# Agilent Cary WinUV Software with Spectroscopy Configuration Manager and Spectroscopy Database Administrator (SCM/SDA)

## Compliance with 21 CFR Part 11

## Introduction

Part 11 in Title 21 of the Code of Federal Regulations includes the US Federal guidelines for storing and protecting electronic records and applying electronic signatures. The intent of these guidelines is to ensure that applicable electronic records are reliable, authentic and maintained with high integrity.

This technical note describes features and functionality of Agilent Cary WinUV (version 4.X and later) in combination with SCM and SDA for data management and electronic traceability, which enable customers to implement the guidelines of 21 CFR Part 11.

This document examines each section of 21 CFR Part 11 and provides a recommended approach using the Agilent Cary WinUV, the application software, with SCM/SDA (version 3.1 or higher). This solution provides the necessary controls for system access, user roles management, data transfer and audit trails. It also ensures secure record keeping and provides capabilities for data archiving.

## Agilent Cary WinUV with SCM/SDA: 21 CFR Part 11 Compliance

Using Agilent Cary WinUV with SCM/SDA provides support for all compliance requirements mandated by 21 CFR Part 11 for a closed system. In particular it ensures:

- Accurate and complete copies of records,
- Administration for user accounts and passwords,
- Administration for user access privileges within the application,
- Mandatory login to SCM before allowing access to Cary WinUV,
- Electronic signature functionality, and
- Records of changes captured in user-independent time-stamped audit trails

These settings can be configured during installation to meet specific standard operation procedures and security guidelines. This includes customizable user roles and privileges that provide levels of access to the application software and functionality to individual users or groups. Changes to the security configuration can be made only by a dedicated system administrator.

Details of the system design and configuration options are outlined in the manual Agilent Spectroscopy Configuration Manager (SCM) Software: 21 CFR Part 11 Compliance Booklet (part number G9272-90009) available with the installation media. Further information on validated installation scenarios is available in the Pharma Software Installation Instructions for 21 CFR Part 11 Environments (part number G6861-90025).

**Table 1.** Applicable sections of 21 CFR Part 11 for Agilent Cary WinUV with SCM/SDA operated in a closed system (✓= applicable, N/A = not applicable)

| Possible Scenarios for Cary WinUV in a closed system | Electronic signature based on User ID and Password |
|---|---|
| 11.1, 11.2, 11.3<br>Scope, implementation, definition | ✓ |
| 11.10<br>Controls for closed systems | ✓ |
| 11.30<br>Controls for open systems | N/A |
| 11.50<br>Signature manifestations | ✓ |
| 11.70<br>Signature record linking | ✓ |
| 11.100<br>e-Sig general requirements | ✓ |
| 11.200(a)<br>e-Sig not biometric | ✓ |
| 11.200(b)<br>e-Sig biometric | N/A |
| 11.300 (a), (b), (d)<br>Controls for ID codes and passwords | ✓ |
| 11.300 (e), (c)<br>Token cards and other ID devices | N/A |

## Meeting the Regulatory Requirements of 21 CFR Part 11

The following table describes how the features and functionality of Agilent Cary WinUV with SCM and SDA enables laboratories to meet the regulatory requirements of 21 CFR Part 11.

| 11.10 | Control for closed systems | | |
|---|---|---|---|
| **Section** | **Question** | **Response** | **Agilent Cary WinUV used with SCM/SDA** |
| 11.10(a) | Has the system been validated in order to ensure the ability to discern invalid or altered records?<br>What Quality Management System supports the system validation? | Yes | Agilent develops its products according to the well-established "product lifecycle" concept, which is a phase review process for software and hardware development, in order to ensure consistent product quality. This process requires the system to be subjected to an evaluation process before release to ensure software features and capabilities have consistent and intended performance.<br>Agilent delivers a fully qualified data handling system together with all necessary services, which are needed to implement such a system to meet the requirements of the FDA regarding 21CFR Part 11. A validation certificate is provided with each copy of the software.<br>Electronic records generated by Cary WinUV are stored in a protected proprietary format using a secure algorithm. If such a record is altered through another application, this will be detected by the system when trying to read the record. |
| 11.10(b) | Is the system capable of generating accurate and complete copies of all required records in both human readable and electronic form suitable for inspection, review and copying by the FDA? | Yes | The system is able to generate accurate and complete copies of all records. Specifically, all method and data files generated by Cary WinUV are stored in the SDA database as complete files in the original format.<br>The result file that includes the electronic record, data, method audit trail, operator identification and electronic signatures can be loaded at any time using the Cary WinUV software on a client PC, as a copy of the original data for review or inspection by the FDA. "Printed" reports are traceable to the original electronic files. |
| 11.10(c) | Are the records protected for accurate and convenient retrieval throughout the record retention period? | Yes | Records generated by Cary WinUV are stored in the SDA database. Once stored, records are protected against modification or deletion. The SCM/SDA has been designed so that any results, data or methods files generated by Cary WinUV are automatically stored in the SDA database.<br>Data stored in the SDA database resides in a protected storage location or archive. Additional procedural controls should be defined and implemented by the system administrator based on company-wide security policies to manage practices such as archiving and server maintenance, access to client computers and password policy management.<br>Records can be retrieved at any time by a user with the appropriate access privileges to the application. |
| 11.10(d) | Is system access limited to authorized individuals? | Yes | System access is dependent on the user having a valid and authorized user identification and password combination. Access to the system is only available for users who have been explicitly added by the system administrators. The system administrators also determine the levels of access and functionality to both Cary WinUV and the SCM/SDA. The management of Cary WinUV users, roles and privileges occurs in the SCM.<br>Access to Cary WinUV requires the entry of both identification components: user ID and password. Password administration is performed by the system administrator depending on internal standard operating procedures. The system supports password aging, and can be used to enforce minimum password length and composition. All access violations, such as a login failure due to incorrect password, are recorded in the SCM System and Security audit trail. In addition, the system can be locked, both manually and set as an automatic log out after a configurable period of non-attendance.<br>All file and software functionality access is controlled by specific privileges and roles assigned to individual users or groups of users. The Cary WinUV privileges are available to allow limited system access to authorized individuals and control the access level of different user roles. The system offers several pre-defined user roles, to which more can be added or customized by the system administrator. Depending upon access restrictions, menu items, graphical elements or views in the application can be enabled or disabled. |

| 11.10 | Control for closed systems | | |
|---|---|---|---|
| **Section** | **Question** | **Response** | **Agilent Cary WinUV used with SCM/SDA** |
| **11.10(e)** | Is there a secure, computer-generated audit trail that independently records the date and time of operator entries and actions that create, modify or delete electronic records? | Yes | All actions related to creating, modifying or deleting electronic records are recorded in a secure, computer-generated, time-stamped audit trail. The audit trial lists all modifications, date and time of the change, the user ID and reason for the change if applicable. Entries in the audit trail are user-independent, and cannot be altered or deleted by the user.<br>Cary WinUV together with SCM/SDA ensures that all data is stored along with raw data and results. A Cary WinUV result batch file contains all the method, sample and data associated with the record, as well as the application audit trail, to maintain full data integrity.<br>Cary WinUV and SCM/SDA provide two types of audit trails:<br>1. SCM Audit Trails: The SCM audit trails record user access to the system as well as any changes made by the system administrator within the SCM. The recorded activities include items such as file save events, application logon or logoff, and electronic signatures as well as any changes to user accounts or privileges and profiles. The SCM audit trails can be archived and retrieved at any time.<br>2. Cary WinUV Audit Trail: The application has a single audit trail that captures all changes within the software. This includes changes to the method and data analysis parameters. These changes are tracked with user ID, date and time and instrument serial number. |
| **11.10(e)** | When records are changed, is previously recorded audit trail information left unchanged? | Yes | When any change occurs to a Cary WinUV file, the changes require a new filename associated only with that electronic record. In addition, an entry in the audit trail is generated, and this is automatically saved with the associated electronic record. These audit trail entries are non-editable and non-deletable and document that the original file has been changed, the time and date and operator.<br>Strict revision control of the data generated by Cary WinUV is achieved by forcing automatic storage of the result set in the SDA database before any further action, such as loading new methods, or closing the application. |
| **11.10(e)** | Are electronic audit trails saved at least as long as their subject electronic records and available for agency review and copying? | Yes | All Cary WinUV audit trail information is automatically saved with the associated electronic record and is available during the retention period. System-related activities such as logon events that are automatically documented in the SCM audit trail are unbreakably linked to the system.<br>The audit trail can be viewed and printed from within the Cary WinUV software. |
| **11.10(f)** | Are operational system checks used to enforce permitted sequencing of steps and events? | Yes | When a sequencing of events is required, system checks enforce it. A few examples are:<br>• If only approved methods are to be used in QA/QC, this can be achieved by restricting user access to the approved methods stored in the SDA database.<br>• Within Cary WinUV, sequencing of events are enforced with regards to electronic records in that the software ensures that required settings and facilities are available before allowing data to be collected and analyzed, or ensuring files are saved before Cary WinUV is closed.<br>All events within the system are ordered and time stamped within the audit trail. |
| **11.10(g)** | Are authority checks in place to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the current operation? | Yes | Users cannot gain access to Cary WinUV or to SCM/SDA without a valid user ID, password and account. Only a successful logon to the system offers access to files and general software functionality, spectrophotometric software functions or archival and approval functionality. The user must authenticate with a valid user ID, password and account. This applies at application initiation and after every inactivity timeout or manual logout. User-access to specific functionality in the software is further restricted by the privileges assigned to the individual user. These privileges can be combined into roles if necessary.<br>Upon entry of a user ID and password, the system checks whether the user ID, password, group and project and whether the given password is valid and in accordance with the defined account policies and password settings. |

| 11.10 | Control for closed systems | | |
|---|---|---|---|
| **Section** | **Question** | **Response** | **Agilent Cary WinUV used with SCM/SDA** |
| **11.10(h)** | Are device checks used to determine, as appropriate, the validity of the source of data or operational instruction? | Yes | Access to the instrument is limited to the configured device only. The system is able to recognize instrument models and serial numbers and uses proprietary binary communications. The instrument type, firmware revision number and serial number are passed from the spectrophotometer to the Cary WinUV software. The instrument serial number is recorded in the Cary WinUV report, which is stored in the SDA database. Qualification of the software must be executed to ensure that devices and software are functioning properly. |
| **11.10(i)** | Do the persons who develop, maintain, or use electronic records and signature systems have the education, training and experience to perform their assigned tasks? | Yes | Records of the educational and employment history of Agilent employees are verified and can be made available during an on-site audit. In addition, all relevant Agilent Technologies employees have attended training workshops for regulatory requirements.<br>Users of Cary WinUV or the SCM/SDA will be required to show records of education, training and/or experience with the system. Agilent provides a basic familiarization during the installation of the product for system users. Training courses for administrators as well as users are available. |
| **11.10(j)** | Have written policies that hold individuals accountable and responsible for their actions initiated under their e-signatures in order to deter record and signature falsification been established and followed? | N/A | It is the responsibility of the organization implementing e-signatures to develop written policies which ensure that individuals responsible for signing documents understand that their electronic signature is as equally binding as their handwritten signature. |
| **11.10(k)(1)** | Are there adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance? | N/A | While documentation is available for the users and administrators of the system, controls over the storage and distribution of this material are the responsibility of the organization that implements and uses the system. |
| **11.10(k)(2)** | Are there formal revision and change control procedures to maintain an audit trail that documents time-sequenced development and modifications of systems documentation? | Yes | Agilent Technologies' quality process includes written formal revision and change control procedures for system documentation. All revisions to the documents kept are time stamped and audit-trailed. |

| 11.30 | Control for open systems | | |
|---|---|---|---|
| **Section** | **Question** | **Response** | **Agilent Cary WinUV used with SCM/SDA** |
| **11.30** | Are there procedures and controls used to protect the authenticity, integrity and confidentiality of the electronic records from their creation point to the point of their receipt? | N/A | The system is a closed system. |
| **11.30** | Are additional measures used to ensure the confidentiality of the electronic records from the point of their creation to the point of their receipt? | N/A | The system is a closed system. |

| 11.50 | Signature manifestation | | |
|---|---|---|---|
| **Section** | **Question** | **Response** | **Agilent Cary WinUV used with SCM/SDA** |
| 11.50(a) | Do signed electronic records contain information associated with the signing that clearly indicates all of the following:<br>• The printed name of the signer;<br>• The date and time when the signature was executed; and<br>• The meaning associated with the signature? | Yes | The Cary WinUV results can be electronically signed and approved by users with specific Approval privileges. The electronic signature and approval manifestation includes:<br>• User ID in addition to the full name of the signer<br>• Signer's title or profile<br>• Date and time that the signature was applied<br>• User-configurable meaning associated with the signature<br>All signatures are saved with the result file. |
| 11.50(b) | Are these items part of any human readable form of the electronic record? | Yes | Electronic signature events are automatically captured in the computer generated system audit trail, and are only possible by a user with the relevant access privileges, and a valid user identification and password.<br>The electronic signature will appear in the Cary WinUV report, which is both displayed electronically and can be printed. |

| 11.70 | Signature/record linking | | |
|---|---|---|---|
| **Section** | **Question** | **Response** | **Agilent Cary WinUV used with SCM/SDA** |
| 11.70 | Is the electronic signature linked to its respective electronic record to ensure that the signature cannot be excised, copied or otherwise transferred to falsify an electronic record by ordinary means? | Yes | Within Cary WinUV signatures and approvals can be entered and require a system checked user ID and password.<br>Electronic signatures cannot be transferred from one record or file to another, including the automatic entry in the application audit trail, which is always saved with the electronic record. |

| 11.100 | Electronic signatures - general requirements | | |
|---|---|---|---|
| **Section** | **Question** | **Response** | **Agilent Cary WinUV used with SCM/SDA** |
| 11.100(a) | Is each electronic signature unique to one individual and not reused by, or reassigned to, anyone else? | Yes | The Cary WinUV signature and approval tool employs two distinct identification components: unique user ID and password. Each user requires a unique and valid user identification and password. |
| 11.100(b) | Are the identities of the individuals verified before the organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature? | N/A | This is the responsibility of the organization that plans, implements and operates the system. Such a verification process is a system requirement that is set before implementing electronic signature procedures or assigning electronic signature privileges to an individual. |
| 11.100(c) | Has the organization delivered its declaration of e-signature use to FDA prior to or at the time of such use?<br>Is it in paper form with a traditional hand-written signature?<br>Can additional certification or testimony be provided so that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature? | N/A | It is the company's responsibility, before submitting electronically signed documentation to the FDA, to register their intent to use electronic signatures. In addition, training programs must be in place to ensure that users signing documents electronically understand the legal significance of their electronic signature. |

| 11.200 | Electronic signature components and controls | | |
|---|---|---|---|
| **Section** | **Question** | **Response** | **Agilent Cary WinUV used with SCM/SDA** |
| **11.200(a) (i)** | Does the e-signature employ at least two distinct identification components such as user ID and password? | Yes | The Cary WinUV signature and approval tool employs two distinct identification components: unique user ID and password. Each user requires a unique and valid user ID and password. No two users can have the same user ID/password combination. |
| **11.200(a) (1)(i)** | When an individual executes a series of signings during a single, continuous period of controlled system access, is the first signing executed using all the electronic signature components? | Yes | When an individual signs the first of a series of documents during a single period of controlled access, the user is required to enter both signature components: user ID and password. |
| **11.200(a) (1) (i)** | When an individual executes a series of signings during a single, continuous period of controlled system access, is each subsequent signing executed using at least one electronic signature component that is only executable by, and designed to be used by, the individual? | Yes | Both components, a user ID and password, are required for a user executing a series of continuous electronic signatures for Cary WinUV signature application. |
| **11.200(a) (1) (ii)** | When an individual executes a series of signings not performed during a single, continuous period of controlled system access, does each signing executed require all signature components? | Yes | Each signature when not performed during a continuous period of controlled system access requires all signature components. |
| **11.200(a) (2)** | Are controls in place to ensure that only their genuine owners can use the electronic signature? | Yes | Cary WinUV used with the SCM/SDA can be configured so that an administrator assigns an initial password to a user for a new account or forgotten password, but the user is required to change that password on their first login. In this way, the user ID and password combination is known only to the individual. No two users can have the same user ID/password combination. |
| **11.200(a) (3)** | Are the electronic signatures to be administered and executed to ensure that the attempted use of an individual's electronic signature by anyone other than its genuine owner requires the collaboration of two or more individuals? | Yes | Cary WinUV used with the SCM/SDA can be configured so that an administrator assigns an initial password to a user for a new account or forgotten password, but the user is required to change that password on their first login. In this way, the user ID and password combination is known only to the individual. No two users can have the same user ID/password combination.<br>The enforcement of this policy is the responsibility of the organization that operates the system. Therefore, it requires active collaboration with the purpose of sharing passwords to enable irregular use of another users' identification. |
| **11.200(b)** | Are electronic signatures based on biometrics designed to ensure that only their genuine owners can use them? | N/A | The system does not support signatures based on biometrics at this time. |

| 11.300 | Controls for identification codes/passwords | | |
|---|---|---|---|
| **Section** | **Question** | **Response** | **Agilent Cary WinUV used with SCM/SDA** |
| **11.300(a)** | Are controls in place to ensure the uniqueness of each combined identification code and password maintained, such that no two individuals have the same combination of identification code and password? | Yes | Cary WinUV used with SCM/SDA requires users to authenticate with user ID and password. Each user in the system must be unique and assigned to a specific user account. Each user requires a unique and valid user identification and password. |
| **11.300(b)** | Are controls in place to ensure that the identification code and password issuance is periodically checked, recalled, and revised? | Yes | All aspects of password administration such as password aging, history and minimum length can be designated with the SCM. The administrator can define a time frame in which passwords are periodically revised automatically. Users can be prevented from reusing passwords. |
| **11.300(c)** | Are there loss management procedures in place to electronically disable lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information? | N/A | The system does not support devices that bear or generate identification codes, such as tokens or cards, at this time. |
| **11.300(d)** | Are transaction safeguards in place to prevent unauthorized use of passwords and/or identification codes? | Yes | Only the user knows their user ID and password. Passwords are always displayed as asterisks and are stored encrypted so that even an administrator cannot see them.<br>All attempts to access the system including both successful and unsuccessful logon attempts are recorded in the SCM System Audit Trail. |
| **11.300(d)** | Are transaction safeguards in place to detect and report in an immediate and urgent manner, any attempts at their unauthorized use to the system security unit and, as appropriate, to organizational management? | Yes | The SCM user policy can be configured so that a defined number of unauthorized access attempts locks out the user account.<br>All attempts to access the system including both successful and unsuccessful logon attempts are recorded in the SCM System Audit Trail. |
| **11.300(e)** | Are there controls in place to initially test devices that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner? | N/A | The system does not support devices that bear or generate identification codes, such as tokens or cards, at this time. |

To learn more about Agilent molecular spectroscopy products visit:
www.agilent.com/chem/molecularspectroscopy
To learn more about Agilent compliance software visit:
www.agilent.com


Published on December 3, 2014
Publication Number: 5991-5406EN

The Measure of Confidence

Agilent Technologies