White Paper

Agilent
Trusted Answers

Support for Title 21 CFR Part 11 and Annex 11 compliance: Agilent MassHunter GC/MS Software Products

Valid for MassHunter GC/MS Data Acquisition Version 13.0 and Data Analysis Version 12.1 Update 2

Overview

U.S. Food and Drug Administration (US FDA) Part 11 in Title 21 of the Code of Federal Regulations (CFR), and its European Union (EU) analog, Eudralex Chapter 4, Annex 11, describe the requirements for electronic records and electronic signatures for regulated pharmaceutical and Biopharmaceutical organizations.

21 CFR Part 11 was first written into law in 1997 and subsequently updated in 2003. The intent of these guidelines is to ensure that all appropriate electronic records are attributable, legible, contemporaneous, original, accurate, and maintained with integrity.

This white paper is a resource for users of Agilent Networked Workstation for GC/MS systems whose organizations must comply with these regulations. MassHunter Acquisition for GC/MS controls acquisition and processing of GC/MSD, GC/TQ, and GC/Q-TOF systems.

It is the responsibility of the user and their organization to ensure that the functionalities provided by MassHunter for GC/MS are used appropriately to ensure compliant operation for laboratory data acquisition and processing. In addition to the technical controls MassHunter for GC/MS provides, the user organization must establish procedural controls – standard operating procedures (SOPs) – to address relevant non-technical requirements and to fill gaps that are not provided from the software feature set. For example, controls such as internal audit programs, must also be established to ensure that system operators follow the SOPs.

Appendix 1 provides a detailed description of how MassHunter for GC/MS supports users and their organizations in fulfilling the requirements of each section of 21 CFR Part 11 and the related sections of EU Annex 11. The descriptions assume that system access, including instrument hardware and software, is controlled by the staff responsible for the electronic records contained on the system. Thus, the system is designed as a "closed system" as defined in 21 CFR Part 11.3(b)(4).

21 CFR Part 11

21 CFR Part 11 covers three specific elements of a regulated laboratory's operation:

- Security of electronic records
- Attribution of work
- Electronic signatures (if used)

Security

As per ISO/IEC 17799, also known as ISO/IEC 27002, security can be interpreted as "the right people, having the right access, to the right information." Regulated organizations must be able to both verify the identity of system users and limit system access to trained, authorized individuals (11.10(d), (i) and (g); 11.100(b)). Because laboratory staff have different responsibilities based on their job assignments, data access and controls must be segregated to make sure that they can perform only allowed operations on data records that are required to fulfill their responsibilities.

Attribution of work

Attribution of work refers to documenting the "Who, what, when, where, and why?" of work performed. Automated audit trails independently record users' actions, thus connecting laboratory staff to the work they perform. Audit trail entries enable staff and regulatory inspectors to reconstruct the complete history of an electronic record.

- **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 pre-defined reasons to provide consistency and to enable searching and sorting of entries.

eSignatures

While 21 CFR Part 11 does not require the use of eSignatures, it does provide regulations for their use when they are used. In this case, the system must ensure that eSignatures:

- Are irrevocably linked to their respective records
- Show the full name of the signer, date and time, as well as the meaning of, or reason for, the signature (such as review, approval, responsibility, or authorship)
- Are present whenever the signed records are displayed or printed

Topology

Workstation topologies are not supported for compliance and regulatory customers.

Network Workstation with the following versions of content management are supported topologies for regulatory customers:

- ECM 3.5 HF6, ECM 3.6 and ECM XT 2.7 and ECM XT 2.8 for SQ and TQ
- ECM XT 2.7 and ECM XT 2.8 only for QTOF

Compatibility

Software compatibility:
MassHunter GC/MS Data Acquisition Version 13.0 and MassHunter Quantitative Analysis Version 12.1 Update 2 are supported. Older versions of MassHunter are incompatible and must be upgraded to the specified version or higher.

Raw data and results created with previous versions of MassHunter software (Acquisition and Data Analysis) would require data migration. Contact Agilent for additional information on migration services.

eSignature functionality is available in MassHunter Quantitative Analysis 12.1 Update 2 with ECM XT 2.7 and 2.8.

"Separation of duty, as a security principle, has as its primary objective the prevention of fraud and errors. This objective is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users."

– Botha, Eloff, IBM Systems Journal[1]

eSignature functionality for ECM 3.5 and 3.6 is available within the Content Management system only. It does not have technical control and will need procedural control. Contact Agilent for migration services from ECM 3.5/3.6 to ECM XT 2.7/2.8. We recommend upgrading to ECM XT 2.7/2.8 if you need eSignature functionality.

Hardware compatibility: Please refer to Appendix 2.

Appendix 1. Satisfying the requirements set forth in US FDA Title 21 CFR Part 11 and related global regulations using MassHunter for GC/MS

Appendix 1 table notes

Column one

The table addresses 21 CFR Part 11 requirements in the order that they are presented in the US FDA reference document.[2] Related requirements such as those found in EU Annex 113 follow each section of Part 11.

Column two

For completeness, column two lists all requirements of 21 CFR Part 11 and other related global requirements. "System" refers to the analytical system used to acquire and process data.

Most requirements are fulfilled by either technical control (i.e., software functionality) or procedural controls (i.e., SOPs). Technical controls are controls provided by the software and hence the software supplier, while procedural controls are the responsibility of the user organization. 21 CFR Part 11 requirements listed in **bold** are requirements **addressed by technical controls**. Other global requirements are listed in regular font. Requirements that must be addressed by procedural controls are listed in blue.

Column three

Some requirements involve both technical and procedural controls. Responsibilities for each requirement are listed in column three. "S" refers to analytical system supplier. "U" refers to the user organization. Rows containing requirements that must be exclusively addressed by the user organization are shown in blue. Blue may also be technical controls the user will be responsible to implement.

Column four

If available and where appropriate, related global requirements and comments are provided in column four. This column also pertains to the Chinese translation of the requirements outlined in column 2 in English, within the context of China Food and Drug Administration (CFDA). A product may choose to remove references to the Chinese translation.

Column five

Column five indicates with a "yes," "no," or "partially" whether the requirement can be satisfied using the technical controls provided in MassHunter for GC/MS. A "partially" response denotes that the requirement is only partially met by technical controls and may rely on procedural controls to be fully satisfied. "N/A" indicates that the requirement is not applicable to the CDS.

Column six

Column six explains how the regulatory requirement can be satisfied using

the technical controls provided by MassHunter for GC/MS. Column six also provides additional recommendations for the user organization when relevant.

1. Validation

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using MassHunter for GC/MS? If no, what is the recommendation?
Part 11 11.10(a)	1.1 Is the system validated to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records?	S, U	Required by all regulations. This is a typical example of shared responsibility between the system supplier and the user organization. While the user organization has ultimate responsibility for validation, some tasks can only be done and must be delivered by the software supplier, e.g., validation activities during development and related documentation. 第五章系统 第十三条在计算机化系统使用之前，应当对系统全面进行测试，并确认系统可以获得预期的结果。当计算机化系统替代某一人工系统时，可采用两个系统（人工和计算机化平行运行）的方式作为测试和验证内容的一部分。 第五章系统 第十三条在计算机化系统使用之前，应当对系统全面进行测试，并确认系统可以获得预期的结果。当计算机化系统替代某一人工系统时，可采用两个系统（人工和计算机化平行运行）的方式作为测试和验证内容的一部分。	Yes	Agilent Technologies has extensively verified the performance of MassHunter for GC/MS using tests that evaluate accuracy, reliability and consistent performance. However, the user organization is required to qualify and validate their analytical system based on their defined intended use. With respect to MassHunter for GC/MS, "regulated records" are: – Acquisition Methods – Acquired Data – Acquisition Sequences – Tune Files – Data Analysis Methods – Data Analysis Results – Acquisition Method Audit Trail – Acquired Data Audit Trail – Sequence Audit Trail – Data Analysis Method Audit Trail – Data Analysis Result Audit Trail – Activity Log The integrated solution of MassHunter with OpenLab ECM incorporates the use of byte-order dependent check sums at each file transfer operation to ensure that record transfers are valid between the components. During data acquisition, two copies of the Tune Files are generated. One copy is embedded within the Data File/Raw Data stored in OpenLab ECM, which is controlled, while the other is saved on the local C drive. It is the user organization's responsibility to maintain the integrity of this record stored on the C drive. Agilent has a range of compliance and validation services available for purchase, see www.agilent.com/chem/services for more details.
Annex 11	1.2 Is infrastructure qualified?	U	Annex 11. Principle B Brazil GMP 577	No	

2. Accurate copies and secure retention and retrieval of records

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using MassHunter for GC/MS? If no, what is the recommendation to customers?
Part 11 11.10(b)	2.1 Is the system capable of generating accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the FDA?	S, U	第五章系统 第十九条以电子数据为主数据时，应当满足以下要求： （一为满足质量审计的目的，存储的电子数据应当能够打印成清晰易懂的文件。	Yes	The system generates the following controlled records that can be viewed (V) and printed (P) in a pdf format: – Tune Parameters (V and P) – Acquisition Methods (V and P) – Acquired Data (V and P) – Analysis Results (V and P) – Analysis Reports (V and P) – Sequences (V and P) – Sequence Logs (V and P) – Audit Trails (V and P) – Electronic Signatures (V (all) and P (PDF only))
Annex 11	2.2 Is it possible to obtain clear printed copies of electronically stored e-records?	S, U	Annex 11.8.1 Brazil GMP 583	Yes	The system generates the following controlled records that can be viewed (V) and printed (P) in a pdf format: – Tune Parameters (V and P) – Acquisition Methods (V and P) – Acquired Data (V and P) – Analysis Results (V and P) – Analysis Reports (V and P) – Sequences (V and P) – Sequence Logs (V and P) – Audit Trails (V and P) – Electronic Signatures (V (all) and P (PDF only))
Brazil	2.3 Are there controls to ensure that the data backup, retrieval and maintenance process is duly carried out?	S, U	Brazil 585.2 第五章系统 第十九条以电子数据为主数据时，应当满足以下要求： （三）应当建立数据备份与恢复的操作规 程，定期对数据备份，以保护存储的数据供将来调用。备份数据应当储存在另一个单独的、安全的地点，保存时间应当至少满足本规范中关于文件、记录保存时限的要求。	Yes	A backup and restore solution with instructions is available as a separate add-on service. It is the responsibility of the user organization to control data backup, data retrieval, and maintenance, including regular backups of data acquisition and data analysis computers.
Part 11 11.10(c)	2.4 Does the system protect records to enable their accurate and ready retrieval throughout the records retention period?	S, U	China GMP 163	Yes	All raw data, metadata, and result data generated by MassHunter for GC/MS Software is stored in a protected location in ECM. Physical security (control of physical access to servers) is the responsibility of the user organization. It is the user organization's responsibility to develop a review by exception protocol based on a risk-based assessment of unplanned events, such as network connectivity loss which would initiate a failover mode.
Annex 11	2.5 Are data checked during the archiving period for accessibility, readability, and integrity?	U	Annex 11.17	N/A	It is the user organization's responsibility to check data during archival for accessibility, readability, and integrity.
Annex 11	2.6 If relevant changes are made to the system (e.g., computer equipment or programs), is then the ability to retrieve the data ensured and tested?	S, U	Annex 11.17	Yes	Agilent ensures that all minor and service updates released for a given major version (e.g., Quant 12.0) remain compatible, allowing previously generated data to be available (opened and processed) in subsequent updates (e.g., Quant 12.1, 12.2, and all related service updates such as 12.1 Update 1). Additionally, data acquired using version 11 are tested and remain compatible for use in Quant 12.0 and later versions. For data generated in versions prior to 11, a built-in tool is provided to convert them into a Quant 12-compatible format. It is the user organization's responsibility to test and validate that the data are available for retrieval based on the customer's intended use.

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using MassHunter for GC/MS? If no, what is the recommendation to customers?
Annex 11	2.7 Are data secured by both physical and electronic means against damage?	S, U	Annex 11.7.1 Brazil GMP 584 第五章系统 第十条系统应当安装在适当的位置，以防止外来因素干扰。 第五章系统 第十九条以电子数据为主数据时，应当满足以下要求： （二）必须采用物理或者电子方法保证数据的安全，以防止故意或意外的损害。日常运行维护和系统发生变更（如 计算机设备或其程序）时，应当检查所存储数据的可访问性及数据完整性。	Yes	All raw data, metadata, and results data generated by MassHunter software are stored in a protected location in ECM 3.X. OpenLab ECM 3.5/3.6 and OpenLab ECM XT has a mechanism to notify the admin after a set number of failed login attempts. Physical security (control of physical access to servers) is the responsibility of the user organization. It is the user organization's responsibility to develop a review by exception protocol based on a risk-based assessment of unplanned events such as network connectivity loss, which would initiate operational continuity.
Annex 11	2.8 Does the system allow performing regular backups of all relevant data?	S, U	Annex 11.7.1 China GMP 163 Brazil GMP 585 21 CFR Part 211, 68 b	Yes	It is the responsibility of the user organization to control data backup, data retrieval, and maintenance. A backup and restore solution with instructions is available as a separate add-on service.
Annex 11	2.9 Is the integrity and accuracy of backed-up data and the ability to restore the data, checked, validated, and monitored periodically?	U	Annex 11.7.2 China GMP 163 Brazil GMP 585 Part 211, 68 b	N/A	While backing up data is the responsibility of the user organization, the system is designed to allow backup of all relevant files and includes utilities to perform data backup and restoration. The backup and restore add-on solution enables user organizations to schedule backups. It also provides a procedure for restoring data in case of data loss. Detailed instructions are included in the documentation provided with the solution. For more information, refer to the Agilent OpenLab Server and OpenLab ECM XT Administration Guide.

3. Authorized access to systems, functions, and data

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using MassHunter for GC/MS? If no, what is the recommendation to customers?
Part 11 11.10(d)	3.1 Is system access limited to authorized persons?	S, U	China GMP 183 163 Brazil GMP 579, ICH Q7.5.43	Yes	Each user is identified by a unique ID and password combination. Entry of both is required to access the system.
	3.2 Is each user clearly identified, e.g., through his/her/their own user ID and Password?	S, U	Several Warning Letters Please refer to US FDA Warning Letters for examples.	Yes	Each user is identified by a unique ID and password combination. Entry of both is required to access the system. It is the user organization's responsibility to ensure unique identities of authorized persons.

4. Electronic audit trail

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using MassHunter for GC/MS? If no, what is the recommendation to customers?
Part 11 11.10(e)	4.1 Is there a secure, computer-generated, time-stamped audit trail to independently record the date and time of operator entries and actions that create, modify, or delete electronic records?	S	China GMP 163 第五章系统 第十六条计算机化系统应当记录输入或确认关键数据人员的身份。只有经授权人员，方可修改已输入的数据。每次修改一个已输入的关键数据均应当经过批准，并应当记录更改数据的理由。应当根据风险评估的结 果，考虑在计算机化系统中建立一个数据审计跟踪系统，用于记录数据的输入和修改。	Yes	MassHunter has a secure, computer-generated, time-stamped audit trail that records actions such as "create", "modify", and "delete" for the following electronic records: – GC/MS Tune Parameters (V and P): Yes – GC/MS Acquisition Methods (V and P): Yes – GC/MS Acquired Data (V and P): Yes – GC/MS Analysis Results (V and P): Yes – GC/MS Analysis Reports (V and P): Yes – GC/MS Sequences (V and P): Yes – GC/MS Sequence Logs (V and P): Yes – GC/MS Audit Trails (V and P): Yes – MassHunter Quant Results: Yes – MassHunter Quant Method: Yes – OpenLab ECM eSignature: Yes – MassHunter Quant eSignature: Yes File actions performed through OpenLab ECM, including file deletion, are tracked through the OpenLab ECM audit trail and activity log.
FDA GLP	4.2 Does the audit trail record who has made which changes, when, and why?	S	FDA 21 CFR P art 58.130 e	Yes	The audit trail includes the user ID, date and time of the change, and the before and after values together with the reason why the change was made. The system can be configured so that the user is required to enter a reason for changes which is then recorded in the Audit trails. The reason can be either freeform or predefined by the system administrator.
Annex 11	4.3 Can the system generate printouts indicating if any of the e-records have been changed since the original entry?	S	Annex 11, 8.2	Yes	The system can be configured so that the user is required to enter a reason for changes to the records, which is then recorded in the Audit trails. Audit trails for records can be printed from any audit trail window. MassHunter Acquisition for GC/TQ, GC/MSD and GC/Q-TOF systems, MassHunter Quantitative Analysis and OpenLab Server or ECM XT each have this capability.
FDA CGMP	4.4 Does the audit trail include any modifications to an established method employed in testing? Do such records include the reason for the modification?	S	21 CFR Part 211.194 8b	Yes	The system can be configured so that the user is required to enter a reason for changes to the records, which is then recorded in the Audit trails. Audit trails for records can be printed from any audit trail window. MassHunter Acquisition for GC/TQ, GC/MSD and GC/Q-TOF systems, MassHunter Quantitative Analysis and OpenLab Server or ECM XT each have this capability.
	4.5 Is the audit trail function configured to be always on and can it not be switched off by system users?	S, U	Warning Letter Please refer to US FDA Warning Letters for examples.	Yes	For GC/MS, Audit trails are always on and cannot be deactivated by any user.
Annex 11	4.6 Is audit trail available in a generally intelligible form for regular review?	S	Annex 11, 9	Yes	All audit trails are human-readable. Audit trails are readily available in a configurable viewer accessed from the local machine or from a central location. The audit trail viewer indicates which audit trail entries have been reviewed and approved.
	4.7 Can audit trail contents be configured such that only relevant activities are recorded for meaningful review of audit trail information?	S	Implicitly required by Annex 11 with many warning letters related to review of audit trails.	Yes	Audit trail contents are preprogrammed and not configurable. Audit trails are linked to the record and all entries relevant to the record are viewable. MassHunter allows the audit trail to be filtered prior to displaying its contents to address user preferences for reviewing the information.

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using MassHunter for GC/MS? If no, what is the recommendation to customers?
Part 11 11.10(e)	4.8 Is previously recorded information left unchanged when records are changed?	S		Yes	MassHunter for GC/MS logs all data entry additions, modifications, and deletions. Any changes to files stored in OpenLab ECM are saved as new revisions/versions, preserving the original file. When accessing files for further reprocessing, users select the file version they wish to use, depending on their permissions.
Part 11 11.10(e)	4.9 Is audit trail documentation retained for a period at least as long as that required for the subject electronic record?	S, U		Yes	Audit trail information is stored within the electronic record and cannot be separated from it. MassHunter audit trails are linked with the record and are preserved so long as the record is kept in OpenLab ECM 3.X, OpenLab Server, or ECM XT. OpenLab ECM 3.X, OpenLab Server, and ECM XT allow for configurable retention policies to meet data lifecycle management. It is the user organization's responsibility to manage and retain records in accordance with their retention policy.
Part 11 11.10(e)	4.10 Is audit trail available for review and copying by the FDA?	S		Yes	MassHunter audit trails can be viewed and printed for review.
Annex 11	4.11 Is it possible to obtain clear printed copies of electronically stored e-records (e.g., e-audit trail?)	S	Annex 11, 8.1	Yes	MassHunter audit trails can be viewed and printed for review.

5. Operational and device checks

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using MassHunter for GC/MS? If no, what is the recommendation to customers?
Part 11 11.10(f)	5.1 Are there operational system checks to enforce permitted sequencing of steps and events, if required?	S, U		Yes	The system supports standard MassHunter workflows, requiring users to follow a defined sequence of steps. Only those with specific permissions are authorized to operate the system. Laboratories can enforce common workflow restrictions through User Groups. MassHunter Acquisition and Quant function based on predefined methods, which can be restricted to prevent editing while still allowing execution by users. However, it is the responsibility of the user organization to configure the users based on their intended use.
Part 11 11.10(g)	5.2 Are there authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand?	S, U	Part 211, 68 b	Yes	MassHunter manages access and user capabilities through role-based permissions linked to the user login credentials. Certain actions, such as electronically signing a record or deleting a file, require additional permissions/authority checks to ensure only authorized individuals can perform these operations/actions. Users cannot access the software modules of MassHunter without valid user authentication (user ID, password, and account). Once logged in, access to files and software functionalities—including but not limited to signing records, entering data, or modifying records—is strictly controlled by the privileges assigned to the user to maintain data integrity and security. However, it is the responsibility of the user organization to configure the users based on their intended use.

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using MassHunter for GC/MS? If no, what is the recommendation to customers?
Annex 11	5.3 Is the system designed to record the identity of operators entering, changing, confirming or deleting data including date and time?	S	Annex 11, 12.4	Yes	Each user is uniquely identified by a user ID and password, both of which are required for system access. The audit trail and activity log capture the identity of operators performing actions within the system, including the user ID, date and time of the change, the previous and updated values, and the reason for the modification.
Part 11 11.10(h)	5.4 Does the system allow use of device checks to determine, as appropriate, the validity of the source of data input or operational instruction?	S	There are two equally valid interpretations of this requirement. Systems should be designed such that: 1. Proper communication is confirmed between the computer and the "source" of data input (i.e., the instrument) prior to transmission of instructions to or data from the "source." 2. Regulated records created by the system must unambiguously indicate the "source" of the data (i.e., which instrument or component generated the data.)	Yes	The instrument identification, through serial number, instrument ID, and IP address, is recorded with the data and may be included in reports as required. 1. The system is designed to continually ensure a valid connection between the instrument and the computer workstation. 2. Identification of instrument components such as GC modules and MS instruments are supported in the system.
Part 11 11.10(i)	5.5 Is there documented evidence that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks?	U	China GMP 18 Brazil 571	N/A	It is the responsibility of the user organization to maintain documented evidence that the persons who develop, maintain, or use electronic record and electronic signature systems have the education, training, and experience needed to perform these tasks. Agilent software professionals involved in development of MassHunter have received training in relevant aspects of data integrity.
Part 11 11.10(j)	5.6 Is there a written policy that holds individuals accountable and responsible for actions initiated under their electronic signatures, in order to determine record and signature falsification? 5.7 Have employees been trained on this procedure? (Implied requirement of Part 11 11.10(j))	U		N/A	It is the responsibility of the user organization to establish a written policy (SOP) that holds staff responsible for the actions initiated under their electronic signatures.
Part 11 11.10(k)	5.7 Are there appropriate controls over systems documentation including: 1. Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance? 2. Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	U	China GMP 161 第五章系统 第十七条计算机化系统的变更应当根据预定的操作规程进行，操作规程应当包括评 估、验证、审核、批准和实施变更等规定。计算机化系统的变更，应经过该部分计算机化系统相关责任人员的同意，变更情况应有记录。主要变更 应当经过验证。 第五章系统 第十一条应当有详细阐述系统的文件（必要时，要有图纸），并须及时更新。此文件应当详细描述系统的工作原理、目的、安全措施和适用范围、计算机运行方式的主要特征，以及如何与其他系统和程序相接。	N/A	1. It is the responsibility of the user organization to establish systems documentation. 2. Agilent maintains development and testing documentation for MassHunter and OpenLab ECM. Upon request, this documentation is available for review.

6. Data integrity, date, and time accuracy

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using MassHunter for GC/MS? If no, what is the recommendation to customers?
Annex 11	6.1 Do computerized systems that exchange data electronically with other systems include appropriate built-in checks for the correct and secure entry and processing of data?	S	Annex 11.5	Yes	The integrated solution of MassHunter with OpenLab ECM 3.X or XT incorporates the use of byte-order-dependent checksums at each file transfer operation to ensure that record transfers are valid between the systems.
Annex 11	6.2 Is there an additional check on the accuracy of the data? This check may be done by a second operator or by validated electronic means.	S, U	Annex 11-6 Brazil GMP 580 ICHQ7-5.45 第五章系统 第十五条当人工输入关键数据时(例如在称重过程中输入物料的重量和批号),应当复核输入记录以确保其准确性。这个复核可 以由另外一个操作人员完成,或采用经验证 的电子方式。必要时,系统应当设置复核功能,确保数据输入的准确性和数据处理过程的正确性。	Yes	The integrated solution of MassHunter with OpenLab ECM 3.X or XT utilizes byte-order-dependent checksums during each file transfer operation to ensure the validity of record transfers between systems. As part of the e-signature process, the system can be configured to require a second operator/user to review and validate the results. However, it is the user organization's responsibility to establish procedures for additional checks and to ensure data accuracy.
Part 11 11.10(e) 11.50(a)	6.3 Are controls established to ensure that the system's date and time are correct?	S, U	Annex 11.14	Yes	The MassHunter application accurately records every action performed by both the user and the system, along with precise timestamps. However, to ensure that timestamps remain relevant and accurate, it is recommended to configure the system to reference a time server for precise synchronization of the system date and time. This configuration is managed and controlled by the operating system.
Part 11 11.10(e) 11.50(a)	6.4 Are timestamps with a clear understanding of the time zone reference used implemented for systems that span different time zones?	S, U	Annex 11.14	Yes	All time data is time stamped in Coordinated Universal Time (UTC)/Greenwich Mean Time (GMT) and displayed in the local time of the computer used. However, to ensure the timestamps remain relevant and accurate, it is recommended to configure the system to reference a time server for precise synchronization of the system date and time. This configuration is managed and controlled by the operating system.

7. Control for open systems (only applicable for open systems)

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using MassHunter for GC/MS? If no, what is the recommendation to customers?
Part 11 11.30	7.1 Are there procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt?	N/A		N/A	MassHunter is not intended to be deployed as an "Open" system as per 21 CFR Part 11 11.3(b)(9)
Part 11 11.30	7.2 Are there additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality?	N/A		N/A	MassHunter is not intended to be deployed as an "Open" system as per 21 CFR Part 11 11.3(b)(9)

8. Electronic signatures – signature manifestation and signature/record linking

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using MassHunter for GC/MS? If no, what is the recommendation to customers?
Annex 11	8.1 When electronic signatures are used, do they have the same impact as hand-written signatures within the boundaries of the company? Are they permanently linked to their respective record? Do they include the time and date that they were applied?	S, U	Annex 11.14 ICH Q7.6.18 第五章系统 第二十三条电子数据可以采用电子签名的方式，电子签名应当遵循相应法律法规的要求。	Yes	The user organization must establish the legal impact of electronic signatures. Signatures are permanently linked to their respective records. Signed electronic records includes the date and time the signature was executed.
Part 11 11.50 (a)	8.2 Do signed electronic records contain information associated with the signing that clearly indicates all of the following: 1. The printed name of the signer? 2. The date and time when the signature were executed? 3. The meaning (such as review, approval, responsibility, or authorship) associated with the signature?	S		Yes	For MassHunter Quant for ECM XT install electronic signature manifestation includes: 1. The User ID, Full name of the signer 2. The date and time the signature was executed 3. The meaning of the signature. For MassHunter Quant for 3.X install electronic signature manifestation includes: 1. The Username of the signer 2. The date and location 3. The reason
Part 11 11.50 (b)	8.3 Are the items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section subject to the same controls as for electronic records and are they included as part of any human readable form of the electronic record (such as electronic display or printout)?	S		Yes	All electronic signatures are displayed in a human-readable form and may be printed.
Part 11 11.70	8.4 Are electronic signatures and handwritten signatures linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means?	S, U		Yes	Handwritten signatures are not addressed by the system and must be managed procedurally by the user's organization. For MassHunter Quant for ECM XT, electronic signatures are embedded in the electronic record and cannot be modified, overwritten or deleted. For MassHunter Quant for ECM 3.X, installation, electronic signatures are applied and recorded within the ECM 3.x audit trail. Once a file is signed, the e-signature metadata (user's full name and username, title, location, reason, and time stamp) is captured in the following locations: – **Audit Trail:** Tracks the details of the electronic signature application, including timestamps and user information. – **File Properties:** Stores relevant metadata related to the electronic signature for easy reference. – **System Activity Log:** Logs system-level activities, including the application of electronic signatures, providing an additional layer of traceability.
Part 11 Preamble	8.5 Is there a user-specific automatic inactivity disconnect measure that would "de-log" the user if no entries or actions were taken within a fixed short timeframe?	S	Part 11 Preamble section 124	Yes	Automatic session locking enables the user organization to configure a time after which the user is automatically logged-out.

9. Electronic signatures general requirements and signature components and controls

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using MassHunter for GC/MS? If no, what is the recommendation to customers?
Part 11 11.100(a)	9.1 Is each electronic signature unique to one individual and not reused by, or reassigned to, anyone else?	S, U		Yes	– The combination of username/user ID and password is unique and cannot be reused or reassigned. Duplicate user IDs are not permitted, ensuring that each user has a distinct login and signature, with both the user ID and password required for electronic signatures. – The system supports Active Directory (AD) integration for user authentication, but it requires customers to configure this setup. OpenLab Server or ECM XT-administered users are uniquely managed to prevent duplicate user ID/password combinations. – The user organization is responsible for defining and enforcing the username and password policy.
Part 11 11.100(b)	9.2 Does the organization verify the identity of the individual before the organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature?	N/A		N/A	It is the responsibility of the user organization to verify the identity of staff before it establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature.
Part 11 11.100 (c)	9.3 Are persons using electronic signatures, prior to or at the time of such use, certified to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures? 9.4 Do persons using electronic signatures, upon agency request provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature?	N/A		N/A	It is the responsibility of the user organization to verify that staff using electronic signatures meet these requirements.
Part 11 11.200(a) (1)	9.5 Do electronic signatures that are not based upon biometrics employ at least two distinct identification components, such as an identification code and password?	S, U		Yes	Electronic Signature authentication within OpenLab ECM 3.5/3.6, OpenLab Server, or ECM XT requires both a username/user ID and password.
Part 11 11.200(a) (1) (i)	9.6 When an individual executes a series of signings during a single, continuous period of controlled system access, is the first signing executed using all electronic signature components?	S		Yes	Both identification username/user ID and password are required to make all electronic signatures.
Part 11 11.200(a) (1) (i)	9.7 When an individual executes a series of signings during a single, continuous period of controlled system access, are subsequent signings executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual?	S		Yes	Both identification username/user ID and password are required to make all electronic signatures.
Part 11 11.200(a) (1) (ii)	9.8 When an individual executes one or more signings not performed during a single, continuous period of controlled system access, is each signing executed using all of the electronic signature components?	S		Yes	Both identification username/user ID and password are required to make all electronic signatures.
Part 11 11.200(a) (2)	9.9 Are controls in place to ensure that electronic signatures that are not based upon biometrics are used only by their genuine owners?	U		N/A	It is the user organization's responsibility to ensure that usernames and passwords are known only by the assigned individuals and are traceable to individual users.
Part 11 11.200(a) (3)	9.10 Are the electronic signatures administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals?	S, U		Yes	Misuse of electronic signatures by anyone other than the owner would require intentional cooperation of a user and the System Administrator.

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using MassHunter for GC/MS? If no, what is the recommendation to customers?
Part 11 11.200(b)	9.11 Are electronic signatures based upon biometrics designed to ensure that they cannot be used by anyone other than their genuine owners?	N/A		N/A	Biometric authentication is not supported in MassHunter GC/MS Acquisition and MassHunter Quantitative Analysis.

10. Controls for identification codes and passwords

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using MassHunter for GC/MS? If no, what is the recommendation to customers?
Part 11 11.300(a)	10.1 Are controls in place to maintain the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password?	S, U		Yes	MassHunter GC/MS Acquisition and MassHunter Quantitative Analysis does not allow duplicate username/user IDs.
Part 11 11.300(b)	10.2 Are controls in place to ensure that identification code and password issuance are periodically checked, recalled, or revised (e.g., to cover such events as password aging)?	S, U		Yes	Password expiration is configurable via either the Windows Domain or locally in the application itself. The user organization should configure password expiration based on a documented risk assessment.
Part 11 11.300(c)	10.3 Are there procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromise tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls?	U	第五章系统 第十四条数据的输入或修改只能由经许可的人员进行。杜绝未经许可的人员输入数据的手段有：使用钥匙、密码卡、个人密码和限制对计算机终端的访问。应当就输入和修改数据制订一个授权、取消、授权变更，以及改变个人密码的规程。必要时，应当考虑系统能记录未经许可的人员试图访问系统的行为。对于系统自身缺陷，无法实现人员控制的，必须具有书面程序，相关记录本及相关物理隔离手段，保证只有经许可的人员方 能进行操作。	N/A	It is the responsibility of the user organization to establish these procedures.
Part 11 11.300(d)	10.4 Are their transaction safeguards in place to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts of their unauthorized use to the system security unit, and, as appropriate, to organizational management?	U	第五章系统 第十四条数据的输入或修改只能由经许可的人员进行。杜绝未经许可的人员输入数据的手段有：使用钥匙、密码卡、个人密码和限制对计算机终端的访问。应当就输入和修改数据制订一个授权、取消、授权变更，以及改变个人密码的规程。必要时，应当考虑系统能记录未经许可的人员试图访问系统的行为。对于系统自身缺陷，无法实现人员控制的，必须具有书面程序，相关记录本及相关物理隔离手段，保证只有经许可的人员方 能进行操作。	N/A	MassHunter authentication can use Windows domain authentication, as such transaction safeguards can be configured as part of the Windows password policy setup. It is the user organization's responsibility to configure the transaction safeguards for the Windows system.
Part 11 11.300(e)	10.5 Are their controls for initial and periodic testing of devices, such as tokens or cards that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner?	U		N/A	It is the responsibility of the user organization to establish controls to test devices initially as well as periodically to ensure they function properly and have not been altered in an unauthorized manner.

11. System development and support

Part 11 and Others	Requirement	S, U	Other associated regulations and comments	Yes/No	If yes, how, specifically, is the requirement satisfied using MassHunter for GC/MS? If no, what is the recommendation to customers?
Annex 11	11.1 Has the software or system been developed in accordance with an appropriate quality management system?	S, U	Annex 11 4.5 Brazil GMP 577 GAMP 5 This is a shared responsibility between the system supplier and the user organization. The user should require the supplier to provide documented evidence that software is developed within the framework of a quality management system (QMS). 第二章原则 企业应当能够提供与供应商质量体系和审计信息相关的文件。	Yes	MassHunter is developed within the ISO 9001 Quality Management Standard defined by Agilent.
Brazil	11.2 Is there a formal agreement when the software supplier subcontracts software and maintenance services. Does the agreement include the contractor's responsibilities?	S, U	Brazil GMP 589 This is a shared responsibility between the system supplier and the user organization. The supplier must have such an agreement with the subcontractor, and the user must verify that the agreement is in place. 第二章原则 第四条企业应当注重计算机化系统供应商的管理，制定相应的操作规程。供应商提供产品或服务时（如安装、配 置、集成、验证、维护、数据处理等），企业应当与供应商签订正式协议，明确双方责任。	Yes	Agilent requires formal agreements with all suppliers (Refer to the section 4.0 of the Agilent Quality Manual, Document Number: AQM01).
ICH Q10	11.3 For outsourced (development and support) activities, is there a written agreement between the contract giver and contract acceptor?	S, U	ICHQ10, 2.7 c **Note:** If applicable to your product	Yes	Agilent requires formal agreements with all suppliers (Refer to the section 4.0 of the Agilent Quality Manual, Document Number: AQM01).
ICH Q10	11.4 Are the responsibilities and communication processes for quality related activities of the involved parties (contractors) defined?	S, U	ICHQ10, 2.7 c **Note:** If applicable to your product	Yes	Agilent defines and enforces the responsibilities of all suppliers to ensure compliance with ISO 9000 standards and alignment with organizational objectives.
Part 11 11.10(i)	11.5 Are personnel developing and supporting software trained?	S, U	This is a shared responsibility between the system supplier and the user organization. The supplier must ensure its staff is trained, and the user should have assurance, e.g., through audits that SW developers are trained and that this training is documented. 第三章人员 第五条计算机化系统的"生命周期"中所涉及的各种活动，如验证、维护、管理等，需要各相关的职能部门人员之间的紧密合作。在职责中涉及使用和管理计算机化系统的人员，应当接受相应的使用和管理培训。确保有适当的专业人员，对计算机化系统的设计、验证、安装和运行等方面进行培训 和指导。	Yes	All Agilent personnel are required to be trained.

Appendix 2: Hardware compatibility

Note: Agilent releases GC and MS firmware updates independent of software releases. All Agilent GC instrument driver revisions have been designed to be backward compatible with the installed instrument base. Agilent recommends always using the latest module firmware revision to provide the highest system capability.

Supported gas chromatographs, inlets, and detectors

	Module Type	Inlets	Detectors
8890	G3540A	S/S, P/P, COC, PTV,	TCD, FID, NPD, FPD ECD,
		PCM, VI, MMI, HT-PTV	µECD, Dual W FPD, AIB, XCD
	G3542A	S/S, P/P, COC, PTV,	TCD, FID, NPD, FPD ECD,
		PCM, VI, MMI, HT-PTV	µECD, Dual W FPD, AIB, XCD
	G3543A	S/S, P/P, COC, PTV,	TCD, FID, NPD, FPD ECD,
		PCM, VI, MMI, HT-PTV	µECD, Dual W FPD, AIB, XCD
	G3545A	S/S, P/P, COC, PTV,	TCD, FID, NPD, FPD ECD,
		PCM, VI, MMI, HT-PTV	µECD, Dual W FPD, AIB, XCD
8860	G2790A	S/S, P/P, COC, PCI	TCD, FID, NPD, µECD, FPD,
			FPD+
8850	G3940A	S/S, P/P, COC	TCD, FID
	G3941A	S/S, P/P, COC	TCD, FID
Intuvo 9000	G3950A	S/S, MMI	TCD, FID, NPD, FPD ECD,
			µECD, XCD
	G3952A	S/S, MMI	TCD, FID, NPD, FPD ECD,
			µECD, XCD
	G3953A	S/S, MMI	TCD, FID, NPD, FPD ECD,
			µECD, XCD
7890B and 7890A+	G3440B	S/S, P/P, COC, PTV,	TCD, FID, NPD, FPD ECD,
		PCM, VI, MMI, HT-PTV	µECD, Dual W FPD, AIB, XCD
	G3442B	S/S, P/P, COC, PTV,	TCD, FID, NPD, FPD ECD,
		PCM, VI, MMI, HT-PTV	µECD, Dual W FPD, AIB, XCD
	G3443B	S/S, P/P, COC, PTV,	TCD, FID, NPD, FPD ECD,
		PCM, VI, MMI, HT-PTV	µECD, Dual W FPD, AIB, XCD
	G3445B	S/S, P/P, COC, PTV,	TCD, FID, NPD, FPD ECD,
		PCM, VI, MMI, HT-PTV	µECD, Dual W FPD, AIB, XCD
7890A	G3440A	S/S, P/P, COC, PTV,	TCD, FID, NPD, FPD ECD,
		PCM, VI, MMI, HT-PTV	µECD, Dual W FPD, AIB
	G3442A	S/S, P/P, COC, PTV,	TCD, FID, NPD, FPD ECD,
		PCM, VI, MMI, HT-PTV	µECD, Dual W FPD, AIB
	G3443A	S/S, P/P, COC, PTV,	TCD, FID, NPD, FPD ECD,
		PCM, VI, MMI, HT-PTV	µECD, Dual W FPD, AIB
	G3445A	S/S, P/P, COC, PTV,	TCD, FID, NPD, FPD ECD,
		PCM, VI, MMI, HT-PTV	µECD, Dual W FPD, AIB

Gas chromatographs supported hardware and firmware

Module No.	Module Name	Minimum Firmware	Recommended Firmware
G3940A	8850 GC	3.0.0	3.0.0
G2790A	8860 GC	2.4.0	3.0.0
G3540	8890 GC	2.4.0	3.0.0
G3650A	Intuvo 9000 GC	2.4.0	3.0.0
G3952A	Intuvo 9000 GC	2.4.0	3.0.0
G3953A	Intuvo 9000 GC	2.4.0	3.0.0
G3440B	7890B GC	B.02.03.2	B.02.06
G3442B	7890B GC	B.02.03.2	B.02.06
G3443B	7890B GC	B.02.03.2	B.02.06
G3440A	7890A GC	A.01.16	A.01.16
G3442A	7890A GC	A.01.16	A.01.16
G3443A	7890A GC	A.01.16	A.01.16
G4567A	7650 GC ALS Injector	A.10.02	A.10.05
G4513A	7693 GC ALS Injector	A.10.09	A.11.07
G4514A	7693 GC ALS Tray	A.10.16	A.12.04
G4515A	7693 GC ALS BCR/Mixer	A.10.05	A.10.05
G4516A	7693 GC ALS Injector 6890Plus ALS card	A.01.06	A.01.07
G4517A	7693 GC ALS External Controller for GC 68xx	A.01.06	A.01.06
G4521A	7693 GC ALS LVI Syringe Carriage	N/A	N/A
G4522A	7693 GC ALS Cooling Accessory	N/A	N/A
G4520A	7693 GC ALS Tray with BCR Mixer	A.10.16	A.12.04

Headspace samplers supported hardware and firmware

	Module Type	Description	Minimum Firmware	Recommended Firmware
7697A	G4557A	7697A Headspace Sampler, 111 vials	A.01.08.3	A.01.08.4
	G4556A	7697A Headspace Sampler, 12 vials	A.01.08.3	A.01.08.4
8697	G4511A	G4511A Headspace Sampler (GC FW Minimum 2.4.0)	1.2.0.36	1.4.0.10

Mass spectrometers supported hardware and firmware

Module No.	Module Name	Minimum Firmware	Recommended Firmware
G3171A G3172A G3174A G3243A	5975C Single Quadrupole MSD	7.02.29	7.02.29
G3170A	5975C VL Single Quadrupole MSD	7.02.29	7.02.29
G3175A G3176A	5975E Single Quadrupole MSD	7.02.29	7.02.29
G7037A G7038A G7039A G7040A	5977A Single Quadrupole MSD	6.00.36	6.00.36
G7035A G7036A	5977E Single Quadrupole MSD	6.00.36	6.00.36
G7076B G7077B G7078B G7079B	5977B Single Quadrupole MSD	6.00.36	6.00.36
G7076C G7077B G7078C G7079C	5977C Single Quadrupole MSD	6.00.36	6.00.36
G7010AA G7011AA	7000A Triple Quadrupole MS	059G3	059G3
G7010AA G7011AA	7000B Triple Quadrupole MS	059G3	059G3
G7010BA G7011BA	7000C Triple Quadrupole MS	059G3	059G3
G7010BA G7011BA	7000D Triple Quadrupole MS	059G3	059G3
G7012AA G7013AA	7010A Triple Quadrupole MS	059G3	059G3
G7012BA G7013BA	7010B Triple Quadrupole MS	059G3	059G3
G7010CA G7011CA	7000E Triple Quadrupole MS	10-3-24	10-3-24
G7012CA G7013CA	7010C Triple Quadrupole MS	10-3-24	10-3-24
G7012DA G7013DA	7010D Triple Quadrupole MS	10-3-24	10-3-24
G3850AA G3851AA	7200A Quadrupole Time of Flight MS	22B	22B
G3851BA	7200B Quadrupole Time of Flight MS	22B	22B
G7250AA	7250A Quadrupole Time of Flight MS	02S	02S

CTC PAL3 samplers supported hardware and firmware

Module No.	Module Name	Minimum Firmware	Recommended Firmware
G7367B	PAL3 Series II RSI 85 cm	3.1.21	4.13
G7368B	PAL3 Series II RSI 120 cm	3.1.21	4.13
G7370B	PAL3 Series II RTC 120 cm	3.1.21	4.13
G7395B	PAL3 Series II RSI 160 cm	3.1.21	4.13
G7396B	PAL3 Series II RTC 160 cm	3.1.21	4.13
G7366A/B	PAL3 Series 1.5 LSI	2.4.63	2.4.63
G7367A	PAL3 Series 1.5 RSI 85 cm	2.4.63	2.4.63
G7368A	PAL3 Series 1.5 RSI 120 cm	2.4.63	2.4.63
G7370A	PAL3 Series 1.5 RTC 120 cm	2.4.63	2.4.63
G7366A	PAL3 Series I LSI	2.4.5	2.4.5
G7367A	PAL3 Series I RSI 85 cm	2.4.5	2.4.5
G7368A	PAL3 Series I RSI 120 cm	2.4.5	2.4.5
G7370A	PAL3 Sereis I RTC 120 cm	2.4.5	2.4.5

References

1. Botha, R. A.; Eloff, J. H. P. Separation of Duties for Access Control Enforcement in Workflow Environments. *IBM Systems Journal– End-to-end security* **2001**, *40(3)*, 666–682.
2. U.S. Food and Drug Administration. CFR - Code of Federal Regulations Title 21. Title 21—Food and Drugs, Chapter I—Food and Drug Administration Department of Health and Human Services, Subchapter A— General. Part 11 Electronic Records; Electronics Signatures. [Online] https://www.accessdata.fda. gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11.
3. European Commission Health and Consumers Directorate-General. Public Health and Risk Assessment. Pharmaceuticals. EudraLex. The Rules Governing Medicinal Products in the European Union. Volume
4. Good Manufacturing Practice. Medicinal Products for Human and Veterinary Use. Annex 11. Computerised Systems. [Online] https://ec.europa.eu/health/sites/default/files/files/eudralex/vol-4/annex11_01-2011_ en.pdf.
5. Agilent OpenLab Server and OpenLab ECM XT Administration Guide. https://www.agilent.com/cs/library/usermanuals/public/openlab-server-ecmxt-v2.8-administration-guide-en.pdf.

www.agilent.com/gcms/masshunter-acquisition-software

DE79436489

Printed in the USA, March 12, 2025
5994-8187EN

Agilent
Trusted Answers