21 CFR Part 11 Compliance Features of the LC/MSD Trap Security Pack 1.0 Software

Technical Overview

Patrick Perkins, Frank Kuhlmann, and Bryan Miller
Agilent Technologies

Introduction

The 1997 FDA ruling 21 CFR Part 11 defined criteria for FDA acceptance of electronic records and electronic signatures.[1] Intended to reduce requirements for paper records, 21 CFR Part 11 precipitated sweeping changes in the pharmaceutical industry. In February 2003, the FDA issued a draft guidance document that more narrowly defined the scope and application of 21 CFR Part 11.[2] This draft document limited 21 CFR Part 11 applicability to certain records required by the predicate rules (GLP, GMP, etc.), as well as to electronic records generated by medium- and high-risk systems. The latter are defined as systems that generate data relevant to product quality, product safety, and public health. This definition encompasses the majority of the chromatography data systems used in the pharmaceutical industry.

Agilent maintains an ongoing commitment to help customers comply with regulatory requirements. This has led to development of a wide range of software and compliance services. This application note presents compliance features available in the security pack software for the Agilent 1100 Series LC/MSD Trap ion trap mass spectrometer. Also discussed are Agilent compliance services and training available for this instrument.

While compliance is ultimately the responsibility of the laboratory, and there are aspects of compliance (such as records retention, change control, and password protection policies) that only the laboratory can address, Agilent's comprehensive compliance products and services help to streamline the compliance process.

Agilent Technologies

Requirements of 21 CFR Part 11

The regulations in 21 CFR Part 11 are designed to ensure data integrity, security and traceability. In 21 CFR Part 11, the FDA distinguishes between open and closed systems and requires different controls for each. The LC/MSD Trap software is designed for the closed systems that typify pharmaceutical firms. These are systems where there is physical access control to the site itself, and where the company has a firewall in place for network applications. For closed systems, the rule mandates the following:

- System validation
- Ability to create accurate and complete copies of records
- Limited system access
- Protection of electronic records so they can be retrieved throughout the records retention period
- Audit trails
- Operational system checks to ensure that steps are followed in the correct order
- Authority checks
- Device or terminal checks
- Training
- Written policies that hold persons responsible for actions with their electronic signatures
- Controls over system documentation

The LC/MSD Trap Security Pack 1.0 Software, along with Agilent's extensive compliance services, helps users meet many of these requirements.

System validation

System validation ensures accuracy and reliability of analytical systems. To this end, Agilent maintains a highly-trained service organization to perform installation qualification and operational qualification for the LC/MSD Trap. Installation qualification (IQ) ensures that all components of the system are received and properly installed.

Operational qualification/performance verification (OQ/PV) ensures that the system meets specified performance criteria through analysis of specific samples under documented conditions.

Performance qualification (PQ) is an ongoing validation program that laboratories use to prove that an instrument performs according to a specification appropriate for its routine use. A good PQ program helps laboratories to address small instrument problems before they become major issues. Agilent-certified engineers are trained to perform preventive maintenance, which supports a laboratory's ongoing performance qualification efforts and can be combined with PQ to minimize downtime.

For proper system validation, it is also important that the system vendor develops the product using a validated lifecycle with appropriate controls. Agilent develops its hardware and software products according to a well-defined product development lifecycle, to ensure a consistent level of product quality and conformity with regulations.

Complete copies

To meet 21 CFR Part 11 requirements, the system must allow the creation of "accurate and complete copies of records in both human-readable and electronic form." The LC/MSD Trap achieves this via storage of the metadata and audit logs required to reconstruct the events which lead to the reported results. Data can be copied to CD or DVD using standard copy utilities. Audit trails can be printed, either directly as text files, or after import into spreadsheet programs. Data and results can also be printed.

Limited system access and password protection

21 CFR Part 11 mandates that access to systems be limited to authorized individuals. The LC/MSD Trap security pack software addresses this aspect of the rule by requiring that each user log on with a valid password. The software includes a User-Management Administration Tool that makes it easy for a system administrator to set up operators, their passwords, and their rights (see Figure 1).

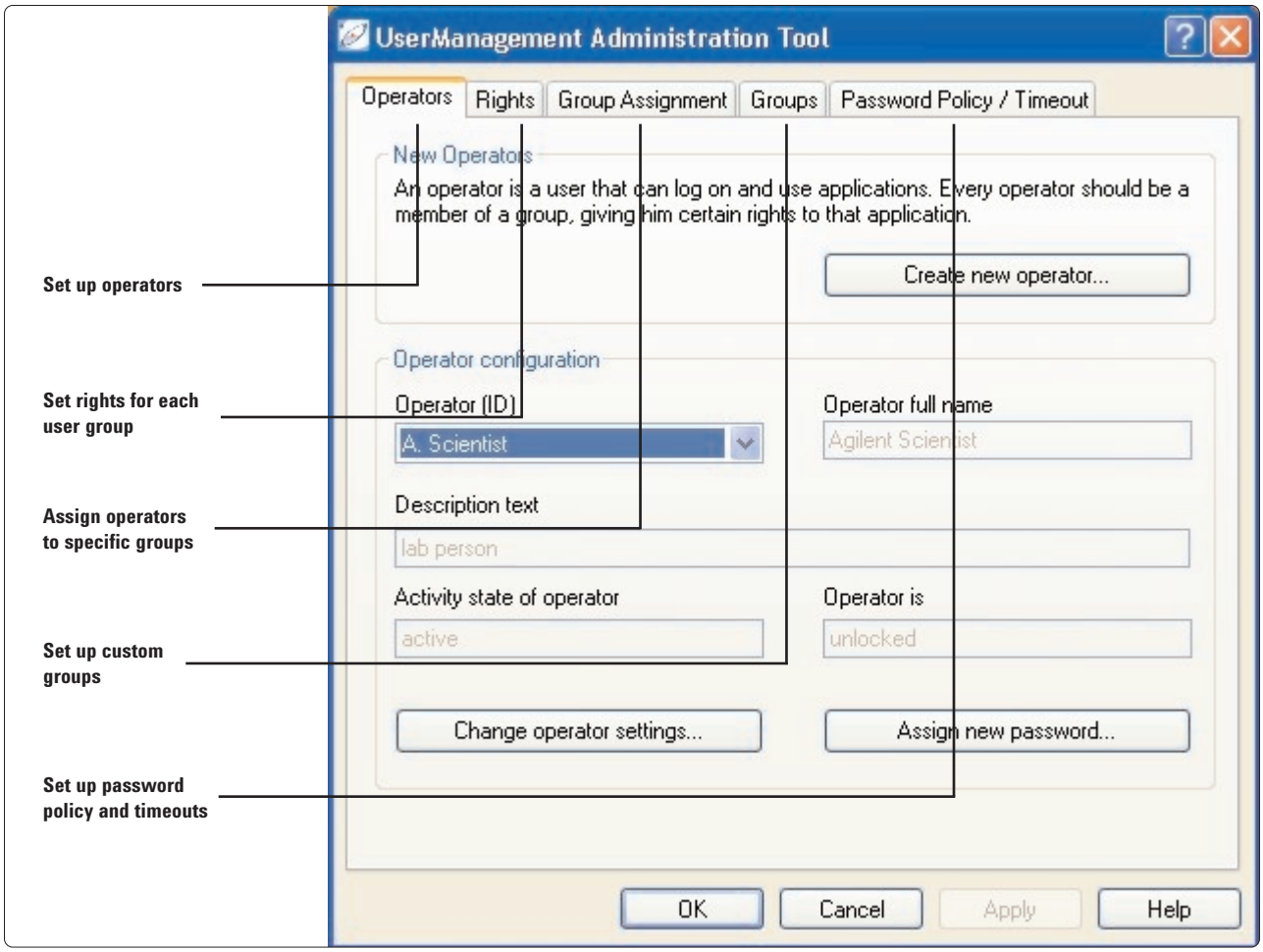

Figure 1. Easy setup of operators, passwords, and rights

The system administrator assigns each user to one or more user groups. The user groups determine the user's rights, so that some users can have a wide range of access and control, while others can be limited to only the minimum functions they require. For convenience, the software includes preconfigured user groups for administrators, operators, project managers, scientists, and service personnel. New groups can be created by cloning established groups, or by starting completely fresh.

An important requirement of 21 CFR Part 11 is that only the users themselves know their individual passwords. The LC/MSD Trap security pack software ensures that this is the case by preventing even the system administrators from knowing other users' passwords. While the system administrator assigns the initial user password, the user must change it at first logon.

21 CFR Part 11 also requires that to prevent unauthorized access, the software application must timeout after a period of inactivity. As shown in Figure 2, the system administrator can customize the timeout setting. He can also customize other aspects of the password policy, such as password length and expiration.

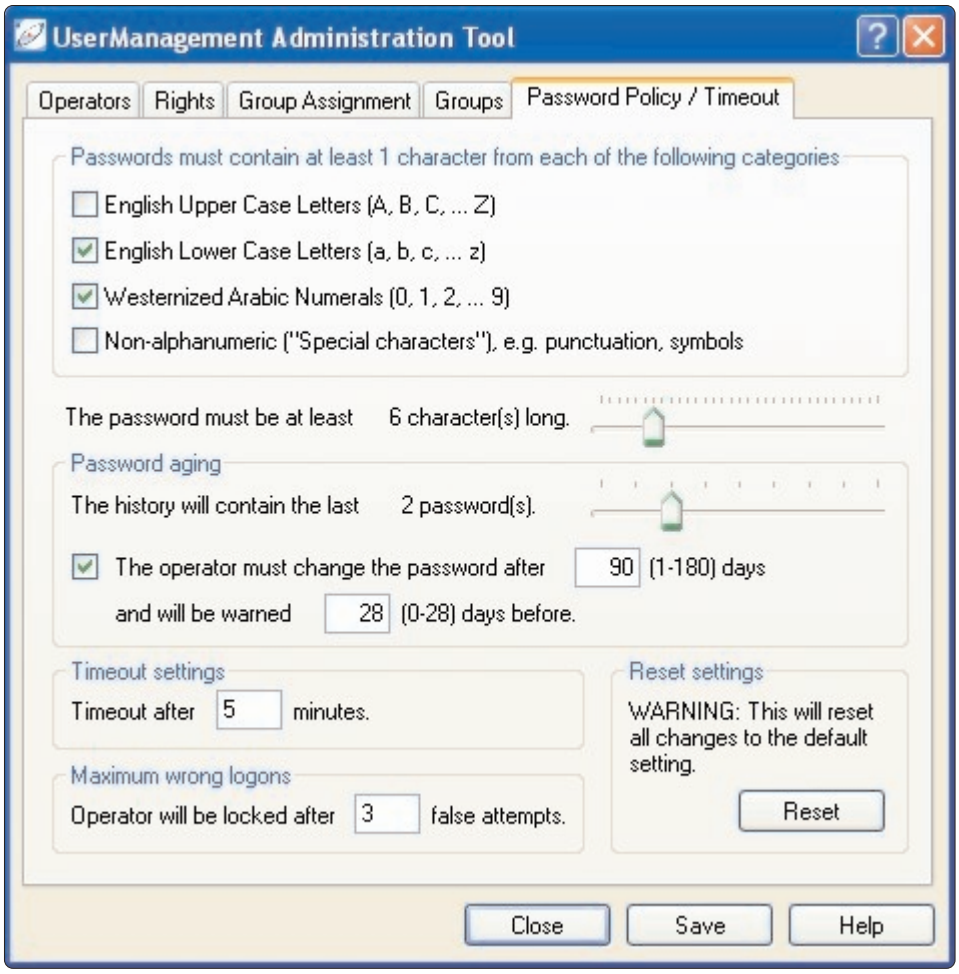

Figure 2. Customizable password policies

When laboratories have multiple LC/MSD Trap systems, the system manager can install the UserManagement Administration Tool on a central server. This server can also be one of the LC/MSD Trap control PCs. The server allows user administration to be managed efficiently for the entire laboratory using a single central PC.

Protection of electronic records

21 CFR Part 11 requires that electronic records (data) be protected so that they can be accessed throughout the records retention period. There are features within the software to guard against overwriting data. The LC/MSD Trap security pack software also employs data versioning so that processed data is never overwritten; rather, multiple copies are maintained as part of a "result history." As shown in Figure 3, this history can be conveniently opened using a menu item in DataAnalysis. Individual processed results and processing parameters can be reloaded and easily examined by the user or FDA inspectors. The capability to delete results is controlled as a separate user privilege that can be withheld from all users, and the deletion process is recorded and maintained in the results history.

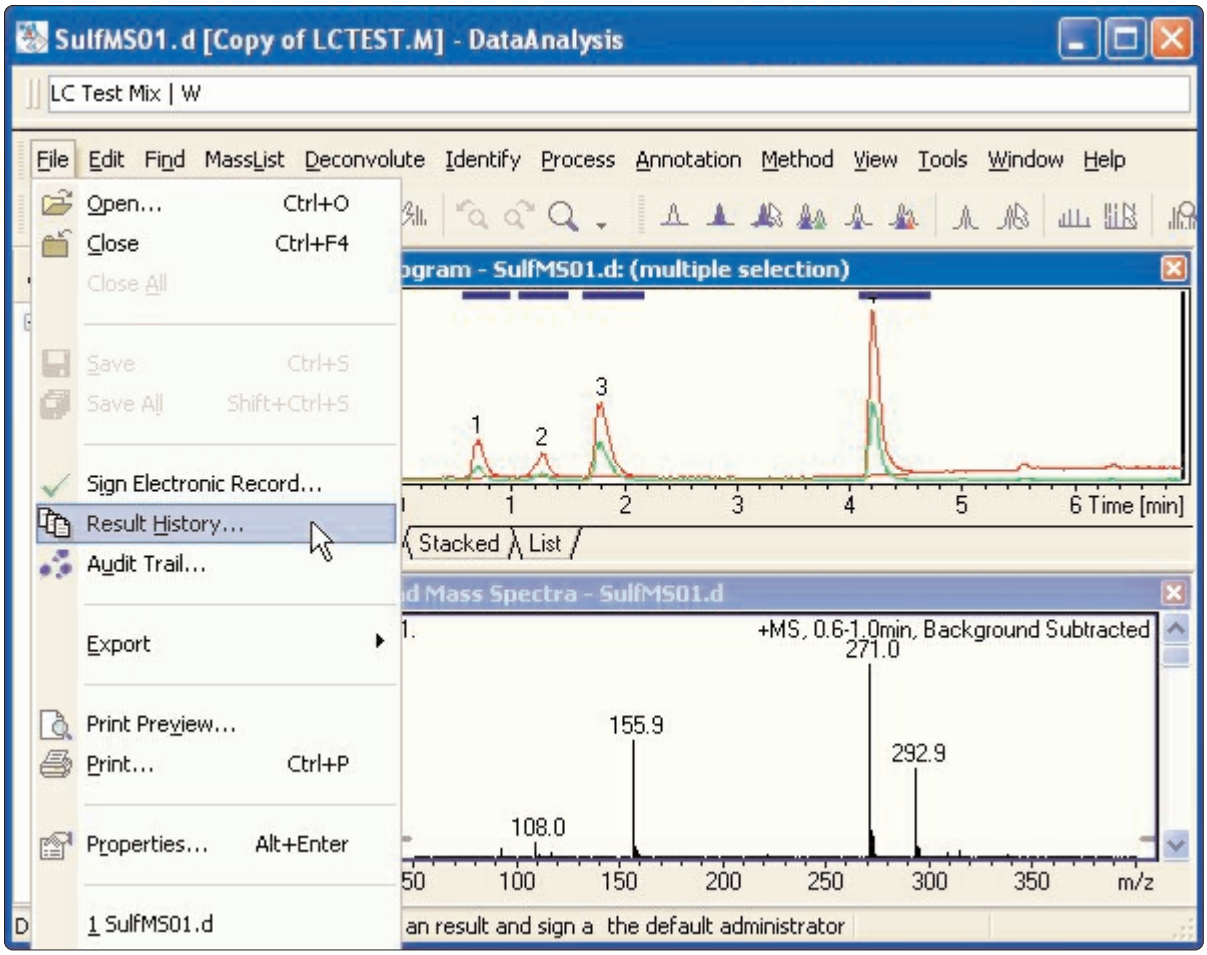

Figure 3. Easy access to Result History

Audit trails

Audit trails track how data records are changed, for example, during the course of results review. The LC/MSD Trap security pack software tracks system events and user actions in computer-generated, time-stamped, secure, user-independent, human-readable audit trails, as shown in Figure 4. Audit trails track all operations for the system, methods, and analyses. The audit trails for data and methods are accessed via the **Electronic Record** button shown at the top of Figure 4.

The user and system audit trails are accessed via the other two buttons shown at the top of Figure 4. The user audit trail gives information on who logged on, at what time, and from which client PC. This audit trail records logon attempts that failed because the user name and/or password were entered incorrectly. The system audit trail records when the LC/MSD Trap software was started, by whom, and which version of software was used. It also records which methods were loaded, by whom, and when.

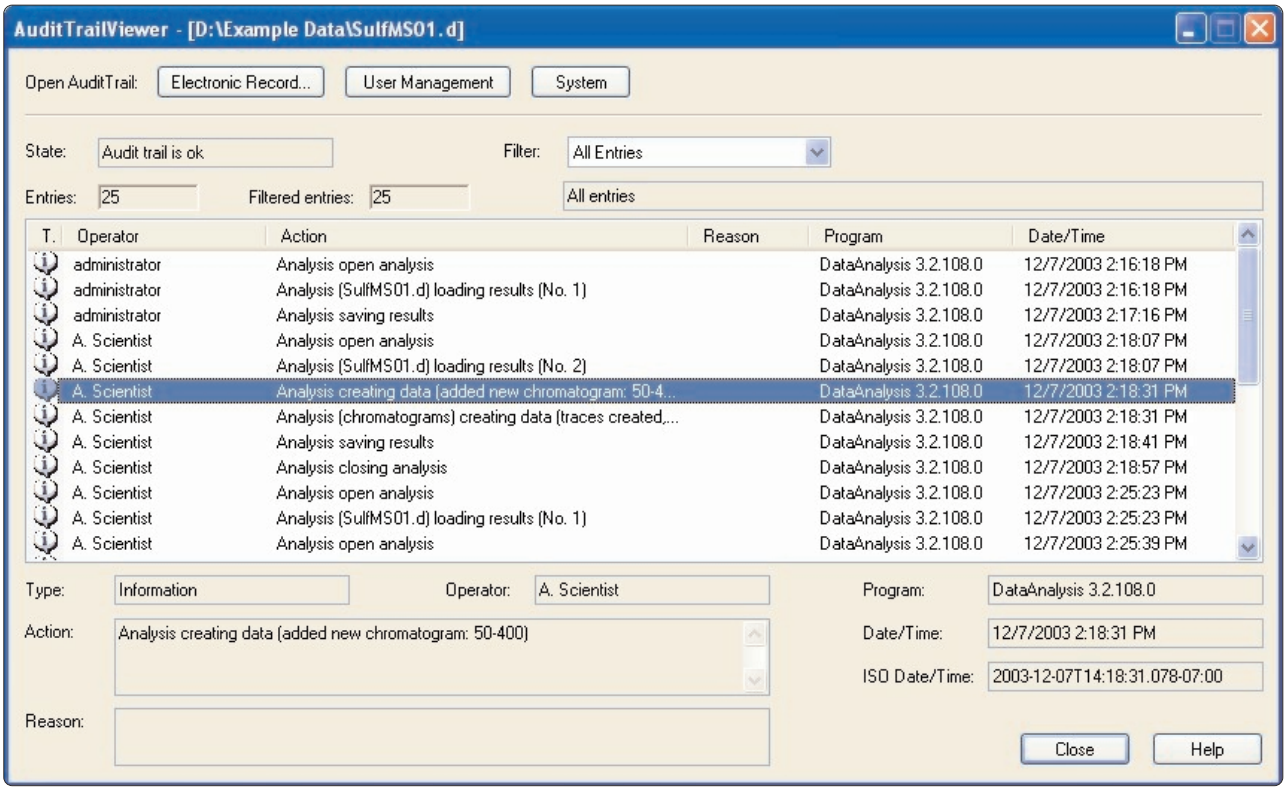

Figure 4. Audit trail for DataAnalysis

Operational system checks

Operational system checks ensure that processes are followed in the correct order. The LC/MSD Trap software achieves this by requiring that steps be accomplished in a logical order. For example, to prevent untracked changes to methods, acquisition start will always trigger retrieval of the stored method (method of record).

Authority checks

The LC/MSD Trap security pack software performs authority checks to ensure that only authorized individuals use the system, alter a record, or electronically sign a record. The software accomplishes this by requiring all users to log on with their user name and password both initially and after timeouts. If a user attempts to perform a function for which he lacks the right, the software alerts him and the command fails to execute.

Training

The FDA rule requires training for those who develop, use, and maintain electronic records. Agilent offers both basic and advanced training for LC and LC/MSD Trap users. Comprehensive software familiarization exercises and example data are included with the LC/MSD Trap. A software tutorial that covers data acquisition, data analysis, and automation is available for free on the Agilent website. In addition, Agilent offers compliance-related courses on instrument qualification and method validation. Free e-seminars are available on specific compliance and application-based topics.

Electronic signatures

The LC/MSD Trap security pack software enables use of electronic signatures. In compliance with the FDA rule, these electronic signatures use two distinct identification codes—a user ID and a password. (See Figure 5.) Both must be reentered each time a record is signed. As an added safeguard against password "guessing," the administrator can set password aging policies, can force password changes at any time, and can automatically lock users out if they enter their password incorrectly too many times.

Tools are provided to make it straightforward to load and sign processed results that have been previously saved. Both DataAnalysis and QuantAnalysis maintain a Result History. For DataAnalysis, the Result History pertains to each individual data file, while for QuantAnalysis the Result History pertains to each quantitation set. An example is shown in the background of Figure 5. These histories allow one to rapidly load, examine, and sign previous versions of the processed results, along with the full set of processing parameters.

Conclusions

While the scope of 21 CFR Part 11 has been narrowed, most analytical instruments used in regulated industries still need to comply with this FDA rule. The LC/MSD Trap Security Pack 1.0 Software provides customers with critical compliance tools. Agilent compliance services and Agilent training complete the total compliance solution for this instrument.

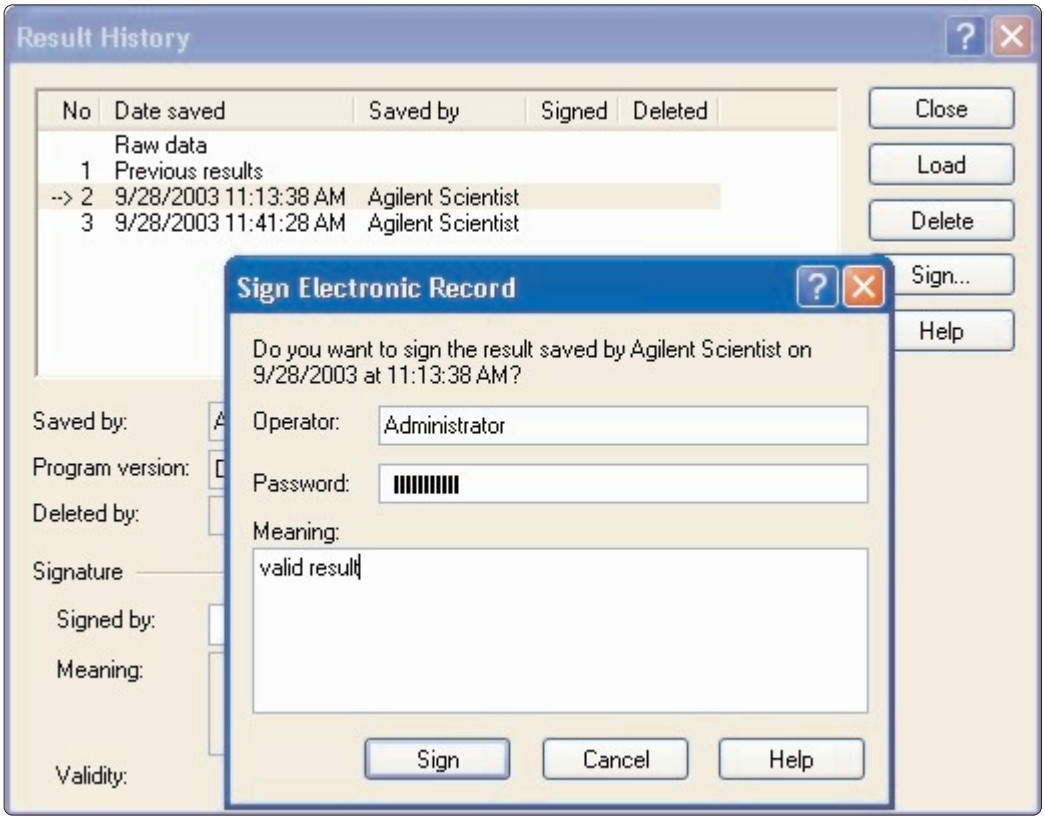

Figure 5. Electronic signature requires both operator name and password

References

1. "21 CFR Part 11. Electronic Records; Electronic Signatures; Final Rule Electronic Submissions; Establishment of Public Docket; Notice," Department of Health and Human Services, Food and Drug Administration, Federal Register, March 20, 1997.
2. "Guidance for Industry Part 11, Electronic Records; Electronic Signatures—Scope and Application," Department of Health and Human Services, Food and Drug Administration, February, 2003.

Authors

Patrick Perkins, Frank Kuhlmann, and ***Bryan Miller*** are scientists at Agilent Technologies in Santa Clara, California U.S.A.

www.agilent.com/chem

Printed in the U.S.A. February 25, 2004
5989-0624EN

Agilent Technologies