



# MassHunter Data Acquisition User Management and Audit Trail

## Quick Start Guide

|   |    |
|---|----|
| Getting Started Overview                  | 3  |
| Enable User Management and Audit Trail    | 4  |
| Getting Started for System Administrators | 6  |
| Getting Started for Users                 | 13 |
| Where to Find More Information            | 15 |

This guide describes how to install and use the User Management and Audit Trail feature. See the online help for more information on these features.

## What is User Management and Audit Trail?

21 CFR Part 11 is a result of the efforts of the US Food and Drug Administration (FDA) and members of the pharmaceutical industry to establish a uniform and enforceable standard by which the FDA will consider electronic records equivalent to paper records and electronic signatures equivalent to traditional handwritten signatures. For more information, see <http://www.fda.gov/RegulatoryInformation/Guidances/ucm125067.htm>.

## What is User Management and Audit Trail?

User Management and Audit Trail includes the following features which support 21 CFR Part 11 compliance:

- Hash Signature for data files allow you to check the integrity of files during a compliance audit
- Roles that restrict actions to certain users

### NOTE

User Management and Audit Trail does not cover the full scope of the technical requirements outlined in 21 CFR Part 11. For the complete set of MassHunter data integrity tools, refer to the MassHunter Compliance Mode quick start guides.

---

## Getting Started Overview

### What is User Management and Audit Trail?

# Getting Started Overview

The following diagram shows the steps for administrators and other users to get started with User Management and Audit Trail. This guide and the online Help explain these steps.

#### Administrators

[See page 4.](#)

Enable User Management and Audit Trail

[See page 10.](#)

Assign users to the appropriate groups/roles

[See page 11.](#)

Set up a shared account for Windows logon

[See page 11.](#)

Check integrity of methods and data files

[See page 12.](#)

Check audit trail of methods

#### All Users

[See page 13.](#)

Log in to MassHunter Acquisition software

[See page 6.](#)

Access to some menu items and toolbar buttons may be restricted by your role

[See page 14.](#)

Temporarily lock the application while you are away from the computer

## Enable User Management and Audit Trail

### What is User Management and Audit Trail?

# Enable User Management and Audit Trail

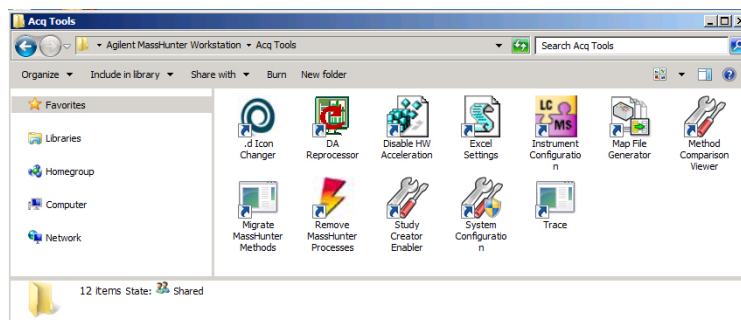
User Management and Audit Trail is included with your MassHunter Data Acquisition software. However, User Management and Audit Trail must be enabled before it will take effect.

#### NOTE

You must have the following minimum version numbers of MassHunter Workstation software components installed for User Management and Audit Trail to work correctly:

- MassHunter Data Acquisition for Triple Quad LC/MS B.08.01 or later
- MassHunter Data Acquisition for TOF/Q-TOF LC/MS B.08.00 or later

- 1 Go to the Agilent MassHunter Program folder under **Acq Tools** and double-click **System Configuration**. If MassHunter Data Acquisition for TOF/Q-TOF is installed, the available tools are different.

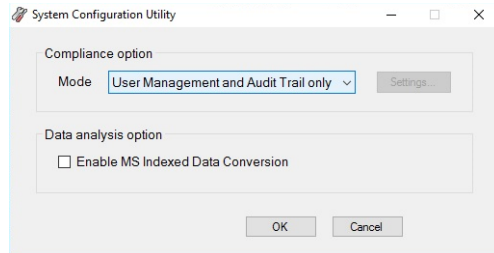


You can also start this program from the **Start** Menu.

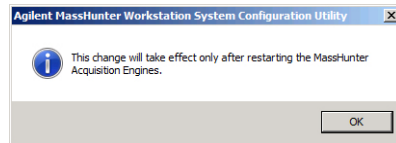
## Enable User Management and Audit Trail


### What is User Management and Audit Trail?

- 2 Select **User Management and Audit Trail only** from the **Mode** drop-down list box. Then, click **OK**.



- 3 Click **OK** in the following message:



- 4 Stop the MassHunter Acquisition Engines:
  - In the system tray, right-click the System Launcher icon and click **Shutdown Engines**.
  - Click **Remove MassHunter Processes** (  ) in the **Acq Tools** folder.

You can disable User Management and Audit Trail mode using this utility. When User Management and Audit Trail is enabled, the default user groups are automatically created. If you disable the User Management and Audit Trail program, these user groups are not removed.

**See also** “Verify that the User Management and Audit Trail roles are present” on page 9.

# Getting Started for System Administrators

The activities in this section can be performed by system administrators only.

The MassHunter Data Acquisition program supports Study Manager and the submission of studies to the Study Queue. These applications work under Audit Trail and require that users specify a user name and password before Study Manager tasks can be executed.

## What are roles?

Roles are groups to which users can be assigned that establish the actions (or privileges) that users can perform in the MassHunter Data Acquisition software. Three roles: **Acq\_Manager**, **Acq\_Chemist**, and **Acq\_Operator**, are automatically installed with the MassHunter Data Acquisition software and are described in more detail below.

### Acq\_Manager Role

Users in the **Acq\_Manager** role will have *all the following privileges in the Acquisition program*:

- Modify\_MS\_Method
- Save\_Method
- Run\_Samples
- Edit\_Well\_Plate\_Types
- MS\_Tune
- Lock\_Worklist\_Setting
- Unlock\_and\_Close\_Application

## Getting Started for System Administrators

### What are roles?

Users in the **Acq\_Manager** role will have *all the following privileges in the Study Manager program*:

- START\_STUDYMANAGER
- CLOSE\_STUDYMANAGER
- SUBMIT\_STUDY
- START\_STUDY\_QUEUE
- STOP\_STUDY\_QUEUE
- LOCK\_ACQ\_CONSOLE
- MOVE\_STUDY\_UP
- MOVE\_STUDY\_DOWN
- EDIT\_STUDY
- DELETE\_STUDY
- RESUBMIT\_STUDY
- UNLOCK\_AND\_CLOSE\_APPLICATION
- CHANGE\_SETTINGS

### Acq\_Chemist Role

Users in the **Acq\_Chemist** role will have the same privileges as the **Acq\_Manager** role listed above in the Acquisition program, *with the exception of*:

- Unlock\_and\_Close\_Application

Users in the **Acq\_Chemist** role will have the same privileges as the **Acq\_Manager** role listed above in the Study Manager program, *with the exception of*:

- LOCK\_ACQ\_CONSOLE
- DELETE\_STUDY
- RESUBMIT\_STUDY
- EDIT\_STUDY\*
- UNLOCK\_AND\_CLOSE\_APPLICATION
- CHANGE\_SETTINGS

\*Only the person who submitted a study or the Acq\_Manager can edit a study.

## Getting Started for System Administrators

### What are roles?

#### Acq\_Operator Role

Users in the **Acq\_Operator** role have *only the privileges listed below in the Acquisition program*:

- Run\_Samples
- Edit\_Well\_Plate\_Types
- Modify\_Device\_Settings

In other words in the Acquisition program, users in the **Acq\_Operator** role *cannot* modify MS methods, save methods, tune the MS, lock worklist setting, edit Study Settings, or unlock and close the application if it has been locked by another user.

Users in the **Acq\_Operator** role have *only the privileges listed below in the Study Manager program*:

- START\_STUDYMANAGER
- START\_STUDY\_QUEUE
- CLOSE\_STUDYMANAGER
- STOP\_STUDY\_QUEUE
- SUBMIT\_STUDY
- EDIT\_STUDY\*

\*Only the person who submitted a study or the Acq\_Manager can edit a study.

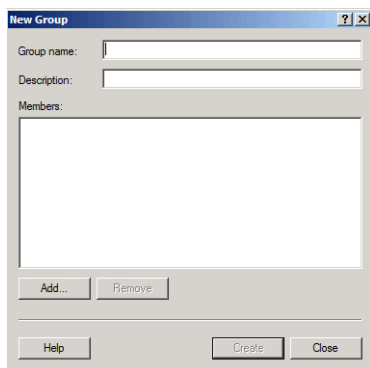
In other words in the Study Manager program, users in the **Acq\_Operator** role *cannot* lock the acquisition console, move a study up or down in the Study Queue, delete a study, resubmit a study unlock and close the application and change settings if it has been locked by another user.



# Verify that the User Management and Audit Trail roles are present

Check to make sure that the user groups required for using User Management and Audit Trail roles have been successfully added to the system during installation as follows:

- 1 Click **Administrative Tools** from the Control Panel.
- 2 Double-click **Computer Management**.
- 3 In the Computer Management window, select **System Tools > Local Users and Groups > Groups** from the navigation pane on the left side of the window.
- 4 Verify that **Acq\_Manager**, **Acq\_Chemist**, and **Acq\_Operator** appear in the list of groups on the right side of the screen. The **Acq\_No\_Privileges** may also be available.
- 5 *If these user groups are not present, then add them as follows:*
  - a Select **New Group** from the Action menu to open the New Group dialog box.



- b Type in a name for the new group (i.e. **Acq\_Manager**, **Acq\_Chemist**, and **Acq\_Operator**).
  - c (optional) Type in a description of the group.
  - d Click **Create**.
  - e Repeat **step a** through **step d** for the other two groups.
- 6 Add users to the User Management and Audit Trail groups as described in **“Assign users to the appropriate user groups/roles”** on page 10.

## Assign users to the appropriate user groups/roles

Do this step to add users to the appropriate user groups, keeping in mind the privileges and restrictions of each role in User Management and Audit Trail described on the previous page.

- 1 Open **Computer Management** as follows:
  - a Select **Administrative Tools** from the Control Panel.
  - b Select **Computer Management**.
- 2 In the Computer Management window, select **Local Users and Groups > Groups** from the navigation pane on the left side of the window.
- 3 Right-click on the group of interest (i.e. **Acq\_Manager**, **Acq\_Chemist**, or **Acq\_Operator**) and select **Properties** from the shortcut menu.
- 4 Click **Add** on the Group Properties dialog.
- 5 On the Select Users dialog box, type in the user names in the text box that you want to add to the group, then click **Check Names**. The complete computer name and user name will be filled in for each user.
- 6 Click **OK** to complete the process.

### Alternate method

If you are adding a single user to a group, it may be easier to access User Accounts as follows:

- 1 Select **User Accounts** from the Control Panel.
- 2 Select the user you want to add to the group on the **Users** tab in the User Accounts window, then click **Properties** to assign that member to one of the User Management and Audit Trail groups.
- 3 If the user you want to add to the group *does not already exist on the local machine*, click **Add** to add them to the local machine and to the desired User Management and Audit Trail group.

## Set up an account for Windows logon

Do this step to create a shared account for logging on to Windows.

The computer used to acquire data from the instrument using MassHunter Workstation Acquisition software is often used by multiple people. For convenience, a common shared account can be used for all users to log on to Windows. Each user must then log in to the MassHunter Workstation Acquisition program separately with their personal password to set up methods and batches, and to acquire data. See “**Log in to User Management and Audit Trail**” on page 13.

- 1 Create a common user account on the local system as follows:
  - a Select **Administrative Tools** from the Control Panel.
  - b Select **Computer Management**.
  - c Create a user account as described in the online help for Windows Computer Management. This common shared account can be completely separate from the user accounts that access the acquisition system.
- 2 Add the new user account to the **Power Users** group as described in “**Assign users to the appropriate user groups/roles**” on page 10.

This common shared account *must* be a member of the local **Power Users** group.

## Check the integrity of data files

User Management and Audit Trail generates hash checksums for acquired data files using a secure hash algorithm. This hash code (checksum) serves as a digital signature for the file. This hash code is generated only if **User Management and Audit Trail only** or **Compliance (with ECM)** mode is enabled. See “**Enable User Management and Audit Trail**” on page 4.

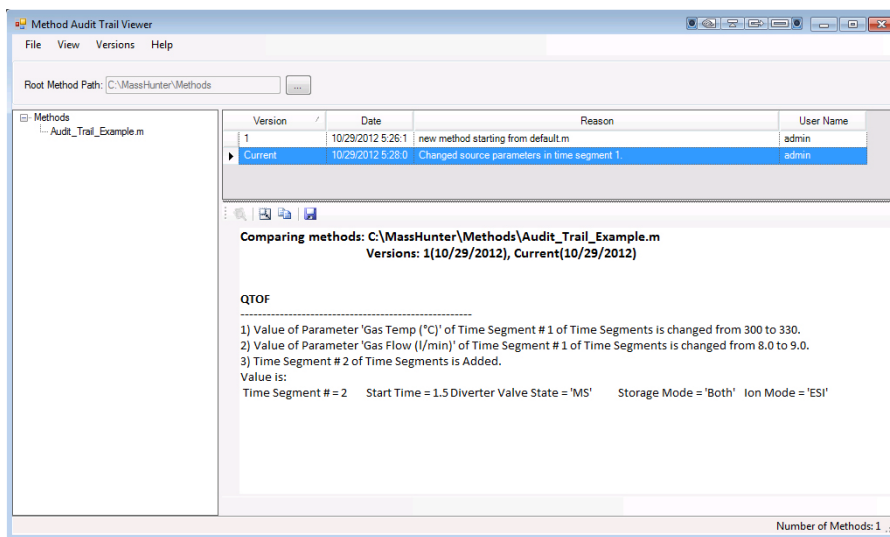
If you have installed the Compliance software for MassHunter Quantitative Analysis software, then you can check whether acquired data (\*.d files) have been tampered with, using the Check Batch Files tool. See the *MassHunter Quantitative Analysis Audit Trail and Compliance Quick Start Guide* for instructions on using the Check Batch Files tool.

## Check the audit trail for methods

User Management and Audit Trail also lets you track the changes that have been made to a method. The users that are allowed to edit a method are asked to give a reason for the change when they save the method. The old version is saved within the method folder.

In the Method Audit Trail Viewer program, you can see a list of all of the different versions of a method, when the method was modified, the reason for the modification and the user that modified the method.

To start the Method Audit Trail Viewer program, click the **Tools > Audit Trail** command in the Data Acquisition program. The online Help contains additional information about this program.



# Getting Started for Users

This section gives some tips for using User Management and Audit Trail.

## Log in to User Management and Audit Trail



- 1 Double-click the Data Acquisition program icon on your desktop:
- 2 If User Management and Audit Trail is enabled, the MassHunter Workstation Logon dialog box opens:

A screenshot of the "MassHunter Workstation Logon" dialog box. It has a blue title bar and a light gray background. There are three input fields: "User Name" (a text box with a dropdown arrow), "Password" (a text box), and "Domain" (a text box with a dropdown arrow). At the bottom, there are two buttons: "OK" and "Cancel".

- 3 Enter your **User Name**, **Password**, and **Domain**. Then, click **OK**.

Notice that if you are assigned to the **Acq\_Operator** role, your access to the following items in the MassHunter Workstation software is restricted. These items will be dimmed on the screen, so they cannot be selected.

### Tuning

- All Tune features, except for **Checktune** on the Autotune tab

### Method editing

- MS device setpoint tabs
- **Method > Save** command and corresponding toolbar button
- **Method > Save As** command

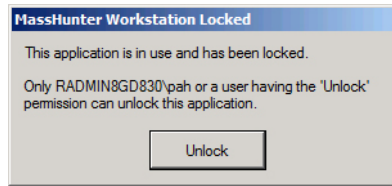
### Other

- **Tools > Well-plate Type Editor**

## Lock your Acquisition session when unattended

When you are going to be away from your computer for awhile, do these steps to lock the Acquisition session. This allows someone else to use the computer but not to interfere with acquisition in progress.

1 Click **Lock Session** from the File menu. The following dialog box is displayed:



2 To unlock your computer on your return, click **Unlock**.

3 When the MassHunter Workstation Unlock dialog box appears, enter your **User Name**, **Password**, and **Domain**, and then click **OK**.

### NOTE

In addition to the user who locked the session, a session can also be unlocked by any user who is assigned to the Acq\_Manager role (see "[Acq\\_Manager Role](#)" on page 6). If the session is unlocked by a user in the Acq\_Manager role, the current session is terminated and a new one can be started.

## Where to Find More Information

Agilent Web Site

# Where to Find More Information

You can access more information about User Management and Audit Trail as follows.

## Agilent Web Site

To view support information for User Management and Audit Trail and other Agilent products, see:

<http://www.agilent.com>

## MassHunter Workstation Online Help

You can access MassHunter Workstation online Help from the **Help** menu in the software or by pressing the **F1** key in the MassHunter Workstation windows or dialog boxes.

## Other Manuals

Your MassHunter Data Acquisition program includes several guides, including the Quick Start Guide and Familiarization Guide. You can open these guides from the Resource Apps for your system.

## In This Book

This guide describes how to install and use the User Management and Audit Trail features. This guide applies to MassHunter Data Acquisition for TOF/Q-TOF LC/MS version B.09.00 and 10.0 or higher, and MassHunter Data Acquisition for TQ LC/MS version B.09.00 and 10.0 or higher until superseded.

[www.agilent.com](http://www.agilent.com)

© Agilent Technologies, Inc. 2018

December 2018



G3335-90226 Revision C

