

21 CFR 11 Assistant Software

21 CFR Part 11 Compliance Booklet



Agilent Technologies

Notices

© Agilent Technologies, Inc. 2001-2004, 2009-2010

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

8510191800

Edition

Sixth edition, October 2010

Printed in Australia

Agilent Technologies, Inc.

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.

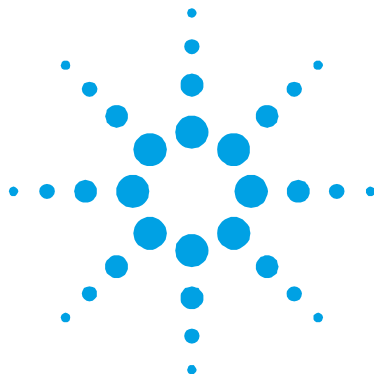
Contents

1. Introduction	7
21 CFR Part 11 products for spectroscopy instruments	8
System requirements	8
How to use this booklet	9
2. Compliance With the 21 CFR 11 Assistant Software	11
Definitions	12
Electronic Records	12
Closed versus open systems	12
Non-biometric versus biometric signatures	13
The 21 CFR 11 Assistant software's approach to security	13
Controls for Electronic Records	15
Accurate and complete copies	16
Audit trails	17
Protection of records	18
Validation	19
Education, training and experience	19
Controlled system documentation	20
Operational and device checks	20
Controlling access and checking authority	21
The user identification code and password	21
Establishing unique user identification codes	22
Controlling user identification codes and passwords	23
Using electronic signatures	25

Providing the tools for compliance	26
3. Compliance Assessment Checklist	27
4. Things To Do Before Installing the 21 CFR 11 Assistant Software	29
Windows administrator requirements	29
System requirements	30
Preparing Windows Event logs	31
User accounts	31
5. Checklist for the 21 CFR Part 11 Assistant Software	33
Before installation	33
During installation	34
After installation	34
6. Installation of the 21 CFR 11 Assistant Software	37
Function of the 21 CFR 11 Assistant software	37
Uninstalling the software	39
7. Ongoing SOPs and Notable Items	41
Setting Windows Event logs	41
Ongoing standard operating procedures	42
Archiving Agilent application electronic records	42
Archiving Windows Event logs	42
Archiving the 21 CFR 11 Assistant software logs	43
Checking for breaches of security	43
Locking the Application	43
Identifying signed and approved files	44

Exporting data to LIMS/databases 44

This page is intentionally left blank.



1. Introduction

21 CFR Part 11 products for spectroscopy instruments	8
System requirements	8
How to use this booklet	9

Effective August 20, 1997, the United States Food and Drug Administration (FDA) released Part 11 “Electronic Records; Electronic Signatures” of Title 21 of the Code of Federal Regulations (referred to as 21 CFR Part 11). This rule states the conditions under which the FDA considers electronic signatures and electronic records to be trustworthy, reliable and equivalent to traditional handwritten signatures on paper. In this manner, it defines the conditions under which an organization must operate to meet its record keeping and record submission requirements when it uses electronic records and signatures rather than paper records and handwritten signatures.

The Preamble to the 21 CFR Part 11 rule states, “the use of electronic records as well as their submission to the FDA is voluntary”. However, where an organization does decide to use electronic records and electronic signatures, the requirements of the rule must be met in full for all relevant electronic records.

21 CFR Part 11 products for spectroscopy instruments

For selected spectroscopy instrument systems, Agilent provides 21 CFR Part 11 capable software that assists you to meet the requirements of the 21 CFR Part 11 rule. For a list of systems that currently have 21 CFR Part 11 capable software, refer to the Agilent web site, alternatively, contact your local Agilent representative.

The information in this publication refers only to the versions of software that are listed on the Agilent Web site.

System requirements

It is important to use the correct operating system for this product. The exact operating system requirements for each product can be found on the Agilent Web site.

In addition to requiring particular operating systems, at least one NTFS (New Technology Filing System) formatted directory must be available in order to use the software. Alternative file systems such as FAT (File Allocation Table) and HPFS (High Performance File System) are not adequate substitutes.

Agilent does not support, recommend or warrant the use of this 21 CFR Part 11 capable software product in conjunction with Microsoft® Windows® networks. The software should only be operated with users registered on the local PC and with data being saved to protected directories located on the local PC. However, it is possible for the PC to be connected to a Windows network so that files stored on the local PC by the Agilent 21 CFR Part 11 software can be archived to a network location using third party software.

NOTE

Throughout this booklet, "Windows" refers to Windows NT®, Windows 2000 and Windows XP SP2, unless otherwise specified.

For further information about system requirements, please refer to the 'Things to do before installing the 21 CFR Part 11 Assistant software' section.

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 Web site www.agilent.com

How to use this booklet

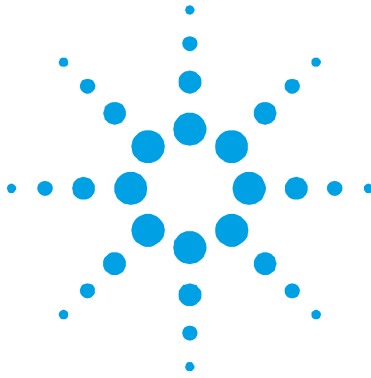
This booklet provides information about:

- How the 21 CFR 11 Assistant software meets the requirements of the 21 CFR Part 11 rule (Section 2)
- A summary compliance checklist (Section 3)
- A checklist of things to do (Section 4)
- Things to do before installing the 21 CFR 11 Assistant software (Section 5)
- Software installation (Section 6)
- Ongoing standard operating procedures (Section 7)

After reading about how the 21 CFR 11 Assistant software meets the requirements of the 21 CFR Part 11 rule, system administrators should work through the checklist of things to do, referring to the appropriate sections of the booklet for more detail. It is important to read the booklet thoroughly, as failure to perform certain tasks could mean that the installation will not meet the requirements of the 21 CFR Part 11 rule.

Detailed software installation instructions are provided with the software. You should also refer to the 'Late Breaking News' document supplied with the AA software packages for troubleshooting issues.

This page is intentionally left blank.



2. Compliance With the 21 CFR 11 Assistant Software

Definitions	12
The 21 CFR 11 Assistant software's approach to security	13
Controls for Electronic Records	15
Controlling access and checking authority	21
Providing the tools for compliance	26

This chapter discusses the major requirements of the 21 CFR Part 11 rule. It describes how the application software used by Agilent's spectroscopy instruments can be used to assist organizations to become compliant with the 21 CFR Part 11 rule. It is important to note that the installation of Agilent's application software alone will not ensure compliance with the rule. The user organization must establish a range of policies and standard operating procedures that complement the facilities provided by the software in order to ensure compliance with the rule.

Definitions

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

Electronic Records

An electronic record is defined in Section 11.3 (b) (6) 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) 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 rule does not apply to paper records that are transmitted by electronic means.

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

Closed versus open systems

The 21 CFR Part 11 rule defines the controls required for both closed and open systems. A closed system is “an environment in which system access is controlled by the persons who are responsible for the content of electronic records that are on the system” (Section 11.3 (b) (4)). This contrasts with an open system that is “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)). 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. On the other hand a stand-alone PC or a private network managed by the organization itself is a closed system.

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

Non-biometric versus biometric signatures

The 21 CFR Part 11 rule allows the use of either electronic signatures based upon biometrics or not based upon biometrics. Biometric signatures are those that verify the user's identity by measuring the unique "physical feature(s) or repeatable actions" of the user (Section 11.3 (b) (3)). Agilent has chosen to implement non-biometric electronic signatures which are "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)).

The 21 CFR 11 Assistant software's approach to security

The 21 CFR Part 11 rule provides detailed requirements for controls for closed systems. The purpose of such controls is to ensure the authenticity, integrity and confidentiality of the electronic records and "to ensure that the signer cannot readily repudiate the signed record as not genuine" (Section 11.10).

To provide the security required for compliance with the 21 CFR Part 11 rule, the 21 CFR 11 Assistant software uses the Microsoft Windows operating system security functions, and in particular the NTFS permission rights. These security functions provide:

- Access controls and authority checks via the use of user identification codes and passwords.
- Electronic record security via the use of protected directories.
- Time and date stamped audit trails.

The use of user identification codes and passwords enables control over who can log on to the system and who can perform particular functions within the Agilent application software. It also provides the mechanism to allow electronic signature of electronic records. The use of protected directories prevents all users, other than the authorized system administrator, from changing or deleting files. The Windows operating system event logs augment the audit trails resident in the application software.

The system administrator must set up the required users. It is important that a number of simple requirements are followed when this is done to ensure that compliance with the 21 CFR Part 11 rule is maintained. When each user account is being established in Windows the following must be adhered to:

- In the “User Name” field, a unique user identification code must be entered.
- In the “Full Name” field, the user’s full name (not just one name or a nickname) must be entered.
- In the “Description” field, either the individual’s title or user group designation must be entered.
- In the “Password” and “Confirm password” fields, a case sensitive password of at least six characters must be entered. (Initially the system administrator must provide a temporary password.)
- The “User must change password at next logon” check box must be selected.
- The “Password never expires” and “User cannot change password” check boxes must be cleared.

As stated above, the unique user identification code is fundamental to the security of the system. The text of the “User Name”, “Full Name” and “Description” fields are included in reports and audit logs to identify the user who has changed or signed electronic records. It is essential that the “Full Name” field contains the user’s full name as it is a specific requirement of the 21 CFR Part 11 rule that the “printed name of the signer” is indicated on signed records (Section 11.50 (a) (1)). Users are also required to change their password when they first log on to the system, to ensure the security of the password.

Once the system administrator has set up the users, the 21 CFR 11 Assistant software guides the system administrator through the required steps to set up the security. This covers the following issues:

- Privilege groups—assigning users to a privilege level. The privileges are created when the 21 CFR 11 Assistant software is run. Each privilege allows a different level of access within the Agilent application software. When certain functions are not allowed, the appropriate software controls are disabled.
- Directory protection—specifying which directories will be protected and who will have access to each protected directory. The protected directories must be located on the local PC (i.e. the PC connected to the instrument).
- Executable protection—restricting access to the Agilent application software by specifying the directory containing the Agilent application executable files and who will have access to each executable.
- Logon warning message—defining the warning message that is displayed at logon to Windows. The purpose of this message is to warn unauthorized operators of the consequences of using the restricted PC. The message may be edited to suit the user organization's requirements.
- Account policies—adjusting the account policies regarding password expiry period and number of unsuccessful logon attempts before lockout.

In addition, the 21 CFR 11 Assistant software automatically sets a number of Windows policies relating to password length, history and aging (see Section 6 for more details).

Controls for Electronic Records

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

Accurate and complete copies

Section 11.10 (b) 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 application software utilizes the Windows copy function to produce electronic copies of files within and between protected directories on the local PC. The application can load and display its electronic records (incorporating the audit trails) stored in a protected directory on the local PC. These items can also be printed using the application software. The accuracy of the electronic copy is confirmed using a checksum, as required by Section 11.10 (a). 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 review of the records, independent of the application software. The file formats available include ASCII, PRN, RTF and HTML.

Audit trails

Section 11.10 (e) requires the use of “secure, computer-generated, time-stamped audit trails to independently record the date and time” of activities within the system. To meet this requirement, Agilent systems utilize audit logs provided by the Agilent application software and by the Windows operating system. Audit logs are created by the application software. The application forces the complete collection of data including such things as method, instrument data, final results, etc. These audit logs also record who made the changes, when and why. When changes are made, the previous value and the new value 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. The reason for change, or text stating that no reason was given, is stored with the record. The data and methods are also stored together. The application software and the operating system write to the Windows event log(s), recording 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 of which they are a part. Once the Windows event logs have been set to manual deletion (by the 21 CFR 11 Assistant software), they can only be archived or cleared by an authorized system administrator.

The 21 CFR 11 Assistant software (version 1.2.0.1086 or greater) creates a log of changes each time it is run. This log is automatically stored in an encrypted format in a protected directory on the local PC (the protected directory is created by the system administrator). These log files can only be viewed using the 21 CFR 11 Assistant software, therefore only an administrator has access to these logs.

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)), and that the audit trails associated with the records must also be retained (Section 11.10(e)). 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 standard operating procedures to ensure that electronic records generated by Agilent’s spectroscopy instruments are stored in such a manner that they can be retrieved and used over an extended period of time. This will also require the customer to consider issues such as storage media, file formats, etc.

Section 11.10 (e) also requires that previously recorded information cannot be obscured by record changes. As discussed earlier, all electronic records are stored in protected directories. The 21 CFR 11 Assistant software automatically sets the security access to the protected directories so that users (other than the authorized system administrator) cannot delete or alter records.

When changes are made to records by authorized users, the audit log records who made the changes, and the date and time of the change. Changes made to AA records are saved as a new file. The original file is not changed.

The system administrator must have the ability to delete records so that they can clear the directories following routine archiving of data.

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

A record created on a non-21 CFR Part 11 system that is opened on a 21 CFR 11 system does not become a 21 CFR Part 11 file and will not be identified as such.

In the case of AA records, those created on non-21 CFR Part 11 systems can be opened and used. However, the record cannot be converted to a 21 CFR Part 11 file (no “padlock” icon shown) and the record cannot be signed. It is possible to use the worksheet from a non-21 CFR Part 11 record as the basis for a worksheet on a 21 CFR Part 11 system. The new worksheet will be treated the same as one created on a 21 CFR Part 11 system.

A record created on a 21 CFR Part 11 system cannot be changed or signed on a non-21 CFR Part 11 system. AA records can only be opened as read only files on non-21 CFR Part 11 systems. These features ensure additional protection of the electronic records.

Validation

Section 11.10 (a) requires “validation of systems to ensure accuracy, reliability, consistent intended performance and the ability to discern invalid or altered records”. 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, maintenance and archiving procedures. Agilent offers installation qualification (IQ) and operation qualification (OQ) documentation and services. Agilent can also assist the user organization with ongoing performance qualification (PQ) if required.

Education, training and experience

The user organization must establish its own procedures 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)). This applies to personnel within the user organization as well as to Agilent personnel.

Agilent ensures that all their staff are suitably qualified on the basis of 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 for the duration of employment as appropriate.

Agilent's customer support representatives must also satisfactorily complete a rigorous curriculum for certification, including, but not limited to, factory training and formal classroom and laboratory study. Throughout their careers, customer support personnel maintain their technical proficiency by attending training courses and reviewing technical bulletins and associated material.

Controlled system documentation

Section 11.10 (k) requires the user organization to maintain appropriate controls over distribution, access and use of documentation for system operation and maintenance. The user organization must also ensure that revision and change control procedures incorporate an audit trail that documents time-sequenced development and modification of systems documentation.

Operational and device checks

Section 11.10 (f) refers to the "use of operational system checks to enforce permitted sequencing of steps and events as appropriate". In comment 59 of the Preamble to the 21 CFR Part 11 rule, it states "use of operational checks ... is not required in all cases". Comment 79 of the Preamble 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". The Agilent application software defines the sequence of events within an analysis. If an operator is not given access to method modification, then the operator does not have the ability to change the sequence of events within the analysis being carried out by the spectroscopy instrument. Therefore operational system checks are not required.

Section 11.10 (h) refers to the “use of device (terminal) checks to determine as appropriate, the validity of the source of data input or operational instruction”. In comment 85 of the Preamble to the 21 CFR Part 11 rule, it 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 sources of data input are an instrument connected to a PC running the appropriate Agilent application software or, for pre or post run functions such as method development and data approval, a PC running the appropriate Agilent application software. There are no alternative sources, so device checks are not required.

Controlling access and checking authority

The user identification code and password

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)). Agilent’s systems use a combination of user identification code and password. The mechanism is used to provide both the ability to carry out authority checks and the ability to sign or authorize electronic records.

Sections 11.10 (d) and (g) 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 used to log on to the PC represent a valid user.

- Checks that the logged on user is authorized to run particular applications.
- Checks that the logged on user is authorized to carry out particular activities/functions within the application.
- Checks that the logged on user is authorized to save records to a particular protected directory.
- Checks that the user identification code and password used to sign (as an operator) a particular electronic record represent a valid user.
- Checks that the user identification code and password used to approve a particular electronic record represent a user with the authority to approve a record.
- Checks that the user identification code and password used to unlock an application represent a valid user.

Establishing unique user identification codes

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

In order to meet the requirement that electronic signatures are “used only by their genuine owners” (Section 11.200 (a) (2)), the system administrator must establish a user identification code for each individual requiring access to the system. No common user identification codes should be issued to groups of people, and users should be advised not to share their passwords with others.

There are a number of methods used to prevent unauthorized use of the system during an extended period of inactivity on the PC, depending on the application software being used.

In the AA software, a built in Lock function is available. This replaces the need for the CTRL+ALT+DEL and password protected screen saver functions, as it can be set to activate after a defined period of inactivity. In addition, if the user is planning to be absent from the immediate vicinity of the system while still logged on, they can manually activate the lock function. To unlock the application, a valid user must enter their user identification code and password. It is also possible for the user who unlocks the application to be different from the user who originally opened the application. In this instance, subsequent activities are recorded in the audit logs as being carried out by the new user.

Controlling user identification codes and passwords

The methods used to establish passwords and the policies 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 system administrator must provide a temporary password when setting up a user and, as mentioned previously, the system 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 system, 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)).

Section 11.300 (b) requires that passwords are periodically revised. Agilent’s system allows the Administrator to set the period after which passwords must be changed. The system requires that each time the user changes their password it must be different from the 12 (Windows NT) or 24 (Windows 2000 or XP) previous passwords used. The 21 CFR 11 Assistant software sets these parameters automatically at installation, but they can be adjusted by the system administrator to suit the organization’s requirements. However, it must be noted that in order to comply with the 21 CFR Part 11 rule, these functions should not be turned off. The 21 CFR 11 Assistant software sets these policy settings on the local PC.

It is important to note that if a user forgets their password, the system administrator can only disable and then enable the user's account. More importantly, if the system administrator forgets their 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. Given these consequences, it is essential that the system administrator maintains a secure and effective means of remembering their passwords.

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)). In Agilent's systems, the user account is disabled following a defined number (usually three) of failed attempts to enter the correct user identification code and password combination. When the user is attempting to log on, they are logging on to the PC itself. Therefore, if the logon attempt fails they do not gain access to use the PC and do not, at any stage, gain access to the application software. In addition, the user must ask the system administrator to re-enable the user account. Each failed attempt to enter an authorized user identification code and password combination is recorded in either the Windows Security event log or the Windows Application event log. Therefore the system administrator must routinely and regularly check the event logs 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 or unlock an application.

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

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)).
- Verifying the identity of an individual before they are permitted to use an electronic signature (Section 11.100 (b)).
- 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)).

The Agilent systems provide an additional tool for the user organization to remind users of their obligations. The systems display a warning message at the time of logon to the PC. A default warning message reminds users or unauthorized operators of the consequences of using the restricted PC. However, the system administrator can use the 21 CFR 11 Assistant software to either alter the default message to suit the precise requirements of the user organization or to prevent any message from displaying.

A signature can be executed to a record either at the time that the operation that generates the record takes place, or at a later time.

As required by Section 11.50, the electronic records signed using the application software will show the printed name of the signer, the date and time 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 may enter customized text as appropriate. In addition, Agilent’s system will show the user’s title or user group designation if this was entered into the “Description” field when the user was established. These details will be displayed on screen when the record is viewed as well as in the printed output of the record.

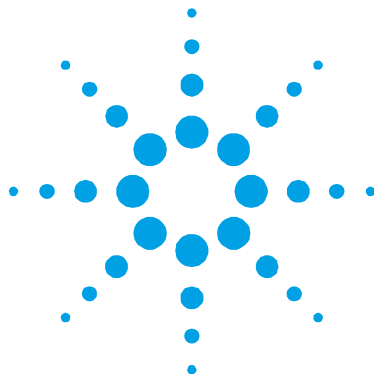
The Agilent systems ensure that the signature “cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means” (Section 11.70). The AA application software does this by linking the signature to the electronic record for which it is intended by means of a unique digital value that is inserted into the method and data records. It is not possible to associate/store a signature with a record by any method other than that provided by the application software.

Section 11.200 (a) (1) requires that during a series of signings by one individual, the first signing requires both the user identification code and the password to be entered. Subsequent signings by that individual require at least the password to be entered. However, when a series of signings takes place not during a single continuous period of controlled system access, both the user identification code and the password must be entered for each signing. The Agilent application software requires both the user identification code and password to be entered for all signings.

Providing the tools for compliance

Agilent provides a comprehensive solution to assist the users of its spectroscopy instruments to comply with the complex 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 policies and 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.

For further information concerning Agilent’s spectroscopy instruments please contact your local Agilent office or visit the web site at www.agilent.com.



3. Compliance Assessment Checklist

The following checklist summarizes how Agilent's spectroscopy instruments meet the requirements of the 21 CFR Part 11 rule. This checklist only considers those controls applicable to a "closed system", as each of Agilent's spectroscopy instruments satisfies the defined requirements of a closed system. It also considers only those controls applicable to non-biometric signatures. This checklist is only applicable when the nominated version of the application software is installed and operated in accordance with Agilent's recommended instructions.

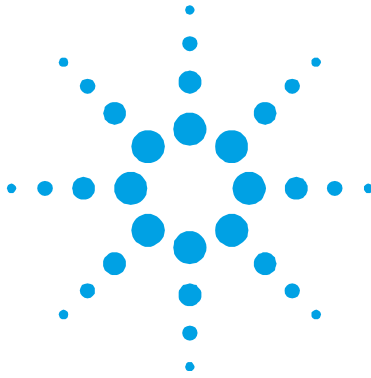
21 CFR Part 11 Section	Brief Description of Requirement	Compliant
11.10 (a)	Validation of systems	✓
11.10 (b)	Accurate & complete copies of records	✓
11.10 (c)	Protection of records	✓
11.10 (d)	Limiting access to authorized individuals	✓
11.10 (e)	Secure computer-generated time-stamped audit trails	✓
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

(continued)

Compliance Assessment Checklist

21 CFR Part 11 Section	Brief Description of Requirement	Compliant
11.10 (i)	Suitable education, training & experience	User's SOP
11.10 (j)	Accountability & 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
11.50 (a) (1)	Signed electronic records include printed name of signer	✓
11.50 (a) (2)	Signed electronic records include time & date of execution	✓
11.50 (a) (3)	Signed electronic records include meaning of 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
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	✓
11.300 (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

Compliance with the 21 CFR Part 11 rule, as outlined above, can only be assured if the Agilent application is installed on a compatible Microsoft Windows operating system using NTFS directories and the operating system has been configured in accordance with Agilent's recommended configuration.



4. Things To Do Before Installing the 21 CFR 11 Assistant Software

Windows administrator requirements	29
System requirements	30
Preparing Windows Event logs	31
User accounts	31

The 21 CFR 11 Assistant software uses Microsoft Windows “New Technology” operating system functionality to implement the record keeping and security requirements of the 21 CFR Part 11 rule. The exact version of Microsoft Windows operating systems available for each software product can be found on the Agilent Web site.

This chapter outlines the Windows administrative tasks that must be performed prior to installing 21 CFR Part 11 Assistant software. These include tasks such as making room for new records and setting up password policies.

Windows administrator requirements

Installation of the 21 CFR 11 Assistant software must be carried out by an experienced Windows system administrator. This is because it is necessary to perform fundamental Windows administrative tasks such as setting up users, groups, protected directories and so on.

The Windows administrator should develop a secure and effective means of remembering their password. If the administrator cannot log on, they will not be able to perform the Windows administration tasks essential for the function of the 21 CFR 11 Assistant software. In the event that the Windows administrator does lose their password, the only way to solve the problem is to reformat the hard drive and re-install everything, including the Windows operating system, and set up accounts, policies etc., from the beginning.

System requirements

The 21 CFR 11 Assistant software can only run on a local PC. Agilent does not support, recommend or warrant the use of the 21 CFR 11 Assistant software products in conjunction with Windows networks. The software should only be operated with users registered on the local PC and with data being saved to protected directories located on the local PC.

The Agilent application software must be installed on the PC that is connected to the instrument. It cannot be installed on a server. In addition, shared PCs are not supported.

However, it is possible for the PC to be connected to a Windows network so that files stored on the local PC by the 21 CFR 11 Assistant software can be archived to a network location using third party software.

Even though the software is not being run in conjunction with a network, **Network connection** must still be selected when installing the Windows operating system for the 21 CFR 11 Assistant software to operate. If an existing PC is being used, and network options have not been installed, the Windows installation CD will be required to change the settings.

At least one NTFS (New Technology Filing System) formatted directory must be available in order to install the software and allow files to be securely saved to protected directories. Alternative file systems such as FAT (File Allocation Table) and HPFS (High Performance File System) are not adequate substitutes.

Preparing Windows Event logs

In addition to writing data to audit logs stored within files created by the Agilent application software, events are also written to the inbuilt Windows Application Event log by the 21 CFR 11 Assistant software and to the inbuilt Windows Security Event log by the Windows operating system.

Prior to installing the 21 CFR 11 Assistant software, the system administrator should archive and clear the Windows Application, System and Security Event logs. This is because, during installation, the “autodelete” event setting is changed to “manual” deletion. If any of the logs is already full, the 21 CFR 11 Assistant (see section 0) will not be able to run.

The Windows operating system does not notify the user when event logs are full. Therefore, it is important to ensure that the capacity of each log file is increased significantly from the default 512 kb setting. The log sizes should be sufficiently large to record the day’s activities.

NOTE

Once the 21 CFR Part 11 Assistant software is installed and running, the system administrator will need to archive and clear the Windows logs at regular intervals to prevent them from filling up. Refer to the Section 7 for more information about this required standard operating procedure.

User accounts

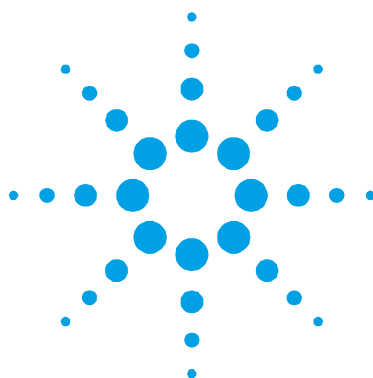
In order to meet 21 CFR Part 11 requirements, the parameters listed below must be implemented when setting up user accounts in Windows. If existing user accounts are to be used and they do not have the following parameters, they must be changed to meet these requirements.

- The user name (user identification code) must be unique for each user. This information is included in reports and audit logs to identify the user who has changed or signed electronic records.

Things To Do Before Installing the 21 CFR 11 Assistant Software

- The full name of the user must be entered in the **Full Name** field. This information is included in reports and audit logs to identify the user who has changed or signed electronic records.
- The individual's title or user group designation must be entered in the **Description** field. This information is included in reports and audit logs to identify the user who has changed or signed electronic records.
- The **Password** (and **Confirm Password**) fields cannot be left blank. The password should consist of at least six characters and be case sensitive. Initially, the system administrator must provide a temporary password.
- The **User must change password at next logon** check box must be selected. This sets up a system of passwords, known only by the user, that are changed at regular intervals. The "User cannot change password" and "Password never expires" check boxes must be cleared, as this would cause non-compliance with 21 CFR Part 11 requirements regarding the use of passwords.

Consideration should also be given to establishing groups of users who have similar roles. This makes it possible to assign access or privileges to a number of users at once. It also makes it easy to add new users (who are to have the same access and privileges as an existing group of users) to the system.



5. Checklist for the 21 CFR Part 11 Assistant Software

- Before installation 33
- During installation 34
- After installation 34

This chapter features a checklist of the major tasks that need to be carried out in order to use the 21 CFR 11 Assistant software. It is divided into tasks that need to be completed before, during and after installation of the software. Where applicable, references to sections of this booklet where more information can be found are included.

Before installation

Task	Page	Complete
Designate an experienced Microsoft Windows administrator to perform the installation.	29	
System administrator must develop a secure and effective means of remembering their password.	29	
Select "Network Connection" when installing the Windows operating system.	30	
Ensure that at least one NTFS directory is available for installation of software and saving of records.	30	
Archive and clear the Windows Application, System and Security Event logs on the local PC.	31	
Increase the size of the Windows Application, System and Security Event logs significantly from the default of 512 kb.	31	

continued

Checklist for the 21 CFR Part 11 Assistant Software

Task	Page	Complete
Ensure that user accounts have been configured as follows:	31	
Each user has a unique identification code.	31	
A full name has been entered for each user.	31	
Each user has a title or user group in the "Description" field.	31	
A password has been entered in the "Password" and "Confirm password" fields.	31	
Passwords are case sensitive and consist of at least six characters.	31	
"User must change password at next logon" is selected.	31	
"User cannot change password" and "Password never expires" are de-selected.	31	

During installation

Task	Page	Complete
Install the software according to the installation instructions supplied with the software.	37	
Refer to the "Late Breaking News" document.	37	

After installation

Task	Page	Complete
Ensure that the Windows Application, System and Security Event logs are set to "Do not overwrite events (clear log manually)".	41	
Ensure that appropriate SOPs are implemented to address elements of the 21 CFR Part 11 rule including (but not necessarily limited to):		
Personnel should have suitable education, training and experience.	19	
Appropriate controls over distribution, use of and access to documentation.	20	
Revision and change controls for documentation include audit trails.	20	
Individuals are held accountable and responsible for their electronic signatures.	25	

continued

Task	Page	Complete
The identity of an individual is verified before they are permitted to use an electronic signature.	25	
The FDA is notified that electronic signatures are intended to be equivalent to handwritten signatures.	25	
Ensure that the following SOPs are also implemented:		
Regularly archive the Agilent application electronic records.	42	
Regularly archive and clear the Windows Application, System and Security Event logs.	42	
Regularly archive the 21 CFR 11 Assistant software log files (only for 21 CFR 11 Assistant version 1.2.0.1086 or greater).	43	
Regularly check the Windows Security and Application event logs to detect attempted unauthorized use of user identification code and password combinations.	43	
Ensure the application is locked during absences from the workstation.	43	
Develop a method to distinguish between signed and unsigned files.	44	

This page is intentionally left blank.



6. Installation of the 21 CFR 11 Assistant Software

Function of the 21 CFR 11 Assistant software	37
Uninstalling the software	39

Once the system has been prepared as outlined in Section 4, the 21 CFR 11 Assistant software can be installed. To do this, refer to the software installation instructions supplied with the software package. You should also refer to the “Late Breaking News” document that is supplied with the AA software package.

Function of the 21 CFR 11 Assistant software

The 21 CFR 11 Assistant software is an application that allows the system administrator to set up the following:

- User privileges
- Protected directories
- Protected executables
- Logon warning message and account policy settings

See Section 2 for more information about these functions.

NOTE

Only users with administrator privileges can run the 21 CFR 11 Assistant software (i.e. the user must be a member of the local PC Administrator Group).

Most of these parameters can be set up using standard Microsoft Windows operating system features; however, the 21 CFR 11 Assistant software provides a more efficient setup method. The 21 CFR 11 Assistant software also enables you to nominate the protected directories to which the application software will save files.

The 21 CFR 11 Assistant software consists of a number of screens to follow through. Once selections have been made on each screen, the Next button is clicked to move to the next screen. The last screen of the 21 CFR 11 Assistant software shows a log of all the changes made during the current session. For 21 CFR 11 Assistant software version 1.2.0.1086 or greater, this log is automatically stored in an encrypted format in a protected directory on the local PC (the protected directory is created by the system administrator).

The 21 CFR 11 Assistant software automatically changes a number of PC settings to save the administrator having to make these changes manually. These changes include

- “Enforce password history” policy set to “12 passwords remembered” (Windows NT) or “24 passwords remembered” (Windows 2000 & XP).
- “Minimum password age” policy set to five days.
- “Minimum password length” policy set to six characters.

The following account policies can be set on the local PC during installation using the 21 CFR 11 Assistant software:

- The “Maximum password age” policy.
- The “Account lockout threshold” policy.

Uninstalling the software

If at any stage the particular spectroscopy system is no longer required to meet the requirements of the 21 CFR Part 11 rule, the system administrator should uninstall the 21 CFR Part 11 Assistant software. Refer to the online help for instructions on how to uninstall the software.

NOTE

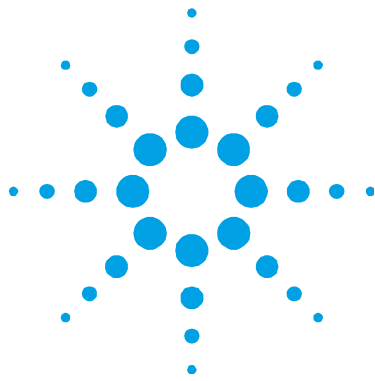
Only the system administrator is able to uninstall the 21 CFR Part 11 Assistant software.

If there are no plans to reinstall 21 CFR Part 11 Assistant software, you may wish to restore some of the operating system features (such as user settings, protected directories, password policies, etc.) that were changed during installation of the software to their initial state.

NOTE

Files generated on a 21 CFR Part 11 system are not fully accessible in a non-21 CFR Part 11 system. See section 2 for details.

This page is intentionally left blank.



7. Ongoing SOPs and Notable Items

Setting Windows Event logs	41
Ongoing standard operating procedures	42

There are a number of ongoing standard operating procedures that should be implemented once the 21 CFR 11 Assistant software has been installed. This chapter outlines those tasks and includes extra information to ensure 21 CFR 11 Assistant software is used to its full potential.

NOTE

A number of standard operating procedures that address specific elements of the 21 CFR Part 11 rule are detailed in Section 2. See the “After installation” section of Section 5 for a list of these SOPs and ensure they are implemented in addition to the SOPs outlined in this section.

Setting Windows Event logs

Ensure that the Windows Application, System and Security Event logs are set to “Do not overwrite events (clear log manually)”. This ensures that events are not overwritten and therefore not obscured as required by the 21 CFR Part 11 rule.

Ongoing standard operating procedures

It is important that the following standard operating procedures be implemented when using the 21 CFR 11 Assistant software.

Archiving Agilent application electronic records

A standard operating procedure should be developed 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 along with the relevant Windows event logs and the 21CFR 11 Assistant software log files as necessary.

Archiving Windows Event logs

It is extremely important that the Windows Application, System and Security Event logs do not reach full capacity. This is because during installation, the “autodelete” log setting is changed to “manual” so that events are not overwritten. If a log becomes full and there is no room for events to be recorded, records crucial for compliance with the 21 CFR Part 11 rule will not be created.

To prevent the Windows Event logs reaching full capacity, the Application, System and Security Event logs should be regularly archived and cleared. It is recommended that archiving and clearing should occur on a daily basis.

NOTE

Another measure that must be taken to prevent the logs from reaching full capacity is to increase the log size from the default 512 kb.

A standard operating procedure should be developed to ensure that Windows event logs are archived and stored with the associated electronic records generated by the Agilent application software, and that they can be retrieved and used over an extended period of time.

Archiving the 21 CFR 11 Assistant software logs

The 21 CFR 11 Assistant software (version 1.2.0.1086 or greater) creates a log of changes each time it is run. This log file is automatically stored in an encrypted format in a protected directory on the local PC. (The protected directory is created by the system administrator when the 21 CFR 11 Assistant software is run).

A standard operating procedure should be developed to ensure that the 21 CFR 11 Assistant software log files are archived and stored with the associated electronic records generated by the Agilent application software, and that they can be retrieved and used over an extended period of time.

Checking for breaches of security

The system administrator should check the Windows Security and Application event logs in the Event Viewer regularly for occurrences of failed attempts to use a user identification code and password combination. These can result from attempts to logon on to the PC, to sign or approve a record or 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 PC or to the application software. Only the system administrator is able to re-enable the user account.

NOTE

The account lockout threshold policy can be set to a value that suits the user organization, using the 21 CFR 11 Assistant 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 PC. This helps ensure that no unauthorized person can access the application.

Users of the AA software can lock the application by using the built in lock function within the software. It is recommended that the built in automatic lock (timeout) function is activated.

Identifying signed and approved files

When using the 21 CFR Part 11 Assistant software, it may be desirable to approve data some time after it is created. For example, a user may perform an analysis but the approver may not be available immediately to approve the data. In this situation, the user organization should develop a standard operating procedure to distinguish approved from unapproved files. For example, unapproved files could be saved in one subdirectory, and approved files in another. Alternatively, user organizations could develop a naming convention to distinguish between unapproved and approved files.

Exporting data to LIMS/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 and HTML.

End of Document