
Compliance Guide

# Using the Thermo Scientific Dionex Chromeleon 7 Chromatography Data System (CDS) to Comply with 21 CFR Part 11

Thermo SCIENTIFIC

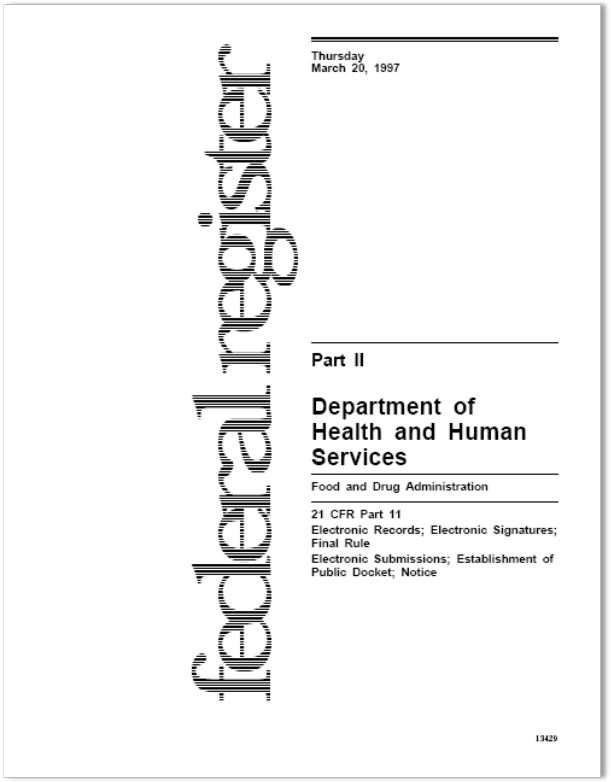
# Table of Contents

# Introduction

The Electronic Records and Signatures Rule, known as 21 CFR Part 11, was established by the U.S. Food and Drug Administration (FDA) in order to define requirements for the use of electronic documents in lieu of paper records. The law, published in the Federal Register on March 20, 1997 and in effect since August 20, 1997, specifies the system elements, controls, and procedures that are necessary to ensure the trustworthiness of electronically stored records.

Compliance requires both procedural controls and administrative controls, such as Standard Operating Procedures (SOPs), training, administration to be put in place by the user, in addition to the technical controls and elements that the system can offer. Therefore no product alone can fully meet the regulatory requirements. However, products with integrated functions that support 21 CFR Part 11 requirements can significantly ease the task of achieving and maintaining full compliance with the law.

Part 11 has a total of 19 requirements. Some of them are specific to Part 11; others are more generic requirements of some or all FDA regulations. This document lists all 19 requirements but highlights and focuses on sections of 21 CFR Part 11 that are relevant to the Thermo Scientific™ Dionex™ Chromeleon™ Chromatography Data System software and describes in detail how it facilitates compliance with the requirements.


federal register

Thursday
March 20, 1997

Part II

Department of Health and Human Services

Food and Drug Administration

21 CFR Part 11
Electronic Records; Electronic Signatures; Final Rule
Electronic Submissions; Establishment of Public Docket; Notice

13429

# PART 11—Electronic Records; Electronic signatures

## Subpart A— General Provisions

### § 11.1 SCOPE

a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations.

c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2, unless paper records are specifically required.

e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspections.

The Chromeleon CDS has been designed to fully meet the requirements of 21 CFR Part 11 Electronic Records and Electronic Signatures, providing features that allow users to implement controls in accordance with their interpretation. This fulfills the requirements for the entire life cycle of the electronic records.

The electronic records of the Chromeleon CDS are described in Section § 11.3 of this document, which discusses their creation, modification, maintenance, archiving, and retrieval. Transmission of electronic records to agencies is discussed in Section § 11.2.

With each shipment of Chromeleon CDS, Thermo Fisher Scientific provides detailed user documentation, certificates of software validation, and support documentation for on-site system validation.

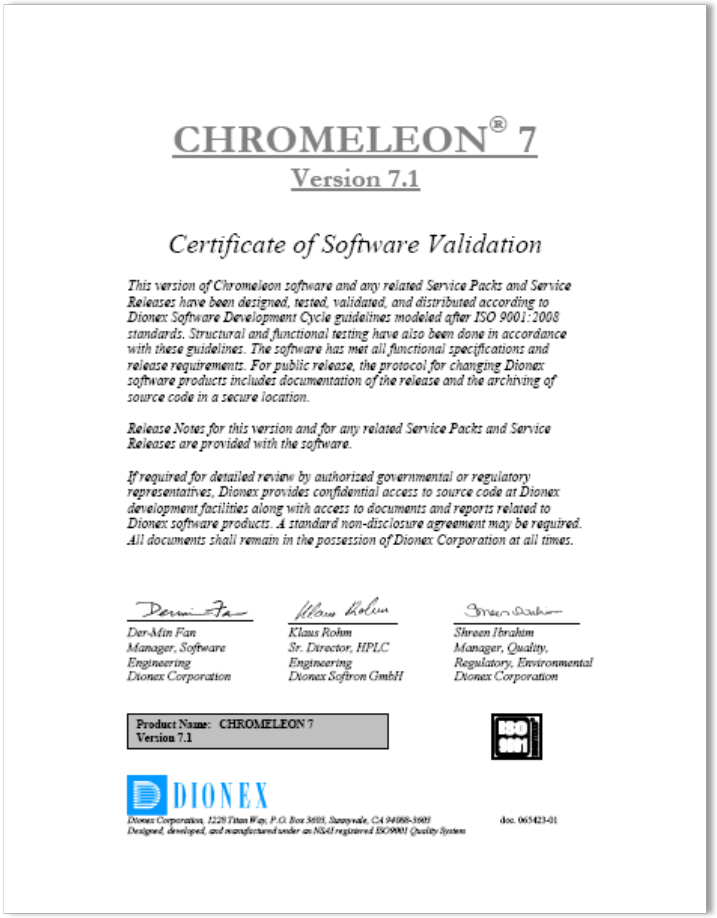
Thermo Fisher Scientific stores copies of all versions of its software documentation and source code in multiple secure locations—including a fireproof vault. Documentation includes product requirements, product specifications, design specifications, project schedules, test plans, test results, and validation documentation. All of these documents are produced for every release in accordance with the Thermo Fisher Scientific Design Control Procedure, which has been registered to ISO 9001 and is periodically audited. All Thermo Fisher Scientific documents and source code are available for inspection by FDA at Thermo Fisher Scientific facilities.

To be prepared for a possible FDA audit, customers should retain the following documents at their facilities:

- Certificate of Software Validation (Figure 1), which is included on the distribution media with the software.
- Completed Installation Qualification records (blank forms and procedures for the hardware installation are available from Thermo Fisher Scientific; the software automatically performs software IQ tests to

verify that program files are correctly installed, and stores the results on the system; software installation qualification procedures and protocols can also be obtained from Thermo Scientific representatives).

- Operational Qualification and Performance Qualification records for the systems and methodologies used (Chromeleon CDS includes utilities and report forms that help laboratories standardize and automate the software and hardware OQ and hardware PQ tests).
- Site specific standard operating procedures for security and records management.



CHROMELEON® 7

Version 7.1

*Certificate of Software Validation*

*This version of Chromeleon software and any related Service Packs and Service Releases have been designed, tested, validated, and distributed according to Dionex Software Development Cycle guidelines modeled after ISO 9001:2008 standards. Structural and functional testing have also been done in accordance with these guidelines. The software has met all functional specifications and release requirements. For public release, the protocol for changing Dionex software products includes documentation of the release and the archiving of source code in a secure location.*

*Release Notes for this version and for any related Service Packs and Service Releases are provided with the software.*

*If required for detailed review by authorized governmental or regulatory representatives, Dionex provides confidential access to source code at Dionex development facilities along with access to documents and reports related to Dionex software products. A standard non-disclosure agreement may be required. All documents shall remain in the possession of Dionex Corporation at all times.*

*Der-Min Fan*
*Manager, Software Engineering*
*Dionex Corporation*

*Klaus Rohm*
*Sr. Director, HPLC Engineering*
*Dionex Softron GmbH*

*Shreen Ibrahim*
*Manager, Quality, Regulatory, Environmental*
*Dionex Corporation*

Product Name: CHROMELEON 7
Version 7.1

DIONEX

*Dionex Corporation, 1228 Titan Way, P.O. Box 3603, Sunnyvale, CA 94088-3603*
*Designed, developed, and manufactured under an NSAI registered ISO9001 Quality System*

doc. 065423-01

**Figure 1: Thermo Fisher Scientific includes an electronic copy of the Certificate of Validation on the software distribution media.**

## § 11.2 IMPLEMENTATION

a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

- (1) The requirements of this part are met; and
- (2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records.

Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission

Chromeleon CDS produces electronic reports which are protected together with their raw data, as described in Section § 11.3. Chromeleon users can easily export copies of electronic records in Portable Document Format (PDF) for submission to agency units, in accordance with FDA guidelines. The PDF files faithfully preserve the contents and formatting of the Chromeleon CDS reports (Figure 2), including fields listing the people who electronically signed the records.

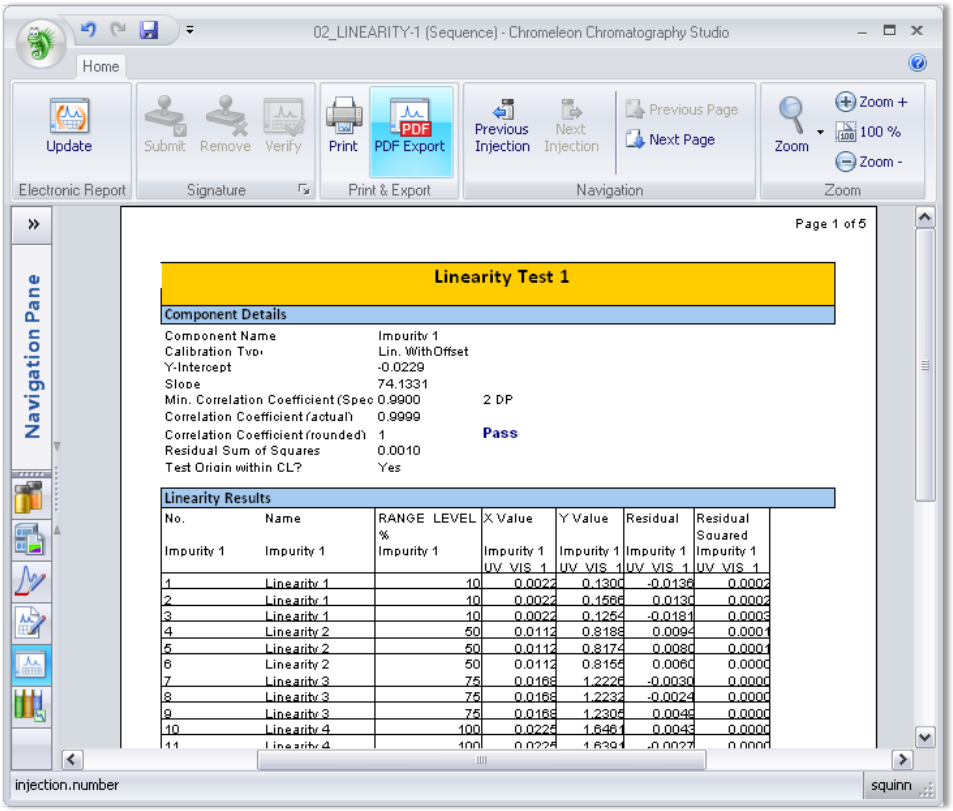



**Figure 2: Chromeleon CDS reports can be exported as PDF files for convenient submission of results to regulatory agencies, and as XLS files for convenient collation with other tabular data.**

## § 11.3 DEFINITIONS

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

b) The following definitions of terms also apply to this part:

- (1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201–903 (21 U.S.C. 321–393)).
- (2) Agency means the Food and Drug Administration.
- (3) Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.
- (4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.
- (5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.
- (6) Electronic record means any combination of text, graphics, data, audio, pictorial or other information representation in digital form, that is created, modified, maintained, archived, retrieved or distributed by a computer system.
- (7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.
- (8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.
- (9) Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

The Chromeleon CDS is normally implemented in a closed-system environment, where those persons responsible for the electronic records, control access to the system. These persons include system administrators, who maintain user accounts, plus any other persons (e.g. laboratory managers) who are granted roles with relevant privileges to control access to locations where Chromeleon CDS data are stored. The Chromeleon CDS security system (Figure 3) supplements the security systems of the chosen operating system and relational database management software by providing control over specific chromatography related resources and operations, in addition to files and records.

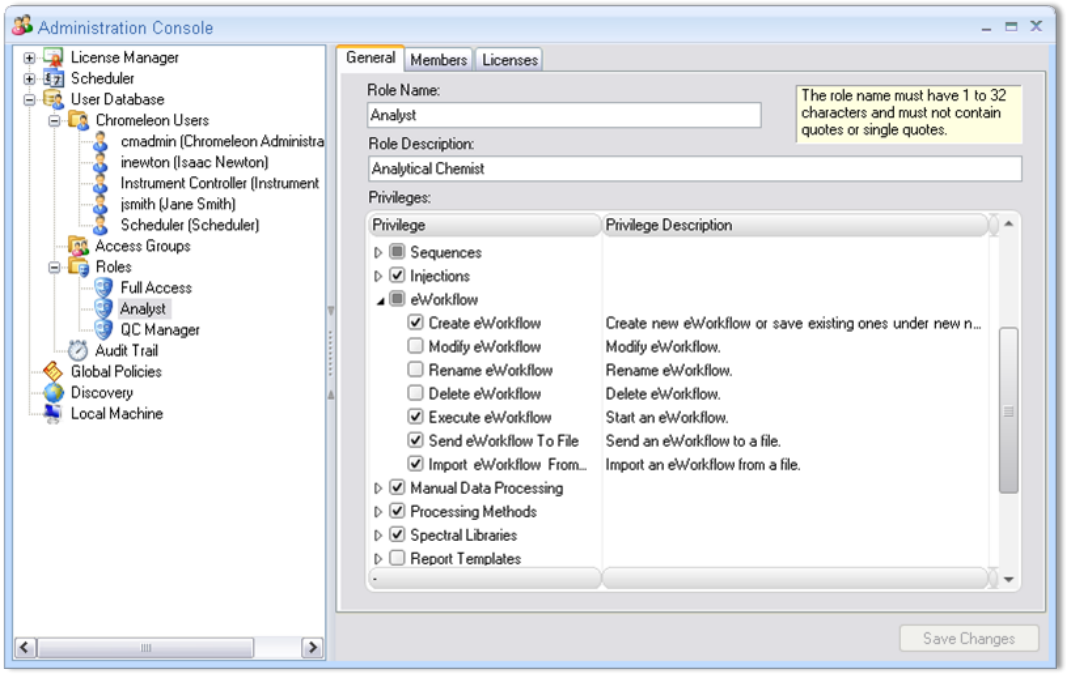



**Figure 3: Chromeleon CDS's Administration Console where privileges can be grouped into Roles and the different roles assigned to users.**

Digital signatures are implemented in the Chromeleon CDS (see Sections § 11.50, § 11.100, and § 11.200.)

With respect to 21 CFR Part 11, the primary electronic records in the Chromeleon CDS are the injection sequences. Each sequence has all of the information pertaining to the analysis of a set of samples (Figure 4). A typical sample set includes calibration standards, check standards, blank injections, and unknowns. Included with each sequence are the following items:

- Injection information (injection names, injection IDs, sequence information, method assignments, correction factors, comments, injection custom variables)
- Method information (instrument control methods, processing methods, spectral libraries)
- Detector data (chromatograms, diode-array data sets)
- Report templates (report template files)
- Electronic reports with signatures
- Audit trails (instrument audit trails, data audit trails, electronic signature information).

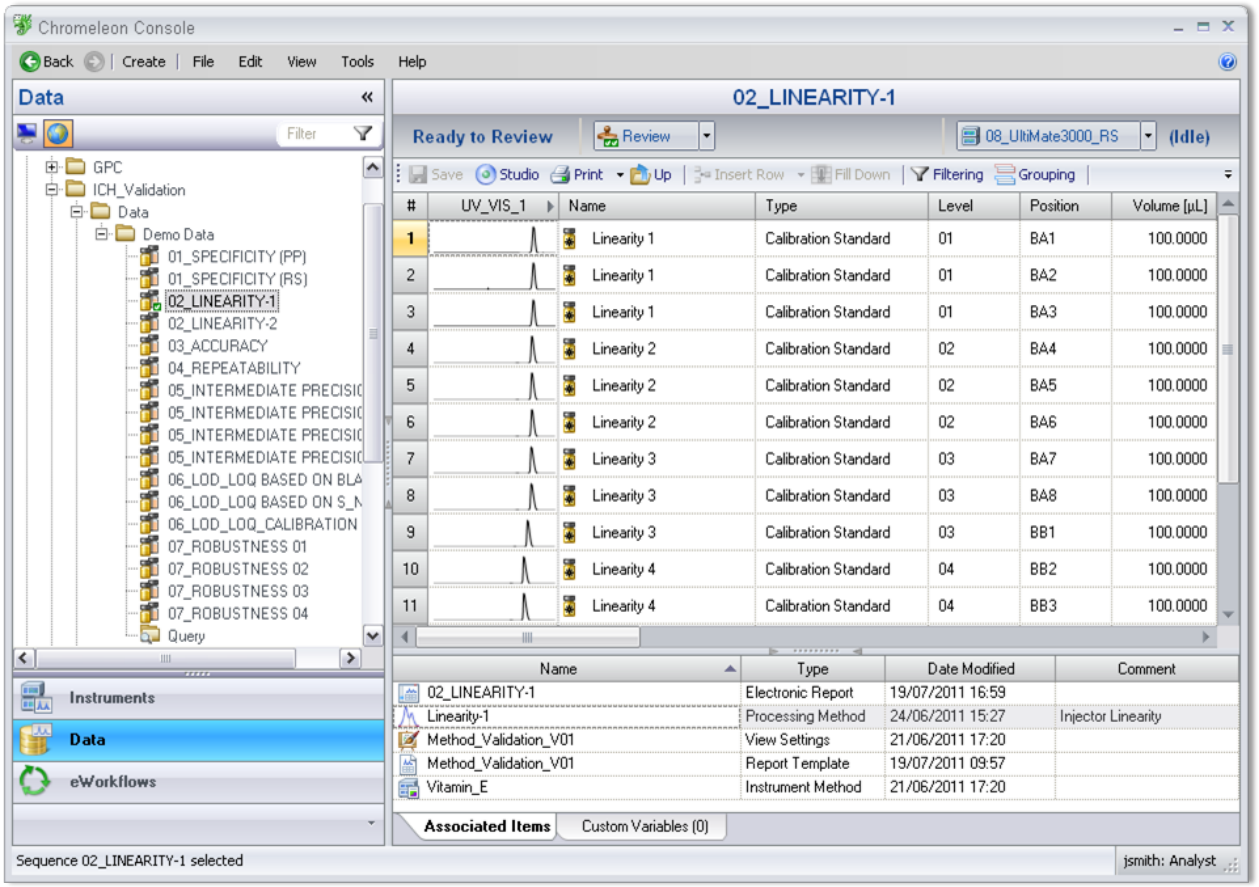



**Figure 4: Sequences, represented by two vials in the Data category, are Chromeleon CDS's primary electronic records. Each sequence includes all details of the analysis of a sample set.**

The Chromeleon CDS calculates results dynamically, so reports update instantly as new data are included or method settings are modified. This dynamic updating prevents inconsistencies between the settings and the reported data. Modifications are only permitted prior to the application of electronic signatures, and audit trails keep track of all of the modifications, as described under Section § 11.10 of this document. When the operator is satisfied with the results, they can submit them for approval, which begins the electronic signoff process (see Section § 11.50). Before the operator's electronic signature is applied, all of the source data and settings required to produce the report are automatically locked, and a hash code is calculated using the report contents, the operator's identification, and the current date and time. The operator is presented with an electronic representation of the finished report, and is then prompted to enter his or her signature password. Upon entry of the password, an unalterable copy of the report is stored, along with the hash code needed to verify its authenticity. A similar process is followed by the reviewer (if any) and the approver (if any) of the submitted report. If anyone finds a need to make changes to the source data or report, the signatures must first be removed by an appropriate authority.

The Chromeleon CDS can also generate backup files of the electronic records cited in 21 CFR Part 11, for data recovery and/or archiving purposes. Contents of backup files cannot be accessed outside of the CDS; the contents of an export must be restored into the system before they can be read. The audit trail keeps track of all export and import operations.

## Subpart B—Electronic Records

### § 11.10 CONTROLS FOR CLOSED SYSTEMS

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

Validation of chromatography systems generally includes installation qualification (IQ) and operational qualification (OQ) of instruments and software, as well as ongoing performance qualification (PQ). Thermo Scientific offers a wide range of validation services, ranging from on-site tests performed by Thermo Scientific service technicians to automated routines built into the software. The software features integrated tools for validating the performance of the chromatography data system as well as the instruments used with it. A simple menu command runs the Chromeleon CDS IQ (Figure 5), which checks all system files and generates a detailed report.

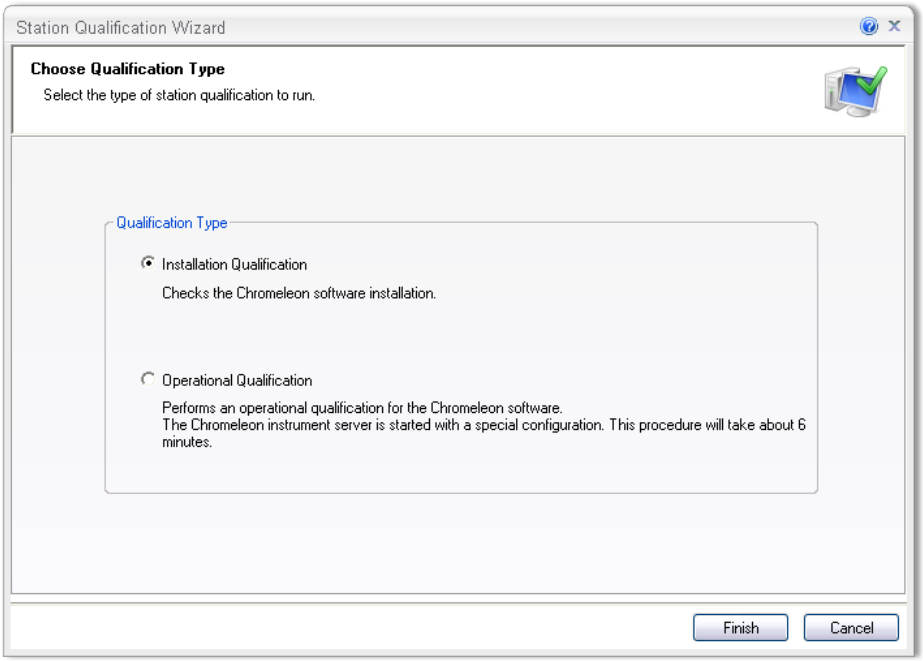



**Figure 5: Chromeleon CDS's integrated validation tools, such as the Software Installation Qualification, standardize and automate validation tests.**

Another command runs the Chromeleon CDS OQ, which generates reports using a standard data set to verify that the output is reproducible. IQ, OQ and PQ of the entire system are easily performed using Chromeleon CDS's qualification wizards, which automate the setup of sequences and generation of reports for

qualification tests. They include checks for many important instrument parameters like gradient and flow precision, detector linearity, noise and drift and injector linearity (Figure 6).

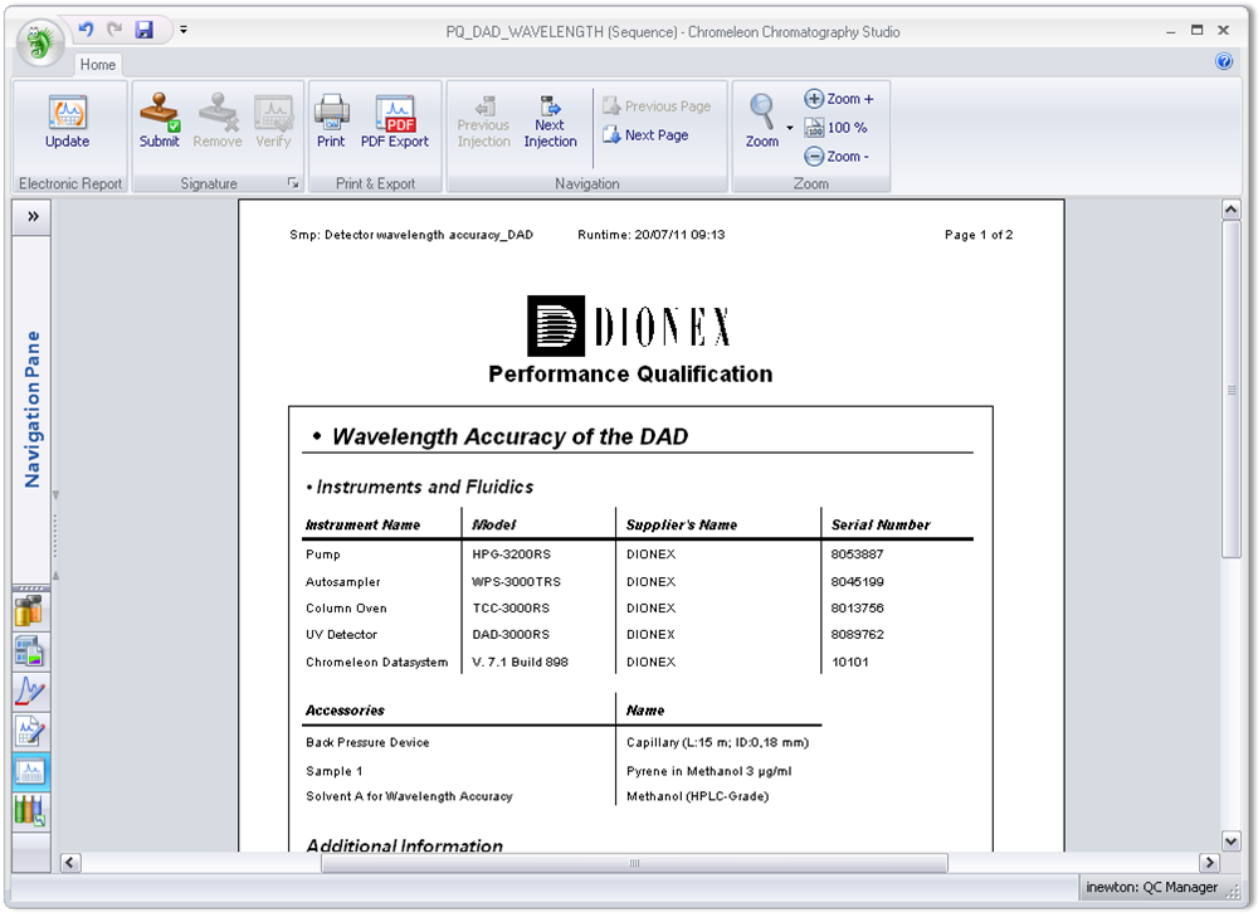



**Figure 6: Chromeleon CDS's Performance Qualification reports provide detailed analysis of the performance of each component of the chromatography system.**

In addition to simplifying the task of performing IQ, OQ, and PQ tests, these tools ensure that all users perform the qualification tests consistently and in compliance with SOPs.

Consistency of system and method performance can be automatically monitored during sample analysis using System Suitability tests. A wizard makes it easy to select common peak quality and reproducibility tests, or configure any number of custom tests using almost any reportable formula (Figure 7). Tests can be performed on one or more individual injections, or span across multiple injections.

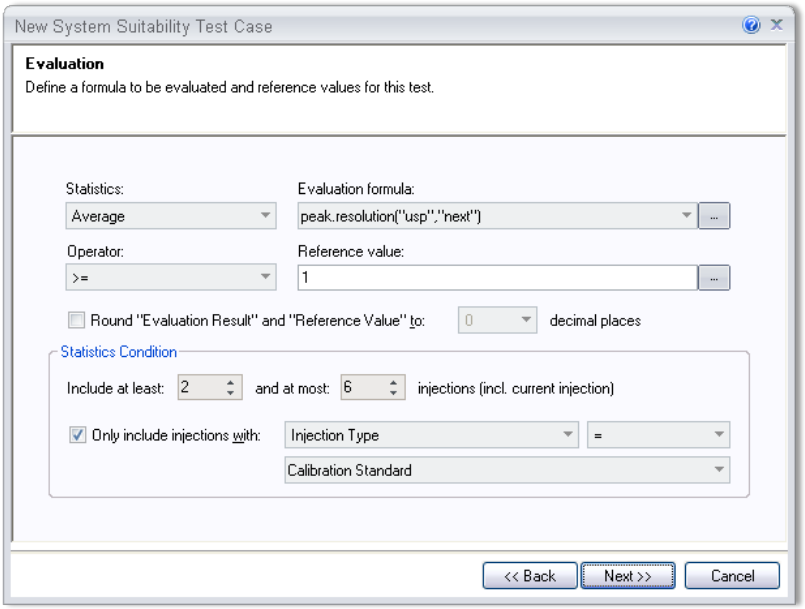



**Figure 7: Any combination of System Suitability tests can be defined for any method to verify system performance during sample analyses.**

Chromeleon CDS's Data Audit Trail (discussed in detail in Section § 11.10 (e), tracks all changes made to all data objects that are done within the application. The Audit Trail details, for each event, the corresponding date and time, name of object, affected data object, object version number, operator identification, type of change, and comments. In Chromeleon CDS's reports, any peak that has been manually manipulated is automatically flagged and clearly indicated (Figure 8).

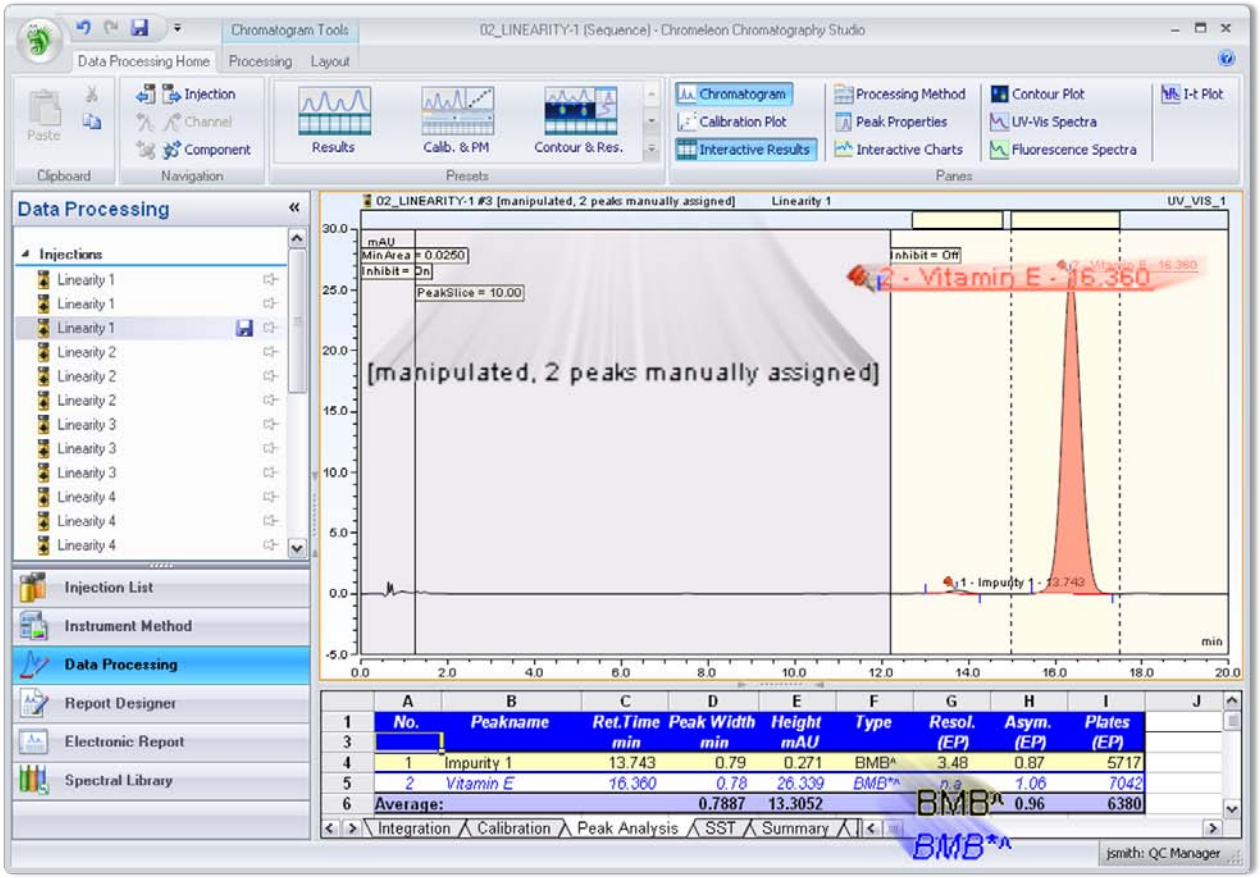



**Figure 8: Chromeleon CDS clearly indicates when a peak's integration has been modified.**

Data corruptions due to defects or failure of storage devices or media, or to deliberate attempts to modify signed records, are detected and reported by Chromeleon CDS (see Section § 11.70).

b) 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 agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

Chromeleon CDS provides complete functionality for locating and viewing the electronic records on the system, and for generating complete, accurate paper and electronic copies for agency submissions. Printed copies include time/date stamps to facilitate traceability of paper documents. Electronic copies are produced in Portable Document Format (PDF) as per agency guidelines, as discussed in Section 11.2. All formats can also have a unique watermark to ensure authenticity and clearly identify the originating source.

c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

Chromeleon CDS provides several layers of protection to ensure that accurate records can be readily retrieved. The foundation for record protection is a secure operating system that provides positive user tracking and prevents unauthorized access to computers and files. Thermo Fisher Scientific recommends the use of Microsoft Windows XP or Windows 7, with the NTFS file system.

The next layer of protection is a combination of controlled Windows services and a secure relational database platform, which ensures that even those users who have access to files at the operating system level cannot read or modify records through means outside the secured application. Thermo Fisher Scientific recommends the use of Oracle Database 11g or Microsoft SQL Server 2008 as the relational database platform for secured, multi-user environments.

Beyond the protections afforded by the operating system and database platform, the Chromeleon CDS provides a comprehensive, chromatography oriented security system that controls access to data (See Section § 11.10 (d). This ensures that only authorized users are able to access records and make changes; any such changes are tracked by computer-generated audit trails, as described in Section § 11.10 (e).

Records can be electronically signed, which simultaneously locks them and documents the signing authority, as described in Section § 11.50. Modifying items that have not been signed off can either be allowed or disallowed by the system administrator. If modifications are allowed, the Data Audit Trail tracks changes and retains details for all versions thus providing the user with a means to reconstruct and revert back to prior versions. Modifying signed-off items are not allowed.

The CDS facilitates long-term record storage (archiving) through its built-in file transfer and restore tools (Figure 9). When a file transfer of data is created, all relevant raw data, corresponding methods, sequence data, report formats, and audit trails are included.

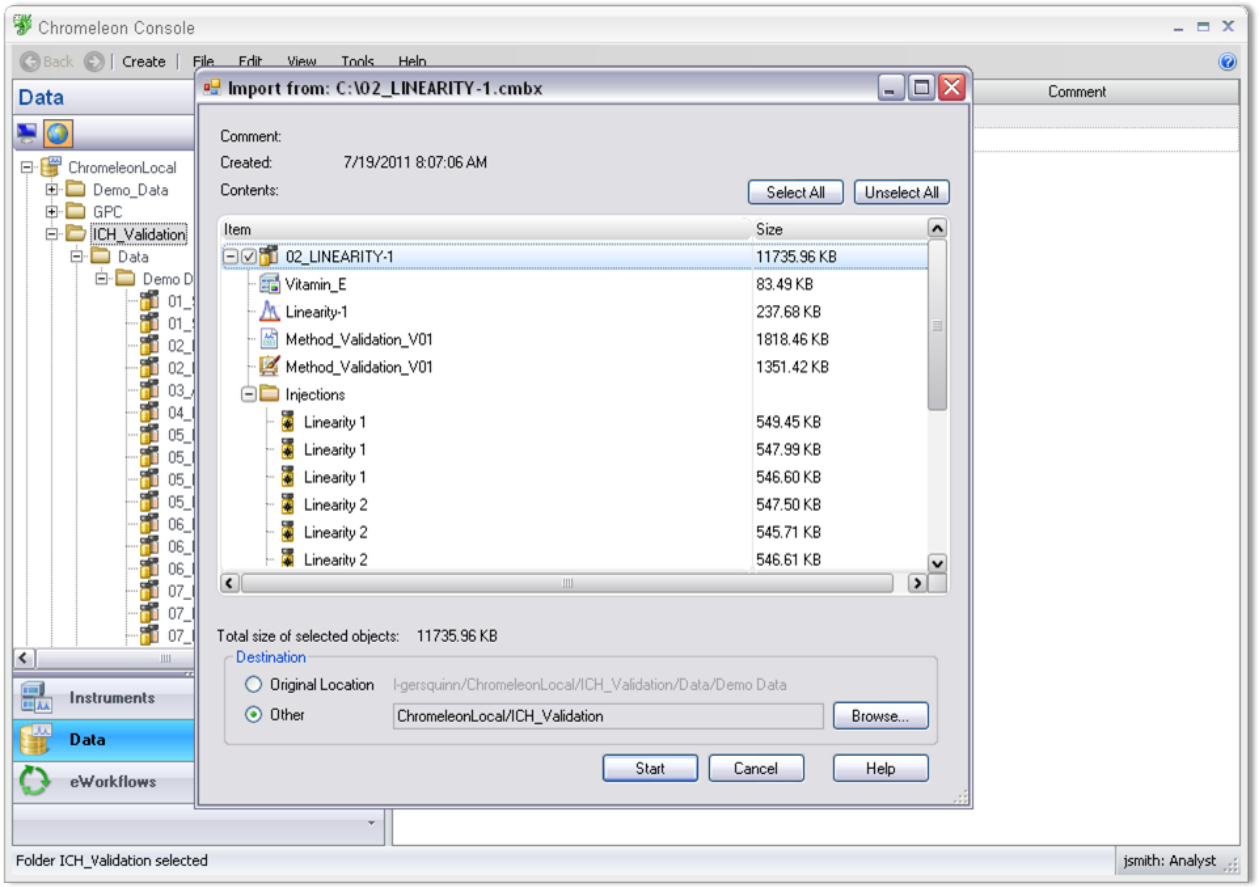



**Figure 9: Chromeleon CDS's integrated Send to and Import from utilities facilitate long-term storage of electronic records, while ensuring security and completeness of the records.**

## d) Limiting system access to authorized individuals.

The software's advanced security system supports an unlimited number of security levels and is designed to fit the chromatography workflow. Over 130 different privileges can be allocated as appropriate to an unlimited number of different Roles (Figure 10). A Role is a collection of user privileges that define what the users that have this Role are allowed to do in Chromeleon CDS (for example, Lab Managers are typically granted privileges to modify integration, whereas Operators might only have privileges to create and run sequences). Two Roles would therefore be created to differentiate between the different tasks. Users can be a member of several roles and choose a Role at logon. The privileges are not cumulative therefore a user is only permitted to perform the actions that have been assigned to the Role they log-on with. These allow detailed definitions of privileges for different user groups and allow the same user to perform multiple Roles in a controlled manner.

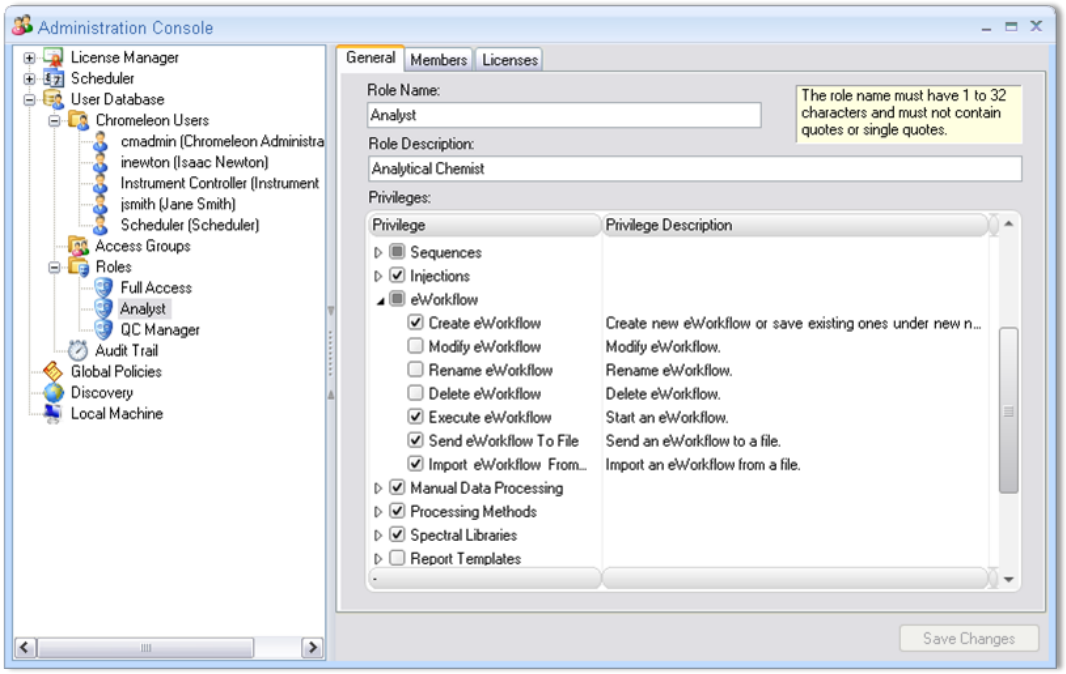



**Figure 10: Chromeleon CDS's comprehensive, chromatography specific security system gives the System Administrator detailed control over each user's access and privileges for instruments and data.**

In addition to Roles, the software supports Access Groups. These are used to control access to different instruments and data objects. Access controls can restrict individual users, groups of users via users with the same Roles and can also restrict privileges that a user has been assigned by the Roles. For example, a Lab Manager in Quality Control may have privileges to access and modify analysis data for released products, but can be denied access to data on new compounds being generated by the Discovery group. The Lab Manager might also have access to view and operate all instruments in all laboratories but could be prevented from interrupting a running instrument in the Discovery Group. Once the Access Groups have been created, access to specific data sources, folders, and/or instruments can be controlled by setting properties for the respective item (Figure 11). Users are only allowed to see the items to which they have been granted access, providing an additional level of security for sensitive data.

Folders and individual injections or groups of injections can also be locked to prevent modification of their contents; privileges for locking and unlocking can be separately granted to different Roles, as appropriate. Injection locking is an additional feature that must be enabled by the administrator, however, electronically signed records are automatically locked, as discussed in Section § 11.50.

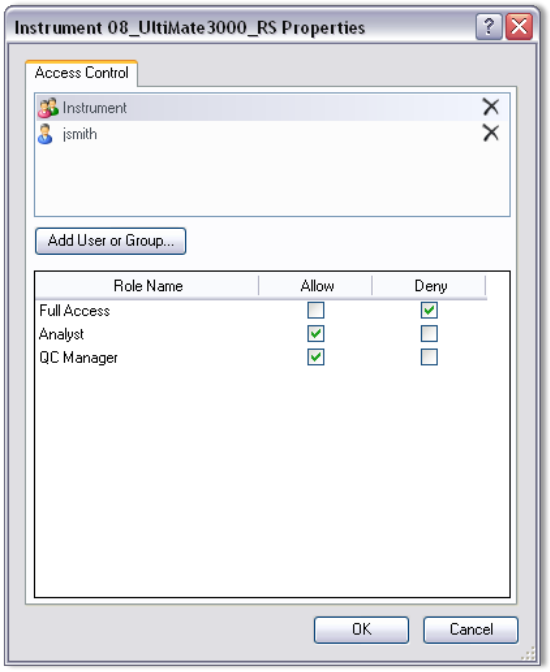



**Figure 11: Chromeleon CDS controls access to data sources, individual folders and instruments. Users who are not members of an Access Group assigned to an item cannot access or see the item.**

Chromeleon CDS security system provides the user management capabilities most often requested by system administrators:

- Users are identified by User Name, Full Name, and Job Title throughout the software (Figure 12)
- Password controls—such as minimum password length, password uniqueness requirements, and password age limits—can be enforced
- User and password audit trails are automatically maintained (Figure 13)
- Users can be automatically locked out after a preset number of login failures (Figure 14)
- Client sessions can be automatically locked after a specified period of inactivity (Figure 15).

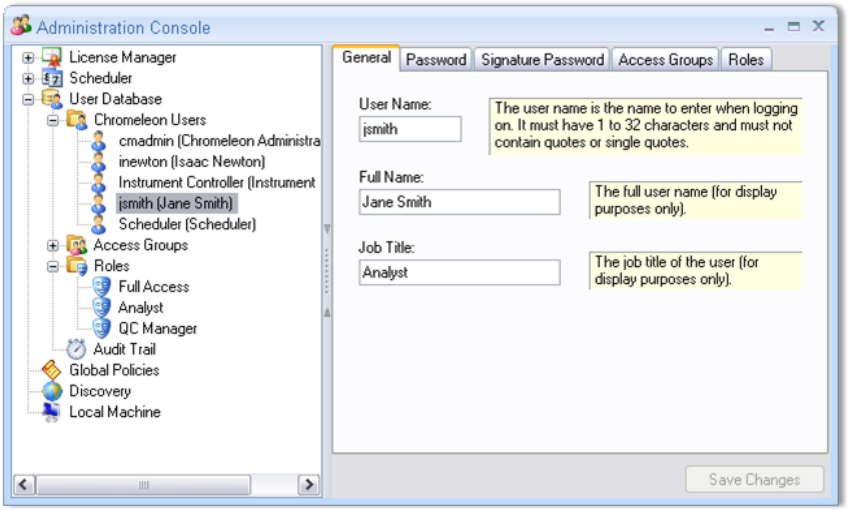



**Figure 12: Users are identified by User ID, User Name, and Job Title throughout the software.**

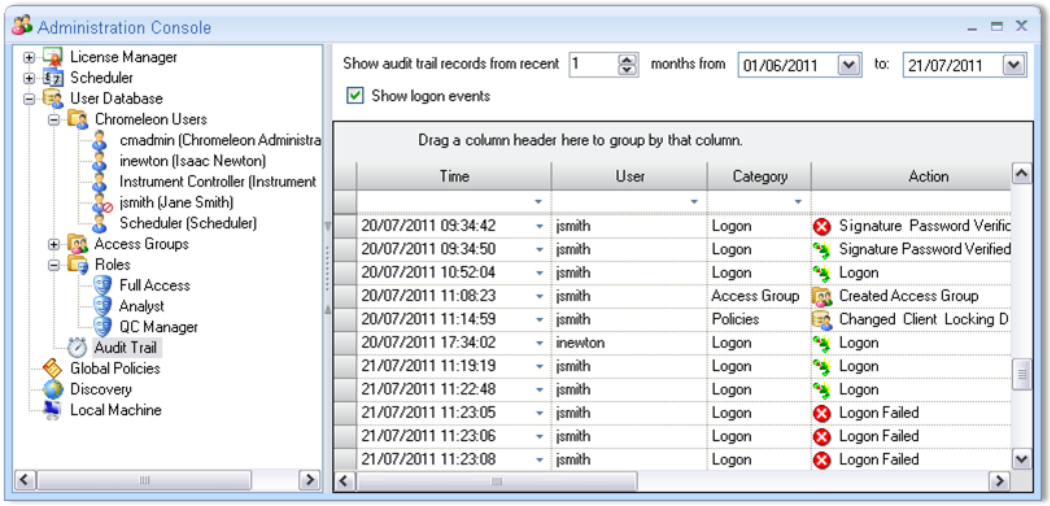



**Figure 13: User and password history logs are automatically maintained.**

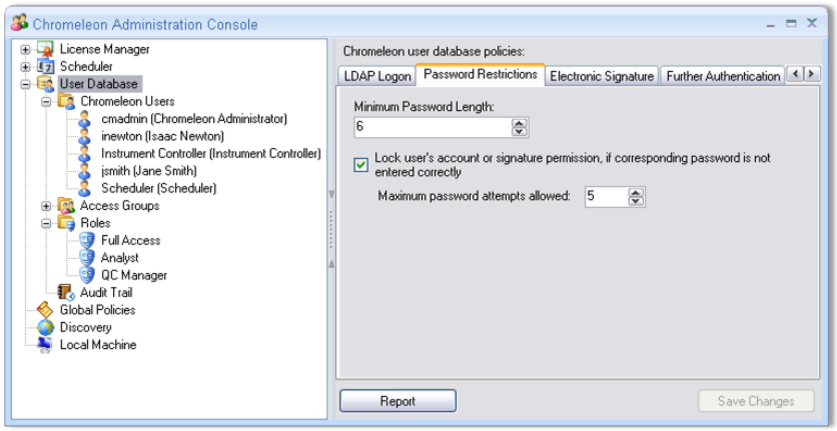



**Figure 14: Users can be automatically locked out after a preset number of login failures.**

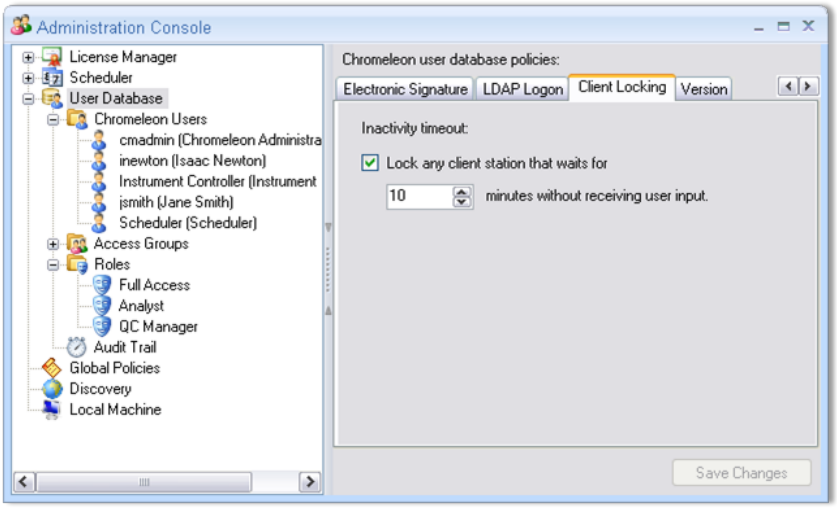



**Figure 15: The administrator can set an inactivity timeout policy to help ensure that unauthorized people do not gain access to the system in the event that an authorized user fails to log out before stepping away from a client station.**

e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

Chromeleon CDS automatically tracks all operator entries and actions that create, modify, or delete electronic records. It does this by maintaining two types of secure, computer-generated, time-stamped audit trails: Instrument and Data audit trails. Both audit trails record the time and date of each event, along with the identification of the operator involved. Changes to records add new entries to the audit trails, such that previously recorded information is not obscured, and the system administrator has fine control over who is allowed to make changes to data and audit trails. An Instrument audit trail is automatically created and maintained for each instrument. Each Instrument audit trail completely documents all events associated with data acquisition and instrument control, including:

- Users connecting to instruments, whether for control or simply to monitor activity
- Sequence starts and stops
- Control commands sent to instruments from an instrument control program or a direct user action
- Responses received from instruments, including any status messages, warnings, or errors
- Instrument configuration changes

Any instrument's daily audit trail can be reviewed (Figure 16) and all events are fully searchable by filtering using 'find as you type' text entry or can be grouped together. Events pertaining to a particular sequence can also be viewed in real time during instrument operation (Figure 17), or included as a report object (Figure 18). This detailed documentation not only helps with 21 CFR 11 compliance, it also improves productivity by

eliminating the need for manual logging of events and by providing the operators with useful information for keeping track of their work and troubleshooting any analysis problems that might occur.

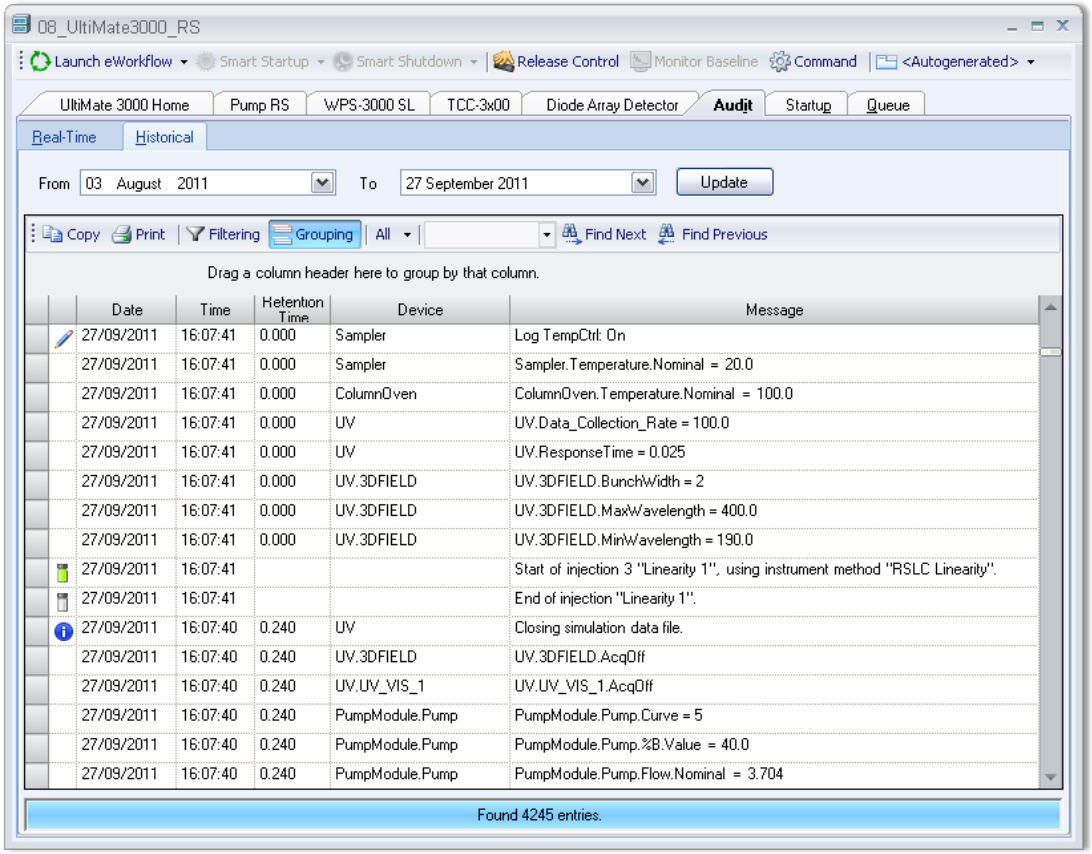



**Figure 16: The Chromeleon CDS automatically maintains a complete log of each instrument's daily activities.**

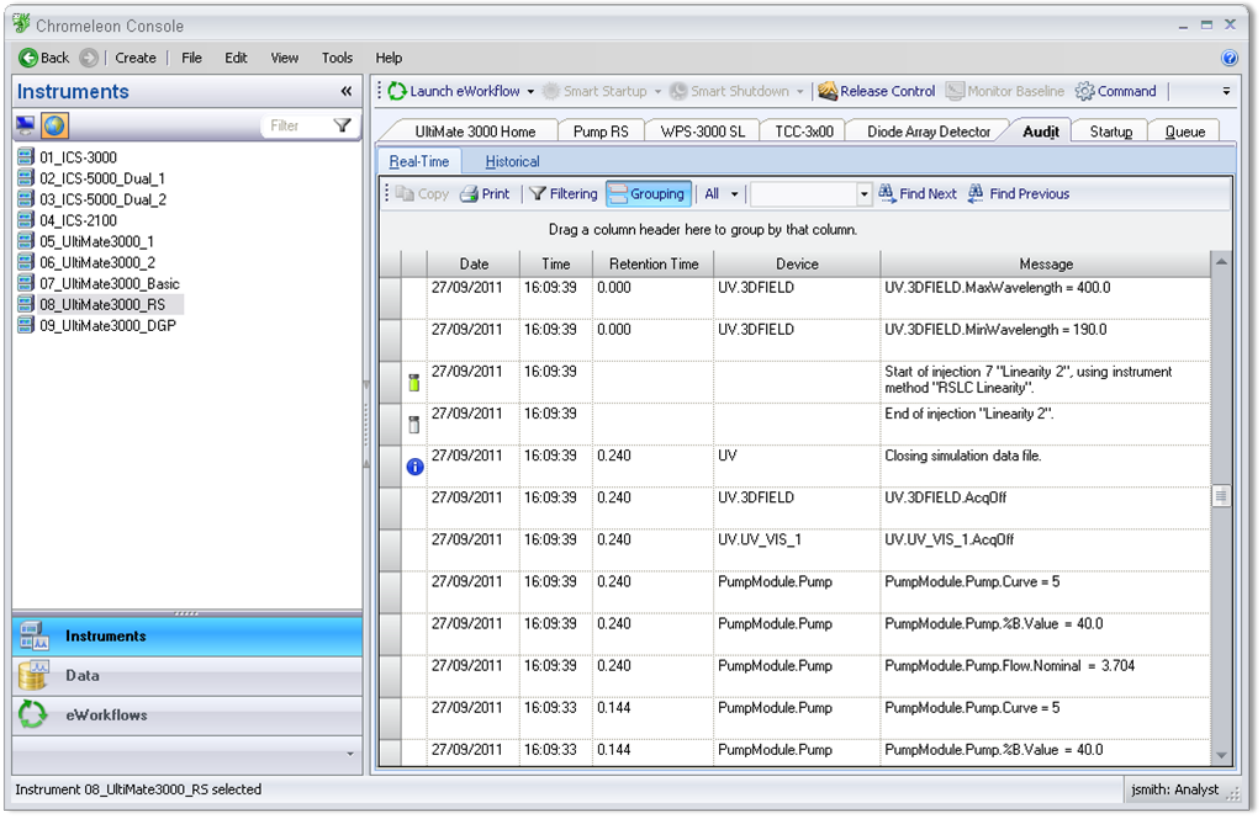



**Figure 17: System log events that pertain to the current sequence can be viewed in real time during sample analysis.**

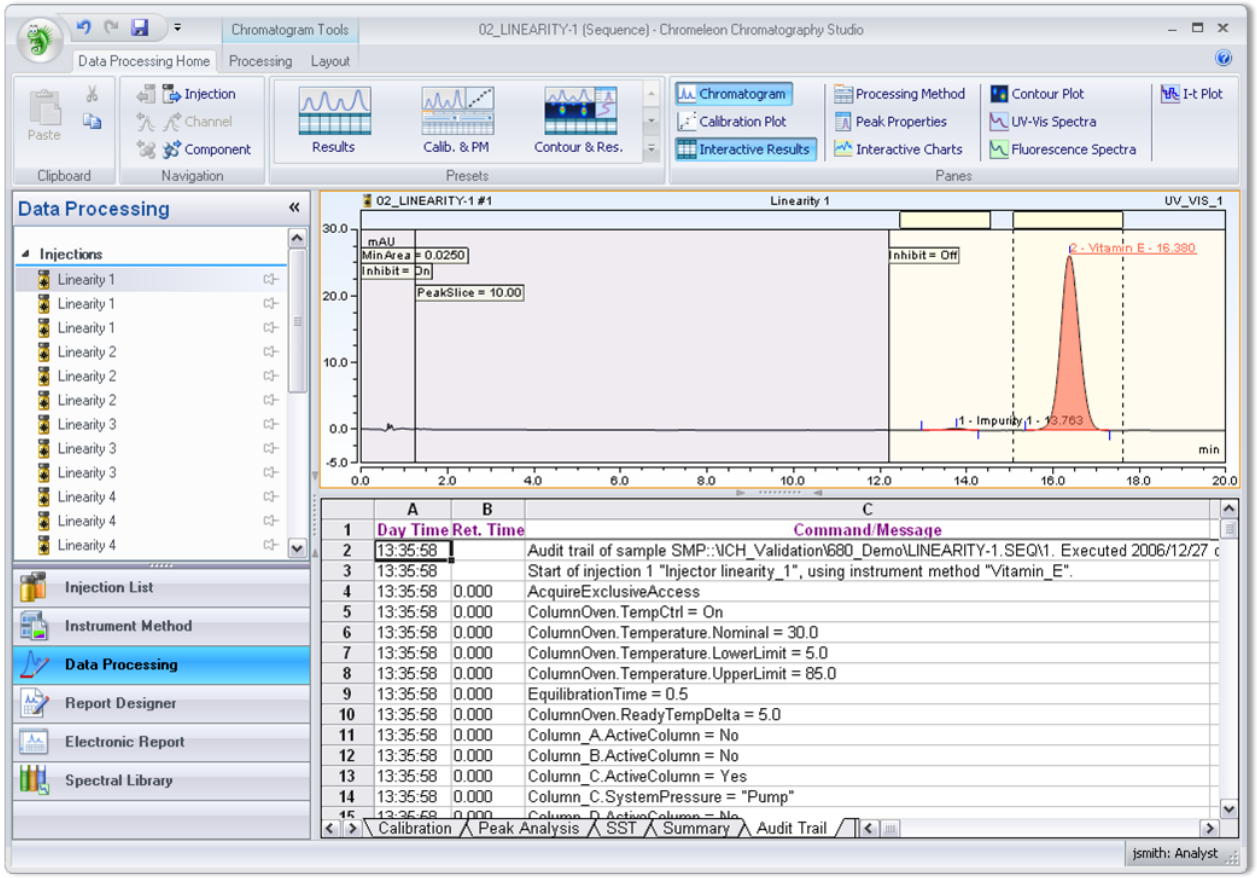



**Figure 18: The System Log events for a sequence can be included in the report along with the analytical results, providing full traceability.**

The Data Audit Trail keeps detailed records of all changes made to data objects and electronic records in a Chromeleon CDS Data Vault. It documents the creation of sequences and related data—including injection entries, instrument methods, processing methods, view settings and report templates—as well as all modifications made after the analysis. (Post-run modifications include changes to sequence entries, methods and reports; manual baseline adjustments; and any relocation, archiving, or deletion of data.)

The recording of the Data Audit Trail can be enabled by the Chromeleon CDS System Administrator for any chromatography Data Vault. Audit trails are easily accessible by simply right-clicking on an item and selecting {Show Data Audit Trail} from the context menu (Figure 19). Authorized users can view the Data Audit Trail at any desired level of the information hierarchy: individual objects (injection, instrument method, processing method, report template, and so on), directory folder, or entire Data Vault. All events are fully searchable and Chromeleon CDS  provides the operator with different search tools consisting of grouping events together and filtering using ‘find as you type’ text entry .

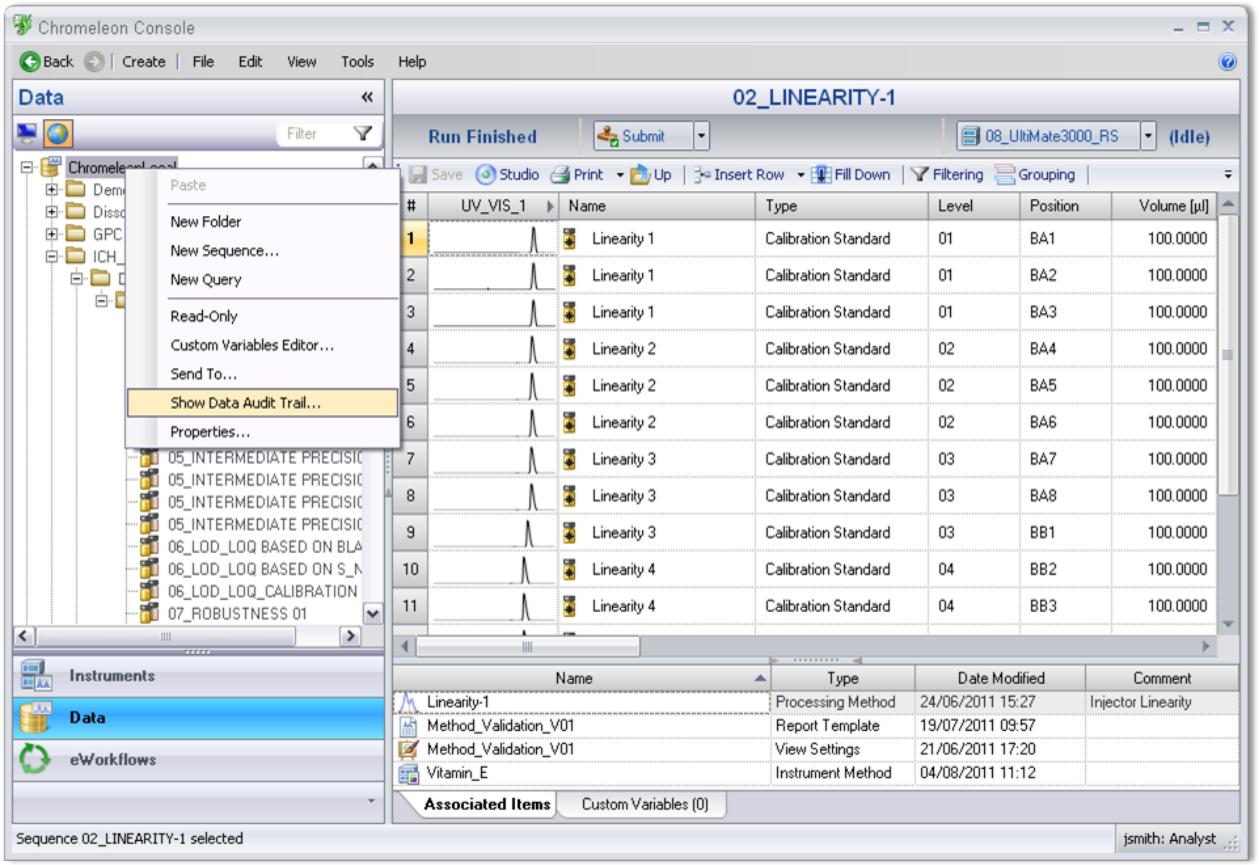



**Figure 19: The Modification History for any sample, sequence, folder or data source can be instantly accessed using the Show Data Audit Trail command.**

The Data Audit Trail display (Figure 20) lists, for each event, the corresponding date and time, name of object, affected data object, object version number, operator identification, type of change, and comments. Versions can be compared displaying differences between selected versions with all changes, deletions and additions clearly indicated and none of the entries obscured. Chromeleon locks records as soon as they enter the electronic signature process. Locked records cannot be modified by anyone, and the System Administrator can restrict who has the privilege to unlock records. Electronically signed records cannot be unlocked without removing the signatures. Chromeleon CDS Data Audit Trail keeps track of all Lock and Unlock operations and of all actions in the electronic signature process.

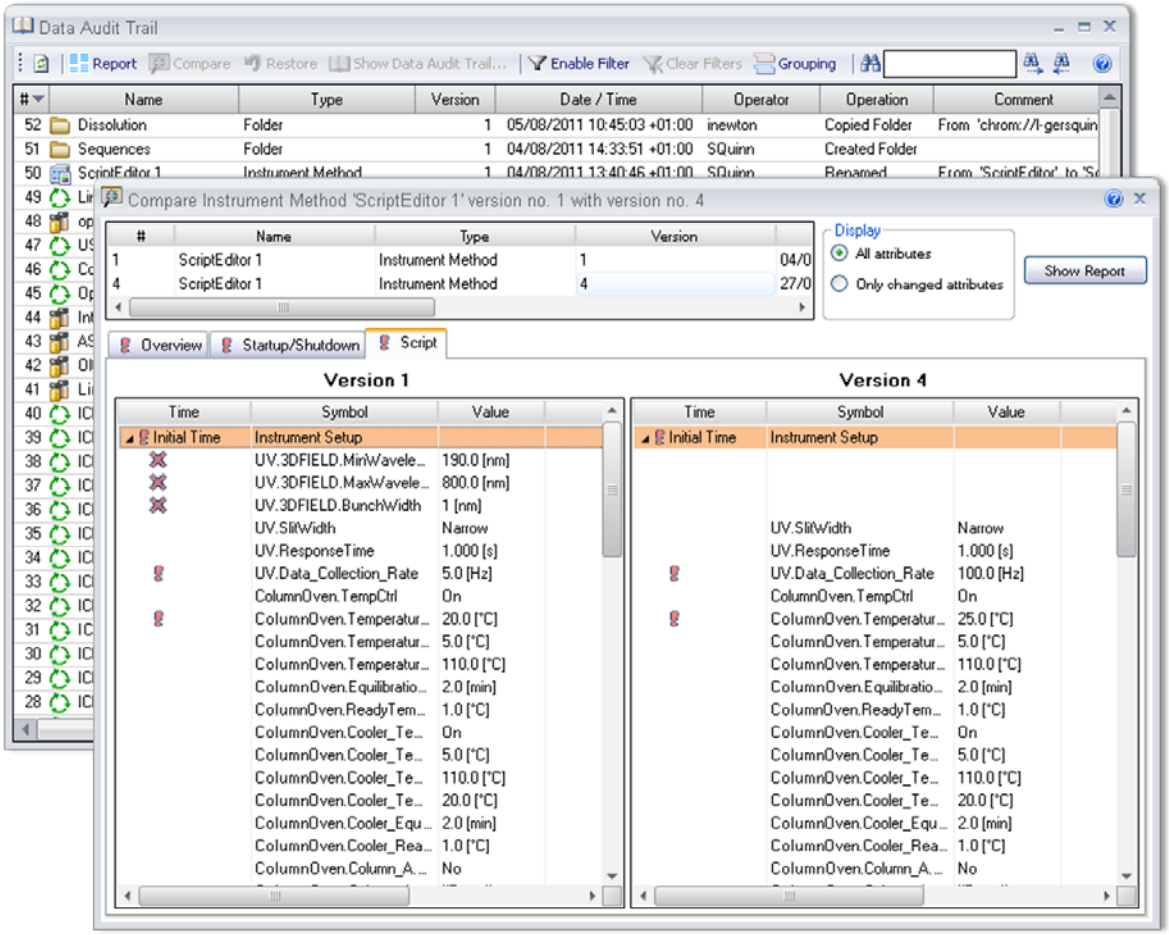



**Figure 20: Chromeleon CDS's Modification history tracks all changes to all data objects and lists the before and after state of each variable associated with each change.**

The System Administrator can also prohibit the modification of existing data objects. The binary nature of the audit trail files makes the possibility of falsification extremely remote. However, in an unsecured operating system, it could be possible for a user to gain access at the operating system level, stop the Windows service that protects the files and delete or corrupt one of the files cited above. Thus, Thermo Fisher Scientific recommends that regulated laboratories store all data on secured computers running Windows XP or Windows 7 with the NTFS file system.

Chromeleon provides complete functionality for viewing all audit trails on the system, and for printing hard copies of the audit trails at any time.

f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

The Chromeleon CDS has a context-sensitive structure that hides or disables functions that are not relevant, not appropriate, or not permitted within the current context. This structure helps ensure that steps and events occur in the proper sequence. For example, if a sequence has been configured to have signature levels of Submitter and Approver, it cannot be approved until it has been signed by a submitter. The software also provides a feature titled eWorkflows which is an electronic procedure for automating the laboratory processes related to a chromatographic analysis. It assists the user in creating an appropriate sequence with predefined associated files and a well-defined structure (Figure 21). In addition Chromeleon CDS also provides additional Wizards (Figure 22) and many step-by-step procedures with detailed instructions in on-line Help (Figure 23) to further guide users. The Chromeleon CDS performs numerous error checks when instruments are configured, when instrument methods are defined, and when sequences are readied for execution (Figure 24). Any conflicts must be resolved before the user is allowed to proceed.

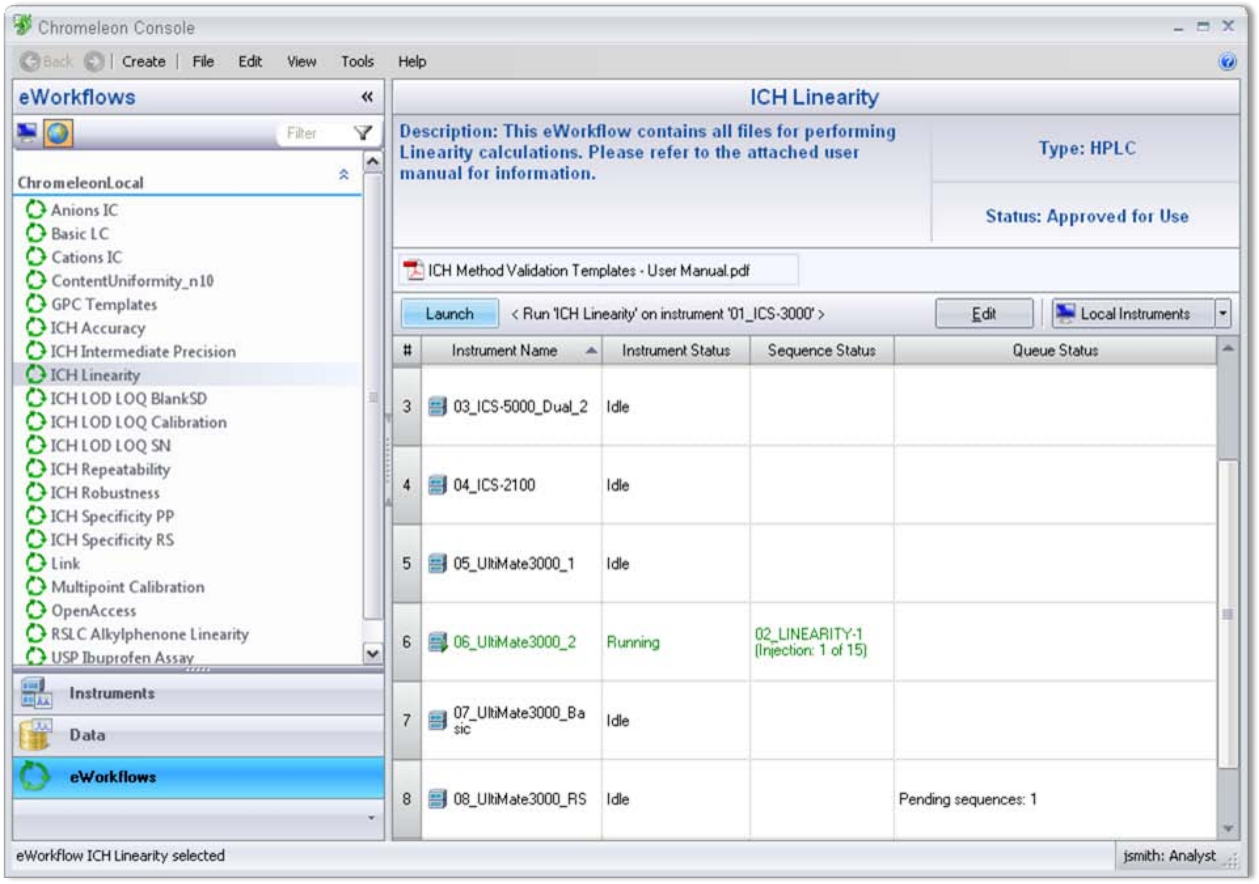
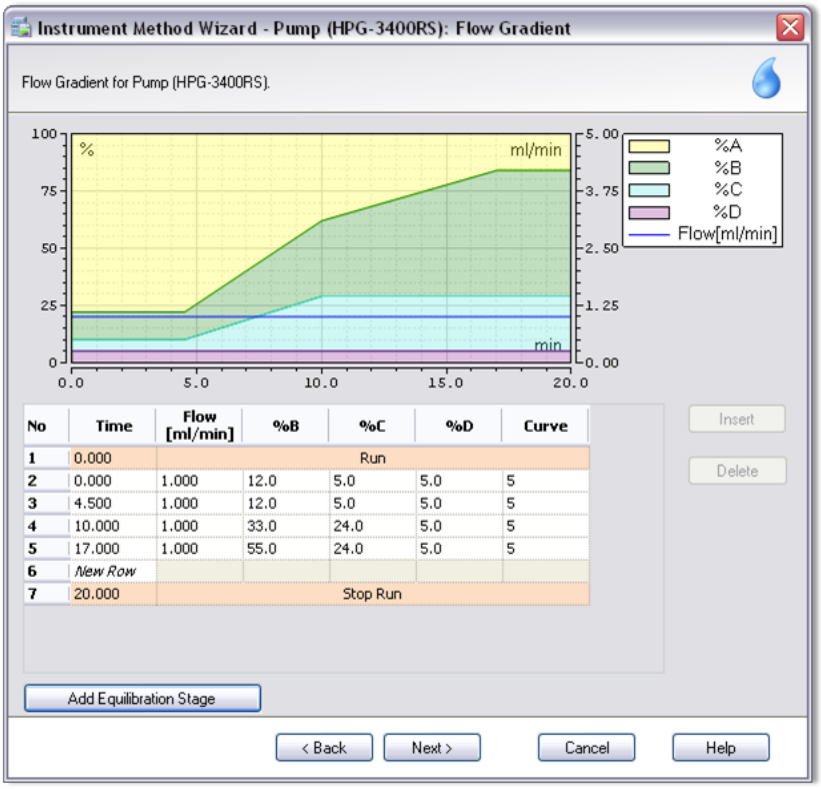



**Figure 21: Chromeleon CDS eWorklfows for automating the laboratory processes related to a chromatographic analysis.**




| No | Time | Flow [ml/min] | %B | %C | %D | Curve |
|---|---|---|---|---|---|---|
| 1 | 0.000 | Run | | | | |
| 2 | 0.000 | 1.000 | 12.0 | 5.0 | 5.0 | 5 |
| 3 | 4.500 | 1.000 | 12.0 | 5.0 | 5.0 | 5 |
| 4 | 10.000 | 1.000 | 33.0 | 24.0 | 5.0 | 5 |
| 5 | 17.000 | 1.000 | 55.0 | 24.0 | 5.0 | 5 |
| 6 | *New Row* | | | | | |
| 7 | 20.000 | Stop Run | | | | |

**Figure 22: Chromeleon CDS Instrument Method Wizard guides the user through the steps required to create instrument control programs.**

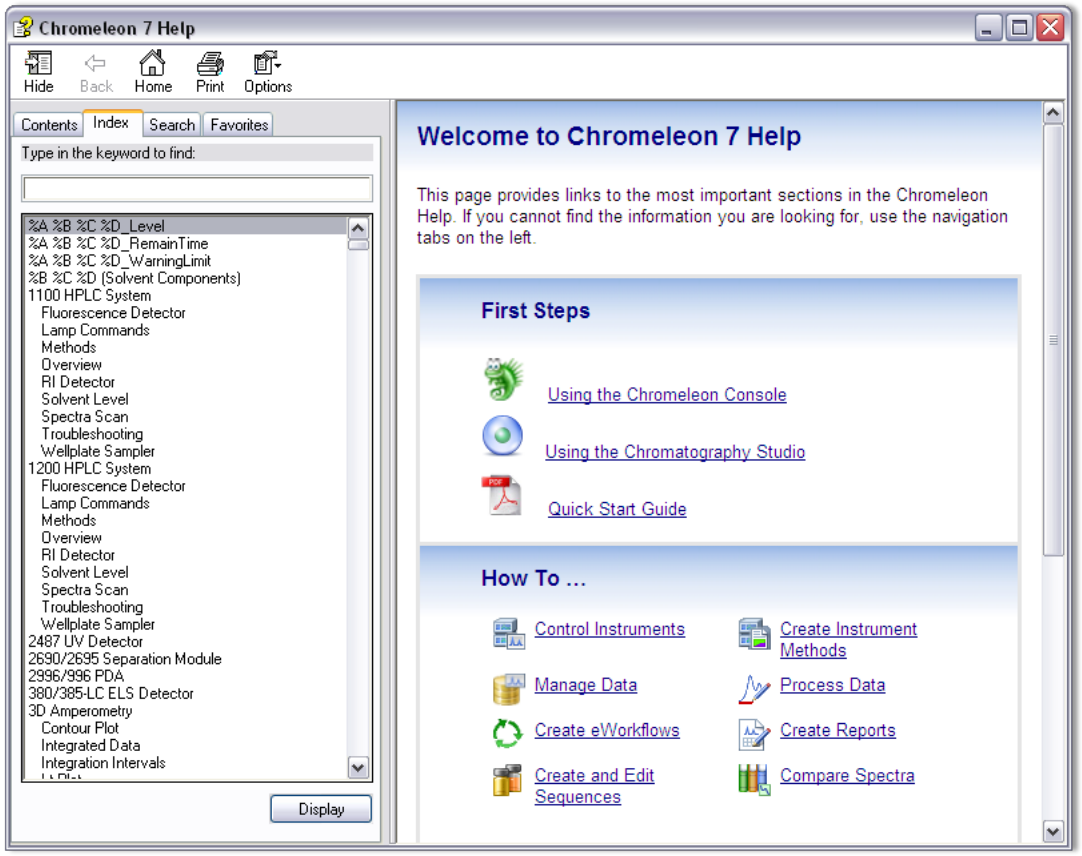



**Figure 23: Chromeleon CDS's on-line Help provides background information as well as step-by-step procedures for all common chromatography operations.**

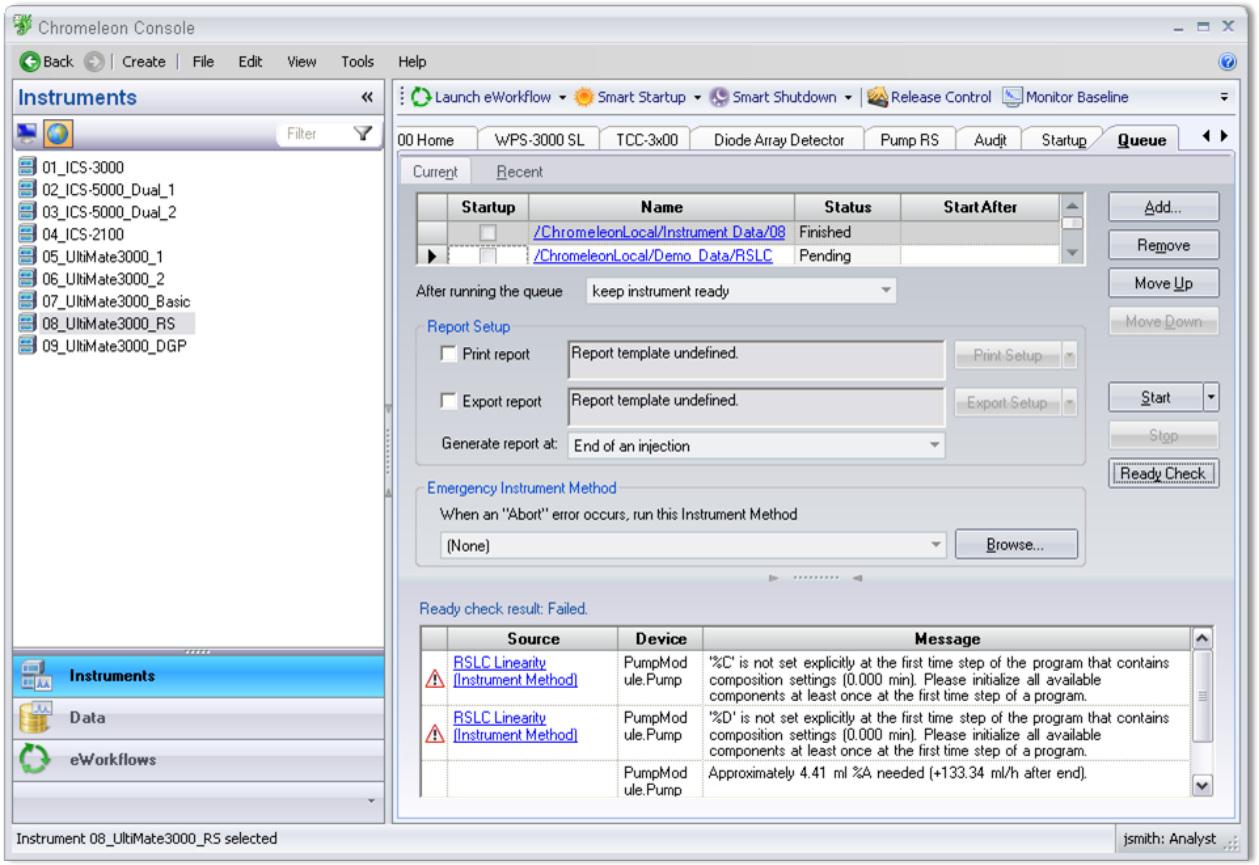



**Figure 24: Before executing any sequence or batch of sequences, Chromeleon CDS automatically checks that the instruments are present and functioning, the control programs are valid for the selected instruments, all parameters of the sequence are valid, and sufficient disk space is available for data storage.**

g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

Chromeleon CDS provides a comprehensive, chromatography-specific security system that controls access to instruments and data, and defines the types of operations that each class of users can perform on the items to which they are granted access (as described under Section § 11.10 (d)). It also controls who is authorized to electronically sign specific sequences (as described under Section § 11.50).

h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

Upon installation, the Chromeleon CDS automatically performs a Software Installation Qualification to verify that all software components are correctly installed. A report is stored to disk and can be printed. Password-controlled log-ins is used to prevent unauthorized access and to identify users at the operating system level

*and* at the Chromeleon CDS level, regardless of where they log in. Whenever possible, Chromeleon CDS records specific information about the actual instruments used (serial numbers, operating conditions, vial positions injected, etc.)

i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

Thermo Fisher Scientific provides appropriate training for its developers, service engineers, and support personnel on a regular basis. Records of training are maintained in accordance with training policies registered to ISO 9001. Thermo Fisher Scientific provides on-site introductory training for users at the time of installation; additional training is recommended for laboratory managers and for support personnel. System administrators should also attend advanced Chromeleon CDS training courses. Off-site classes are regularly conducted in Thermo Fisher Scientific field offices. Custom on-site training courses are also available.

j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

k) Use of appropriate controls over systems documentation including:

- (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
- (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

Thermo Fisher Scientific supplies user documentation in electronic format on the same read-only media as the software, so that the two are always synchronized. Release notes providing a history of changes from release to release are provided with the software.

## § 11.30 CONTROLS FOR OPEN SYSTEMS

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

As is the case with practically all systems in analytical laboratories, the Chromeleon CDS is generally implemented in a closed system environment, with an appropriate security system in place, and the laboratory applying full control on who will access the system. An open system in a laboratory would be one where the data is stored on a server that is under the control of a 3rd party. Other examples for open systems are websites where everyone has access.

## § 11.50 SIGNATURE MANIFESTATIONS

a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

- (1) The printed name of the signer;
- (2) The date and time when the signature was executed; and,
- (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

Chromeleon CDS's comprehensive implementation of electronic signatures provides all the functionality required by Section § 11.50, while satisfying laboratory workflow needs. With each individual user granted access to Chromeleon CDS, the System Administrator can grant an individual a signature password which is separate and distinct from the login password. Functions such as minimum password length, password uniqueness requirements, password age control, and password history are supported for signature passwords as they are for login passwords.

In association with electronic signatures, the Chromeleon CDS user manager provides privileges for signing results, for removing signatures, and for modifying sequence signature requirements. Also, for each injection sequence in Chromeleon, users with appropriate security clearance (i.e. the user privilege Modify Signature Requirements) can define up to three signoff levels (Submit, Review, and Approve) (See Figure 25).

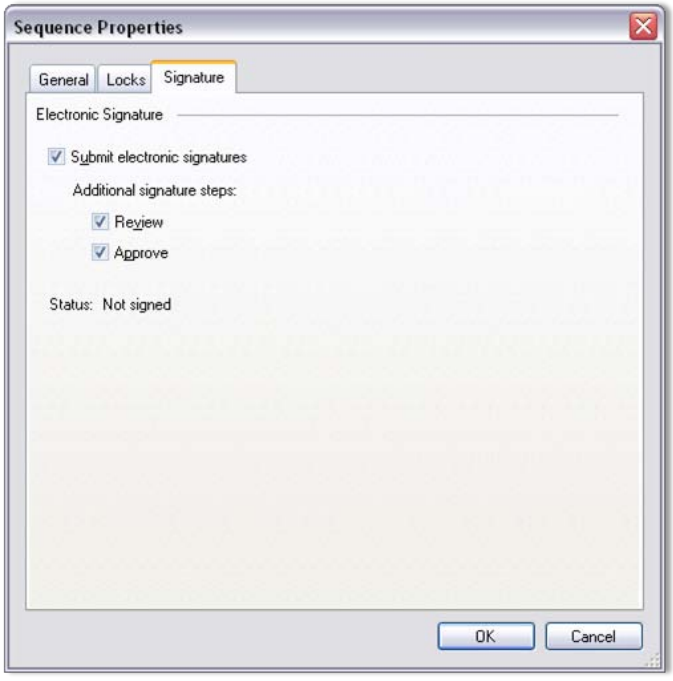



**Figure 25: The list of authorized signatories for submission, review, and approval of results can be specified separately for each sequence**

Applying electronic signatures is a simple, straightforward process. The submitter chooses the desired sequence and selects the ***Submit*** button in the Sequence Status bar (Figure 26). The Chromatography Studio opens in the Electronic Report category and if the user has the relevant privileges, chooses which report pages to include in their final signed off report (Figure 27). Results are recalculated and then an on-screen display of the report is visible (Figure 28). When satisfied with the report, the submitter proceeds to signoff (Figure 29), where they enter their individual signature credentials and any desired final comments. After the correct password has been entered, the current state of the sequence is frozen and protected and no further changes are possible (Figure 30). The sequence is marked with a special icon indicating that it has been signed and the signatory controls in Chromeleon CDS indicate the next step in the signing process if required.

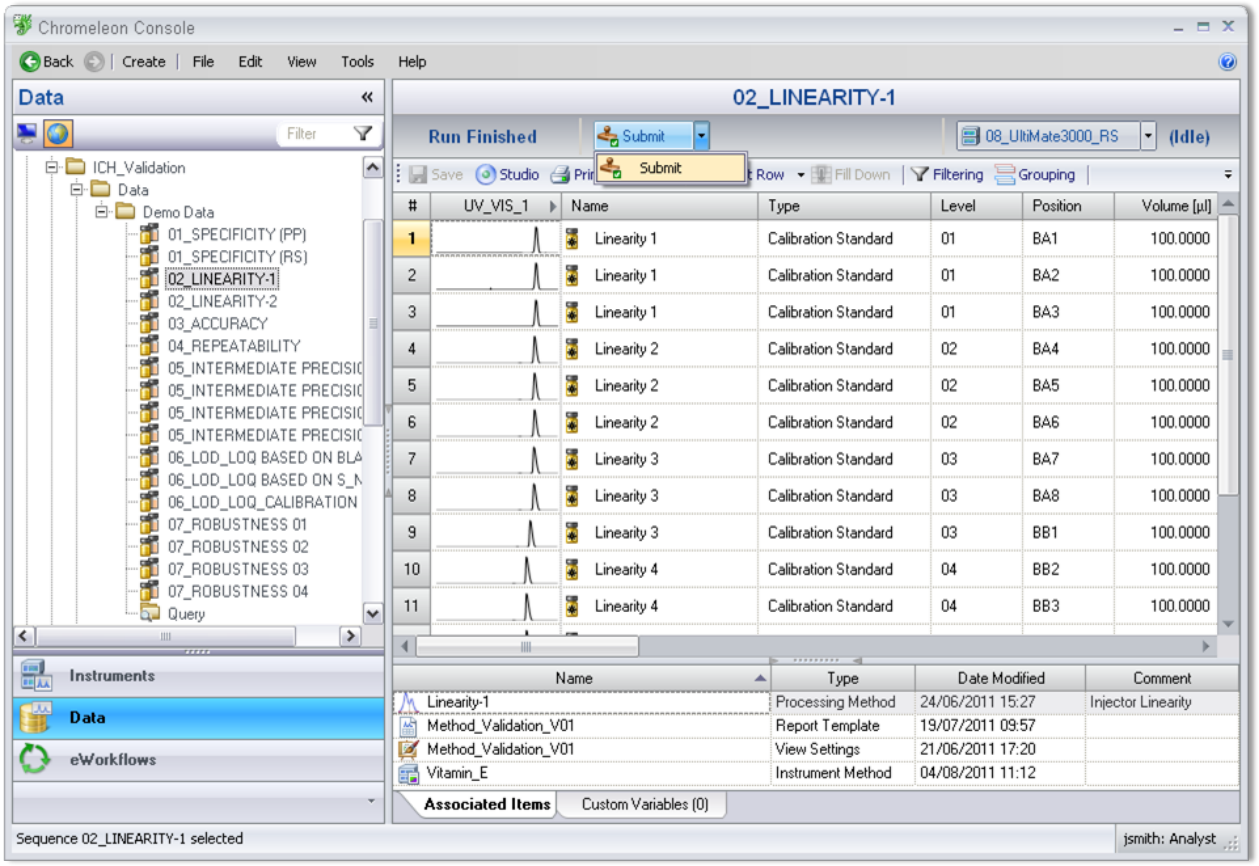



**Figure 26: To sign a sequence, the user begins by selecting the corresponding toolbar button.**

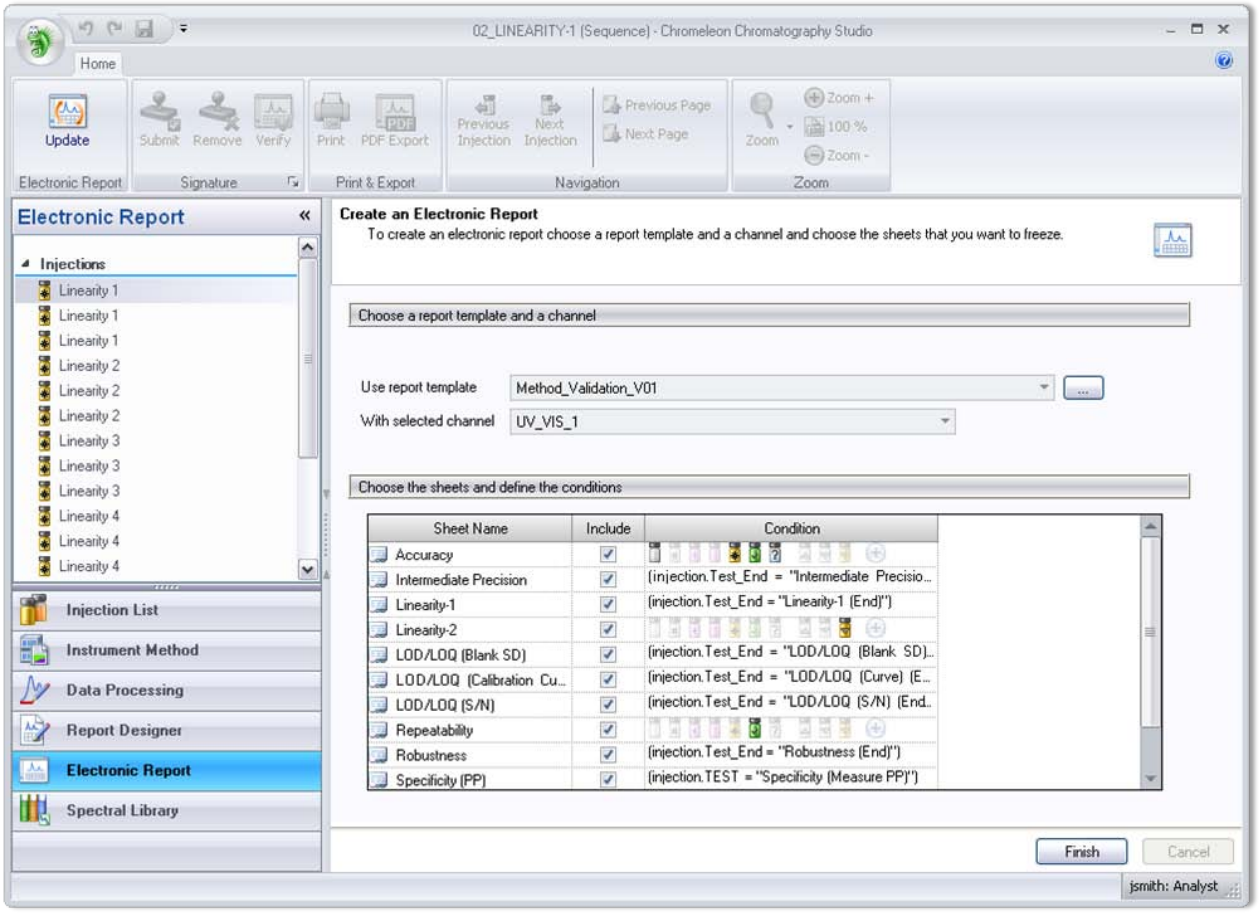



**Figure 27: If permissible the user specifies which report sheets and which injections should be included in the electronic signoff.**

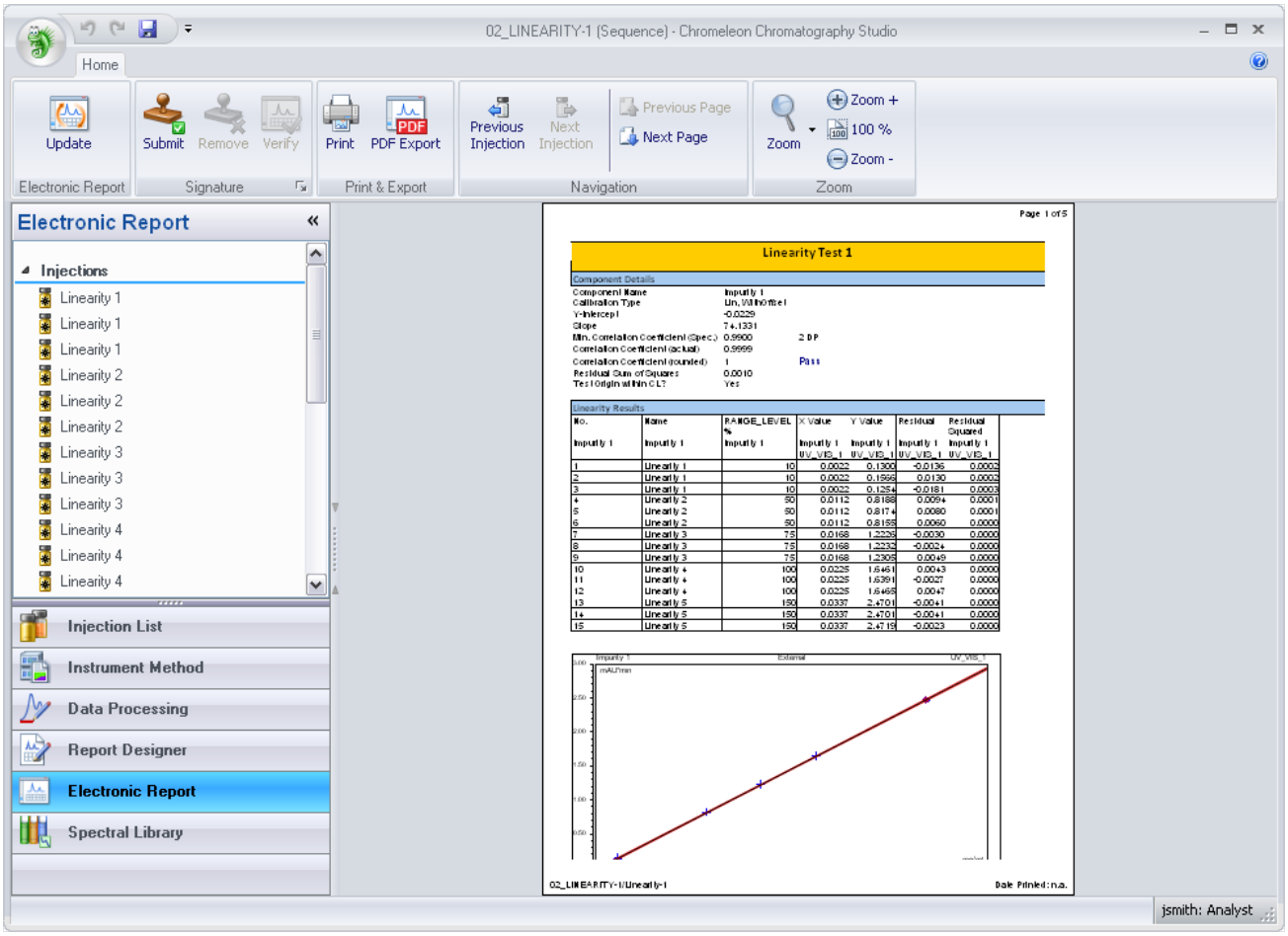



**Figure 28: Chromeleon CDS locks all the sequence data against modification, then recalculates and freezes all report sheets.**

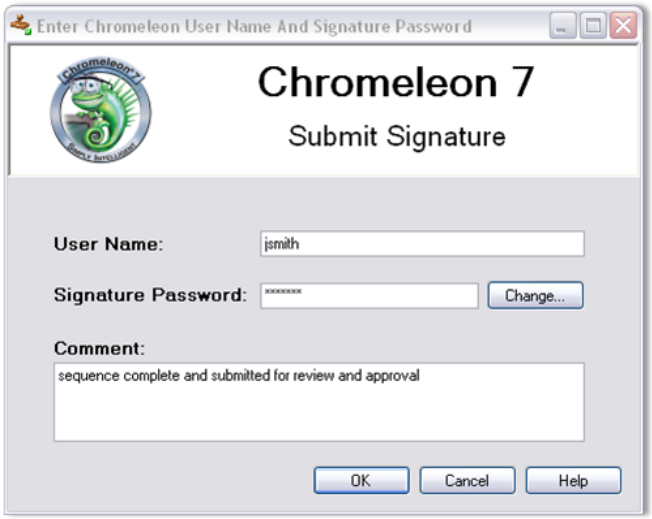



**Figure 29: Users enter their individual signature credentials and any desired final comments to sign off sequence.**

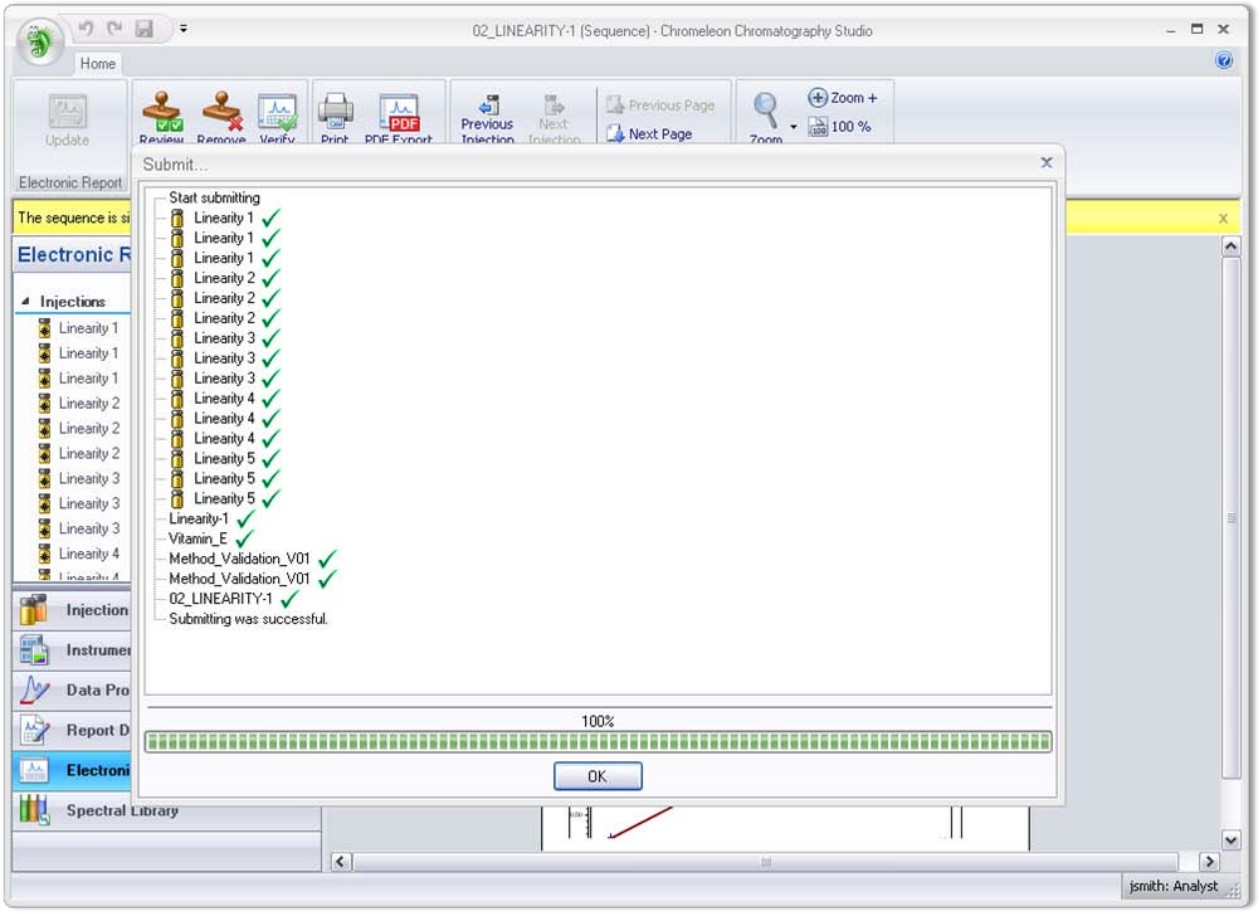



**Figure 30: Using the signature data and the report contents, Chromeleon CDS calculates a hash code that becomes an integral part of the encrypted final report and certifies its authenticity.**

Reviewers and approvers follow the same steps as submitters, but they can only review or approve sequences that have been first signed by a submitter. If a problem is found with the report, an authorized user can undo the signature of the submitter so that necessary modifications can be made; in this case, the report must be resubmitted with a new signature. Any of the variables related to electronic signatures (such as signoff status, name of signatory, job title, meaning of the signature, time/date signed, and so forth) can be included in reports and used for database queries. Sequences awaiting review and approval can be quickly located by running a simple query.

## § 11.70 SIGNATURE/RECORD LINKING

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied or otherwise transferred so as to falsify an electronic record by ordinary means.

With the Chromeleon CDS, electronic signature data are stored as integral parts of sequence, such that it cannot be excised, copied, or otherwise transferred by ordinary means. When an electronic signature is applied, Chromeleon generates a unique hash code that cannot be generated without the application. The hash code is stored along with the sequence data in the database. It is only possible to create a valid hash code using the Chromeleon CDS. Any user can use the *Verify* toolbar button to quickly confirm the integrity of electronically signed documents (Figure 31). The software recalculates the unique hash code and confirms that nothing has been altered since the document was created (Figure 32). Thermo Fisher Scientific does not provide functionality for execution of handwritten signatures to electronic records at this time.

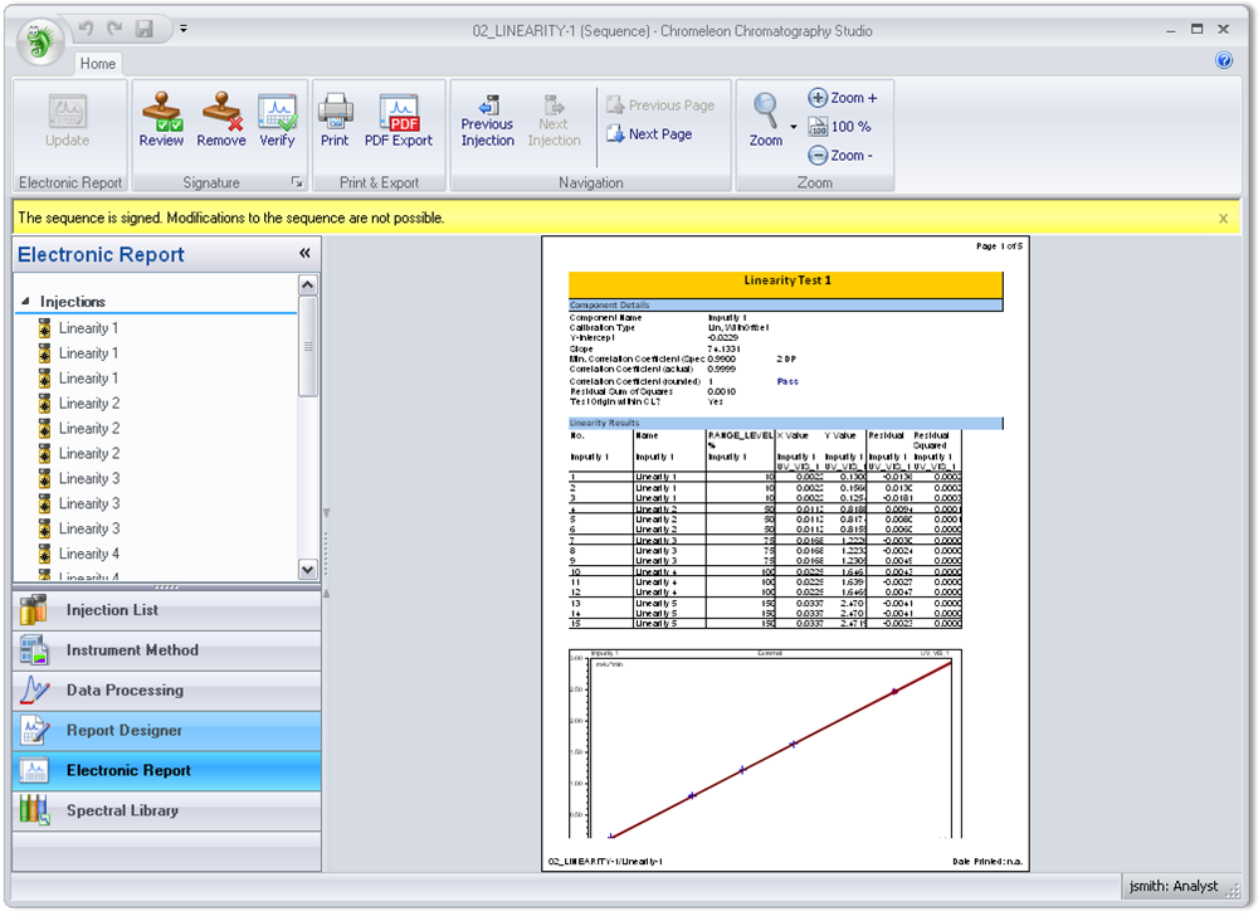



**Figure 31: Electronically signed sequences and reports are marked with special icons. Signatures can be checked by selecting the *Verify* toolbar button or menu command.**

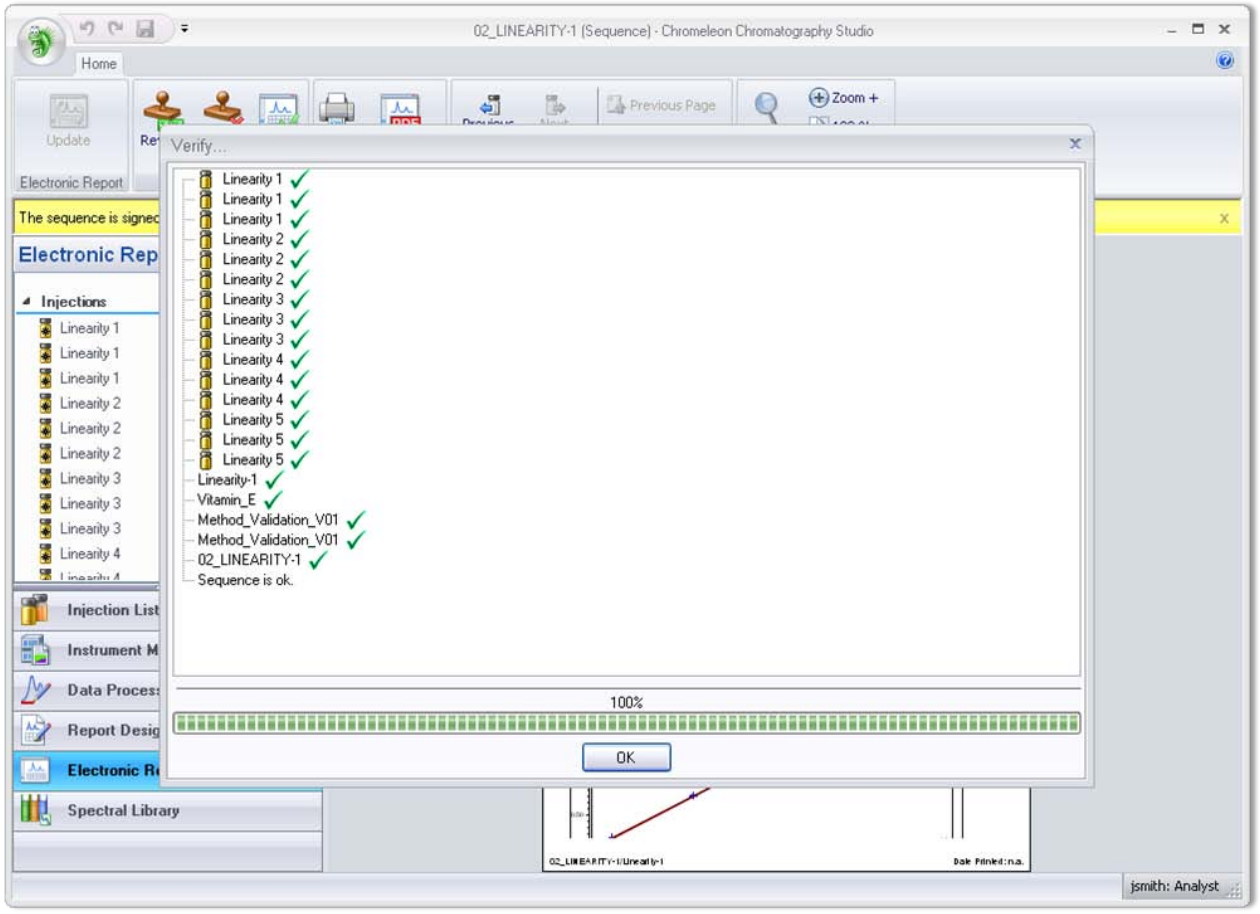



**Figure 32: When an electronically signed sequence is verified, the unique hash code is recalculated and compared against the stored value.**

## Subpart C—Electronic Signatures

### § 11.100 GENERAL REQUIREMENTS

a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

Chromeleon CDS's electronic signatures are implemented using a combination of a user's unique login name and a signature password. Because the software requires a unique login name for each individual, each signature combination is unique. Chromeleon CDS does not require that each user's signature password be unique, as this may compromise security. For example, a user might enter a password and if they encounter a "password not available" or other relevant message they might realize that they had entered part of the combination to another person's signature.

Chromeleon CDS maintains a history of login and signature passwords, and prohibits re-use of the previously used password. The System Administrator can require users to change passwords when they next log in, and can set an expiration interval for passwords (Figure 33).

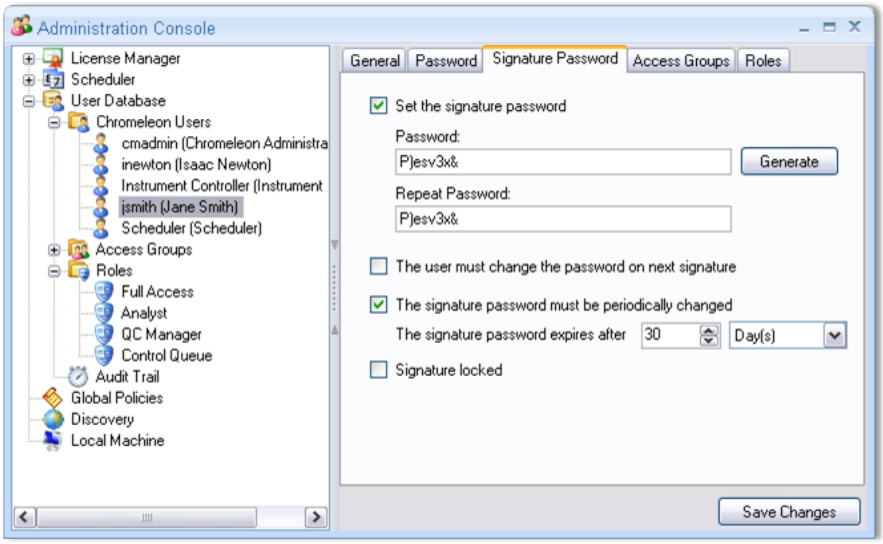



**Figure 33: The System Administrator can set password requirements, inactivity timeouts, automatic account disabling, and other policies.**

(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

- (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857.

- (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

## § 11.200 ELECTRONIC SIGNATURE COMPONENTS AND CONTROLS

a) Electronic signatures that are not based upon biometrics shall:

- (1) Employ at least two distinct identification components such as an identification code and password.
- (i) When an individual executes a series of signings during a single continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.
- (ii) When an individual executes one or more signings not performed during a single continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.
- (2) Be used only by their genuine owners; and
- (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

Chromeleon CDS's electronic signatures are implemented using a combination of a user's unique login name and a signature password. The user can be forced to enter their unique user name and signature password each time a sequence is electronically signed. Continuity of sessions can be easily enforced through an option that automatically logs a user out if no system activity is detected for a period of time whose length is specified in advance by the System Administrator. These features satisfy the requirements of subsections (i) and (ii). Because the login name is unique for each individual, each person's signature combination is unique, and can only be used by its genuine owner. Of course, system users must not reveal their passwords to anyone else; attempted use of the signature by anyone other than the genuine owner would require collaboration of two or more individuals.

## § 11.300 CONTROLS FOR IDENTIFICATION CODES/PASSWORDS

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:
a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.
b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised, (e.g., to cover such events as password aging).
c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.
d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and 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.
e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information, to ensure that they function properly and have not been altered in an unauthorized manner.

Each person's signature combination is unique as detailed in sections § 11.100 and § 11.200. Chromeleon CDS facilitates administration of password maintenance through controls such as minimum password length, password age limit, and passwords re-use prevention. The System Administrator can use these controls to force users to regularly change their passwords to new, unique expressions of a specified minimum length. The System Administrator can also require any user to change a password at next login, and can disable or delete any user account if necessary. Attempts to breach the security system can be thwarted through automatic account deactivation, which can be set to disable any account after a specified number of failed login attempts (Figure 14).

All security-related events (user and group configuration changes, successful logins, failed logins, and electronic signings) are automatically tracked in Chromeleon CDS's user management database. A convenient viewer makes it easy for System Administrators to view particular events of interest with in-built filtering using 'find as you type' text entry or grouping events together (Figure 13). At this time, use of devices bearing identification codes or passwords is not explicitly supported.

# References

http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11

Guidance for Industry1 Part 11, Electronic Records; Electronic Signatures - Scope and Application; http://www.fda.gov/RegulatoryInformation/Guidances/ucm125067.htm

http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/ucm124787.htm

**www.thermoscientific.com/chromeleon**



**Australia** +61 3 9757 4486
**Austria** +43 1 333 50 34 0
**Belgium** +32 53 73 42 41
**Brazil** +55 11 3731 5140
**China** +852 2428 3282
**Denmark** +45 70 23 62 60
**France** +33 1 60 92 48 00
**Germany** +49 6126 991 0
**India** +91 22 2764 2735
**Italy** +39 02 51 62 1267
**Japan** +81 6 6885 1213
**Korea** +82 2 3420 8600
**Netherlands** +31 76 579 55 55
**Singapore** +65 6289 1190
**Sweden** +46 8 473 3380
**Switzerland** +41 62 205 9966
**Taiwan** +886 2 8751 6655
**UK/Ireland** +44 1442 233555
**USA and Canada** +847 295 7500

Thermo SCIENTIFIC
Part of Thermo Fisher Scientific

TG70197_E 07/16S