

# MicroLab FTIR Software 21 CFR Part 11 Compliance

## Technical Overview



### Introduction

Electronic data submitted to the United States FDA must comply with specifications set forth in the Code of Federal Regulations, Title 21 Part 11 (21 CFR Part 11). This code specifies that data be protected and verified to ensure validity to the same standard as signed, paper-based data. The Agilent MicroLab FTIR software provides features that allow for 21 CFR Part 11 compliance. MicroLab FTIR provides logon security, data security, electronic signature capability, audit trail capability and validation of system performance, as required by the regulations. These features provide the tools for compliance with the 21 CFR Part 11 regulations, while keeping the versatile, easy to use nature of the standard MicroLab software package. The combination of the powerful, innovative, intuitive and reliable Cary 630 FTIR hardware with the secure and easy to use MicroLab software provides confidence and performance for both novice and advanced users.



**Agilent Technologies**

## Logon security

Access to the MicroLab FTIR software is user name and password controlled. This ensures that only authorized users can make measurements and access the data. Additionally, a permission level is assigned for each user, which defines the actions that the user can take within the software; these levels are assigned by the software administrator. For instance, a Technician can run a 'public' method, but cannot edit any methods. Another example is that a user must have E-signer rights in order to validate data or methods. Multiple levels can be set to an individual user in order to customize access for each user. A detailed breakdown of the roles available in the MicroLab software is given in Table 1.

## Data security

MicroLab FTIR software data and methods have built-in security features to ensure the authenticity and integrity of the records. An internal security feature checks to ensure that the data has not been tampered with by an outside source. This security feature is checked each time the data is displayed, the method is activated or the data is reported. The user is alerted if evidence of tampering is found. Furthermore, the MicroLab software automatically saves all data collected, and prevents overwriting the data with a unique file name format. Additionally, the MicroLab software does not allow data to be deleted, ensuring that any collected data is preserved within the software. Not only are these data collection features required by the 21 CFR Part 11 regulation, they also ensure that no valuable data is lost by accidental deletion or modification.

## Electronic signatures

Electronic signature capabilities are at the core of 21 CFR 11 compliance. Like a physical signature on a paper record, the e-signature indicates that a method or data file has been reviewed and approved by the signer. MicroLab FTIR software provides e-signatures at all levels for both data collection and method development. Users with the e-signature role assigned to their profile can sign methods, results and system performance verification at the review, approval or submission level.

**Table 1.** Summary of the roles available in 21 CFR Part 11 MicroLab FTIR software

	- Does not have this capability	x	Has this capability		
User level	Technician	Service	E-signer	Developer	Admin
Method Edit	-	x	-	x	x
All Methods	-	-	-	-	x
Create New	-	x	-	x	x
Make Public	-	-	-	-	x
Activate	x	x	x	x	x
Full Edit Capabilities	-	-	-	-	x
Reference Templates	-	-	-	-	x
Edit	-	-	-	-	x
Activate	-	-	-	-	x
<b>21 CFR 11 functionality</b>					
E-sign			x		
21 CFR 11 Audit Trail button			x		
<b>Advanced features</b>					
System Check	x	x	x	x	x
Diagnostics	x	x	x	x	x
Clean Validity	x	x	x	x	x
Gain Adjust	-	x	-	-	x
Date Time Format	x	x	x	x	x
Library Management	-	-	-	x	x
New Library	-	-	-	x	x
Add to Library	-	-	-	x	x
Delete From Library	-	-	-	x	x
Delete Library	-	-	-	x	x
User Management	-	-	-	-	x
Change Password	x	x	x	x	x
21 CFR 11 System Log	-	-	-	-	x

An example of the types of signatures is shown in Figure 1. To sign a file, the user must enter their user name and password as authentication. The signatures are an integral part of the data file and the record of them cannot be removed from the file. The software also tracks changes made to the file after an e-signature is applied and marks the signature as obsolete if the data is reprocessed or modified in any way.

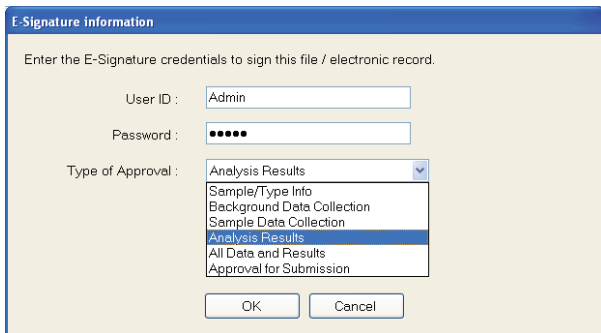


Figure 1. E-signature approval levels for results

## Audit trail and system log information

The 21 CFR Part 11 regulation states that an electronic 'Audit Trail' must be kept for both the system and for data files. The audit trail on the data provides a means to ensure that the data was collected and processed using the correct parameters. The system (instrument) audit trail provides a record of file creation or deletion as well as a record of any errors that were encountered. The MicroLab FTIR software provides a detailed accounting of all the system functions (system log) as well as a log of creation or modification of data files (audit trail). In addition, an audit trail is also kept for the methods. These three types of logs ensure that any changes that were made to the data, methods or system are tracked and accounted for.

The system log provides access to user logons, instrument initializations, re-analysis of data and security issues. An example of the system log is shown in Figure 2. Only users with administrator rights can access the system log. The system log can be printed to a PDF file for further record keeping. The system log gives the administrator visibility to who has been using the system and if those users have made any changes. This helps the administrator ensure that the instrument is being used according to established procedures.

The audit trail is attached to results, methods and system check data. The results audit trail keeps a record of everything that happened to the data file to the current state including collection parameters, quantitative processing, library searching and any reprocessing. This record allows managers to ensure that data was collected and processed correctly,

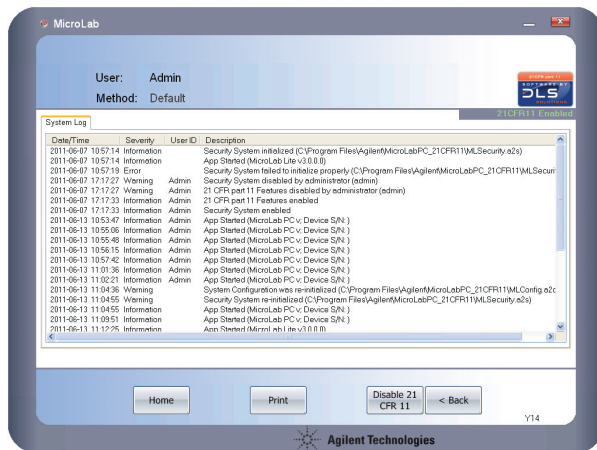


Figure 2. Example System Log

providing further assurance in the quality of the data. An example of a 'Results Audit Trail' is shown in Figure 3. Most users find the Results audit trail to be the most useful feature of the 21 CFR Part 11 software. Similarly, the 'Methods Audit Trail' tracks changes that were made to spectral methods, the user who made those changes and any e-signatures applied to the method(s). This gives managers a way to track the history of a method, ensuring that it is defined correctly to accomplish the measurement goals. Likewise, the audit trail on system checks provides a record of when the system check was run and by whom; e-signatures that are applied to the 'System Check Results' are also captured in the audit trail.

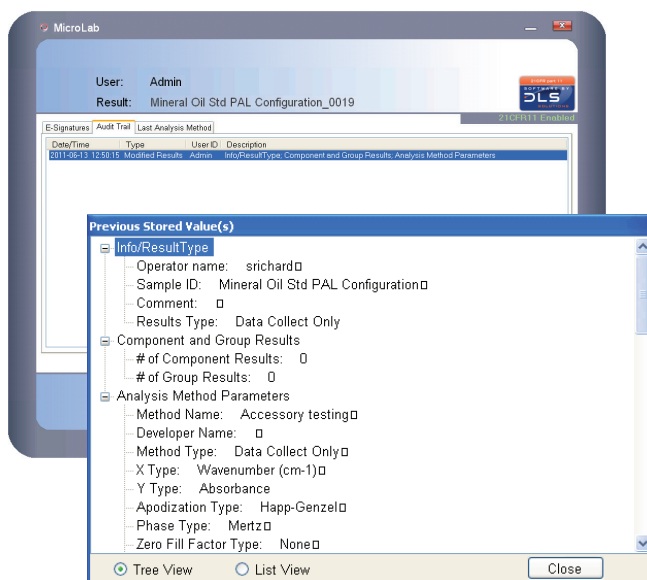


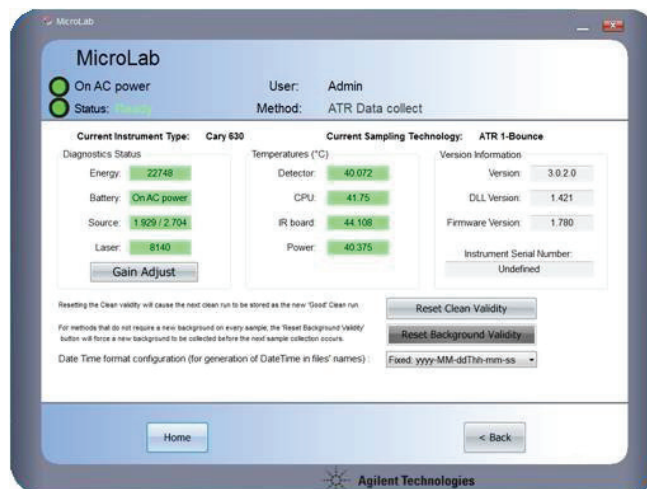
Figure 3. Example Results Audit Trail in MicroLab FTIR 21 CFR Part 11 compliant software

Data from the audit trail can be displayed in either a tree or listed view. In the tree view, each section can be expanded to give more information. The tree view allows the user to scan the audit trail to find the most appropriate section, and then expand it to find the information desired. All of the audit trails can be printed to a PDF file for further record keeping of the results, methods, or system check history.

## Validation of system performance

The 21 CFR Part 11 regulation states that software should have the ability to verify the system performance. The MicroLab FTIR software contains several levels of performance checks, which are used to ensure that the system is operating to specification before any measurement is made. At the lowest level, the MicroLab software checks basic system diagnostics to ensure that quality data is being collected; data collection is not allowed within the software unless the manufacturer's specifications are met on the source voltage, interferogram intensity, laser voltage, and detector temperature. Furthermore, checks are done as the data is being collected to ensure consistent reproducible data is being collected. In addition to these checks occurring behind the scenes, the software contains an easy to read diagnostics screen. The color-coded diagnostics gives a quick picture of the instrument health, which the user can easily verify. The diagnostic values are also saved with each sample result, so the manager or data reviewer can ensure that the instrument was running properly when data was collected. An example of the diagnostics screen is shown in Figure 4.

MicroLab FTIR software also provides an automated installation and operational qualification test (Automated IQ/OQ). IQ/OQ is a yearly requirement in most regulated cases. The Auto IQ/OQ conducts a series of tests, which validate all aspects of the instrument's performance. These tests are based on ASTM E1421; signal-to-noise, stability and frequency accuracy and precision are tested against Agilent specifications. At the conclusion of the Automated IQ/OQ, a PDF report is generated showing the diagnostic values, the test results, the specifications for the tests and pass/fail criteria. The Auto IQ/OQ test can be electronically signed, which is also shown in the report.



**Figure 4.** Diagnostic values are saved with each sample result. Color-coded results (red, yellow, green) allow for a quick visual check of the instrument performance.

This feature allows users to routinely run the IQ/OQ test to ensure the instrument is operating correctly, without the need for a factory service call.

## Reporting capabilities

MicroLab FTIR software can generate reports for results, methods, and systems tests all in PDF format. The PDF format allows the report to be reviewed on almost any computer and further prevents editing or tampering with the reports. The reports show the file name, date, time, e-signature status in addition to the results or method information. These reports allow the archival of results for either agency or management review. The complete format of the MicroLab reports provides all of the required information in a single easy-to-use format.

## Conclusion

Agilent Technologies' MicroLab FTIR software with the 21 CFR Part 11 add-on provides users with compliance features required in the pharmaceutical industry in an easy-to-use format. The combination of MicroLab's method driven, simplified format along with audit trail, e-signature, security and performance testing features provides confidence in collected data.

**[www.agilent.com/chem](http://www.agilent.com/chem)**

Agilent shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance or use of this material.

Information, descriptions, and specifications in this publication are subject to change without notice.

© Agilent Technologies, Inc. 2011

Published September 1, 2011

Publication number: 5990-8672EN



**Agilent Technologies**