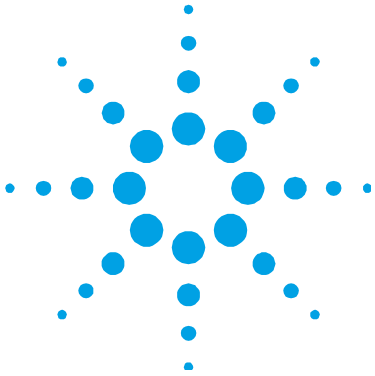


Spectroscopy Configuration Manager (SCM) Software

21 CFR Part 11 Compliance Booklet

Agilent Technologies

Notices

Manual Part Number

G9272-90009

Edition

First edition, September 2014

Printed in USA

Agilent Technologies Australia (M) Pty Ltd

679 Springvale Road

Mulgrave, Victoria, 3170, Australia

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.

Contents

This page is intentionally left blank.

1. Introduction

Background

The Food and Drug Administration (FDA) of the United States (USA) regulates the food and drug industry of the USA with the Code of Federal Regulations (CFR). The FDA is within the Department of Health and Human Services and manages the Center for Devices and Radiological Health.

Title 21 of the CFR describes the requirements and regulations for the food and drug industries. For food and drugs to be used within the USA, they must comply with the requirements of this regulatory body. In particular, manufacturers must register with the FDA and obtain approval for a license to distribute their product within the USA.

Internationally, FDA regulatory compliance is recognized as a benchmark for the pharmaceutical industry with respect to research, drug development, drug manufacture and sales and marketing of pharmaceutical products.

Part 11 of Title 21 of the Code of Federal Regulations (referred to as 21 CFR Part 11)[1] was released August 20, 1997 and revised April 1, 2005. Part 11, 'Electronic Records; Electronic Signatures' states the rules, definitions and guidelines under which the FDA,

'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.'[1]

The rule defines a standard under which an organization must operate in order to comply with 21 CFR Part 11 and obtain FDA accreditation (licensing).

The 'Preamble' to 21 CFR Part 11 states that,

'the use of electronic records as well as their submission to the FDA is voluntary.'[2]

However, where an organization does decide to use electronic records and electronic signatures, all requirements of the rule must be met in full for all electronic records.

Globally, the most stringent regulatory compliance standards are applied within the Pharmaceutical Industry. The FDA's 21 CFR Part 11 rulings are recognized as being at the forefront of Pharmaceutical compliance with respect to product safety. Subsequently, Agilent's instrument development and technology is focused towards facilitating 21 CFR Part 11 regulatory compliance.

[1] Code of Federal Regulations, Title 21, Food and Drugs, Part 11 'Electronic Records: Electronic Signatures Final Rule', Federal Register 62 (54), 13429-12466. A copy of the final rule can be found at: www.fda.gov

[2] ibid, p 13430.

How to Use This Document

It is important to read this document thoroughly, as failure to perform certain tasks could mean that Agilent's software installation will not assist in meeting the requirements of the 21 CFR Part 11 rule.

This document is aimed to provide scientists, database Administrators and Network Administrators with accurate information as to how Agilent software packages can be readily and efficiently set up in order to comply with 21 CFR Part 11. The majority of information within this document will be easily understood by a scientist or an instrument operator. Some sections of this document describe specific requirements for software set up, which may be more easily understood and applicable to IT personnel. Overall, the information herein will provide the Network Administrator and the Spectroscopy Configuration Manager (SCM) Administrator with the appropriate information, to set up Agilent's software in order to assist the operator to achieve 21 CFR Part 11 compliance.

NOTE The 21 CFR Part 11 guidelines represent only one regulatory body. Agilent's software packages may be applicable to other regulatory guidelines. Contact your local Agilent representative in order to discuss this further.

Applicable Software Packages

This publication describes the approach Agilent has undertaken to assist customers in achieving 21 CFR Part 11 regulatory compliance.

The applicable Agilent software packages that utilize the Spectroscopy Configuration Manager are:

- ICP Expert version 7 or greater
- SpectrAA CFR
- ICP Expert II
- UV Dissolution
- UV Fiber Optic Dissolution
- Cary WinUV Pharma 4.10 or greater

This document provides the following information:

- A detailed description as to how Agilent software (as listed above) assists the operator to meet the requirements of the 21 CFR Part 11 rulings (Section 2 and 3).
- Recommended, on-going Standard Operating Procedures (SOPs) to complement the software and instrument system (Section 4).
- A Compliance Matrix which compares the Agilent software directly with the 21 CFR Part 11 FDA regulation (Section 5).

NOTE Throughout this document, where the term 'UV Dissolution' software is used, this refers to both the UV Dissolution software and the UV Fiber Optic Dissolution software.

System Requirements

The Agilent software packages have been validated on Microsoft® Windows® XP Operating System (32-bit) with Service Pack 3 (except those noted below).

Cary WinUV Pharma version 4.20 software was validated using Microsoft Windows 7 Operating System (32-bit only).

Cary WinUV Pharma version 5.0.0.1005 software for the Agilent Cary 60 UV-Vis spectrophotometer has been validated using Microsoft Windows 7 Operating System (64-bit SP1 only, Enterprise and Pro). This software package will not run on Windows 7 Operating System (32-bit) or Windows XP Operating System (32-bit SP3).

ICP Expert version 7.0 or greater, ICP Expert II version 2.0 software or greater and SpectrAA CFR version 5.2 or greater were validated on Microsoft Windows 7 Operating System (64-bit SP1 only, Enterprise and Pro). These software packages will not run on Windows 7 Operating System (32-bit) or Windows XP Operating System (32-bit SP3).

The 21 CFR Part 11 software was validated under the following configuration:

- Windows 2003 Native Directory – Single Forest / Single Domain model environment (Cary WinUV Pharma version 5.0 and earlier, previous versions of ICP Expert, ICP Expert II version 2.0 or greater and SpectrAA version 5.2 or greater).
- Windows 2008 Native Directory – Single Forest / Single Domain model environment (ICP Expert version 7.0 or greater, ICP Expert II version 2.0 or greater, SpectrAA version 5.2 or greater, Cary WinUV Pharma version 5.0.0.1005 and greater).

Compliance with the 21 CFR Part 11 rule can only be assured if the Agilent application is installed on a compatible Microsoft Windows operating system using compatible databases. The operating system must also be configured in accordance with Agilent's recommended configuration.

NOTE Throughout this document, 'Windows' refers to Windows 7 32-bit SP1 or Windows 7 64-bit SP1, unless otherwise specified.

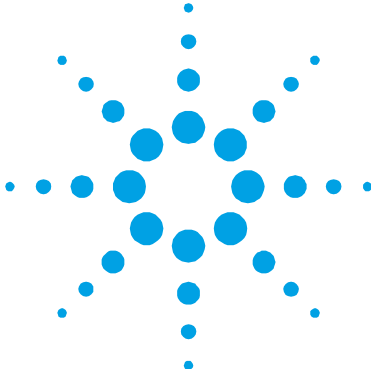
NOTE The most up to date details of the recommended or certified operating systems required for operating the various software packages for all Agilent spectrometers are listed on the Agilent Technologies, Inc. website: www.agilent.com

Installation Configurations

The 21 CFR Part 11 software may be installed in the following configurations:

- Standalone application — where all software components are installed on one computer which controls the instrument and the instrument software.
- Network application — requires a single computer per instrument; where the software components can each be installed on separate computers (unlimited) to form a 21 CFR Part 11 network. When a reference is made to networks in the context of SCM and 21 CFR Part 11, it refers to where the SDA is located on a network.

NOTE Although networks can be used in the SCM system, the software DOES NOT use the security of the networks to protect the data or to set privileges for the instrument users. The software uses its own, inherent, built-in security features, which the system/Network Administrator controls and activates within the software system during installation. This is described in more detail in Section 2.



2. Components of the SCM Software

Agilent provides a comprehensive solution to assist users of Agilent spectroscopy instruments to comply with the requirements of the 21 CFR Part 11 rule. The combination of the tools and facilities provided by the application software and the user organization's standard operating procedures will enable the user organization to ensure that its use of electronic records and electronic signatures comply with the requirements of the FDA.

The major components of the Agilent 21 CFR Part 11 software are:

- Instrument application software,
- Spectroscopy Database Administrator (SDA),
- Spectroscopy Configuration Manager (SCM), and
- Profiles and Privileges.

The combination of these components within the spectrometer forms the basis of the Agilent approach to compliance with 21 CFR Part 11.

Spectroscopy Database Administrator (SDA)

The SDA provides a secure location to store data in a database environment. The software is designed to create and administer database(s). This is controlled by the 'Network Administrator'. It is highly recommended that this person either works within the company's IT Department, or has a strong IT background.

The Network Administrator is responsible for the company network and may be involved in the installation of the software. This person may also be nominated to administer the SDA, particularly if the SDA is installed on an IT Server. A Network Administrator is essential.

Spectroscopy Configuration Manager (SCM)

The Spectroscopy Configuration Manager (SCM) controls the software with respect to assisting compliance with 21 CFR Part 11. The SCM provides the means to create, configure and maintain data in relation to system security, user management and data paths. The following procedures occur within, and are controlled by, the SCM:

- User identifications and passwords are created.
- User access rights to databases are established.
- Electronic signature protocols are specified and assigned.
- The GMT and date stamped audit log on the system activity is stored.
- Profiles and Privileges are set within the SCM.

The SCM is controlled by the 'SCM Administrator' who is responsible for setting user identifications, passwords and data paths. The SCM Administrator will implement company SOPs for passwords and security into the SCM. They review the audit trail of the SCM for system activity and irregularities.

NOTE It is strongly recommended that the Network Administrator and the SCM Administrator are two separate individuals, who do not use the system at any other access or user level.

Profiles and Privileges

A number of system access levels termed profiles are available to be set up within the software system. The SCM controls which applications and/or functions may be run by a particular user and sets up each user's access to the software and database(s).

A user is defined as a person authorized to operate, access or view the software following defined criteria as set by the SCM Administrator. Users range from the most basic level of operation of the system to Manager or Auditor profile.

Users are provided with their own unique logon ID and password. Profiles are set up that group each user type. Each profile allows specific and set access within the software system — this is referred to as User Privileges. The privileges then define what functions may be performed in that application.

The profiles and privileges are created and set when the SCM is installed. At installation, it is up to the requirements of the SCM Administrator to determine what combination of system access levels and definitions are required.

The SCM also sets the level of authority that a user may have with respect to electronic signatures and accessing certain parts of an application. For example, in ICP-OES a Basic user profile may only be able to run existing worksheets, but cannot create their own; a Manager user profile may only review data and have approval authority to sign electronically; a Service user profile may only be able to perform calibrations and Preventative Maintenance (PM) on the instrument.

In addition to a Network Administrator and the SCM Administrator, at least one user is essential. It is strongly recommended that the user does not have the same security access as the Network Administrator or the SCM Administrator.

The ICP Expert 7, SpectrAA CFR, ICP Expert II, Cary WinUV Pharma, UV Dissolution, and UV Fiber Optic Dissolution software packages have the following user profiles defined and set within the system:

- Manager Profile
- Supervisor Profile
- Advanced User Profile
- Service Profile
- Basic User Profile
- Auditor Profile
- Default Profile

NOTE

When using the Cary WinUV Pharma, UV Dissolution and UV Fiber Optic Dissolution software the Service Profile and Default Profile will need to be set by the SCM Administrator. Currently there are no applications and privileges set for these profiles.

When using the SpectrAA CFR software the Manager Profile, Supervisor Profile, Advanced User Profile, Basic User Profile, Auditor Profile, Service Profile and Default Profile will need to be set by the SCM Administrator. Currently there are no applications and privileges set for these profiles.

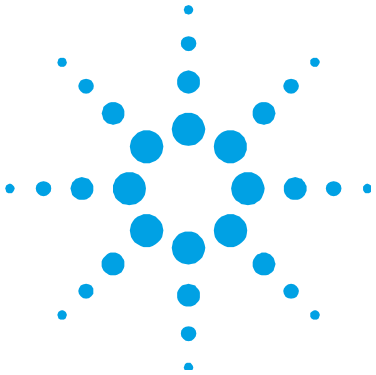
When using ICP Expert 7 software the Default Profile will need to be set by the SCM Administrator. Currently there are no applications and privileges set for this profile.

The user profiles stored in the software can be modified at installation to suit the company's requirements. More profiles can be created in all of the software packages, as required.

Even though the set up and configuration of ICP Expert 7, SpectrAA CFR, ICP Expert II, Cary WinUV Pharma and the UV Dissolution software is essentially identical, in operation the software packages contain differences. The privileges and profiles are specific to the spectroscopy application. Therefore, the privileges and profiles for Cary WinUV Pharma and UV Dissolution will be different to those of ICP Expert II, etc.

When certain functions are not allowed to the User, the software automatically disallows access to those functionalities. This is described in more detail in Software Security section.

This page is intentionally left blank.



3. 21 CFR Part 11 Compliance Using the SCM Software

Overview

This section discusses the major requirements of the 21 CFR Part 11 rule and how Agilent's software, as described herein, can be used as a tool to assist industry and manufacturers to become compliant. It is important to note that the installation of Agilent's application software alone will not ensure compliance with the rule. In order to ensure compliance, the client organization must establish a range of SOPs and other documentation that complement the facilities and operation of the software. These requirements are described in Section 4.

The acquisition of, and retention of raw data and processed data is a key concern to industry with respect to 21 CFR Part 11 compliance. Raw data is defined as the initial acquisition of information; the first point of data recording – being electronic, written, graph, etc., in form. It is critical to regulatory bodies that raw data is stored and subsequently archived appropriately and can then be retrieved as required. Retention of data in a useable form is critical. The initial acquisition of information from Agilent's instruments by the software is raw data in electronic form. The processing of, and manipulation of this data after acquisition is traceable in the audit trail within the software. Files cannot be deleted or written over. Auditing procedures are described in 'Controls for Electronic Records' in this section.

Definitions

There are a number of terms specifically defined within the 21 CFR Part 11 rule. These need to be clearly understood in order to place the rule's requirements in their appropriate context.

Electronic Records

An electronic record is defined in Section 11.3 (b) (6) of the Code[1] as:

'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'.

Section 11.1 (b) of the Code[1] states that the rule applies to:

'records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in [FDA] regulations ...[and to] electronic records submitted to the [FDA] 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.'

The electronic records generated by Agilent's spectrometers will form a component of the electronic records that the client organization must control in line with the 21 CFR Part 11 rule.

NOTE The rule does not apply to paper records that are transmitted by electronic means.

Closed versus Open Systems

The 21 CFR Part 11 rule defines the controls required for both closed and open systems. A closed system is defined by the Code as:

'an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system'

Section 11.3 (b) (4)[1].

This contrasts with an open system which is defined by the Code as:

'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'

Section 11.3 (b) (9)[1].

For example, a public network system such as the internet is an open system, because the access to the network is controlled by people other than those responsible for the control of the electronic records on the system. A private network managed internally by an organization itself is a closed system.

Agilent's spectroscopy instruments and software operate in a closed system. The operation and maintenance of the system is controlled by personnel working within the client organization and is usually governed by SOPs. Therefore, in developing the software to assist in compliance with the 21 CFR Part 11 rule, the controls for closed systems have been implemented.

Each company's SOPs must reflect the roles of the Network Administrator, SCM Administrator, and all applicable user profiles or privileges with respect to the rules of operation and compliance with 21 CFR Part 11. Agilent can assist you with compiling this documentation, on request. Suggested roles are provided with the software as described in the preceding pages.

Non-biometrics versus Biometrics

The 21 CFR Part 11 rule allows the use of either electronic signatures based upon biometrics or not based upon biometrics. Biometrics is defined by the Code as:

'a method of verifying an individual's physical feature(s) or repeatable actions where these features and/or actions are both unique to that individual and measurable'

Section 11.3 (b) (3)[1].

Agilent has chosen to implement non-biometric, electronic signatures which are defined by the Code to be:

'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'

Section 11.3 (b) (7)[1].

Approach to Software Security

The 21 CFR Part 11 rule provides detailed requirements for controls for closed systems. The purpose of such controls is defined by the Code:

'to ensure the authenticity, integrity, and ... confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine'

Section 11.10[1].

To provide the security required for compliance with the 21 CFR Part 11 rule, Agilent has developed the SCM for security and permission rights. The SCM enables the required security functions to be established. Once the SCM Administrator has set up all system Users, the SCM system guides the SCM Administrator through the required steps to set up the security.

The security functions provided by the SCM are:

- Access controls and authority checks via the use of User identification codes and passwords.
- Electronic record security via the use of databases and database protection.
- Time and date stamped audit trails (GMT).

Access Controls and Authority Checks – User ID and Passwords

In order to comply with Sections 11.100 (a)[1] and 11.300 (a)[1], the SCM Administrator must set up unique user identification codes for every individual. User identification codes must never be reused or reassigned to another individual. The SCM ensures that all user identification codes currently active on the system are unique, and that all user identification code and password combinations are unique.

The use of user identification codes and passwords enable control over who can log onto the system and who can perform particular functions within the Agilent application software. It also provides the mechanism to allow electronic signatures on electronic records. The use of databases coupled with the SCM prevents all unauthorized users from changing or deleting files. As a result of correct system set up, users are unable to delete or overwrite changes at any time. The SCM event logs augment the audit trails resident in the application software.

In order to meet the requirement that electronic signatures are, *'used only by their genuine owners'*[1], the SCM Administrator must establish a user identification code for each individual who will require access to the application.

Section 11.200 (a) (2)[1].

No common user identification codes should be issued to groups of people. Users should also be advised not to share their passwords with others and this should be confirmed in the company's SOPs.

It is important that a number of simple requirements are followed to ensure that compliance with the 21 CFR Part 11 rule is maintained. When each user account is being established in the SCM, the following information is required:

- In the ‘Name’ field, a unique user name must be entered.
- The ‘User Identification’ field is the identification the user provides when logging on to a Agilent application. It may be the same as the user’s network ID.
- The ‘Initials’ field is informative only and subsequently is an optional field.
- In the ‘Add password’ field, a case sensitive password of at least six characters must be entered (initially the SCM Administrator must provide a temporary password). When logging onto a Agilent application for the first time, the user will be prompted to change and confirm a new password.
- The SCM Administrator must also set password expiration times. ‘Password expiration for user’ and the ‘Allow to change password’ check box should not be active.
- In the ‘Description’ field, further details about the user may be entered. This field is optional.

As previously stated, the unique user identification field is fundamental to the security of the system. The text entered for the ‘Name’ and ‘User Description’ fields as well as the user’s file path are included in reports and audit logs to identify the user who has changed or signed electronic records. It is essential that the ‘Name’ field contains the user’s full name as it is a specific requirement of the 21 CFR Part 11 rule that ‘printed name of the signer’ is indicated on signed records (Section 11.50 (a) (1))[1].

Logon warning message—displayed when a user logs onto an Agilent application. The purpose of this message is to allow authorized users into the application. Unauthorized users that try to enter the application will be prevented from entering and their attempts and details will be stamped in the SCM audit trail.

Account policies allow the SCM Administrator to adjust the account policies (SOPs) regarding password expiry, period and number of unsuccessful logon attempts before users are locked out.

Electronic Record Security and Database Protection

Database protection specifies which databases will be protected and who will have access to a specific database. For ICP Expert 7, SpectrAA CFR, ICP Expert II, Cary WinUV Pharma and UV Dissolution, the database directory can be located on the local computer or on the organization's private Windows network.

In addition, when the user is created, an association between the user and the database is established by creating a Group and Project file path. Groups and Projects are defined within the software.

For electronic signatures that are not based upon biometrics, the 21 CFR Part 11 rule requires that the system,

'Employ at least two distinct identification components such as an identification code and password.'

Section 11.200 (a) (1)[1].

Agilent's systems use a combination of user identification code, password and a Group/Project path link to the protected database. The mechanism is used to provide the ability to carry out authority checks, the ability to sign or authorize electronic records and the ability to restrict access to specific databases.

Controlling User Identification Codes and Passwords

The methods used to establish passwords and the SOPs used to control them are specifically designed to meet the stringent requirements of the 21 CFR Part 11 rule. The system requires the password to be at least six characters in length. Initially, the SCM Administrator must provide a temporary password when setting up a user and the SCM Administrator must select the option to force the user to change the password at next logon. When the new user first logs on to the application, they are required by the system to change the password immediately. This ensures that only the individual user knows their particular user identification code and password combination and therefore that:

'attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals'

Section 11.200 (a) (3)[1].

Section 11.300 (b)[1] requires that passwords be periodically revised. Agilent's system allows the Administrator to set the period after which passwords must be changed. The SCM sets these parameters automatically at installation, but the SCM Administrator can adjust them to suit the organization's requirements. It must be noted that in order to comply with the 21 CFR Part 11 rule, these functions should not be turned off. The SCM sets these policy settings on the local computer. In the case where networks are used, this will be the computer where SCM is installed as a server.

It is important to note that if a user forgets their password, only the SCM Administrator can disable and then enable the user's account. More importantly, if the SCM Administrator forgets his or her password, no one (including Agilent personnel) has access to the password. The only remedy is to reformat the hard drive, re-install the Windows operating system and re-install the Agilent application software and 21 CFR Part 11 software. Given these consequences, it is essential that the SCM Administrator maintain a secure and effective means of remembering their password.

The 21 CFR Part 11 rule also requires that the system provides safeguards to prevent unauthorized use of passwords and/or identification codes and that any attempts at unauthorized use are detected and reported (Section 11.300 (d))[1]. In Agilent's systems, the user account may be set such that the account is disabled following a defined number (usually three) of failed attempts to enter the correct user identification code and password combination.

The user must ask the SCM Administrator to re-enable the user account. Each failed attempt to enter an authorized user identification code and password combination is recorded in the SCM audit log. Therefore the SCM Administrator must routinely and regularly check the SCM audit log for any such attempts as part of regular maintenance and archiving of audit logs. This facility provides protection against any unauthorized attempts to access the system, sign or approve records, stop a run, or unlock an application.

Section 11.300 (c) and (e)[1] refer to the control of tokens, cards or other devices that bear or generate identification code or password information. Agilent does not use such devices as part of the security of its systems, so these sections are not applicable to the current discussion.

Executable protection—restricting access to the Agilent application software by specifying who will have access to each executable. Users do not have access to delete the executable.

Controlling Access and Checking Authority

Sections 11.10 (d) and (g)[1] of the 21 CFR Part 11 rule require the use of procedures and controls to limit access to the system to authorized individuals and the use of authority checks to ensure that only authorized individuals can use the system and carry out the various functions within the system.

Agilent's systems carry out the following authority checks:

- Checks that the user identification code and password are valid and the user is authorized to run the application.
- Checks that the user is authorized to carry out particular activities/functions within the application.
- Checks via the user identification code and password that the user is authorized to save records to a particular protected database.
- Checks that the user identification code and password entered when signing a particular electronic record (as an operator) represents an authorized user.
- Checks that the user identification code and password used to approve a particular electronic record, represents a user with the authority to approve a record.
- Checks that the user identification code and password used to stop a run, represents an authorized user.
- Checks that the user identification code and password used to unlock an application, represents an authorized user.

There are a number of methods used to prevent unauthorized use of the system during an extended period of inactivity on the computer, depending on the application software being used. The SCM Administrator can set a 'lock-out' for periods of inactivity for increased security. When set, the application will lock automatically after a defined time, or the user can lock the application, using a manual lock function, if they need to leave the area. To unlock the application, the initial user must enter their user identification code and password.

When a user has activated the Lock function, the software can still be accessed by a different user. The second user's logon is totally separate to the initial user's access. In these instances, all logon details, time (GMT) and date, as well as subsequent activities are recorded in the audit logs which specify exactly each users activities.

Controls for Electronic Records

The 21 CFR Part 11 rule contains a range of specific measures to ensure the integrity of both the system operations and the information stored in the system.

Accurate and Complete Copies

Section 11.10 (b)[1] of the 21 CFR Part 11 ruling requires:

'The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the [FDA].'

The Agilent software can export and display its electronic records (incorporating the audit trails) that are stored in a protected database either on the local computer or on the Windows network. These exported items can be printed using the Windows software. The accuracy of the electronic copy is confirmed using a checksum. Invalid or altered records can be discerned *via* the use of a checksum facility in the application software. The completeness of the electronic records also relies on the integrity of the user organization's archive and backup standard operating procedures. The application software provides files that can be used for reviewing the records, independent of the application software.

The file formats available include ASCII, PRN, RTF, XLS, CSV, TXT, and HTML (see table below).

	GRAMSSPC	PRN	RTF	CSV (ASCII)	TXT	HTML	LIM	PDF
ICP Expert 7	No	No	No	No	No	No	No	Yes
SpectrAA CFR	No	Yes	No	No	Yes	No	No	No
ICP Expert II	No	Yes	No	Yes	Yes	Yes	Yes	No
UV Dissolution	Yes	No	Yes	Yes	No	No	No	No
UV Fiber Optic Dissolution	Yes	No	Yes	Yes	No	No	No	No
Cary WinUV Pharma	Yes	No	Yes	Yes	No	No	No	No

Audit trails

The 21 CFR Part 11 ruling, Section 11.10 (e)[1], requires the:

'Use of secure, computer-generated, time-stamped audit trails to independently record the date and time...'

of activities within the system.

In order to meet this requirement, Agilent systems use audit logs provided by the Agilent application software and by the SCM. These combined applications force the complete collection of data including items such as:

- method,
- instrument data,
- final results, and
- recalculations.

These audit logs also record who made the changes, at what time (GMT), date and reason for change. When changes are made, the previous information and the new information for the altered field are recorded. The system will also prompt the user to enter a reason for the change, although including a reason is optional. If a reason is not entered, the audit trail will read, 'No reason given'. Agilent strongly recommend that the company's internal SOPs require a clear, concise reason for change, to be entered into the system's software. The reason for change, or text stating that no reason was given, is stored with the data in the audit trail. The data and methods are also stored together. The application software and the SCM together, record the following:

- authorization attempts,
- access to the application,
- saving of files,
- logon activity, and
- account Privilege and audit policy changes.

The application software audit logs cannot be deleted from the electronic records.

The SCM creates a log of changes each time it is run. This log is automatically stored in an encrypted format in a Nexus database on either the local computer or on a network. These log files can only be viewed using the SCM, ensuring only an Administrator has access to these logs. The audit logs can only be archived or cleared by an authorized SCM Administrator.

In summary, the application software, combined with the SCM, ensures complete, secure, storage of raw data and processed data within the system. The audit trail is complete and users are unable to delete or over-write changes in any manner.

Protection of Records

The 21 CFR Part 11 rule requires:

'...protection of records to enable their accurate and ready retrieval throughout the records retention period.'

Section 11.10 (c)[1].

The audit trails associated with data must be retained (Section 11.10(e)[1]). While the application protects the electronic records and provides an audit trail of any changes to those records, the user organization must also establish rigorous and systematic archiving and backup SOPs. This will ensure that electronic records generated by Agilent's spectroscopy instruments are stored in such a manner that retention of data, archive and retrieval of data, over an extended period of time, is possible.

Section 11.10 (e)[1] also requires that previously recorded information cannot be obscured by record changes. As discussed earlier, all electronic records are stored in a protected database. The SCM software creates a Group, Project and user path to the protected database so that users cannot delete or alter records. Therefore it is not possible for a user to maliciously or accidentally obscure previously recorded information via such utilities as Windows Explorer.

When changes are made to files by authorized users, the audit log will record the user ID and details of who made the changes and the date and time (GMT) of the change. Changes made to UV Dissolution records are saved as a new file and the raw data (original file) is unchanged. Changes made to Cary WinUV Pharma records are saved as a new file and the raw data (original file) is unchanged. Changes made to ICP Expert 7, SpectrAA CFR and ICP Expert II worksheets are made to the original file, and a record of the original and updated information is saved in the audit log.

It is also important to note that Agilent systems provide protection against the indiscriminant transfer of records between 21 CFR Part 11 systems and non-21 CFR Part 11 systems.

Existing electronic methods developed on non-21 CFR Part 11 software cannot be opened in 21 CFR Part 11 software.

It is essential that all data is routinely backed up, as re-formatting the hard drive will remove the data.

Operational and Device Checks

Section 11.10 (f)[1] refers to the:

'*use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.'*

Comment 59 of the Preamble[2] to the 21 CFR Part 11 rule states:

'use of operational checks ... is not required in all cases'.

Comment 79 of the Preamble[2] to the 21 CFR Part 11 rule also states that the purpose of performing operational checks is to ensure that operations (such as manufacturing production steps and signings to indicate initiation or completion of those steps) are not executed outside of the predefined order established by the operating organization. Such checks are not applicable to the operation of a Agilent spectroscopy instrument.

Section 11.10 (h)[1] refers to the:

'use of device (terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.'

Comment 85 of the Preamble[2] to the 21 CFR Part 11 rule states:

'by the use of the term 'as appropriate', it does not intend to require device checks in all cases'.

There may be a situation where it is possible for a number of different devices (such as network terminals) to provide data input or commands but only some of those devices have been selected as legitimate sources of data input or commands. In this situation, device checks would be required to ensure that the device providing data input is in fact one of those that has been selected. In the case of Agilent's spectroscopy instruments, the only legitimate source of data input is an instrument connected to a computer running the appropriate application software. There are no alternative sources, so device checks are not required.

For UV Dissolution, Cary WinUV Pharma and ICP Expert 7, ICP Expert II, and SpectrAA CFR instruments are used and operated directly with the computer and application software; the software application can confirm that the instrument is operational and can validate the performance of the instrument. The files generated are validation files.

Using Electronic Signatures

The user organization is specifically responsible for a number of activities with regard to the use of electronic signatures within the organization. These include:

- Establishing, and adhering to:

'written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification'

Section 11.10 (j)[1].

- Recommended documentation required to be implemented for a 21 CFR Part 11 environment is described in Section 4.
- Verifying the identity of an individual before they are permitted to use an electronic signature, Section 11.100 (b)[1].
- Certifying to the FDA that the electronic signatures used within the organization:

'are intended to be the legally binding equivalent of traditional handwritten signatures'

Section 11.100 (c)[1].

The Agilent systems provide an additional tool for the user organization to remind users of their obligations. The system displays a warning message to unauthorized users at the time of logon to the application. A warning message reminds users or unauthorized operators of their inability to use the application and/or database.

A signature can be executed to a file either at the time that the file is generated, or at a later stage in the process. As required by Section 11.50[1], the electronic records signed using the application software will show:

- The printed name of the signer.
- The date and time (GMT) when the signature was executed and the meaning (such as comment, review or approval) associated with the signature.

- The individual who is executing the signature to the record determines the meaning of the signature.
- The individual enters customized text as appropriate.
- In addition, Agilent's system will show the user's title or user Group designation when the user was established.

The preceding details will be displayed on screen when the record is viewed as well as in the printed output of the record.

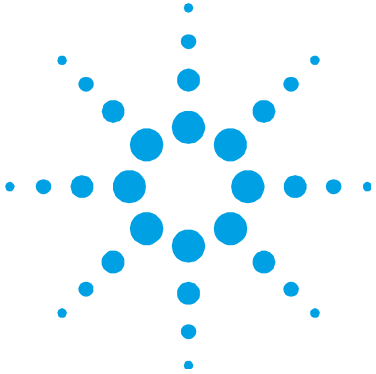
The Agilent systems:

'ensure that the signature cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means'

Section 11.70[1].

The ICP Expert 7, SpectrAA CFR, ICP Expert II, Cary WinUV Pharma and UV Dissolution application software do this by linking the signature to the electronic record for which it is intended by means of a unique digital value that is inserted into the method and data records. It is not possible to associate/apply a signature with a record by any method other than that provided by the application software.

During a series of signings by one individual, the first and subsequent signing requires both the user identification code and the password to be entered. When a series of signings take place, both the user identification code and the password must be entered for each signing (Section 11.200 (a) (1) (i and ii)[1]).



4. Documentation

This chapter describes the documentation component necessary to complement the SCM software. It details the recommended SOPs that the user company needs to develop and implement for regulatory compliance.

Recommended Standard Operating Procedures

There are a number of SOPs and Policies that should be developed and implemented once the SCM software has been installed.

The SOPs required are:

- Archive and retrieval of electronic records from the Agilent software.
- Archive and retrieval of electronic records from SCM software logs.
- Breach of security identification.
- Locking the application.
- Identifying signed and approved files.
- Exporting data to LIMS, directories and databases.
- Education, training and experience.
- Document control system.
- Account policy.
- Reason for change.

- Accountability and responsibility for electronic signatures.
- Verification of Identification
- Declaration of evidence to handwritten signature.
- Roles and responsibilities.
- Security of passwords.

Archive and Retrieval of Electronic Records from the Agilent Software

An SOP is required to ensure that the records generated by the Agilent application software are routinely archived. These should be archived in such a way that they can be readily accessed.

Archiving and Retrieval of Electronic Records from the SCM Software Logs

The SCM software creates a log of changes each time it is run. This log file is automatically stored in an encrypted format in a Nexus database on either the local computer or on a network. An SOP should be developed to ensure that the SCM software audit log files are archived and stored with the associated electronic records generated by the Agilent application software, and that they can be readily accessed and retrieved and used over an extended period of time.

Breach of Security Identification

A SOP should be developed and implemented for the checking of security breaches. The SCM software Administrator should check the SCM software audit trail regularly for occurrences of failed attempts to use a user identification code and password combination. This audit trail will be either on the local computer or the network, depending on where the SCM software is installed. A security breach can result from attempts to log onto the application, to stop a run or to unlock an application. After a defined number of failed attempts (usually three), a user account is disabled. If the logon attempt fails, the person cannot gain access to the application software. Only the SCM software Administrator is able to re-activate the user account.

NOTE The Account lockout threshold policy can be set to a value that suits the user organization using the SCM software.

Locking the Application

Standard operating procedures should include the requirement for users to lock the workstation when absent from the immediate vicinity of the computer. This helps ensure that no unauthorized person can access the application. Users can lock the software application by using the Lock function within the software.

NOTE It is recommended that the SCM software Administrator activate the auto lock function via the SCM software. This will automatically lock the application after a defined period of inactivity.

Identifying Signed and Approved Files

A SOP is required to be developed and implemented for a naming convention for signed files. When using the SCM software for UV Dissolution and Cary WinUV Pharma, a naming convention for signed files is adopted such that a file name extension of the level of signature is added. Therefore, files that do not have signatures will be saved as the standard file name and files with signatures will have the file name extension and the type of signature labeled. For example, filename_operator.bcn or filename_Approval2.bcn. If the approver is not available immediately to approve the data, the file may be re-opened and signed whereby the signature file name extension will be added to the file name. In addition, a procedure may be established where unapproved files are saved in one subdirectory and approved files in another. This way, unapproved files can be easily distinguished and separated from approved files. For ICP Expert 7, SpectrAA CFR and ICP Expert II, where signature file name extensions are not added, a procedure to distinguish files between signed and unsigned may be particularly important.

NOTE When approving at a later date, the Agilent application software must be installed on the computer to ensure the file to be approved can be opened and signed.

Exporting data to LIMS, directories and databases

An SOP should be written and developed for the export of data to LIMS or to other protected directories or databases. To export data from reports for a LIMS (Laboratory Information Management System), or to export records for data warehousing systems, files should be exported to a protected directory from where they can be moved directly into the customer's secure database/LIMS system. File types currently available for exporting data include ASCII, PRN, RTF, XLS, CSV, TXT, XLS and HTML.

Education, Training and Experience

The user organization must establish its own SOPs to ensure that the people:

'who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.'

Section 11.10 (i)[1].

This applies to personnel within the user organization as well as to Agilent personnel.

Agilent ensures that all staff are suitably qualified on the basis of their education, job training and experience, to perform their assigned tasks. In addition, Agilent also identifies and provides any additional training to ensure that personnel acquire the skill, knowledge and experience to perform their jobs to an excellent standard. Records are kept according to Quality Management System practices.

Agilent's customer support representatives must also satisfactorily complete a rigorous curriculum for certification, including factory training and formal classroom and laboratory study. Throughout their careers, Agilent customer service engineers maintain their technical proficiency by attending training courses and reviewing technical bulletins and associated material.

Documentation Control System

Section 11.10 (k)[1] of the 21 CFR Part 11 document requires the:

'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.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.'

A Quality Management System containing a Document Control System is essential within a 21 CFR Part 11 environment. Companies need to develop and implement SOPs which ensure compliance with the Rule. This must include defined procedures and processes with respect to an audit trail, and archive, retrieval and retention of data processes.

Account Policy

Standard operating procedures need to be developed and implemented that detail the requirement and set up of account policies with respect to password configuration and alpha-numeric characters and character history (set by the SCM software Administrator to reflect company SOPs). This includes:

- The 'Define a password history' policy and number of passwords remembered.
- The 'Minimum password length' policy is set to six characters.
- The 'Maximum password age' policy.
- The 'Account lockout threshold' policy.

Reason for Change

An SOP should be developed and implemented that directs individuals to enter an appropriate 'Reason for Change' in the dialog box, when requested to do so. The SOP should also include a rationale, with respect to 21 CFR Part 11 compliance, as to why a concise, accurate 'Reason for Change' data entry is essential.

Accountability and Responsibility for Electronic Signatures

Each company should write and implement an SOP which details the roles, responsibilities and accountabilities for each user and for the SCM software Administrator and Network Administrator.

Verification of Identification

Each company should develop and implement an SOP which details the 21 CFR Part 11 identification requirements for each user, the SCM software Administrator and the Network Administrator. Each person is to have their identification verified with appropriate documentation.

Declaration of Evidence to Handwritten Signature

The 21 CFR Part 11 rule requires each company to formally declare the evidence to handwritten signature, to the FDA. This procedure needs to be appropriately documented in an SOP and the appropriate actions completed.

Roles and Responsibilities

Each company should develop and implement an SOP which details roles and responsibilities for use of the system. Each User Profile, the Network Administrator and the SCM software Administrator need to have their roles, responsibilities, limitations, access levels and authorization levels (electronic signatures) clearly defined.

Security of Passwords

Each company should develop and implement an SOP which incorporates the 21 CFR Part 11 requirements for security of passwords and to ensure that passwords are not shared with others.

Validation Documentation

The 21 CFR part 11 ruling, Section 11.10 (a)[1] requires:

'Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered record.'

The user organization must validate the Agilent application software to ensure that it is suitable for use within its particular regulatory environment. Agilent can provide detailed information regarding its software design, development, testing, and maintenance and archiving procedures.

Long Term Qualification Procedures

The requirements for Performance Qualification (PQ), Preventative Maintenance (PM) and system re-qualification procedures are components of a validation system which need to be clearly documented within the user company's Quality Management System.

This page is intentionally left blank.

5. Checklists

This chapter features a checklist of the recommended SOPs that should be written and implemented by the user organization and a Compliance Matrix which compares the SCM software directly to the FDA's 21 CFR Part 11 regulation.

SOP Checklist

Task	Complete
Ensure that appropriate SOPs are implemented:	
Personnel have suitable education, training and experience.	
There are appropriate controls over distribution, use of and access to documentation.	
Revision and change controls for documentation include audit trails.	
Individuals are held accountable and responsible for their electronic signatures.	
The identity of an individual is verified before they are permitted to use an electronic signature.	
The FDA is notified that electronic signatures are intended to be equivalent to handwritten signatures.	
Regularly archive the Agilent application database electronic records.	
Regularly archive the SCM software audit log files.	
*Regularly check the audit logs to detect attempted unauthorized use of user identification code and password combinations.	
Ensure the application is locked during absences from the workstation.	
Develop a method to distinguish between authorized and unauthorized files.	

*These logs will be located on the local computer or on the network, depending on where the SCM software is installed.

Compliance Matrix

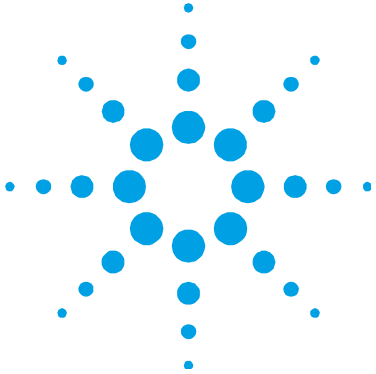
The checklist summarizes how Agilent spectroscopy instruments, together with the SCM software. meet the requirements of the 21 CFR Part 11 rule. This checklist only considers those controls applicable to a 'closed system', with non-biometric signatures. This checklist is only applicable with application software using SDA and SCM and which is installed and operated in accordance with Agilent's recommended instructions.

21 CFR Part 11 reference[1]	Brief description of requirements	Compliant
11.10 (a)	Validation of systems.	✓
11.10 (b)	Accurate and complete copies of records.	✓
11.10 (c)	Protection of records, record retention and retrieval.	✓
11.10 (d)	Limiting access to authorized individuals.	✓
11.10 (e)	Secure computer-generated time-stamped audit trails.	✓
11.10 (f)	Use of operational system checks.	N/A
11.10 (g)	Use of authority checks	✓
11.10 (h)	Use of device checks	N/A
11.10 (i)	Suitable education, training and experience	User's SOP
11.10 (j)	Accountability and responsibility for electronic signatures	User's SOP
11.10 (k)(1)	Controls over distribution, use of and access to documentation	User's SOP
11.10 (k)(2)	Audit trail of modifications to documentation	User's SOP
11.30	Controls for open systems.	N/A
11.50 (a)	Signed electronic records include printed name of signer, time and date of execution, meaning associated with the signature,	✓
11.50 (b)	Subject to same controls as electronic records	✓
11.70	Electronic signatures linked to their records	✓
11.100 (a)	Signatures unique to one individual	✓
11.100 (b)	Organization to verify individual's identity	User's SOP
11.100 (c)	Declaration of equivalence to handwritten signature	User's SOP

continued

21 CFR Part 11 reference[1]	Brief description of requirements	Compliant
11.200 (a)(1)	Use two distinct identification components	✓
11.200 (a)(1)(i)	Use all components on first signing, at least one component on subsequent signings within same session	✓
11.200 (a)(1)(ii)	Use all components on signings in separate sessions	✓
11.200 (a)(2)	Used only by their genuine owner	✓
11.200 (a)(3)	Misuse requires collaboration of ≥2 individuals	✓
11.200 (b)	Biometric electronic signatures	N/A
11.300 (a)	Identification code/password combination to be unique	✓
11.300 (b)	Periodically checked, recalled or revised	✓
11.300 (c)	Loss management procedures for devices	N/A
11.300 (d)	Transaction safeguards to detect and prevent misuse	✓
11.300 (e)	Periodic testing of devices	N/A

This page is intentionally left blank.



6. References

1. Code of Federal Regulations, Title 21, Food and Drugs, Part 11 'Electronic Records: Electronic Signatures Final Rule', Federal Register 62 (54), 13429-12466. A copy of the final rule can be found at www.fda.gov

2. ibid, p 13430.

This page is intentionally left blank.

www.agilent.com

In This Book

The manual describes the following:

- Introduction
- Components of the SCM Software
- 21 CFR Part 11 Compliance Using the SCM Software
- Documentation
- Checklists
- References

Printed in USA
09/14

G9272-90009
Issue 1

Agilent Technologies