WHITE PAPER

Data Integrity – Spectrum 10 Enhanced Security (ES) Software for Infrared Spectroscopy

Introduction

The FDA defines data integrity as "completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA)".[1] ALCOA itself has evolved to ALCOA Plus, which incorporates two of the fundamental definition terms as stated by the FDA; complete, consistent, enduring, and available.[2] Compliance with 21 CFR Part 11 is mandatory for pharmaceutical companies and their suppliers to sell products into the United States, and also applies to other related industries.

PerkinElmer's Spectrum™ 10 Enhanced Security (ES) software platform for infrared spectroscopy provides structural requirements and features to assist with the needs for ensuring data integrity and compliance. It affords the system owner the ability to comply with regulations and incorporate features into the validation plan to exhibit compliance. The purpose of this document is to demonstrate how Spectrum 10 ES meets the technical requirements for 21 CFR Part 11.

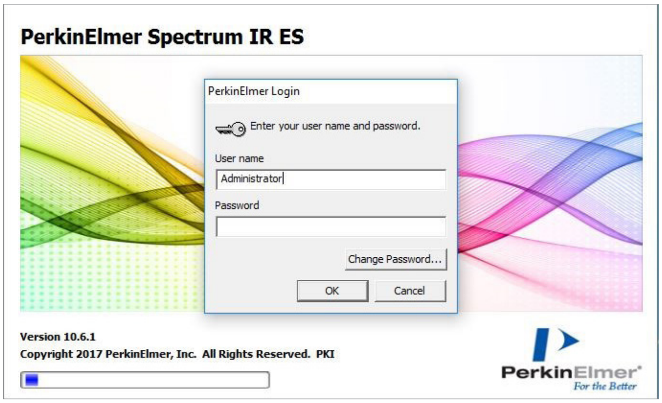
Spectrum 10 ES

Spectrum 10 ES provides tightly controlled setup, collection, and reporting of IR data to meet the technical demands of 21 CFR Part 11 compliance (Figures 1 and 2). In addition, the software has an easy-to-use interface to lower the training requirements for non-specialised operators. Most functions within Spectrum 10 are identical in standard (STD) and ES versions. However, the main differences are related to:

- Logins
- Permissions
- Electronic signatures
- Protection of records
- Working with audit trails

Spectrum 10 ES is compatible with the Spectrum 3™, Frontier™, Spectrum Two™ and Spectrum Two N™, Spectrum 400, Spectrum 100/100N, and Spectrum One/NTS PerkinElmer FT-IR and FT-NIR spectrometers. The software will only read recognized encrypted PerkinElmer file formats.

PerkinElmer®
For the Better



PerkinElmer Spectrum IR ES

PerkinElmer Login

Enter your user name and password.

User name: Administrator

Password:

Version 10.6.1

Copyright 2017 PerkinElmer, Inc. All Rights Reserved. PKI

Figure 1. Login window for Spectrum 10 ES software.

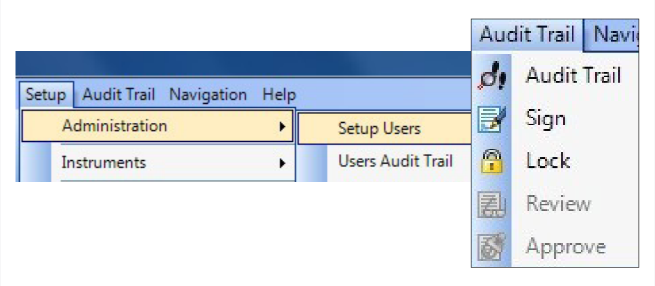
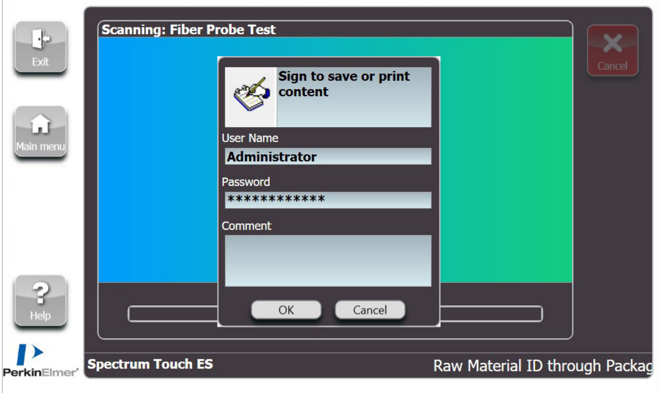


Figure 2. Enhanced security features are shown on the tool bar in Spectrum 10 ES.
Note: 'Setup users' and 'Users Audit Trail' is only available to Administrators.

Also available for IR spectroscopy are PerkinElmer's Enhanced Security AssureID ES and Spectrum Touch™ ES to allow optimized workflow-oriented methods. Spectrum Touch ES provides a simplified, easy-to-use interface for running a pre-designed application (App) to perform a specific analysis, whilst helping comply with 21 CFR Part 11 guidelines (Figure 3). The highly customizable Touch Apps are created using Spectrum 10 ES and Spectrum Touch Developer. Configuration of the ES features is also carried out using Spectrum 10 ES. Spectrum Touch ES is optimized for touch screens to facilitate mobility around a manufacturing environment. However, the software can also be installed on standard computers.



Scanning: Fiber Probe Test

Sign to save or print content

User Name: Administrator

Password: ************

Comment:

Figure 3. Spectrum Touch ES interface demonstrating login required to sign for data generated.

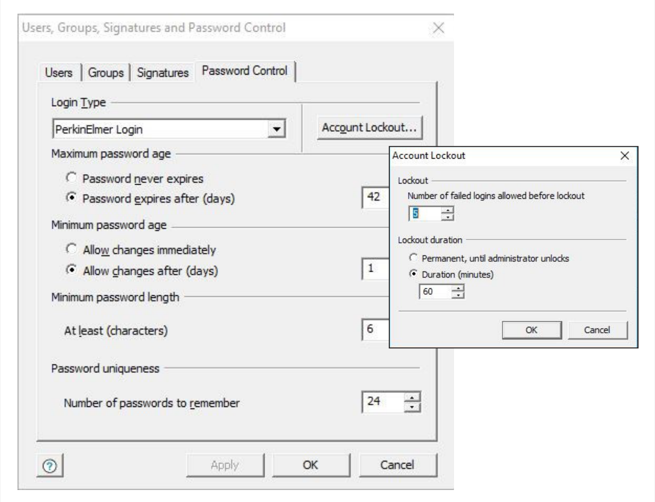
Software Logins

Unique user names and passwords are required for all authorized users to access Spectrum 10 ES software and cannot be reassigned. The instrument Service Mode is also under password control and only available if logged in as a service user. Users can be setup by the Administrator in the software (Figure 4).

Two password login modes are available:

- PerkinElmer login ➞ logins (user name and password) are created for each Spectrum User and remain unique within the system, even after a user has left the company.
- Windows login ➞ login is controlled by the login to the Windows® OS, meaning only one password to remember.

For technical compliance with 21 CFR Part 11, the login security includes administrator-definable features such as password expiration and failed login detection and lockout. All access or attempted access to the system is logged in an audit trail. Users are limited to a specified number of unsuccessful login attempts. If the administrator-defined number of unsuccessful PerkinElmer logins is reached, that user is locked out for a certain period (defined by the administrator) or once they have been unlocked by the administrator. The Spectrum 10 ES Administrator can allocate a new temporary password, which the user is forced to change on its first-time use (i.e. their next login). Due to the high degree of security in Spectrum 10 ES, it is highly recommended that more than one Administrator be created in case one of the Administrators is absent or forgets their password. The software has no 'backdoor' to the security system. If a user is locked out whilst using the Windows login, the company IT administrator will need to unlock their account and/or provide them with a temporary password.



Users, Groups, Signatures and Password Control

Login Type: PerkinElmer Login

Maximum password age
○ Password never expires
● Password expires after (days): 42

Minimum password age
○ Allow changes immediately
● Allow changes after (days): 1

Minimum password length
At least (characters): 6

Password uniqueness
Number of passwords to remember: 24

Account Lockout

Lockout
Number of failed logins allowed before lockout: 5

Lockout duration
○ Permanent, until administrator unlocks
● Duration (minutes): 60

Figure 4. Setup of logins and password control (left) and account lockout (right).

Permissions for Users and User Groups

Spectrum 10 ES enforces authority checks using authorization groups. Each group has its software access rights defined by the selection of permissions. Individual users are assigned to one or more pre-defined groups. At installation, the software has a default set of authorization groups.

Default groups include:

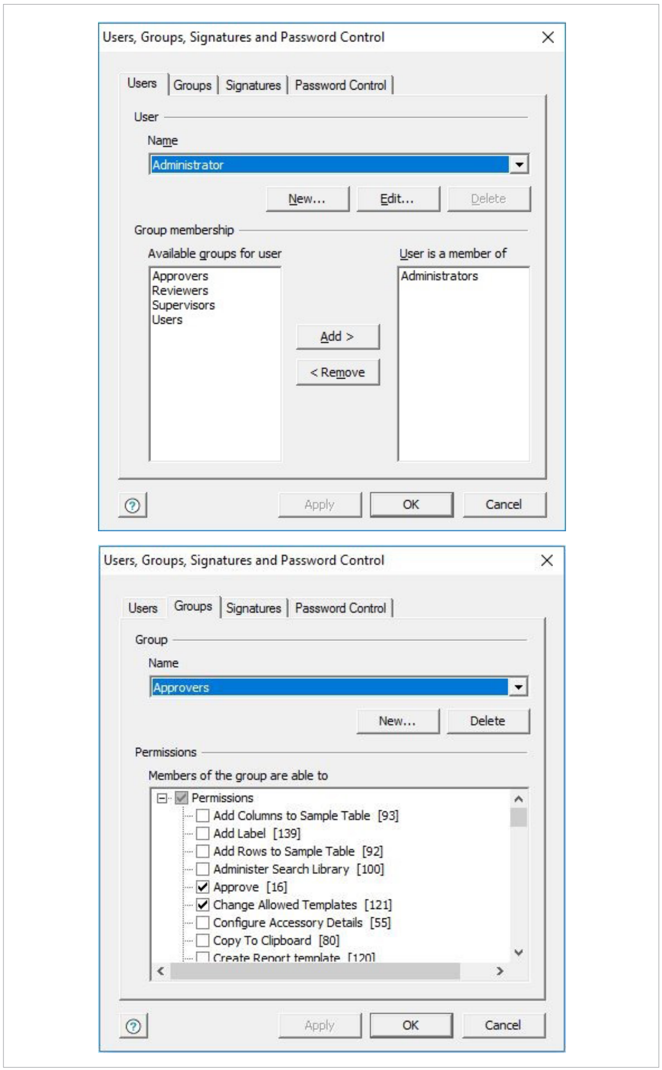
- **Administrators** – major security administration capabilities are set as default (e.g. setting of user/groups logins and permissions). Administrators can be members of other groups (e.g. Users).
- **Supervisors** – have a series of default extended permissions enabled (e.g. saving group workspaces, add/remove instruments etc.), except basic administration permissions. They can also setup and examine users' workspaces.
- **Users** – members can perform all functions in the software, except those associated with Administrators, and Return Workspace, Review and Approve. The users group has fewer default permissions enabled than the supervisor group.
- **Reviewers** – Members of the Reviewers group are intended to act as reviewers of changes, made by other users, requiring an electronic signature. They can also examine others' workspaces.
- **Approvers** – Members of the Approvers group are intended to act as approvers of changes, made by other users, requiring an electronic signature. They can also examine others' workspaces.

Only Spectrum 10 ES Administrators can alter the permissions of the accessible functions for these groups, add new groups, maintain the system, and allocate areas of access to individual users. The groups to which a user belongs can be toggled and define the areas of software they are permitted access to (Figure 5). This allows the application to be customized to the laboratory's most effective workflow according to their specific analytical requirements.

Additionally, Supervisors can setup a default group workspace (Figure 6). This will allow supervisors to transfer their current settings to all groups selected.

Electronic Signatures

Administrators in Spectrum 10 ES can configure Signature Points for certain actions, such as data collection and outputting of results (Figure 7). Signature points can be configured individually, or the same settings can be applied to all Signature Points. Signatures can be entered on exiting, before the action (as appropriate), or by selecting 'Audit Trail' and then 'Sign'. Signatures are also added to report files.



Users, Groups, Signatures and Password Control

User

Name: Administrator

Group membership

Available groups for user:
Approvers
Reviewers
Supervisors
Users

User is a member of:
Administrators

Users, Groups, Signatures and Password Control

Group

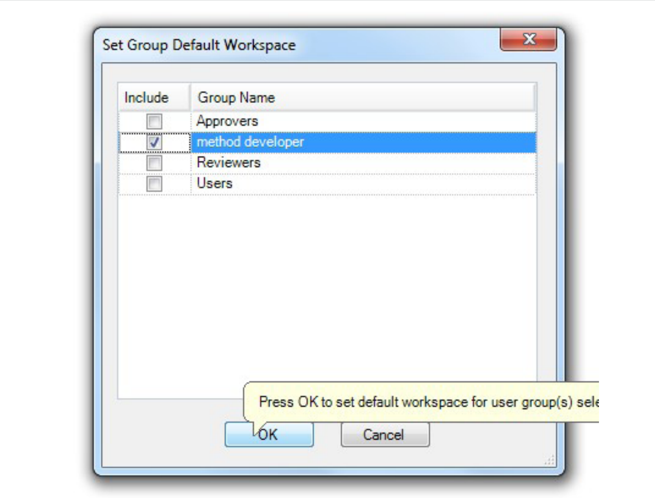
Name: Approvers

Permissions

Members of the group are able to

- ☑ Permissions
  - ☐ Add Columns to Sample Table [93]
  - ☐ Add Label [139]
  - ☐ Add Rows to Sample Table [92]
  - ☐ Administer Search Library [100]
  - ☑ Approve [16]
  - ☑ Change Allowed Templates [121]
  - ☐ Configure Accessory Details [55]
  - ☐ Copy To Clipboard [80]
  - ☐ Create Report template [120]

Figure 5. Setting up group membership (top) and group permissions (bottom).



Set Group Default Workspace

Include	Group Name
☐	Approvers
☑	method developer
☐	Reviewers
☐	Users

Press OK to set default workspace for user group(s) sele

Figure 6. Supervisors' ability to setup group workspaces.

The list of Signature Points within the software is pre-defined, and includes (but is not limited to):

- Loading and saving instrument settings files
- Reporting on ready checks and instrument validation
- Generating reports
- Exporting data
- Deleting graphs
- Creating or making changes to equations and macros
- Approving and reviewing items that have been signed by other users

The user will not be prompted for a signature if 'Signature Required' is not selected for a signature point. If a signature is required, the audit trail will record the user name, date and time when the signature happened, as well as a comment and/or pre-defined reason. Signatures can only be entered by using a user name and accompanying password in the dialog box. The Administrator can decide whether the signature point requires a comment and/or a pre-defined reason. These pre-defined reasons are displayed as a drop-down list at the time of signing. Figure 8 shows examples of available signature dialog box configurations.

Protection of Records

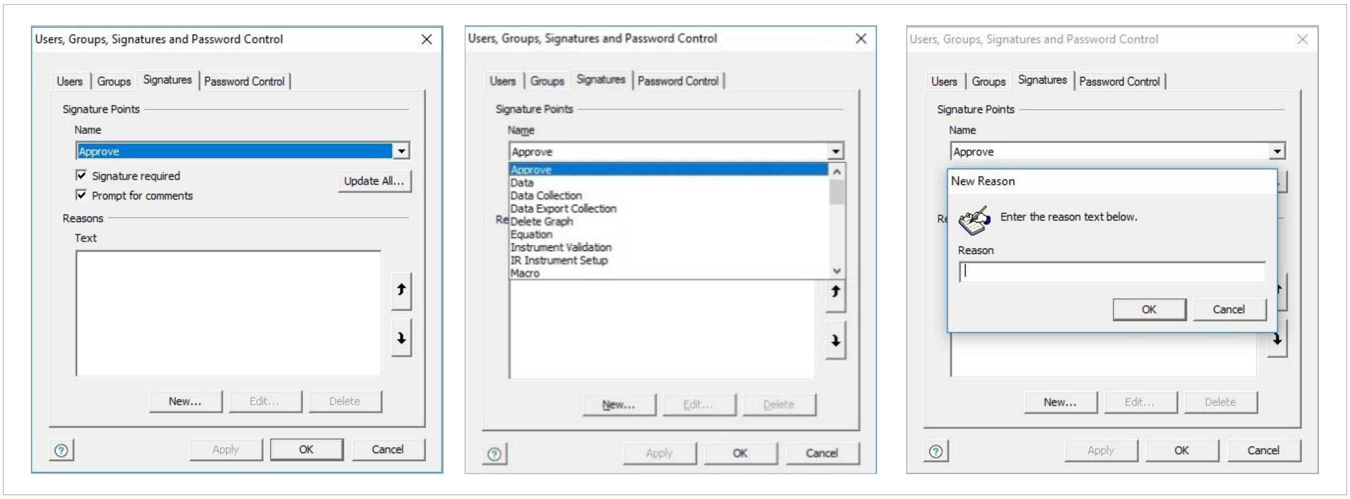
Spectrum 10 ES stores data in a secured SQL database (AssureID ES uses a secure Access database) to ensure complete file protection and data integrity. Many systems use a 'flat file' approach in which spectra are saved as single files (as occurs with Spectrum STD). Utilizing flat files requires more detailed, manual configuration of the Windows® file system to ensure security of results. Flat files are also limited with respect to the audit trail information they can keep. Spectrum 10 ES gives operators the flexibility to use either flat file or database approaches, and this helps them with transitions from a flat file method to the preferred secured database. In addition, Spectrum 10 ES has a security database which handles system security such as logins, passwords, users, groups, and electronic signature policies.

PerkinElmer secured databases are used to manage data, setups and reports. If data has not been signed for when a power failure occurs, that data can still be recovered from the software and be signed for and saved. Workspaces can also be retrieved from the database to reproduce a working environment to replicate that environment at the time the workspace was saved, which includes data and settings.

The FDA is promoting pharmaceutical companies and related industries to review and approve data electronically. This can be achieved locally on a stand-alone configuration, or even remotely with a network database, using Spectrum 10 ES and AssureID ES software. Saving data on a network simplifies data backup for IT groups.

Audit Trails

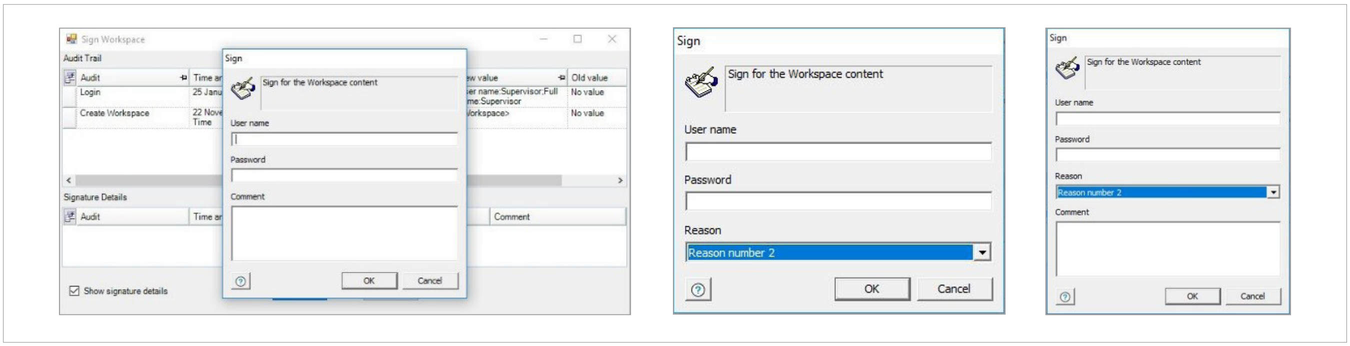
Spectrum 10 ES user and results/workspace audit trails are complete, consistent, and comprehensive, and it is possible to view, print and export these for inspection purposes.



Name: Approve
☑ Signature required
☑ Prompt for comments

Approve
Data
Data Collection
Data Export Collection
Delete Graph
Equation
Instrument Validation
IR Instrument Setup
Macro

Figure 7. Configuring settings for individual Signature Points.



Audit	Time ar	ew value	Old value
Login	25 Janu	er name:Supervisor;Full me:Supervisor	No value
Create Workspace	22 Nove Time	orkspace>	No value

☑ Show signature details

Sign for the Workspace content

Reason: Reason number 2

Figure 8. Signature dialog box configurations.

Results/Workspace Audit Trail

The workspace audit trail (Figure 9) records all settings, processes, and results created in Spectrum 10 ES, examples being obtaining spectra, peak labelling, and library searching. This audit trail also contains details of the user, the date and time stamp when the record was created, modified or deleted, the new value, the old value, and the type of modification. The audit trail file is updated when the changes will take effect. As an example, if the instrument settings are changed, the audit trail will record this information when the scan button is pressed. Therefore, if the instrument settings are changed, and then changed again before scanning, only the latest scan settings will be updated in the audit trail upon scanning. Any changes made to the settings which are subsequently cancelled, without being used, are not recorded.

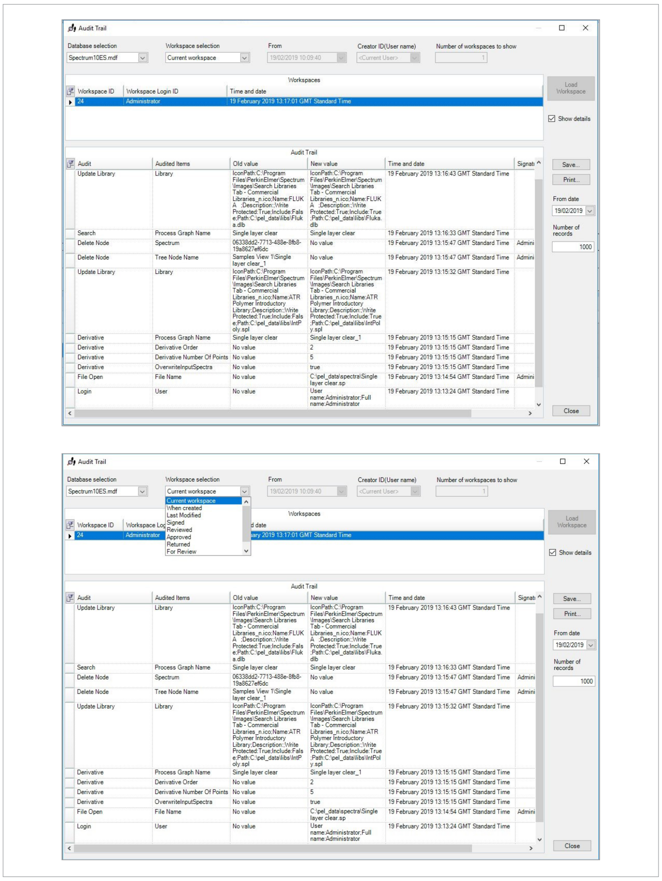
Changes to the records will not obscure previous entries and changes which affect signed data cause a new file (spectrum file, equation, macro etc.) to be created, thus retaining the original. Results or data generated in the software will not be able to be removed or overwritten.

The activities shown in this audit trail can be reviewed, using the same computer or through a network, within Spectrum 10 ES. Workspaces can be loaded, and electronic signatures added using the Return (to analyst), Review or Approve options from the Audit Trail menu, depending on the relevant permissions. The audit trail has a default size of 6 GB but can be increased to 10 GB. Workspaces can be retrieved (Figure 9) to reproduce the working environment at the time the workspace was saved – including data and settings.

Additionally, within the spectra files, a spectrum history is available (Figure 10). This records all sample details, the instrument settings used, any corrections applied during the scan (e.g. AVI), and all actions applied to the data after data collection. The sample history will include the user who performed these actions, which are typically of a processing nature.

Users Audit Trail and Login History

The users audit trail and login history can be viewed by members of the Administrators group only (Figure 11) and are saved in the security database. The users audit trail records all changes to security settings (users, groups, password settings) in compliance with 21 CFR Part 11. The login history details the user, their login and logout times, and the status of the login (e.g. a failed login). It also lists anomalies, such as forced logouts from software crashes. The summary tab contains a list of settings and permissions applied to the workspace and user.



Database selection: Spectrum10ES.mdf
Workspace selection: Current workspace
From: 19/02/2019 10:09:40
Creator ID(User name): <Current User>
Number of workspaces to show: 1

Workspaces

Workspace ID	Workspace Login ID	Time and date
24	Administrator	19 February 2019 13:17:01 GMT Standard Time

☑ Show details

Audit Trail

Audit	Audited Items	Old value	New value	Time and date	Signat
Update Library	Library	IconPath:C:\Program Files\PerkinElmer\Spectrum \Images\Search Libraries Tab - Commercial Libraries_n.ico;Name:FLUKA ;Description:;Write Protected:True;Include:False;Path:C:\pel_data\libs\Fluka.dlb	IconPath:C:\Program Files\PerkinElmer\Spectrum \Images\Search Libraries Tab - Commercial Libraries_n.ico;Name:FLUKA ;Description:;Write Protected:True;Include:True ;Path:C:\pel_data\libs\Fluka.dlb	19 February 2019 13:16:43 GMT Standard Time	
Search	Process Graph Name	Single layer clear	Single layer clear	19 February 2019 13:16:33 GMT Standard Time	
Delete Node	Spectrum	06338dd2-7713-488e-8fb8-19a8627ef6dc	No value	19 February 2019 13:15:47 GMT Standard Time	Admini
Delete Node	Tree Node Name	Samples View 1\Single layer clear_1	No value	19 February 2019 13:15:47 GMT Standard Time	Admini
Update Library	Library	IconPath:C:\Program Files\PerkinElmer\Spectrum \Images\Search Libraries Tab - Commercial Libraries_n.ico;Name:ATR Polymer Introductory Library;Description:;Write Protected:True;Include:False;Path:C:\pel_data\libs\IntPoly.spl	IconPath:C:\Program Files\PerkinElmer\Spectrum \Images\Search Libraries Tab - Commercial Libraries_n.ico;Name:ATR Polymer Introductory Library;Description:;Write Protected:True;Include:True ;Path:C:\pel_data\libs\IntPoly.spl	19 February 2019 13:15:32 GMT Standard Time	
Derivative	Process Graph Name	Single layer clear	Single layer clear_1	19 February 2019 13:15:15 GMT Standard Time	
Derivative	Derivative Order	No value	2	19 February 2019 13:15:15 GMT Standard Time	
Derivative	Derivative Number Of Points	No value	5	19 February 2019 13:15:15 GMT Standard Time	
Derivative	OverwriteInputSpectra	No value	true	19 February 2019 13:15:15 GMT Standard Time	
File Open	File Name	No value	C:\pel_data\spectra\Single layer clear.sp	19 February 2019 13:14:54 GMT Standard Time	Admini
Login	User	No value	User name:Administrator;Full name:Administrator	19 February 2019 13:13:24 GMT Standard Time	

From date: 19/02/2019
Number of records: 1000

Database selection: Spectrum10ES.mdf
Workspace selection: Current workspace
From: 19/02/2019 10:09:40
Creator ID(User name): <Current User>
Number of workspaces to show: 1

Workspaces

Workspace ID	Workspace Log	d date
24	Administrator	ary 2019 13:17:01 GMT Standard Time

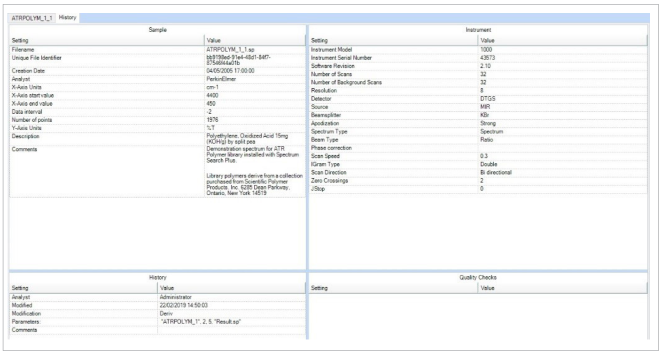
☑ Show details

Audit Trail

Audit	Audited Items	Old value	New value	Time and date	Signat
Update Library	Library	IconPath:C:\Program Files\PerkinElmer\Spectrum \Images\Search Libraries Tab - Commercial Libraries_n.ico;Name:FLUKA ;Description:;Write Protected:True;Include:False;Path:C:\pel_data\libs\Fluka.dlb	IconPath:C:\Program Files\PerkinElmer\Spectrum \Images\Search Libraries Tab - Commercial Libraries_n.ico;Name:FLUKA ;Description:;Write Protected:True;Include:True ;Path:C:\pel_data\libs\Fluka.dlb	19 February 2019 13:16:43 GMT Standard Time	
Search	Process Graph Name	Single layer clear	Single layer clear	19 February 2019 13:16:33 GMT Standard Time	
Delete Node	Spectrum	06338dd2-7713-488e-8fb8-19a8627ef6dc	No value	19 February 2019 13:15:47 GMT Standard Time	Admini
Delete Node	Tree Node Name	Samples View 1\Single layer clear_1	No value	19 February 2019 13:15:47 GMT Standard Time	Admini
Update Library	Library	IconPath:C:\Program Files\PerkinElmer\Spectrum \Images\Search Libraries Tab - Commercial Libraries_n.ico;Name:ATR Polymer Introductory Library;Description:;Write Protected:True;Include:False;Path:C:\pel_data\libs\IntPoly.spl	IconPath:C:\Program Files\PerkinElmer\Spectrum \Images\Search Libraries Tab - Commercial Libraries_n.ico;Name:ATR Polymer Introductory Library;Description:;Write Protected:True;Include:True ;Path:C:\pel_data\libs\IntPoly.spl	19 February 2019 13:15:32 GMT Standard Time	
Derivative	Process Graph Name	Single layer clear	Single layer clear_1	19 February 2019 13:15:15 GMT Standard Time	
Derivative	Derivative Order	No value	2	19 February 2019 13:15:15 GMT Standard Time	
Derivative	Derivative Number Of Points	No value	5	19 February 2019 13:15:15 GMT Standard Time	
Derivative	OverwriteInputSpectra	No value	true	19 February 2019 13:15:15 GMT Standard Time	
File Open	File Name	No value	C:\pel_data\spectra\Single layer clear.sp	19 February 2019 13:14:54 GMT Standard Time	Admini
Login	User	No value	User name:Administrator;Full name:Administrator	19 February 2019 13:13:24 GMT Standard Time	

From date: 19/02/2019
Number of records: 1000

Figure 9. Results/workspace audit trail.



Sample

Setting	Value
Filename	ATRPOLYM_1_1.sp
Unique File Identifier	bb9198ed-91e4-48d1-84f7-87546f44a01b
Creation Date	04/05/2005 17:00:00
Analyst	PerkinElmer
X-Axis Units	cm-1
X-Axis start value	4400
X-Axis end value	450
Data interval	-2
Number of points	1976
Y-Axis Units	%T
Description	Polyethylene, Oxidized Acid 15mg (KOH/g) by split pea
Comments	Demonstration spectrum for ATR Polymer library installed with Spectrum Search Plus. Library polymers derive from a collection purchased from Scientific Polymer Products. Inc. 6285 Dean Parkway, Ontario, New York 14519

Instrument

Setting	Value
Instrument Model	1000
Instrument Serial Number	43573
Software Revision	2.10
Number of Scans	32
Number of Background Scans	32
Resolution	8
Detector	DTGS
Source	MIR
Beamsplitter	KBr
Apodization	Strong
Spectrum Type	Spectrum
Beam Type	Ratio
Phase correction	
Scan Speed	0.3
IGram Type	Double
Scan Direction	Bi directional
Zero Crossings	2
JStop	0

History

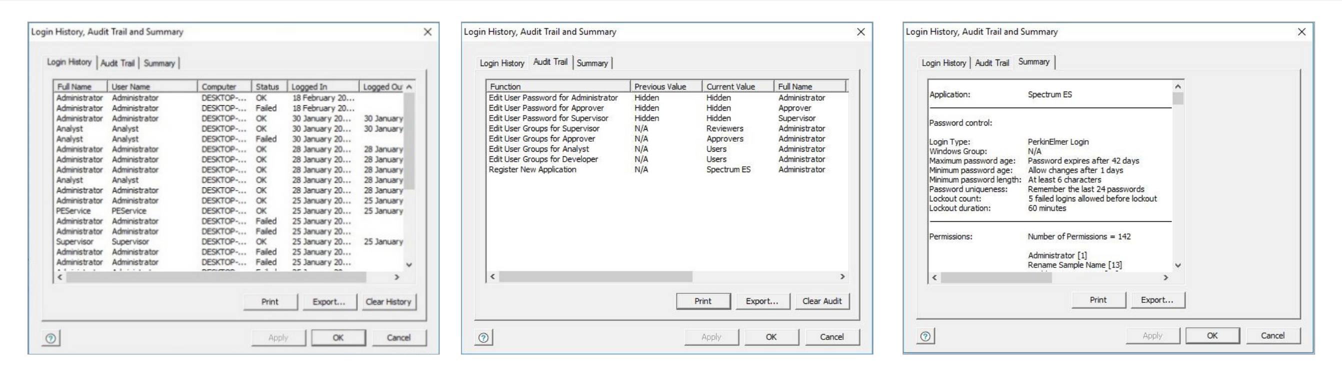
Setting	Value
Analyst	Administrator
Modified	22/02/2019 14:50:03
Modification	Deriv
Parameters:	"ATRPOLYM_1", 2, 5, "Result.sp"
Comments	

Quality Checks

Setting	Value

Figure 10. Spectrum history.

Spectrum 10 ES allows Administrators to view, print, and export the login history and user audit trail for inspection purposes. It is only possible to clear login history and audit trail entries from the dialog that have previously been exported. If the audit trail contains additional entries since it was last exported, only those entries that have been archived will be removed if requested. If none of the entries have been archived, a warning message will be displayed upon attempt to clear the audit trail or login history (Figure 12). The dialog always records when records in the login history or audit trail have been exported and cleared.

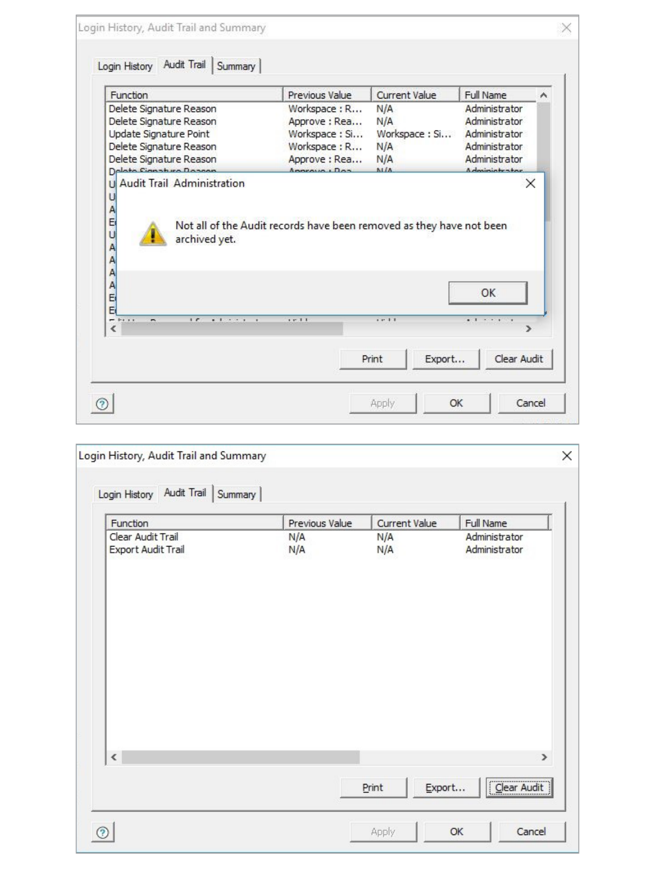


Full Name	User Name	Computer	Status	Logged In	Logged Ou
Administrator	Administrator	DESKTOP-...	OK	18 February 20...	
Administrator	Administrator	DESKTOP-...	Failed	18 February 20...	
Administrator	Administrator	DESKTOP-...	OK	30 January 20...	30 January
Analyst	Analyst	DESKTOP-...	OK	30 January 20...	30 January
Analyst	Analyst	DESKTOP-...	Failed	30 January 20...	
Administrator	Administrator	DESKTOP-...	OK	28 January 20...	28 January
Administrator	Administrator	DESKTOP-...	OK	28 January 20...	28 January
Administrator	Administrator	DESKTOP-...	OK	28 January 20...	28 January
Analyst	Analyst	DESKTOP-...	OK	28 January 20...	28 January
Administrator	Administrator	DESKTOP-...	OK	28 January 20...	28 January
Administrator	Administrator	DESKTOP-...	OK	25 January 20...	25 January
PEService	PEService	DESKTOP-...	OK	25 January 20...	25 January
Administrator	Administrator	DESKTOP-...	Failed	25 January 20...	
Administrator	Administrator	DESKTOP-...	Failed	25 January 20...	
Supervisor	Supervisor	DESKTOP-...	OK	25 January 20...	25 January
Administrator	Administrator	DESKTOP-...	Failed	25 January 20...	
Administrator	Administrator	DESKTOP-...	Failed	25 January 20...	

Function	Previous Value	Current Value	Full Name
Edit User Password for Administrator	Hidden	Hidden	Administrator
Edit User Password for Approver	Hidden	Hidden	Approver
Edit User Password for Supervisor	Hidden	Hidden	Supervisor
Edit User Groups for Supervisor	N/A	Reviewers	Administrator
Edit User Groups for Approver	N/A	Approvers	Administrator
Edit User Groups for Analyst	N/A	Users	Administrator
Edit User Groups for Developer	N/A	Users	Administrator
Register New Application	N/A	Spectrum ES	Administrator

Application:	Spectrum ES
Password control:	
Login Type:	PerkinElmer Login
Windows Group:	N/A
Maximum password age:	Password expires after 42 days
Minimum password age:	Allow changes after 1 days
Minimum password length:	At least 6 characters
Password uniqueness:	Remember the last 24 passwords
Lockout count:	5 failed logins allowed before lockout
Lockout duration:	60 minutes
Permissions:	Number of Permissions = 142
	Administrator [1] Rename Sample Name [13]

Figure 11. Login history and user audit trail.



Function	Previous Value	Current Value	Full Name
Delete Signature Reason	Workspace : R...	N/A	Administrator
Delete Signature Reason	Approve : Rea...	N/A	Administrator
Update Signature Point	Workspace : Si...	Workspace : Si...	Administrator
Delete Signature Reason	Workspace : R...	N/A	Administrator
Delete Signature Reason	Approve : Rea...	N/A	Administrator

Not all of the Audit records have been removed as they have not been archived yet.

Function	Previous Value	Current Value	Full Name
Clear Audit Trail	N/A	N/A	Administrator
Export Audit Trail	N/A	N/A	Administrator

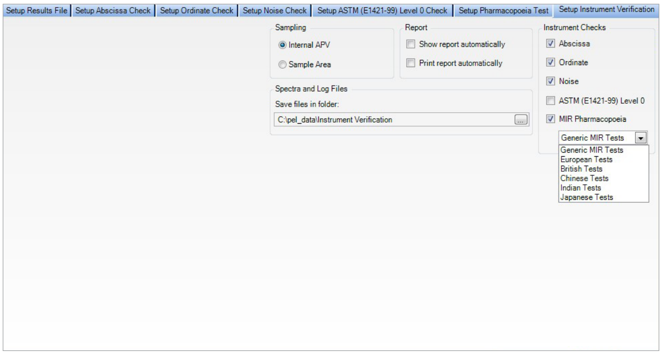
Figure 12. Warning obtained when attempting to clear user audit trail without first exporting (top) and after exporting and clearing the audit trail (bottom).

Spectrum 10 ES Report Designer

An additional feature to satisfy data integrity requirements is Spectrum 10 ES Report Designer. This allows a substantial amount of flexibility in generating reports and saves each report as a secured PDF. These files are encrypted in a unique PerkinElmer format so that any modification will invalidate them, preventing them from loading. Reports can only be generated in Spectrum 10 ES if the appropriate permission has been applied. Similarly, Report Designer can only be opened to create or edit a template if the appropriate permissions have been applied.

Instrument Performance Testing

As with the standard software version, Spectrum 10 ES contains a built-in instrument performance validation solution which can be easily implemented by users to ensure compliance with various Pharmacopeia (Figure 13).



Sampling
● Internal APV
○ Sample Area

Report
□ Show report automatically
□ Print report automatically

Spectra and Log Files
Save files in folder: C:\pel_data\Instrument Verification

Instrument Checks
☑ Abscissa
☑ Ordinate
☑ Noise
□ ASTM (E1421-99) Level 0
☑ MIR Pharmacopoeia

Figure 13. Instrument Verification setup tab in Spectrum 10.

Spectrum 10 ES also performs checks to ensure data collected is valid. As an example, when an accessory is changed, or a higher spectral resolution is selected, Spectrum 10 ES will enforce a new background collection.

In addition, the PerkinElmer OneSource® UOQ program offers laboratories ongoing compliance with continuously evolving regulatory conditions.

The UOQ program includes:

- A protocol which is customizable by the user, including options to test according to pharmacopoeial requirements. When finalized, the protocol is approved and then locked so that changes are not permitted during the testing time.
- Instrument testing by a service engineer according to user defined specifications. Multiple instruments may be tested simultaneously to reduce downtime.
- The UOQ report provides an ultra-secure document including pass/fail results and built-in calculations. This report is 21 CFR Part 11 compliant.
- Digital Archiving of data making it easy to provide information required for audits.

The UOQ program supports FT-IR, UV/Vis, HPLC, UPLC, and GC systems, regardless of equipment manufacturer to allow efficiencies in testing, reporting and review of annual operational qualifications.

Conclusion

PerkinElmer's Spectrum 10 Enhanced Security software platform for Infrared spectroscopy provides additional security and data integrity features for achieving compliance with 21 CFR Part 11. In addition to enhanced access control features, ES software automatically stores data, experimental parameters and audit trail information in secure databases. Data operating parameters and events can quickly and easily be recovered for inspection purposes using the "Audit Trail" feature in the ES software. Electronic signature points can be added for certain actions, defined by the system administrator, and included in the audit trail. The comprehensive instrument validation module also allows straightforward approaches to assess instrument performance.

References

1. Data Integrity and Compliance with Drug CGMP: Questions and Answers; Guidance for Industry, Food and Drug Administration, 2018.
2. The 5P Model for Data Integrity, Institute of Validation Technology, 2018. Available from: http://www.ivtnetwork.com/article/5p-model-data-integrity.

PerkinElmer, Inc.
940 Winter Street
Waltham, MA 02451 USA
P: (800) 762-4000 or
(+1) 203-925-4602
www.perkinelmer.com

For a complete listing of our global offices, visit www.perkinelmer.com/ContactUs