

Agilent G1732BA MSD Security ChemStation

Manager's Guide



Agilent Technologies

Notices

© Agilent Technologies, Inc. 2008

No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Agilent Technologies, Inc. as governed by United States and international copyright laws.

Manual Part Number

G1732-90012

Edition

First Edition, May 2008
Replaces part no. G1732-90008, Nov. 2005

Printed in USA

Agilent Technologies, Inc.
2850 Centerville Road
Wilmington, DE 19808-1610 USA

Acknowledgements

Microsoft®, Windows®, Windows XP®and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

InstallShield® is a registered US trademark of InstallShield Corporation.

Software Revision

This manual is valid for B.02.xx revisions of the Agilent G1732BA MSD Security ChemStation software, where xx refers to minor revisions of the software that do not affect the technical accuracy of this manual.

Warranty

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Agilent disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Agilent shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Agilent and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

Restricted Rights Legend

If software is for use in the performance of a U.S. Government prime contract or subcontract, Software is delivered and licensed as "Commercial computer software" as defined in DFAR 252.227-7014 (June 1995), or as a "commercial item" as defined in FAR 2.101(a) or as "Restricted computer software" as defined in FAR 52.227-19 (June 1987) or any equivalent agency regulation or contract clause. Use, duplication or disclosure of Software is subject to Agilent Technologies' standard commercial license terms, and non-DOD Departments and Agencies of the U.S. Government will receive no greater than Restricted Rights as defined in FAR 52.227-19(c)(1-2) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Safety Notices

CAUTION

A **CAUTION** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a **CAUTION** notice until the indicated conditions are fully understood and met.

WARNING

A WARNING notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

In this guide. . .

This Manager's Guide contains information and procedures needed for the administration of the G1732BA MSD Security ChemStation.

1 Introduction

Chapter 1 describes the purpose of the MSD Security ChemStation.

2 21 CFR Part 11 Compliance

Chapter 2 compares the requirements of the 21 CFR Part 11 regulations with the features of the Agilent G1732BA MSD Security ChemStation. It identifies those requirements that are satisfied by the software and those that are the responsibility of the users, system administrators, and the organization that employs them.

3 Procedures

Chapter 3 describes administrative and configuration tasks that are performed by a MSD Security ChemStation Manager, such as instrument configuration and user management.

Contents

1 Introduction

The MSD Security ChemStation 8

The MSD Security ChemStation File Structure 13

Required Standard Operating Procedures 16

2 21 CFR Part 11 Compliance

Subpart A–General Provisions 18

Subpart B–Electronic Records 22

Subpart C–Electronic Signatures 27

3 Procedures

To Configure an Instrument 32

To Set or Change the Default Printer 34

To Manage Users 35

To Manage Passwords 37

To Unlock a Method 39

To Uninstall MSD Security ChemStation Software 40

1 Introduction

The MSD Security ChemStation 8
- Capabilities and limitations 8
- Product design 8
- Security groups and users 11
- The Windows Administrator 12
- Electronic records and signatures 12

The MSD Security ChemStation File Structure 13
- Versioning 13
- Version files 13
- Version file name syntax 13
- Run directories 14

Required Standard Operating Procedures 16

NOTE The MSD Security ChemStation is software that should be installed on a computer dedicated to this specific application. This software can support either GPIB or local LAN acquisition from one GC/MSD system. Other applications and/or wide area network access should be performed on other computers.

The Agilent G1732BA MSD Security ChemStation and the G1742BA MSD Security ChemStation Upgrade are designed to support the requirements of the U.S. Food and Drug Administration (FDA) regulations on the handling of electronic records and electronic signatures published as 21 CFR Part 11.

The system, hereafter referred to as the MSD Security ChemStation, acquires data from one Agilent Mass Selective Detector (MSD) with an Agilent 6850, 6890, or 7890A Series Gas Chromatograph (GC).

The MSD Security ChemStation

The MSD Security ChemStation is a conventional MSD ChemStation with support for U.S. Food and Drug Administration (FDA) 21 CFR Part 11 regulations. These regulations govern the use of electronic records, electronic signatures, and auditability of systems used in regulated laboratories.

Capabilities and limitations

The MSD Security ChemStation supports the same hardware as the standard MSD Productivity ChemStation. However, it is focused on GC/MSD signal acquisition and will acquire GC detector data only in combination with GC/MSD data acquisition. It will also import and process existing GC/MSD files that contain GC data.

Product design

The MSD Security ChemStation is a standalone application that addresses the requirements of 21 CFR Part 11 through a combination of operating system facilities and programmatic controls. It runs under Microsoft Windows® operating system and takes advantage of the inherent user access security capabilities of Windows. File access privileges are defined on a per user basis for data files, methods, sequences, and results. The operating system security features protect data and manage user access to it. User-based file access is achieved by making use of individual file and folder permissions, and local user and group management.

A mandatory login requires users to enter a user ID and password when starting the application. The user must be a member of a MSD Security ChemStation user group. The access level is determined by the user group membership. The application login is independent of the user who logged in to the operating system.

To discourage unauthorized access, write access to the application and its files is restricted to an internal user called “MSCFR”. This local user is created at installation and has ownership of the MSDChem directory. (Default directory name: MSDChem.)

CAUTION If ownership of this directory is ever changed by the Windows Administrator, the system is immediately compromised and will no longer be 21 CFR Part 11 compliant.

The password of this user is set to a value known only within the MSD Security ChemStation application. It is Agilent-confidential and is not disclosed to other parties.

This arrangement discourages unauthorized access. Even a Windows Administrator cannot access the files without first taking ownership of the MSDChem directory. If ownership of the MSDChem directory is changed, Log entries will show the change of ownership and reveal that security has been compromised. Also, in that case, the following message is displayed at startup of the software: **File system ownership has been changed. System is running in insecure mode.**

If this happens, the only way to restore the system to a secure mode is to uninstall the software, then reinstall it. See page 40 for details on uninstalling the software.

The only Windows group whose members have access to the MSD Security ChemStation file system are Windows BackupOperators. With this design it is possible to implement advanced backup strategies, e.g. with "incremental backup" where already archived files get flagged. Since 21 CFR Part 11 requires that procedures have to be in place to ensure data integrity, it is important to notice that with this design, BackupOperators can modify the ChemStation data without logging on the MSD Security ChemStation and generating audit trails. Thus there should be a Standard Operating Procedure (SOP) in place stating that all ChemStation operators should not be a member of the BackupOperators group. This is because a ChemStation operator could have an interest in modifying data to match some specification. The SOP could

read, e.g. "The system administrator should restrict regular MSD Security ChemStation operators and their managers from modifying data through technical controls."

The preferred means of archiving and restoring data is through the Archive/Restore features in the application, which use the impersonated MSCFR user for appropriate access. System backup can also be used to preserve the file system, as the BACKUP OPERATOR has read access to it. However, the file system cannot be restored incrementally from such a backup, as the BACKUP OPERATOR does not have write access to it.

The application provides audit facilities for recording events during operation. In addition, the Windows Operating System Event Logs record logins and logouts of users, and other significant security events. With the application audit log and the System Event Logs, it possible to review access to the system for security audits.

Security groups and users

The install process creates three local groups (Operators, Analysts, and Managers) corresponding to three levels of user privileges supported by the MSD Security software. Membership of users in these groups determines the level of use that they are permitted in the software application.

Users are created by a Windows Administrator and, if they are to have access to the MSD security system, they are assigned to one of the follwing groups:

MSDOperator Members of this group (Operators) acquire data using existing methods and sequences. An Operator has limited control over GC and MSD parameters, but cannot make permanent changes to methods. Operators can reprocess and integrate data as well as apply manual integration.

MSDAnalyst These group members (Analysts) have all the capabilities of an Operator but can also create, modify, and save methods, tune the MSD, set up retention time locking, import and export files, archive and restore data, and perform other tasks.

MSDManager These group members (Managers) have all the capabilities of both the Operator and Analyst. A Manager also has access to the system configuration and the command line.

Users that are not a member of one of these groups have no access to the MSD Security ChemStation. This prevents unauthorized persons from using the software or making changes to methods, data, and sequences.

NOTE Members of the Windows BackupOperators group have access to the MSD Security data files. See page 9 for details.

NOTE Before going into routine use, it is recommended to disable the built-in Manager, Analyst, and Operator. See "Disabling a user" on page 36.

The Windows Administrator

The Windows Administrator manages all MSD Security ChemStation users and owns the security policies. For administrative tasks, the administrator is required to be a member of the local Windows Administrator group. However, the Windows Administrator does not necessarily need to be a member of any of the MSD Security ChemStation user groups.

Windows Administrators are responsible for overseeing ChemStation usage and managing user access.

A Windows Administrator should be available whenever the system is in use to deal with unexpected events, such as an account lockout, in a timely manner. We recommend having more than one administrator to ensure that there is sufficient coverage for these tasks.

Electronic records and signatures

Methods, sequences, and the data files derived from them are stored as Electronic Records. These records can be electronically signed for approval. A signature is mandatory whenever they are created, modified, or deleted.

The MSD Security ChemStation makes use of electronic signatures. The FDA regulations require that:

> **Persons using electronic signatures shall, prior to or at the time of such use, certify 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.**

The organization should have, as part of their SOPs, a process by which individual system users acknowledge in writing that they accept their full name, when authenticated by user ID and password as an electronic signature, with the same validity as their handwritten signature.

The MSD Security ChemStation File Structure

Versioning

Every time a change is made to a method, a new method version is created by the system. Data files are linked to the exact method version that created them, so they can be reprocessed in exactly the same way at any time.

Version files

A version file is a snapshot of the state of data recorded in the **.m** (method), **.d** (data), or **.s** (sequence) files.

Method and data version files are in the VERSIONS subdirectories of **.m** (method) and **.d** (data) directories.

Sequence version files are in the VERSIONS subdirectory of the sequence directory.

Version file name syntax

<prefix>-<version>.<suffix>

where

<prefix> = **METH**method version
SEQsequence version
ACQacquisition data version
PROCresults data version

<version> = **<year>-<month>-<day>-<hour><minute><second><msec>UTC**

- **<year>** = 4-digit year
- **<month>** = 2-digit zero left padded month
- **<day>** = 2-digit zero left padded day of month
- **<hour>** = 2-digit zero left padded 24-hour clock hour
- **<minute>** = 2-digit zero left padded minutes
- **<second>** = 2-digit zero left padded seconds
- **<msec>** = 3-digit zero left padded milliseconds
- **UTC** = a constant, included as a reminder

<suffix> = a combination of **r**, **v**, and **s**, indicating the kind of hash blocks appended to the file

- **r** = reference block, contains link to other files
- **v** = validation block, system-applied signature of user of record, no explicit authentication
- **s** = signature block, interactively applied signature of user of record, explicit authentication by signature panel

There is no space or other separator in the time field: 152903005 is 15:29:03.005 in 24-hour clock format (a little before 3:30PM). 043000000 is 4:30AM. All times are Universal Coordinated Time (Greenwich Mean Time).

Dashes, UTC, and period are explicit.

The names sort by **<prefix>**, then oldest to newest **<version>**, in a simple alphabetical file listing. The names are unique on a ChemStation. Note that **<version>** does not necessarily coincide with the file creation or modification dates—it is generated in the software command that eventually saves the file.

Run directories

Run directories are where the results of Run Method, Run Sequence, or Import Data Files are stored. The data path to the run directory is configurable. (See the User's Guide for details on setting the data path.)

Run directory name syntax

<prefix>-<version>

where

<prefix> = **Run** results of Run Method
Seq results of Run Sequence
Imp results of Import Data File

<version> = As described above

A **Run-<version>** directory contains the data file and a copy of the method version run on that data.

A **Seq-<version>** directory contains data files, a copy of the sequence that generated the data files, and a copy of each method used in the sequence.

An **Imp-<version>** file contains one data file, and may contain methods copied there after the data file was imported.

There may be multiple versions in the VERSIONS subdirectories within the data, method, and sequence files in these run directories.

Required Standard Operating Procedures

The implementation of 21 CFR Part 11 consists of procedural controls in the laboratory (SOPs, access security rules), and technical controls built into the software.

The design of the Agilent MSD Security ChemStation is based on a closed system that uses procedural controls, such as access security rules established in the laboratory that only give authorized individuals physical access to the systems.

Procedural controls are manifested through SOPs created and enforced by the system owners.

For example, to use electronic rather than handwritten signatures, system owners must create and enforce a written SOP that require users to acknowledge that their electronic signature is to be regarded as equivalent to their handwritten signature. Such signatures must be reported to the FDA before they can be used. It is the responsibility of system owners to ensure that this is done.

Chapter 2 discusses the regulations mandated by the FDA in more detail. In many cases, the notation indicates “Responsibility of the organization”, “Responsibility of an MSDManager”, or something similar. Such responsibilities require a written SOP.

With appropriate SOPs in place, the MSD Security ChemStation enables users to work in compliance with 21 CFR Part 11.

2
21 CFR Part 11 Compliance

Subpart A–General Provisions 18
Sec. 11.1 Scope 18
Sec. 11.2 Implementation 19
Sec. 11.3 Definitions 20
Subpart B–Electronic Records 22
Subpart C–Electronic Signatures 27

The opening paragraph of the U.S. Food and Drug Administration regulations on electronic records and electronic signatures states "The(se) regulations . . . set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper."

The Agilent Technologies G1732BA MSD Security ChemStation and the G1742BA MSD Security ChemStation Update products provide the tools needed to comply with 21 CFR Part 11. When properly used, they produce electronic records and electronic signatures that meet the criteria stated above.

21 CFR Part 11 consists of three parts:

Subpart A–General Provisions states the scope and purpose of the regulations and defines some technical terms.

Subpart B–Electronic Records states the requirements for reliable, trustworthy electronic records.

Subpart C–Electronic Signatures states the requirements for electronic rather than handwritten signatures on electronic records.

Subpart A–General Provisions

This section contains the complete text of 21 CFR Part 11, Subpart A–General Provisions, which defines the purpose, scope, and some technical terms used in the regulations.

Sec. 11.1 Scope

1. The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.
2. This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.
3. Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.
4. Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with Sec. 11.2, unless paper records are specifically required.
5. Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

Sec. 11.2 Implementation

1. For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.
2. For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:
   a. The requirements of this part are met; and
   b. The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (for example, specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (for example, method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

Sec. 11.3 Definitions

1 The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

2 The following definitions of terms also apply to this part:

- **a** Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).
- **b** Agency means the Food and Drug Administration.
- **c** Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.
- **d** Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.
- **e** Digital signature means an electronic signature based on cryptographic methods of originator authentication, computed by using a set of rules and parameters so that the identity of the signer and the integrity of the data can be verified.
- **f** Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.
- **g** Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.
- **h** Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal

mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

i Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Subpart B–Electronic Records

Subpart B is concerned with the controls needed to ensure data integrity, user responsibility, and related matters.

Some additional definitions are needed for the Agilent product:

- Windows user–A person who has a login name and password for Windows.
- Security user–A Windows user with a login name and password that permit use of the MSD Security ChemStation software. Security users are classified as Managers, Analysts, or Operators.
- Windows Administrator–An individual, who is a member of the Windows Administrator group, with responsibility for maintaining system security.
- Organization–The entity, usually a company, that owns the security system.

NOTE MSDManager group members must explicitly be made members of the local Windows Administrator group if the Windows Administrator and MSD Security ChemStation Manager roles are to be held by the same individual.

Table 1 compares the full text of the subpart with the MSD Security ChemStation.

Table 1 21 CFR Part 11, Subpart B–Electronic Records

Subpart B–Electronic Records text Sec. 11.10 Controls for closed systems	Agilent product
Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	Responsibility of the organization. The design of the Agilent MSD Security ChemStation is based on a closed system which is achieved by implementing procedural controls such as access security rules established in the lab, that only give authorized individuals physical access to the systems.
a Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Agilent delivers a fully qualified data handling system together with all necessary services, which are needed to implement such a system to meet the requirements of the FDA regarding 21 CFR Part 11. Electronic records generated by the application are stored in a protected proprietary format using a SHAI secure hash algorithm. If such a record is altered through another application, this will be detected by the system when trying to read the record.
b The ability to generate accurate and complete copies of records in both readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	The electronic record, associated meta data, audit trail, and electronic signature can be reviewed on screen. Printed or screen-viewable versions of reports representing the electronic record can be regenerated from the versions and compared to the originals. To read the electronic format the Agilent MSD Security ChemStation is required.
c Protection of records to enable their accurate and ready retrieval throughout the records retention period.	The Agilent product provides archive/restore functionality for electronic records. Full protection in terms of regulatory agencies also includes application of additional procedural controls, which the organization is responsible for.
d Limiting system access to authorized individuals.	Unique combination of login name and user-supplied password required.

Table 1 21 CFR Part 11, Subpart B–Electronic Records (continued)

Subpart B–Electronic Records text Sec. 11.10 Controls for closed systems		Agilent product
e	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	Audit trails are generated automatically and independent of the user. Record changes create a new version and an audit trail entry; the original version is not altered. Retention is the responsibility of the organization. Each record is stored along with its creation date and time stamp. The associated audit trail lists all modifications with date/time stamp and the user name of the user doing the change.
f	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	The application controls the sequencing of operations to ensure appropriate behavior.
g	Use of 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.	Check is by mandatory login to the application with login name, password, and user classification (Manager, Analyst, Operator).
h	Use of device (for example, terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	User input is strictly controlled. Input data is restricted to acquisition from the MSD or by import with electronic signature attached. Bi-directional connectivity check to the instrument before starting a run. GPIB address or IP address clearly identifies the instrument.
i	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Responsibility of the organization.
j	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	Responsibility of the organization.

Table 1 21 CFR Part 11, Subpart B–Electronic Records (continued)

Subpart B–Electronic Records text Sec. 11.10 Controls for closed systems	Agilent product
k Use of appropriate controls over systems documentation including:	
1 Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	Responsibility of the organization.
2 Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Responsibility of the organization.
Sec. 11.30 Controls for open systems	
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ 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. Such procedures and controls shall include those identified in sec. 11.10, as appropriate, and 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.	The MSD Security ChemStation is designed to operate in a closed system only.
Sec. 11.50 Signature manifestations	
a Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:	
1 The printed name of the signer;	Full user name is stored when user is created and applied in audit trail.
2 The date and time when the signature was executed; and	Entered by the system.

Table 1 21 CFR Part 11, Subpart B–Electronic Records (continued)

Subpart B–Electronic Records text Sec. 11.10 Controls for closed systems	Agilent product
3 The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Required input at time of signature.
b The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	Electronic signatures cannot be overwritten, modified, or deleted.
Sec. 11.70 Signature/record linking	
Electronic signatures and handwritten signatures executed to electronic records shall be 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.	All signatures are electronic, encrypted, and attached to the electronic records. Printed records include the hash value of the electronic record and signature information.

Subpart C–Electronic Signatures

Subpart C is concerned with the creation and use of electronic signatures as valid substitutes for handwritten signatures. Table 2 compares the full text of the subpart with the MSD Security ChemStation.

Table 2 21 CFR Part 11, Subpart C–Electronic Signatures

Subpart C–Electronic Signatures text	Agilent product
Sec. 11.100 General requirements	
a Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Responsibility of the system administrator.
b Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	Responsibility of the organization.
c Persons using electronic signatures shall, prior to or at the time of such use, certify 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.	Responsibility of the organization and each system user (Manager, Analyst, Operator) who uses an electronic signature.
1 The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.	Responsibility of the organization and each system user (Manager, Analyst, Operator) who uses an electronic signature.
2 Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	Responsibility of the organization and each system user (Manager, Analyst, Operator) who uses an electronic signature.

Table 2 21 CFR Part 11, Subpart C–Electronic Signatures (continued)

Subpart C–Electronic Signatures text	Agilent product
Sec. 11.200 Electronic signature components and controls	
a Electronic signatures that are not based upon biometrics shall:	
1 Employ at least two distinct identification components, such as an identification code and password.	System requires a login name, which is also known to the Windows Administrator, and a password, which is known only to the individual.
(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.	The MSD Security ChemStation always requires both signature components.
(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	The MSD Security ChemStation always requires both signature components.
2 Be used only by their genuine owners; and	Each individual is responsible for keeping both signature components secret.
3 Be 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.	Responsibility of the organization. Two tokens, user ID and password, are required for a signature. The password is known only to the user.
b Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Biometric signatures are not supported.

Table 2 21 CFR Part 11, Subpart C–Electronic Signatures (continued)

Subpart C–Electronic Signatures text	Agilent product
Sec. 11.300 Controls for identification codes/passwords	
Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:	
a Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	Identification code (login name) is checked for uniqueness at time of assignment.
b Ensuring that identification code and password issuances are periodically checked, recalled, or revised (for example, to cover such events as password aging).	Responsibility of the organization. SOPs define the password policies implemented as part of the local security policies. Identification codes (login names) are responsibility of a Windows Administrator. Passwords must be changed by users at specified intervals. Proposed password must not duplicate recent values.
c Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised 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.	Responsibility of a Windows Administrator. Devices such as token cards are not supported.
d Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	Windows security logging and account security settings protect and record password and user ID use.

Table 2 21 CFR Part 11, Subpart C–Electronic Signatures (continued)

Subpart C–Electronic Signatures text	Agilent product
Sec. 11.300 Controls for identification codes/passwords	
e 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.	Such devices are not supported.

3 Procedures

To Configure an Instrument 32
To Set or Change the Default Printer 34
To Manage Users 35
- Creating a new user 35
- Disabling a user 36

To Manage Passwords 37
- Password rules 37
- Password aging 37
- Account lockout 38
- Good password practices 38
- Final word 38

To Unlock a Method 39
To Uninstall MSD Security ChemStation Software 40

To Configure an Instrument

Use the following procedure to configure an instrument controlled by the MSD Security ChemStation software.

The Agilent MSD Configuration program allows you to configure an instrument or to view an instrument configuration entered previously.

To configure an instrument:

1. From the Windows **Start** menu, open the MSD Configuration program. Select **Start/All Programs/MSD Security Chemstation/Agilent MSD Configuration.**
2. Log on to the system:
   - If you have not changed the default login name and password for the Manager, enter: **Manager** for the full name, and **CS02security** (case-sensitive) as the password.
   - If you have changed the default Manager login name and password, use that updated information.
3. To configure an instrument, select **1** from the toolbar near the top of the window.
4. You must enter a name for the instrument. Make sure that the **Offline Instrument** option is **not** selected.
5. In the Mass Spectrometer box, select the model number of your MSD and then enter the associated IP Address.
6. In the Gas Chromatograph box, select the model number of your GC and then enter the associated IP Address.
7. Select **OK** to close the MSD Configuration Editor and click **Yes** when prompted.

NOTE The following icons will appear on the desktop: **Instrument #1** and **Instrument #1 Data Analysis**, assuming that you used the default instrument name.

8 Change the Manager name and password, if you have not already done so.

   a On the Control Panel, select **Administrative Tools/Computer Management/System Tools/Local Users and Groups/Users**.

   b Double-click the **Manager** user ID.

   c Change **Full Name** to the actual full name of the person.

   d Click **OK**.

   e Right-click **Manager**.

   f Select **Set Password**. Change the password to something other than the default. See "Password rules"on page 37.

9 Disable the other default accounts.

   a On the Control Panel, select **Administrative Tools/Computer Management/System Tools/Local Users and Groups/Users**.

   b Right-click on **Analyst**. Select **Properties**.

   c Check **Account is disabled**. Click **Apply**, then **OK**.

   d Repeat for user **Operator**.

   e Close the screens.

To Set or Change the Default Printer

NOTE The MSD Security ChemStation printer must be a local printer; the software does not support network printers.

The default printer is defined in the Windows Control Panel. The Set Default Printer icon transfers this information into the security software.

Use this procedure to set or change the default printer:

1. Select **Start/Printers and Faxes**.
2. From the **Printers and Faxes** dialog box, select a local printer (i.e., one that is connected directly to the MSD Security ChemStation computer, and not connected over a network).
3. Select **File/Set as Default Printer** or right-click on the printer and select **Set as Default Printer** from the **Context** menu.
4. Select **File/Close** to close the Printers dialog box
5. Select **Start/Programs/MSD Security ChemStation/Set Default Printer** or click the **Set Default Printer** icon on the desktop to change the MSD Security ChemStation default printer to the new Windows default printer.

NOTE A DOS window is displayed for a short time while the printer is being configured. It confirms that the default printer settings have been applied.

To Manage Users

Creating a new user

To create a new MSD Security ChemStation user:

1 Log on to Windows as a Windows Administrator or other user with administrative privileges.

The login name of a new user should be known only to the system administrator and the individual user.

2 Create the user.

- **a** Select **Start**. Right-click **My Computer** and select **Manage**.
- **b** Open **Local Users and Groups**.
- **c** Click on the **User** folder.
- **d** On the **Action** menu, select **New User**.
- **e** Enter the user name in the **User name** box. **User name** is the login identification.
- **f** Enter the user's full name in the **Full name** box. **Full name** is required by the FDA and the MSD Security ChemStation. The **Full name** represents the user and will be displayed on screen (security monitor) and printed in reports.
- **g** Enter a description in the **Description** box. (Optional)
- **h** Type a password in the **Password** box. It can be replaced by the password chosen by the user at the first log on. The **Password** must comply with the "Password rules"on page 37.
- **i** Click **Create**.
- **j** Click **Close**.

3 Assign the user to a security group.

- **a** Click **Groups** to display the available group names.
- **b** Select one of the MSD Security ChemStation groups: **MSDOperator, MSDAnalyst,** or **MSDManager**. Hold down the **Ctrl** key for multiple selections. If a user is added to more than one group, the user will have the capabilities of the

most powerful group selected. The user may want to log in at times with a lower capability.

c On the **Action** menu, select **Add to group**.

d Click **Add**. Type in the **User name** (*not* the **Full name**) and click **OK**.

e Close the open screens.

Disabling a user

As system users change jobs or leave the laboratory, it will be necessary to remove them from the set of active MSD Security ChemStation users. This is an important administrative responsibility to ensure that invalid and old passwords and accounts do not remain in the system.

The procedure described disables the user account and removes the name from the active users, but does not delete it.

CAUTION Unused accounts should be *disabled,* not *deleted,* so that traceability in audit trails is maintained.

To disable an MSD Security ChemStation user:

1 Log on to Windows as a Window Administrator or other user with administrative privileges.

2 On the Control Panel, select **Administrative Tools/Computer Management/Local Users and Groups**.

3 Double-click **Users**.

4 Right-click the user's name.

5 Select **Properties**.

6 Check **Account is disabled**, click **Apply**, and click **OK**.

To Manage Passwords

Passwords control user access to the MSD Security ChemStation software. It is important to control the use of passwords to make it very difficult for an unauthorized user to gain access.

CAUTION Many of the default settings mentioned below can be changed by a Windows Administrator, either to make the rules more rigid or less stringent to make them comply with your local security policies.

Password rules

Each new user is required to select a password at first log on. The new password should be known only to that user and should be chosen to make it difficult to guess.

The default password settings applied by the MSD Security ChemStation during installation are:

- Must be at least six characters long
- Must contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Nonalphanumeric characters (for example, !, $, #, %)
- Must not contain all or part of your **user name**
- Must be significantly different from your 24 most recent passwords

Password aging

A new password is good for no longer than 90 days. At the end of that time, a user will be required to select a new password.

Account lockout

If a user makes five unsuccessful attempts to login during a 30 minute period, the account will be locked out for 5 hours or until a Windows Administrator unlocks the account.

To unlock an account:

1. Log on to Windows as a Windows Administrator or other user with administrative privileges.

   The login name of a new user should be known only to the system administrator and the individual user.

2. Create the user.
   a. Select **Start**. Right-click **My Computer** and select **Manage**.
   b. Open **Local Users and Groups**.
   c. Click on the **User** folder.
3. Left-click to open the **Users** folder.
4. Double-click the locked user ID.
5. When the screen appears, uncheck the **Account is Locked Out** box.

Good password practices

To help protect the system:

- Never write down your password.
- Never reveal your password to someone else.
- Change your password every 60 to 90 days.
- Be sure that your password is different from any other passwords you use.

Final word

Attacks on passwords use three methods: guessing, dictionary-based attack, and brute force (try all possible combinations).

The rules of the MSD Security ChemStation software, as previously outlined, are intended to prevent the first two methods from being successful. Brute force can always break a password, but it can take months to do so with a properly chosen password.

To Unlock a Method

You may encounter a message stating that a method is locked. If so, that method cannot be used until it is unlocked.

A method is unlocked by executing **cfr_unlockall** in the command line. This must be done by a member of the **MSDManager** group.

To Uninstall MSD Security ChemStation Software

It may be necessary at some point to remove the MSD Security ChemStation software. The uninstall utility does this without removing any methods, sequences, or data.

Uninstall performs two functions:

- It deletes the executable software part of the ChemStation
- It removes the security restrictions on the MSDChem directory

The first task deletes all MSD Security ChemStation programs and some related files from the disk in preparation for installing a new revision of the software. It does not affect any files (methods, sequences, data) that were created by that software.

The second task makes the entire **MSDChem** file tree, which no longer contains any of the programs, accessible to ordinary Windows functions such as copy, edit, delete, and so on.

To uninstall the MSD Security ChemStation software:

1. Log on as a Windows Administrator.
2. Save important information.
   a. Backup or archive any data, methods, libraries, or other files or directories that you want to save.
   b. Close all MSD Security ChemStation applications.
3. Remove the ChemStation software.
   a. On Control Panel, select **Add or Remove Programs**.
   b. Select **Agilent MSD Security ChemStation G1732BA B.xx.xx**.
   c. Click **Change/Remove**.
   d. When the **Modify/Repair/Remove** screen appears, select **Remove** and click **Next**.
   e. Confirm the uninstall. (The uninstall process may take several minutes.)
   f. When the **Maintenance Complete** screen appears, click **Finish** to reboot the computer.

4 Log on again using the same login name as before.

5 Remove MSD users and groups.

   a On Control Panel, select **Administrative Tools**, then select **Computer Management**.

   b Open **Local Users and Groups**.

   c Click **Users**.

   d Delete user **MSCFR**.

   e Delete all MSD Security ChemStation users. (To identify the users, examine the **Description** column. If it mentions MSD Security ChemStation, remove that user.)

   f Double-click **Groups**.

   g Delete groups **MSDAnalyst**, **MSDOperator**, and **MSDManager**.

   h Close all screens.

6 Remove icons from the desktop. (Right-click and delete any MSD Security icons on the desktop.)

7 Remove the MSD Security ChemStation Start menu item.

   a Execute **Start/All Programs**.

   b Right-click and delete **MSD Security ChemStation**.

8 Rename the MSDChem directory. The purpose is to make the name **MSDChem** available for the new installation.

   a Open Windows Explorer.

   b Right-click the **MSDChem** directory and select **Rename**.

   c Supply a new name.

This completes uninstallation of the MSD Security ChemStation software. If you wish to completely remove all Agilent MSD Security ChemStation components from your PC, you must also uninstall the Agilent I/O Libraries and the Agilent Bootp Service, if installed. See steps 9 and 10 below.

9 Uninstall the Agilent I/O Libraries (SICL drivers). From **Add or Remove Programs**, select **Remove SICL Drivers** or **Agilent I/O Libraries/Remove**, as applicable.

10 Uninstall the Agilent Bootp service. From **Add or Remove Programs**, select **Agilent Bootp Service/Remove**. This completes

uninstallation of MSD Security ChemStation software and all related components.



Agilent Technologies

© Agilent Technologies, Inc.

Printed in USA, May 2008

G1732-90012