Technical Note

Ensuring Regulatory Compliance and Data Integrity with MassHunter Software Solutions

Authors

David L Wong, Crystal K Cody, and Robert Ley
Agilent Technologies, Inc.

Abstract

With the latest release of MassHunter Acquisition for LC/TOF and LC/Q-TOF systems, MassHunter Quantitative Analysis, and MassHunter BioConfirm, technical features, technical controls, and data integrity have been implemented to help labs meet the regulatory requirements as defined in 21 CFR Part 11 and EU Annex 11.

Introduction

Paper based approaches to laboratory data integrity are no longer enough to meet today's increased scrutiny of computerized systems. In 1997, the United States Food and Drug Administration introduced Part 11 in Title 21 of the Code of Federal Regulations, commonly known as 21 CFR Part 11. Similar requirements were adopted by its EU analog, EudraLex when Volume 4, Annex 11 was enacted, now commonly known as EU Annex 11. Both 21 CFR Part 11 and EU Annex 11 regulations provide guidance for how to handle electronic records and electronic signatures for regulated pharmaceutical organizations. The intent of these guidelines is to ensure that all appropriate electronic records are attributable, legible, contemporaneous, original, accurate, and maintained with data integrity. This is more commonly known as ALCOA+.

Per the regulations, it is the responsibility of the user and their organization to ensure that the technical controls provided, are used appropriately to achieve compliance-readiness for laboratory data acquisition and processing. In addition to the software's technical controls, the business must also establish procedural controls which are commonly known as Standard Operating Procedures or SOPs to address relevant nontechnical requirements. Governance, for example as an internal audit program, must also be established to assure that system operators follow the SOPs.

When the technical controls are enabled, SOPs have been implemented and are being enforced, this enables a lab to show attribution of work. Attribution of work refers to documenting the ***Who, what, when, where, and why?*** of work performed.

- **Who:** clearly identifies the person responsible for the particular action that creates, modifies, or deletes a record.
- **What:** is the action that took place, including, if applicable, the old value and the new value contained in the record.
- **When:** unambiguously declares the date and time the action took place.
- **Where:** clearly identifies the impacted record.
- **Why:** explains the reason for a change to a regulated record. The reason is often selected from a list of predefined reasons to provide consistency and to enable searching and sorting of entries.

Additionally, within the software itself, automated audit trails independently record user actions thus connecting laboratory staff to the work performed. Audit trail entries enable staff and regulatory inspectors to reconstruct the complete history of an electronic record.

With the introduction of Agilent MassHunter Networked Workstation 11.0 for TOF and Q-TOF LC/MS systems, technical controls have been implemented which enable a system administrator to control access to software features with data integrity achieved, by integrating with Agilent OpenLab Server/ECM XT.

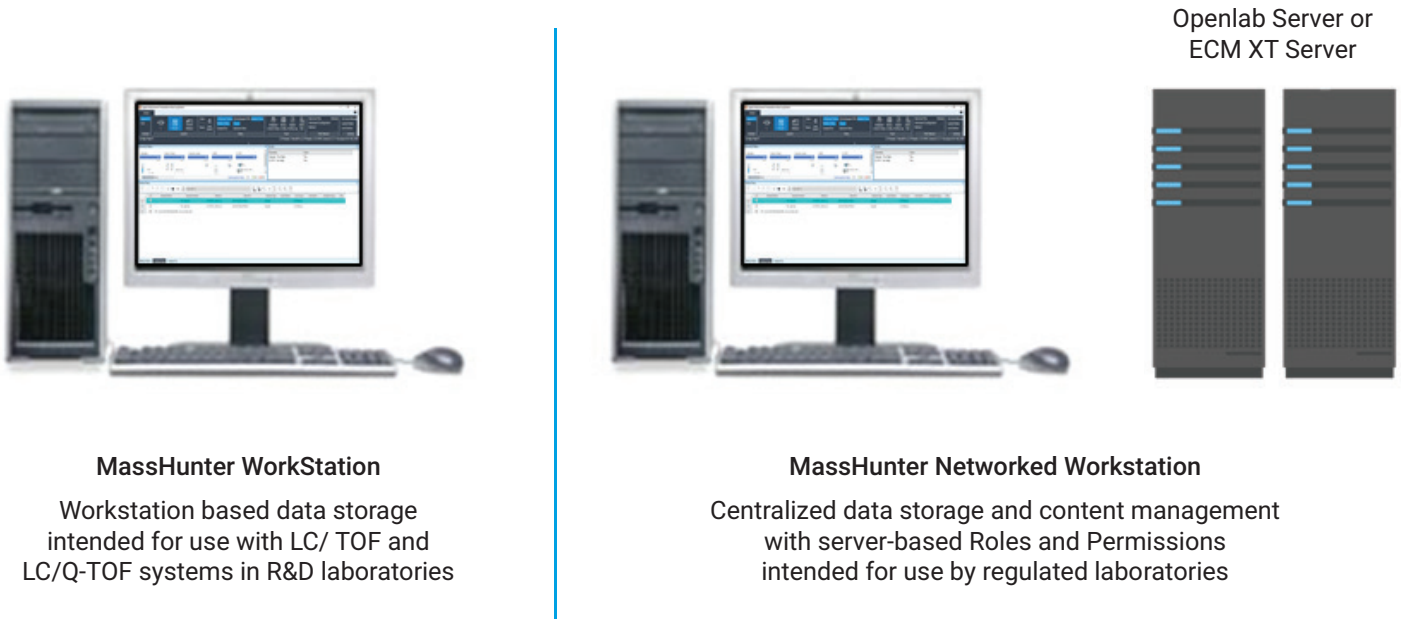

Figure 1. Available Agilent products with the MassHunter 11.0 release.

Highlights on key features

- One location for user and project management for MassHunter Acquisition, Quantitative Analysis, and BioConfirm
- Data integrity with OpenLab Server/ECM XT content management
- Traceability with audit trails and activity logs
- Software feature restrictions with permission control

User Management

User management is one of the key requirements for labs where data integrity is necessary. A user can be defined as an individual who operates instruments where data is being collected. A user can also be an individual who processes the acquired data and generates reports. For the administrator, they need to be able to restrict access to electronic records. Electronic records can be defined as Worklists, Methods, Data Analysis Methods, Reports, Report Templates, and Audit Trails.

In the Control Panel, the administrator of the system can create or add Users. Users are unique in that their Username, Full Name, and Job Title are used by all the applications integrated with Control Panel. Each User is unique and cannot be duplicated or reused.

Roles are a collection of permissions that define what assigned users can or cannot do within MassHunter. At the time of installation, there are five predefined roles that are provided. These roles are Operator, Analyst, Scientist, Lab Manager, and Reviewer. There are no limits on the number of roles that can be created. The lab administrator can use these predefined user roles to create customized roles and assign users to them. If a lab has many users that use the same group of roles, User Groups can be created to manage the permissions and access of those users more easily. Figure 3 shows the descriptions of some of the permissions.

Table 1. Comparison of compliance features in MassHunter 11.0.

	Workstation	Networked Workstation
MH Acquisition 11.0	●	●
MH Quantitation 11.0	●	●
MH BioConfirm 11.0	●	●
Software Licensing	●	●
Audit Trails	●	●
Access Control	● (when activated)	●
Recommended for GxP Labs		●
Revisions/Versioning		●
Server-Based Content Management		●
Single Point Access to Data from Multiple Sources		●

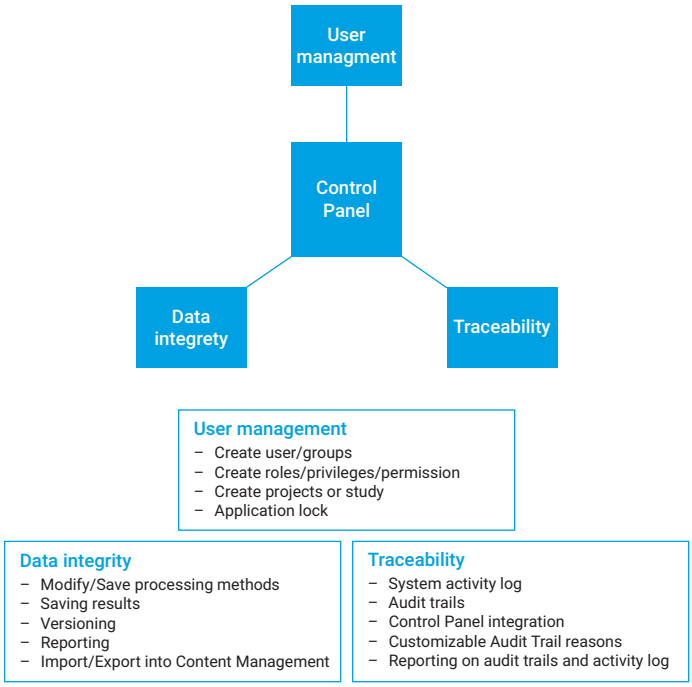

Figure 2. Control Panel features for compliant labs.

Operator	Analyst	Scientist	Lab manager	Reviewer
– Checktune instrument – Apply method – Run samples/worklist – View projects – Generate and print report	– Autotune/checktune – View and edit projects – Apply, load, and save method – Add script – Run samples – Load, save, and run worklist – Generate and print method report	– Manual/autotune instrument – Manage projects – Manage projects/group access – Import data, method, and worklist – Create and save method – Load, save, and run worklist – Generate worklist report – Unlock and close application – Review/export/print audit trail	– Create users/groups – Edit content of project – Create roles/privileges – Assign privileges – Review/export/print all audit trails	– Review projects – Edit content of projects – Load and print method/worklist – Generate worklist report – Review/export/print all audit trails – No data processing or method editing

Figure 3. Comparison of various roles/privileges in data acquisition and data analysis.

Taking a closer look at the Scientist role, any user who is assigned this role can edit or save methods (Figure 4).

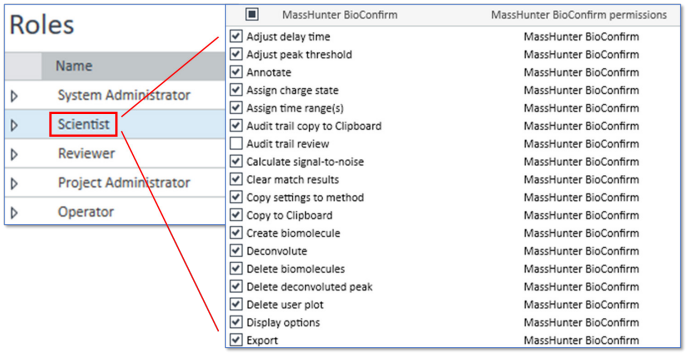

Figure 4. In the Control Panel, the system administrator has full control over all roles with defined privileges for data acquisition and data analysis.

As another example of Roles and Permissions, the role called "MH BioConfirm Operator" is shown in Figure 5A. This role comes with the default permissions as shown in Figure 5B. Any user that is assigned the role of MH BioConfirm Operator can open data files and run methods. However, the MH BioConfirm Operator cannot save method as seen in Figure 5C.

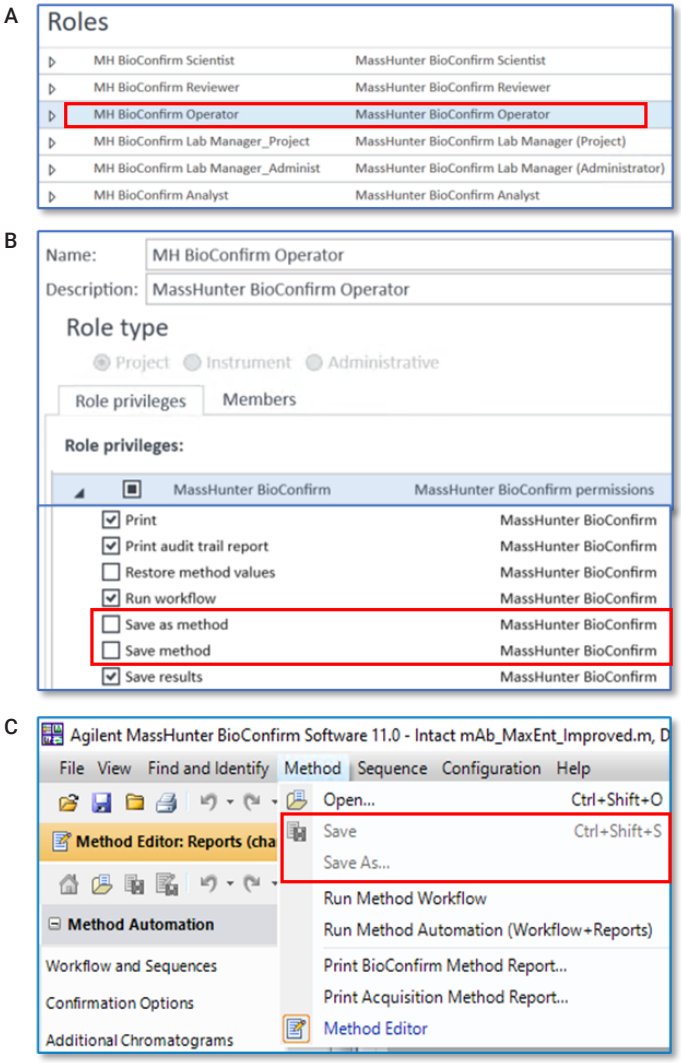

Figure 5. Example of roles and permissions.

Data integrity with OpenLab Server/ECM XT content management

MassHunter 11.0 with OpenLab Server/ECM XT and Control Panel integration supplies several tools for data integrity. These tools include secured and central storage, file encryption, built-in archiving, life cycle management, and file versioning. ECM XT allows a laboratory working in a compliant environment to create a secure area to store and archive data through its lifetime (including its long-term storage). This data integrity solution is very versatile and can fit into any IT (Information Technology) organization, whether large or small. In addition, e-signature functionality built right into ECM XT allows for signing of reports and files in the secure content management system, supplying a fast and accessible solution for signing documentation.

Processing methods, data files, and results are stored in a secure content management system. When a method, data file, or result is needed, it is accessed. For a method, any parameters that were changed are kept as a part of the method and will be used the next time the method is opened for use. For data files, when acquisition or processing is complete, the records are sent to the ECM XT content management server. The records are locked and kept secure until accessed again in the application.

With OpenLab Server and ECM XT, no saved record is ever overwritten. Each time a record is uploaded into content management, any file that changed is versioned. Older versions of records can be accessed in the application. This truly achieves data integrity, as no data can ever be lost.

Occasionally, a user may want to import existing data files or acquisition methods into a project. The **Import Files** tool in Control Panel can be used to import data files, acquisition method files, worklists and report templates from outside content management into the project that the user is working on. For BioConfirm data analysis, data files, processing methods, protein sequences, databases, and report templates can be imported from outside content management into the project with tools present in the application UI (User Interface).

For any records that need to be accessed outside of the controlled environment, export functionality exists in ECM XT. In addition, ECM XT allows for e-signing of documents that are stored on the server. This means if a user generates a report of the results, that report can be signed as being approved and completed.

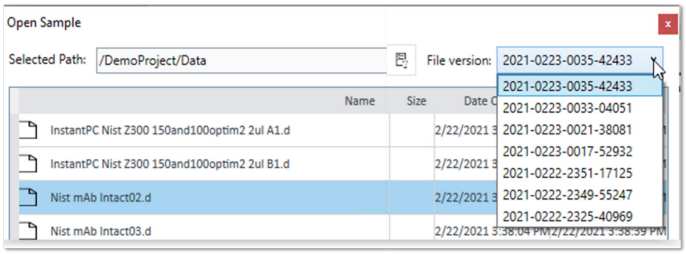

Figure 6. Versioning is enabled in MassHunter data analysis programs.

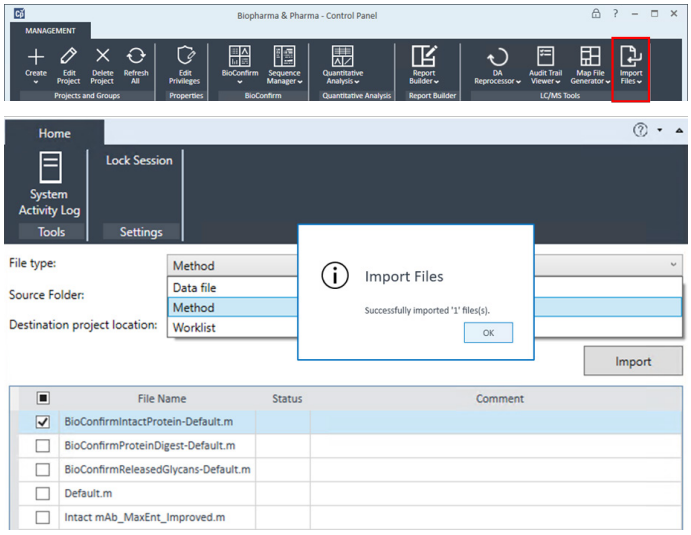

Figure 7. The 'Import Files' feature in Control Panel allows various type of files to be imported/exported into content management. The audit trails are generated automatically to capture such activities meeting regulatory requirements.

Traceability

Another vital component of regulatory compliance is traceability. Traceability is to understand the lifetime of a record. What was done to it, who did it, why it was done, and when it was done are all critical pieces of information necessary to be able to trace the lifetime of a record.

Regulation guidance requires all GMP (Good Manufacturing Practice) electronic records to have "secure, computer-generated, date and time-stamped audit trails." In addition, audit trails should "track actions at the record or system level, such as attempts to access the system or rename or delete a file." To achieve this requirement any change activities must be documented automatically in an audit trail.

With MassHunter 11.0, audit trails are automatically included for all critical files. The audit trail supplies detailed information (5Ws: who, what, when, where, and why) around a particular event. A reviewer of the audit trail can readily obtain a description of the action that triggered an entry, along with all other relevant information (the 5Ws).

There are two types of audit trails in MassHunter: System activity logs, and application record audit trails. The system activity log will track any changes that happen, at an elevated level to the system, such as login/logout actions, opening applications, etc. Application audit trails will track any changes to specific records on the system, such as a change to a method or result file.

Activity logs can be accessed from the Control Panel (Figure 8), and audit trails can be accessed from each application they were created from. Audit trails are created for acquisition and processing methods, worklists, data files, and results. In addition, in BioConfirm an audit trail is created for all entries into the Chemical Data Dictionary and the Sequence Manager, as well as any changes to report templates.

The record specific audit trails can be viewed in a universal audit trail viewer application that provides a consistent user experience across Acquisition, Quantitative Analysis, and BioConfirm. The audit trail viewer allows the user to interrogate the information in the audit trail. It has filtering and searching capabilities to easily be able to find entries of interest.

In addition to being able to view all the audit trail entries for a record, the audit trail viewer has an option to review an audit trail and e-sign the reviewed entries. Having reviewed audit trails is being requested more prominently by regulatory agencies and the Review functionality of the audit trail viewer in MassHunter provides this feature. Any entries that have not been reviewed are a distinct color to make it clear what has been reviewed and what has not.

One of the five pieces of information needed to be tracked in an audit trail is why a user did a particular action. This requires the user to enter some information when they make an entry into the audit trail. Often administrators want to require their users to enter a reason when saving a record, and they want to be able to limit the options a user has for why they are making a change. MassHunter 11.0 has functionality in the Control Panel that allows an administrator to customize this functionality. The administrator can require a reason for change and create some customized prepopulated reasons that the user must choose from. These settings can be customized for each project present on the system.

Finally, all audit trail information can be printed in the form of a report from the Audit Trail Viewer application. The reports will show relevant information about who generated the report and when. In addition, it will show the unreviewed entries in the same distinct color as is seen in the application.

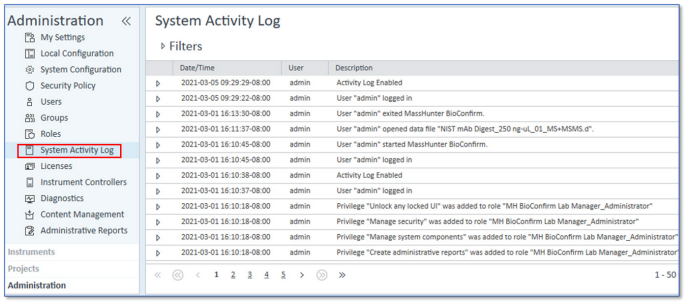

Figure 8. The System Activity Log maintains a complete activity list of all actions that happened to the system.

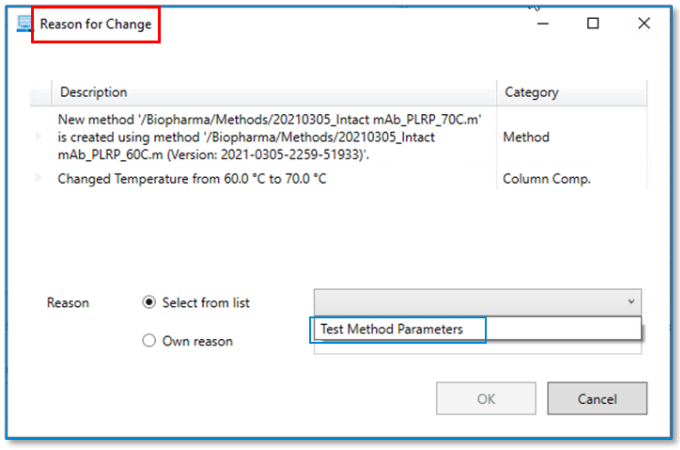

Figure 9. The user needs to enter the reason a record was modified. The reason will appear in the entry in the audit trail for that record.

Security

Other features of the Control Panel include how the records are organized. Within the Control Panel, all electronic records are grouped into projects. A project contains instruments, data files, acquisition and processing methods, protein sequences, worklists, and databases. Also, users can be assigned to specific projects which ensures only users with project access rights can process any data within the project. When a new project is created, MassHunter will configure the project to work with the applications accessing it via the Project settings.

With MassHunter being fully integrated with the Control Panel, the user must first select a project to launch data acquisition. With this design feature, project access control can be enabled based on users or user group permissions. All project-related activities for the system will be captured and recorded in System Activity Log and Audit Trails.

Finally, all data acquisition and data analysis programs can be locked to prevent unauthorized access. A valid user login and password is needed to unlock the programs. While the application is locked, its content is blurred preventing any unauthorized user from viewing detailed information.

Conclusion

Agilent MassHunter 11.0 which includes Acquisition, Quantitative Analysis, and BioConfirm, provides customers with excellent technical control tools for user management, data integrity and traceability. These tools have been carefully designed to enhance flexibility and improve the productivity of system administrators, end users and data reviewers, while providing the data integrity required by regulatory agencies.

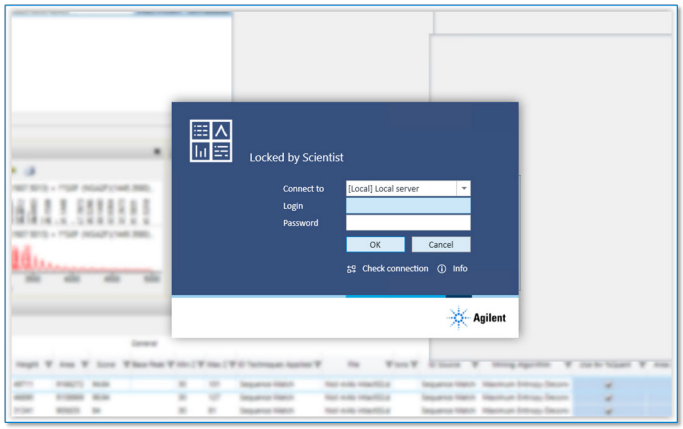

Figure 10. Screenshot of BioConfirm with application lock active.

www.agilent.com/chem

DE44368.6207175926

This information is subject to change without notice.

© Agilent Technologies, Inc. 2021
Printed in the USA, June 24, 2021
5994-3546EN

Agilent
Trusted Answers