- Log server 2-3, 7-10
- Log server, using remote computer as 7-10
- Logging

- remote 7-8, 7-10
- signatures and reasons 8-2
- Logging in to Security Manager 3-3
- LogLynx 10-2
  - backing up the log 10-28
  - clearing the log 10-31
  - exporting 11-7
  - exporting the log 10-29
  - filtering events 10-7
  - importing logs 10-6
  - installing 2-3
  - printing the log 10-32
  - starting 10-3
- Logoff events 7-9
- Logon events 7-9
- Logout
  - automatic 7-12
- Logs
  - backing up 10-28
  - clearing 10-31
  - exporting 10-29
  - filtering 10-7
  - importing 10-6
  - printing 10-32
  - viewing 10-5

## M

- Maintenance group 4-2
- Manage Group dialog box 4-6, 4-7
- Manage User dialog box 4-6, 5-4
- MassLynx
  - checksums 2-5
  - installing 2-3
  - users 5-2
- MassLynx Login dialog 3-3
- MassLynx Security enabled 7-3
- Meanings
  - with signatures 11-14
- Method Developers group 4-2

- Micromass user [2-2](#), [5-2](#)
- Modifyng
  - users [5-3](#)
- Modifying
  - column order in LogLynx [10-5](#)
  - groups [4-4](#)
- N**
- NetBIOS names, using [7-10](#)
- New groups [4-4](#)
- New User dialog bos [5-3](#)
- Non-Regulated groups [4-3](#), [6-2](#)
- O**
- Object access events [7-9](#)
- Opening
  - LogLynx [10-3](#)
  - Security Manager [3-1](#)
- Operating System users [2-2](#), [5-2](#), [11-9](#),  
[11-11](#), [11-17](#), [11-19](#)
- P**
- Passwords [3-3](#)
  - periodic revision [11-19](#)
- Permanent groups [4-2](#)
- Permission check event [10-14](#)
- Policies
  - Audit policy [7-8](#), [11-20](#)
  - Critical error protection [7-4](#)
  - Directory policy [6-3](#)
  - Dual authorization [7-11](#)
  - Forget last username [7-6](#)
  - LIMS policy [7-13](#)
  - MassLynx Security enabled [7-3](#)
  - Printing [9-3](#)
  - Signatures and reasons [8-2](#)
  - signatures and reasons [11-18](#)
  - Tamper detection [7-7](#)
  - Timeout [7-12](#)
  - Use individual INI files [7-5](#)

- Policy change events [7-9](#)
- Printing
  - audit log [10-32](#)
  - data [11-5](#)
  - security settings [9-3](#)
- printing [9-3](#)
- Q**
- QuanLynx [1-2](#)
  - audit logs [10-2](#)
  - LIMS export policy [7-13](#)
  - logs [11-10](#)
  - signatures and reasons [8-3](#)
- Query
  - date/time range [10-7](#)
  - event origin [10-11](#)
  - event type [10-13](#)
- Query dialogs
  - Event Origin [10-12](#)
- Query in LogLynx [10-7](#)
- R**
- Reasons [11-14](#)
  - adding to existing file [8-13](#)
  - allowing freeform reasons [8-7](#)
  - entering [8-11](#)
  - setting the reasons available [8-7](#)
  - viewing [8-12](#)
- Reasons for Change window [8-7](#)
- Reasons policy [8-2](#)
- Regulated environments [1-2](#), [4-7](#), [6-2](#),  
[8-2](#), [9-3](#), [11-1](#), [11-2](#), [11-10](#), [A-1](#)
- Regulated groups [4-3](#), [6-2](#)
- Remote alerts [7-7](#), [7-8](#), [7-10](#), [11-20](#)
- Remote alerts, enabling [7-10](#)
- Remote computer, using as log server  
[7-10](#)
- Remote logging [7-8](#), [7-10](#)
- Removing events from the audit log  
[10-31](#)

- Restricting access to directories 6-2
- Retain settings 2-3, 9-4
- Reviewers group 4-2
- Reviewing information 11-2
- Rights 11-11, A-1
  - assigning to groups 4-7

## S

- Saving
  - security settings 9-2
  - user preferences 7-5
- Security event 10-18
- Security events 7-9
- Security levels 1-1
- Security Manager
  - Logging in 3-3
  - Overview 3-2
  - starting 3-1
  - window description 3-3
- Security Policies
  - Audit policy 7-8, 11-20
  - Critical error protection 7-4
  - Directory policy 6-3
  - Dual authorization 7-11
  - Forget last username 7-6
  - LIMS policy 7-13
  - MassLynx Security enabled 7-3
  - printing 9-3
  - Signatures and reasons 8-2
  - signatures and reasons 11-18
  - Tamper detection 7-7
  - Timeout 7-12
  - Use individual INI files 7-5
- Security rollout file 2-3
- Security rollout files 9-4
- Security settings 2-3
  - exporting 9-4
  - importing 9-4
  - printing 9-3
  - saving 9-2

- Selecting event types to log 7-9
- Settings 9-3
  - exporting 9-4
  - importing 9-4
  - saving 9-2

- Sign Record dialog box 8-11, 8-13

- Signature/Reason Actions dialog box 8-6

- Signatures 11-13, 11-15, 11-16
  - adding to existing file 8-13
  - entering 8-11
  - force all identification components 11-18
  - Identification components 11-17
  - viewing 8-12
- Signatures and reasons 8-2, 11-14
- Starting
  - LogLynx 10-3
  - Security Manager 3-1

## T

- Tamper detection 7-7, 11-4, 11-20, B-1
- TargetLynx 1-2
  - audit logs 10-2
  - LIMS export policy 7-13
  - logs 11-10
  - signatures and reasons 8-3
- Time, logout after 7-12
- Timeout 7-12
- Turning event logging on and off 7-9

## U

- Use individual INI files 7-5
- User preferences
  - retaining 7-5
- Username
  - force entry of 7-6
- Users 5-2, 11-9
  - adding to groups 4-6
  - creating 5-3

- deleting 5-4
- disabling 5-4
- ensure periodic revision of  
    passwords 11-19
- modifying 5-3

## **V**

- Valid records 11-4
- Validity of records
  - ensure 7-7
- Verification event 10-25
- Viewing audit logs 10-5
- Viewing data 11-5

## **W**

- Warning message 11-13
- Windows
  - password 3-3
  - user name 3-3
- Windows users 2-2, 5-2