Integration of Agilent UV-Visible ChemStation with OpenLAB ECM

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 UV-Visible ChemStation (revision B.05.XX) in combination with Agilent OpenLAB Enterprise Content Manager (ECM) for data management, 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 integration of Agilent UV-Visible ChemStation or higher with Agilent OpenLAB Enterprise Content Manager (ECM) revision 3.4.1 SP1.

Agilent UV-Visible ChemStation has a tight integration to OpenLAB ECM. This solution provides the necessary controls for system access, user roles management, data transfer and audit trail. It also ensures secure record keeping and data archiving.

OpenLAB ECM has been successfully implemented by many leading pharmaceutical and life science companies to satisfy compliance requirements such as 21 CFR Part 11.

Agilent UV-Visible ChemStation with Agilent OpenLAB ECM: 21 CFR Part 11 Compliance

The integration of UV-Visible ChemStation with OpenLAB ECM enables the operation of UV-Visible ChemStation in full support of all compliance requirements mandated by 21 CFR Part 11 for a closed system. In particular it ensures:

- Accurate and complete copies of records
- Versioning of all relevant records for traceability
- Preservation of records between their creation and their transfer to OpenLAB ECM immediately after acquisition, reprocessing or interactive modifications
- Controlled copies of the data
- Mandatory login to OpenLAB ECM before allowing access to the ChemStation
- Records of changes captured in user-independent time-stamped audit trails

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

Details and recommendations for configuration of the system are outlined in the manual *Agilent UV-Visible ChemStation OpenLAB ECM Compliance Pack Concept Guide*, Part Number G5182-90000 available on the UV-Visible ChemStation installation media.

The integration of UV-Visible ChemStation with OpenLAB ECM was not specifically designed for operation in an open system.

Table 1. Applicable sections of 21 CFR Part 11 for Agilent UV-Visible ChemStation with OpenLAB ECM operated in a closed system (✓= applicable, N/A = not applicable)

Possible Scenarios for ChemStation in a closed system	Electronic signature based on User ID and Password
11.1, 11.2, 11.3 Scope, implementation, definition	✓
11.10 Controls for closed systems	✓
11.30 Controls for open systems	N/A
11.50 Signature manifestations	✓
11.70 Signature record linking	✓
11.100 e-Sig general requirements	✓
11.200(a) e-Sig not biometric	✓
11.200(b) e-Sig biometric	N/A
11.300 (a), (b), (d) Controls for ID codes and passwords	✓
11.300 (e), (c) 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 UV-Visible ChemStation, in combination with OpenLAB ECM, enables laboratories to meet the regulatory requirements of 21 CFR Part 11.

11.10	Control for closed systems		
21 CFR Part 11	Requirement	Result	UV-Visible ChemStation and OpenLAB ECM Integration
11.10(a)	Has the system been validated in order to ensure the ability to discern invalid or altered records? What Quality Management System supports the system validation?	Yes	Agilent Technologies has extensively validated the performance of UV-Visible ChemStation and OpenLAB ECM with tests written to specifically evaluate accuracy, reliability and consistent performance. The integrated solution of UV-Visible ChemStation with OpenLAB ECM incorporates the use of byte-order dependent check sums at each file transfer operation to ensure that records are valid and unaltered. 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. Agilent Technologies recommends the use of Installation Qualification and Operation Qualification (IQ/OQ) services for UV-Visible ChemStation and OpenLAB ECM to validate the on-site system per compliance requirements.
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	OpenLAB ECM stores all data types, from raw machine data to reports generated by the application software. All files are unaltered and stored in the original format. Raw data, metadata and result data generated by UV-Visible ChemStation are stored and managed in OpenLAB ECM. The result set that holds all this information can be loaded at any time using the ChemStation software on a client PC, as a copy of the original data for review. "Printed" reports are traceable to the original electronic files. User guides are provided which address the generation of electronic copies and the printout of electronic records.
11.10(c)	Are the records protected for accurate and convenient retrieval throughout the record retention period?	Yes	Records generated by UV-Visible ChemStation are stored in a system audit trail and are managed in OpenLAB ECM. Records in OpenLAB ECM cannot be modified or deleted without appropriate access. Any change to a file is automatically recorded in the system audit trail. The integration of UV-Visible ChemStation with OpenLAB ECM has been designed so that all data, metadata and results are automatically stored in OpenLAB ECM. Data stored in OpenLAB ECM resides in a protected storage location or archive media or both. The data is searchable to all users with appropriate privileges. Additional procedural controls should be defined and implemented by the system administrator based on company-wide security policies to manage practices such as archiving, server maintenance, access to client computers and password policy management.

11.10	Control for closed systems		
21 CFR Part 11	**Requirement**	**Result**	**UV-Visible ChemStation and OpenLAB ECM Integration**
11.10(d)	Is system access limited to authorized individuals?	Yes	Each user is identified by a unique user ID and password combination. The system administrator determines levels of access and functionality to both UV-Visible ChemStation and OpenLAB ECM. The management of UV-Visible ChemStation users, roles and privileges occurs in the OpenLAB ECM web client Administration tab. Access to UV-Visible ChemStation and OpenLAB ECM 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 ECM System audit trail. In addition, the system can be locked both privately and non-privately (any user can log in), both manually and set as an automatic log out after a configurable period of non-attendance. All file and software functionality access is controlled by specific privileges and roles assigned to individual users or groups of users. In addition to ECM-specific privileges in ECM user administration, a set of more than 20 UV-Visible ChemStation privileges is 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 for UV-Visible ChemStation access levels, to which more can be added or customized by the system administrator. Depending upon access restrictions, menu items, graphical elements or views in the ChemStation can be enabled or disabled.
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	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 trails cannot be altered or deleted by a user. The UV-Visible ChemStation and OpenLAB ECM integration ensures that all metadata is stored along with raw data and results. A UV-Visible ChemStation result file contains all the method, sample and data associated with the record, as well as the UV-Visible ChemStation audit trail, to maintain full data integrity. The UV-Visible ChemStation and OpenLAB ECM integration provides two types of audit trails: • OpenLAB ECM Audit Trail: The OpenLAB ECM audit trail records who has accessed the system and what operations have been performed during a given period of time. The recorded activities include items such as data storage, versioning, and electronic signatures. Removing records from the database does not affect existing entries in the audit trail. Logon and logoff from UV-Visible ChemStation, as well as user changes, are similarly documented. • UV-Visible ChemStation 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. In addition, the OpenLAB ECM System log keeps a record of all changes to the OpenLAB ECM system, including configuration edits, email notifications, and additions, removals or changes of locations, cabinets, drawers or folders.
11.10(e)	When records are changed, is previously recorded audit trail information left unchanged?	Yes	All entries in UV-Visible ChemStation and OpenLAB ECM audit trails are non-editable and non-deletable. Removal of records from OpenLAB ECM by an authorized user does not affect existing entries in the audit trail. Strict revision control of the data generated by the ChemStation is achieved by forcing automatic storage of the result set in OpenLAB ECM before any further ChemStation action, such as loading new methods, changing modes or closing the application.

11.10	Control for closed systems		
21 CFR Part 11	**Requirement**	**Result**	**UV-Visible ChemStation and OpenLAB ECM Integration**
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 OpenLAB ECM Audit trail information is stored in the OpenLAB ECM repository as part of a file's metadata and kept throughout the electronic records retention period. The OpenLAB ECM audit trails are unbreakably linked to the records. System-related activities such as logon events are unbreakably linked to the system. The UV-Visible ChemStation audit trail is stored with each data file, which is stored in OpenLAB ECM. This ensures an unbreakable link between record and related audit trail. The audit trail can be viewed and printed from within the application software.
11.10(f)	Are operational system checks used to enforce permitted sequencing of steps and events?	Yes	Yes, when a sequencing of events is required, system checks enforce it. For example: • A process that requires sequenced steps is the archive or delete procedure. In OpenLAB ECM, record retention policies can be set up to ensure the controlled deletion of records at the end of the record retention period. These record retention policies include review and arbitration procedures. • 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 OpenLAB ECM. • Within UV-Visible ChemStation 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 the mode is switched or the application is closed. The UV-Visible ChemStation and ECM user privileges are entirely managed by a system administrator and restrict the user to an automatic transfer of the records from ChemStation to OpenLAB ECM. This ensures records are always stored in OpenLAB ECM.
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 OpenLAB ECM 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.
11.10(h)	Are device checks used to determine, as appropriate, the validity of the source of data or operational instruction?	Yes	For UV-Visible ChemStation, instrument serial numbers are transferred electronically from the instrument to the application on the PC. The instrument type, firmware revision number and serial number are passed from the spectrophotometer to the software. The instrument serial number is recorded in the UV-Visible ChemStation full report, which is stored in OpenLAB ECM. Qualification of the software must be executed to ensure that devices and software and functioning properly. User entry fields in UV-Visible ChemStation provide feedback to the user about the entry types and ranges that are valid for a particular field.

11.10	Control for closed systems		
21 CFR Part 11	**Requirement**	**Result**	**UV-Visible ChemStation and OpenLAB ECM Integration**
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 Agilent Technologies employees who work with regulations have attended training workshops for regulatory requirements. Users of UV-Visible ChemStation and OpenLAB ECM will be required to show records or 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	N/A. While documentation is available for ChemStation and OpenLAB ECM for users and administrators, 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		
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?	Yes	When a file is transferred to or within OpenLAB ECM, a byte-order dependent checksum is calculated on the file in its source location. A copy of the file is made in the destination location where a second checksum is calculated. The two values are compared and, if they are identical, the transfer is complete. If the values do not match, an error message is generated. The integration of UV-Visible ChemStation with OpenLAB ECM was not specifically designed for operation in an open 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?	Yes	OpenLAB ECM supports the use of Secure Socket Layer (SSL) encryption for security during data transmission. SSL breaks a single file into very small data packets. These data packets are individually encrypted with configurable 64-bit or 128-bit encryption before being transmitted. On the receiving side, the data packets are decrypted and reassembled. The integration of UV-Visible ChemStation with OpenLAB ECM supports SSL encryption. The integration of UV-Visible ChemStation with OpenLAB ECM was not specifically designed for operation in an open system.

11.50	Signature manifestation		
21 CFR Part 11	**Requirement**	**Result**	**UV-Visible ChemStation and OpenLAB ECM Integration**
11.50(a)	Do signed electronic records contain information associated with the signing that clearly indicates all of the following: • The printed name of the signer; • The date and time when the signature was executed; and • The meaning (such as review, approval, responsibility, or authorship) associated with the signature?	Yes	The UV-Visible ChemStation results contained in the SSIZip file can be electronically signed in OpenLAB ECM. OpenLAB ECM's electronic signature manifestation includes: • User ID in addition to the full name of the signer • Signer's title • Date and time that the signature was applied • Location where the signed occurred • User-configurable meaning associated with the signature Within UV-Visible ChemStation signatures can be entered and require a system checked user ID and password. These are recorded in the ChemStation signature logbook with full name, date and time and reason for signature. All signatures are saved with the result file.
11.50(b)	Are these items subject to the same controls as for electronic records and included as part of any human readable form of the electronic record (such as electronic display or printout)?	Yes	Electronic signatures placed on SSIZip files are viewable in the OpenLAB ECM user interface. Within UV-Visible ChemStation, all signatures are saved with the result file and documented in the signature logbook with date, time, reason and full name of the user who signed the result.

11.70	Signature/record linking		
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	The UV-Visible ChemStation results (SSIZip file) can be electronically signed in OpenLAB ECM. The electronic signature is unbreakably linked to the file. Within UV-Visible ChemStation signatures can be entered and require a system checked user ID and password. These are recorded in the ChemStation signature logbook with full name, date and time and reason for signature. All signatures are saved with the result file. All entries in the signature logbook are non-editable and non-deletable.

11.100	Electronic signatures - general requirements		
11.100(a)	Is each electronic signature unique to one individual and not reused by, or reassigned to, anyone else?	Yes	OpenLAB ECM uses the user ID and password combination unique to each user in the electronic signature feature. User IDs within ChemStation with OpenLAB ECM must be unique and cannot be reused or reassigned to another individual. Regardless of whether ChemStation and OpenLAB ECM uses Windows validated users or OpenLAB ECM administered users, no two users can have the same combination of user ID 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? Is it in paper form with a traditional hand-written signature? 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		
21 CFR Part 11	Requirement	Result	UV-Visible ChemStation and OpenLAB ECM Integration
11.200(a) 1	Does the e-signature employ at least two distinct identification components such as user ID and password?	Yes	Both the OpenLAB ECM electronic signature tool and the UV-Visible ChemStation signature tool employ two distinct identification components: unique 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 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	Either one signature component for an OpenLAB ECM user executing a series of continuous electronic signatures, or both components (user ID and password) for UV-Visible ChemStation 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	OpenLAB ECM 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. Whether OpenLAB ECM uses the company's Windows domain logins to validate the users or OpenLAB ECM administrated users, no two users can have the same user ID/password combination. The system administrator is aware of user IDs when he installs the users. During installation he can force a password change during the first logon. This password is only known to each user as it is defined during the first logon. 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. OpenLAB ECM can be configured so that an administrator can assign 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.
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	OpenLAB ECM can be configured so that an administrator can assign 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. 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	OpenLAB ECM does not support signatures based on biometrics at this time.

11.300	Controls for identification codes/passwords		
21 CFR Part 11	**Requirement**	**Result**	**UV-Visible ChemStation and OpenLAB ECM Integration**
11.300(a)	Are controls in place to ensure the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password?	Yes	UV-Visible ChemStation and OpenLAB ECM requires users to authenticate with user ID and password. Whether UV-Visible ChemStation and OpenLAB ECM uses the company's Windows domain logins to validate users or OpenLAB ECM administrated users, no two users can have the same user ID/password combination.
11.300(b)	Are controls in place to ensure that the identification code and password issuance is periodically checked, recalled and revised (e.g., to cover such events as password aging)?	Yes	If using Windows domain authentication, password renewal interval is configured as part of the Windows password policy setup. The administrator can define a time frame in which passwords are periodically revised automatically. Users are prevented from reusing passwords. If users are administrated in OpenLAB ECM, OpenLAB ECM can be configured such that user passwords are automatically, periodically revised.
11.300(c)	Are there loss management procedures in place to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls?	N/A	Neither OpenLAB ECM nor UV-Visible ChemStation 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	UV-Visible ChemStation / OpenLAB ECM can be configured such that only the user knows their user ID and password. Passwords are always displayed as asterisks and are stored encrypted within the database so that even an administrator cannot see them.
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	OpenLAB ECM can be configured so that a user-defined number of unauthorized access attempts locks out the user account and sends an email notification to a system administrator. The Windows security policy can be configured so that a user defined number of unauthorized access attempts locks out the user account and sends email notification to a system administrator. The system audit trail documents general events such as logon attempts to the computer as well as application or user changes, in the Windows Event log as a central audit repository for all security information. This includes the system and computer ID along with the operator name and application identification, allowing for an immediate check of the potential security leak.
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	Neither OpenLAB ECM nor UV-Visible ChemStation 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/chem/openlab

Published on November 27, 2014
Publication Number: 5991-3449EN

The Measure of Confidence

Agilent Technologies