Waters™

Empower Software Audit Trails and Logs: Empower Functionality to Aid in Vigilant Monitoring as Part of Mature Data Governance

Tim Bara, Tracy Hibbs, Neil Lander, Arjan Timmerman, Fiona O'Leary, Lissa Wang, and Lauren Wood
Waters Corporation, Milford, MA, USA

INTRODUCTION

Audit trails play an important role in the security of a system since they track changes to data and metadata. In this way, an incomplete or absent audit trail can impact data integrity and product quality.

The absence of an audit trail is considered to be "highly significant when there are data discrepancies" according to the FDA[1].

The use of computer-generated, time-stamped audit trails are a significant part of the *Controls for Closed Systems*. *(§11.10(e)) for 21 CFR Part 11*[1] as well as regulations and guidance from across the globe covering CGxP data. When included as an integral part of the data review and periodic review cycle, audit trails enable detection of non-routine or unexpected activity by users and provide a management tool to maintain the integrity of any human interaction with the data in the system. Regulators expect to see that this technical control is being utilized to ensure data integrity in regulated companies. Inspectors from regulatory agencies, including FDA, use audit trails to check if the data presented during routine audits is honest and trustworthy.

The PIC/S Guidance on Data Integrity[2] highlights that data governance maturity involves understanding and accepting residual risks, prioritizing actions, and extending self-inspection to include computerized system logs and audit trails. Ongoing data review and proactive monitoring are advised to maintain control and protect systems and data from risks.

In addition to audit trails, various error and event logs provide valuable information and metrics about activities in your chromatographic environment. According to the April 2016 *OECD Guidance Number 17 for Applications of GLP Principles to Computerized Systems*[3]

"An audit trail provides documentary evidence of activities that have affected the content or meaning of a record at a specific time point." And "Depending on the system, log files may be considered (or may be considered in addition, to an audit trailing system) to meet this requirement."

Here is the perspective from *WHO TRS 996 Annex 05*[4]

"Computer-generated audit trails may include discrete event logs, history files, database queries or reports or other mechanisms that display events related to the computerized system, specific electronic records or specific data contained within the record." As well as "When issues with data validity and reliability are discovered, it is important that their potential impact on patient safety and product quality and on the reliability of information used for decision-making and applications is examined as a top priority."

PIC/S[5] also emphasizes the importance of reviewing logs and alarms as part of maintaining data integrity and ensuring compliance with Good Manufacturing Practice (GMP). Key points are:

- **Regular Review**: Logs and alarms should be reviewed regularly to ensure that any deviations or issues are identified and addressed promptly.
- **Documentation**: All reviews should be documented, including the actions taken in response to any alarms or unusual log entries.
- **Risk-Based Approach**: The frequency and extent of reviews should be based on a risk assessment, focusing on critical systems and processes.

In addition to reviewing logs when an obvious failure occurs, these statements imply the need to review logs as part of routine and periodic data review as a way of determining if there may be a reliability issue.

Such practices help ensure that any potential issues are detected early and managed effectively, supporting the overall goal of maintaining product quality and patient safety.

Accordingly, appropriate data review including the review of audit trails and other logs informed by your risk analysis and mitigation, together with ongoing, proactive monitoring are advised to ensure your processes are in a continued state of control and are protecting your systems and data from unnecessary risk.

The FDA underscores the need for proactive, vigilant monitoring in maintaining control over manufacturing processes, as detailed in their warning letters. This paper focuses on the audit trails, logs, Message Center messages, and capabilities within Waters™ Empower™ Software that can be leveraged to assist in such monitoring as it relates to data review and periodic review.

WHAT IS AN AUDIT TRAIL?

Configuration Manager > System Audit Trail

Project Window > Audit Trails tab

21 CFR Part 11 and other electronic record regulations require electronic audit trails for all data created, reviewed, modified, deleted, and archived. From Part 11, audit trails must be:

- Operator independent – no operator or administrator may change or modify in any way.
- Computer generated (automatically).
- Date and time stamped when the individual created, modified, reviewed, approved or deleted an electronic record in an unambiguous format.
- Secure – adequate security to prevent tampering.

Additionally, any change actions need to be documented automatically in the audit trail and the recorded changes must not obscure previously recorded information (*i.e.*, record the "before" and "after" values).

Finally, the users are required to also record a scientific justification of "why" the changes are being made. This is normally documented in a comment or reason field.

- Empower Software can discern invalid or altered records using entries in the project audit trail. Changes to methods and results automatically create new and discrete versions of those records. This not only preserves the original but allows for comparison by highlighting differences.

AUDIT TRAIL CONFIGURATION

Configuration Manager > View > System Policies > New Project tab / System Audit Trail tab

Configuration Manager > New > Project > New Project Wizard

While most laboratory applications include audit trail capabilities, they must be properly enabled and configured. Audit trails should be enabled prior to any regulated data being collected in an application. While this could be set by default, it might be configured by the vendor upon installation, or it may be configured by the administrators at the regulated company.

Software applications may allow both regulated and non-regulated users to work in the same application but with different audit trail settings for their specific projects. In this kind of configuration, care should be taken to ensure that these working practices are segregated and managed such that regulatory data cannot be created, modified, or deleted in non-regulated/non-audit trailed areas.

OECD Guidance Number 17[3] clearly states that "The ability to make modifications to the audit trail settings should be restricted to authorized personnel." Additionally, audit trail configuration changes should themselves be fully audit trailed.

Empower Project Audit Trail settings can never be modified once a project is created although the configuration does allow some flexibility in the settings available for new Projects. Because companies may be using software applications in a unique way, either alone or in conjunction with other computerized or paper-based systems, it is important for settings to be adjusted to reflect the intended use and acceptable risk of the laboratories.

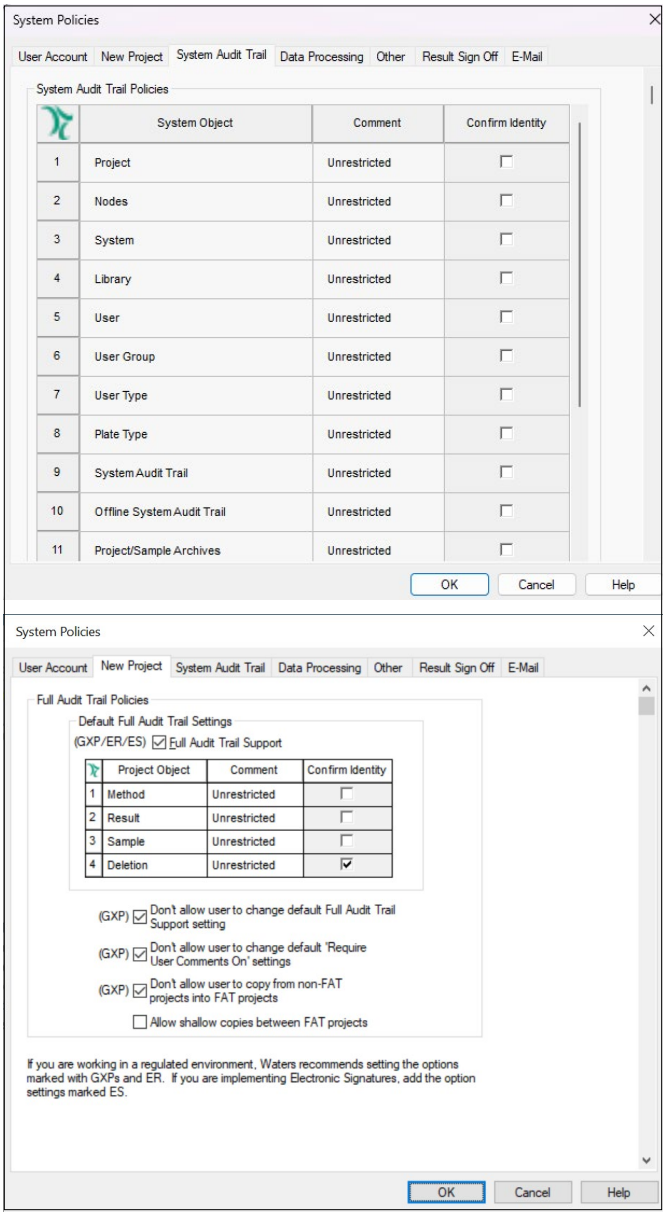


Figure 1. System Policies: The New Project and System Audit Trail Policies for Empower Software can be set by privileged users according to the intended use and acceptable risk of the laboratory.

AUDIT TRAIL TIME STAMPS

Configuration Manager > Nodes > Properties > General tab

Time stamps for record creation as well as audit trails need to be standardized and consistent. It is critical that time sources are synchronized and protected from alteration by users, managers and even administrators. It is common that time stamps are taken from the time of the operating system and, particularly in standalone systems (single computer PC's), this level of protection may be difficult to control. However, in network deployments, it is much easier to synchronize and control access to time sources.

For standalone or site-wide solutions, local time may be preferred. When wider, cross time zone installations are deployed, consideration of UTC or a fixed time zone may be needed, if managing users and instruments in multiple time zones is unobtainable.

- Empower Enterprise solutions allow specific time zones to be specified for clients, acquisition nodes, Citrix clients and servers.

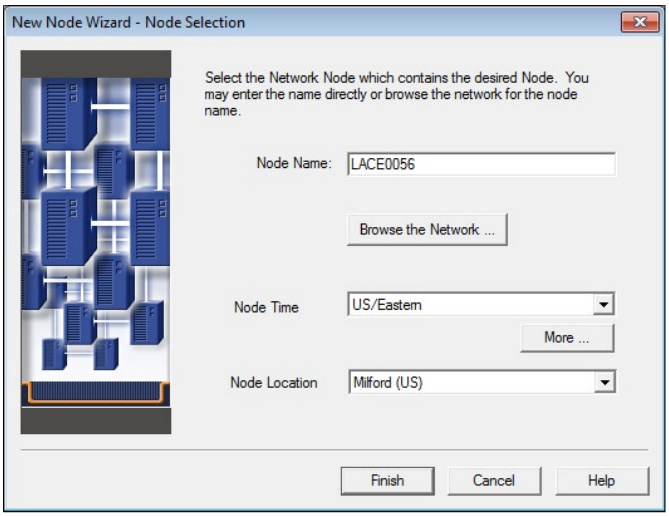


Figure 2. During Node creation in Empower Software, the Node Time Zone and Node Location can be defined.

Understanding how any specific application leverages time stamps (and additional controls put in place in the IT infrastructure) provides confidence in the correct sequencing of actions noted in the audit trails, referred to as "operational system checks to enforce permitted sequencing of steps and events" as stated in *§11.10(f) for 21 CFR Part 11.1.*[1]

Sample Sets | Injections | Channels | Methods | Result Sets | Results | Peaks | Fractions | Sign Offs | Curves | View Filters | Custom Fields | **Audit Trails**

	Action	Details	Change Date
1	Updated Calibration	System: Emp_24_Validation_MJ Method: Jan Imp PM Channel: ACQUITY TUV ChA Calibration ID: 4364	1/6/2017 11:32:42 AM EST
2	Created Calibration	System: Emp_24_Validation_MJ Method: Jan Imp PM Channel: ACQUITY TUV ChA Calibration ID: 4364	1/6/2017 11:32:41 AM EST
3	Created Result Set	Result Set: QPM00012 Sample Set Method: QPM00012 Method: Jan Imp PM Processed How: Process	1/6/2017 11:32:40 AM EST
4	Modified Method	Method: QPM00012 Type: Sample Set Version: 21	1/6/2017 11:32:20 AM EST
5	Altered Sample Set	Sample Set: QPM00012 Sample Set Method: QPM00012 Sample Set ID: 1247 SampleSet Method ID: 4	1/6/2017 11:32:20 AM EST
6	Updated Calibration	System: Emp_24_Validation_MJ Method: Jan Imp PM Channel: ACQUITY TUV ChA Calibration ID: 4296	1/5/2017 3:05:05 PM EST
7	Created Result Set	Result Set: POSS Jan 5 Sample Set Method: POSS Jan 5 Method: Jan Imp PM Processed How: Proce	1/5/2017 3:05:04 PM EST
8	Created Calibration	System: Emp_24_Validation_MJ Method: Jan Imp PM Channel: ACQUITY TUV ChA Calibration ID: 4296	1/5/2017 3:05:04 PM EST
9	Created Calibration	System: Emp_24_Validation_MJ Method: Jan Imp PM Channel: ACQUITY TUV ChA Calibration ID: 4271	1/5/2017 3:05:04 PM EST
10	Created Method	Method: POSS Jan 5 Type: Sample Set Version: 1	1/5/2017 3:04:44 PM EST

Figure 3. An Empower Project Audit Trail showing the time zone included in the time stamp.

AUDIT TRAIL REASONS FOR CHANGE

Configuration Manager > View > System Policies > New Project tab / System Audit Trail tab

Configuration Manager > View > Default Strings

One critical aspect of audit trails is the documentation of the reason "why" an action was performed. This detail cannot be automatically populated by the software application as it requires the input of the user performing the action. User entered reasons allow the user to truly express why an action was performed, while pre-defined reasons are useful for noting common reasons.

- **Empower Software** offers users Silent, pre-defined (Restricted), or user entered (Unrestricted) use of Comments (*i.e.*, reasons; the 'why') to document the reason why an action has been performed.
- **View Filter** functionality allows reviewers to search the audit trail for specific data, specific actions, or specific reasons for actions.
- **Default Strings** functionality allows Comments to be pre-defined in various categories of the software so the analyst can quickly choose the reason for their current action(s). The use of Default Strings provides potential for huge efficiencies for repetitive tasks.
  - Users choose from a list rather than typing the reason.
  - Data mining is faster and more efficient because variation amongst the reasons is eliminated.
  - Defining Comments as Unrestricted allows the use of both pre-defined reasons and user entered text reasons.

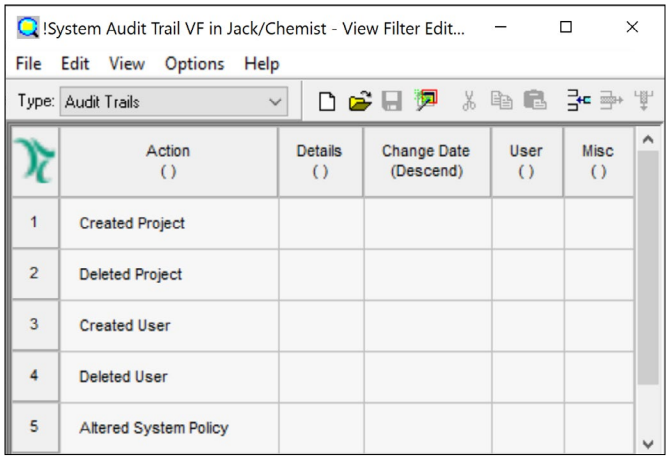


Figure 4. View Filters on Audit Trails can be created to search for specific data including specific users, specific actions, or specific reasons for actions.

ENSURING THE AVAILABILITY OF AUDIT TRAILS

The audit trail documentation must be retained for the same period as the electronic record. Accurate and complete copies must be available in the case of an audit (whether internal or external) for review.

- All records, histories, and audit trails are automatically backed up during security back up routines of Empower Software.
- Empower Project Audit Trails and project level logs are always archived and restored when the Project is archived or restored, ensuring that any metadata relating to a specific analytical result is not lost during the record lifecycle.
- System Audit Trails may be archived to a secure format, readable only in the Empower application, or exported in a converted, non-secure format.
- Archiving the System Audit Trail, like other archiving activities, may be a manual process. With the use of NuGenesis Lab Management System (LMS), this task may be automated.

EMPOWER SYSTEM AUDIT TRAIL

Configuration Manager > System Audit Trail

Configuration Manager > Offline System Audit Trail

'System' in this context refers to the overall Empower Software application and should not be confused with an analytical instrument system.

The Empower System Audit Trail provides a history of actions that affect the overall system configuration and system level objects (unsuccessful login, project backup, changes to system policies *etc.*). Actions that are recorded in the System Audit Trail are documented in the Help topic *Actions recorded in System Audit Trails*.

- Changes to user privileges are tracked.
- All system-level actions in Empower Software, even those performed by administrators, are recorded.
- The Empower System Audit Trail is always active and cannot be deactivated.
- Audit trails are generated automatically and cannot be modified.

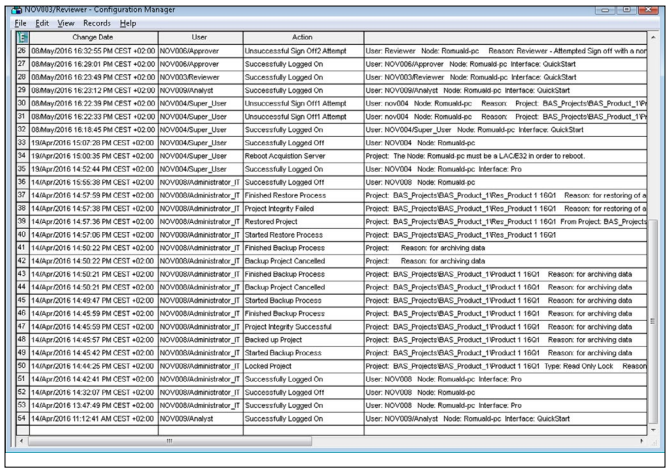


Figure 5. The Empower System Audit Trail which can be filtered and sorted to find and print relevant records.

The Empower Offline System Audit Trail is an area within Configuration Manager where a copy of an archived System Audit Trail can be restored to if a review of them is required. Restoration of a System Audit trail is an action which is recorded in the System Audit Trail.

No new actions are added to the Offline System Audit Trail – and they can be cleared from Configuration Manager once reviews are completed.

EMPOWER PROJECT AUDIT TRAIL

Project Window > Audit Trails tab (available for Projects configured with Full Audit Trail (FAT))

- The Empower Project Audit Trail records actions that users have performed on objects within a Full Audit Trail Project (Altered Sample Set, Created Result, Modified Method, Run Sample Set, *etc.*) and includes reference to the data, metadata, and methods relating to the action. Actions that are recorded in the Project Audit Trail are documented in the Help topic Actions recorded in Project Audit Trails.
- The Project Audit Trail captures the 'who, what, when, and why' of user activity within a Project.
- The Empower Project Audit Trail is active within Full Audit Trail projects and cannot be modified or purged.
- Project Audit Trails can be configured to require comments when a user makes changes to objects within a project.
- User re-authentication can be required on changes to Project objects.

Figure 6. The Empower Project Audit Trail records Project activity performed by users.

ACQUISITION LOG

Project Window > Preview/Publisher > Report Groups > Acquisition Logs

The integrity of data acquisition is important. Although the Instrument Method represents a record of the instrument parameters, you may seek assurance that an analyst has not made changes to these parameters during acquisition or influenced the acquisition in other ways.

Empower Software, Waters, and many third-party instruments have technical controls to prevent altering data.

- When properly configured, the location(s) where raw data is stored is unavailable to Empower Software users.
- Many control panels on chromatographic instruments are locked while they are under Empower Software control, preventing a user from making unrecorded changes to instrument parameters.
- Empower Software permanently stores the exact Instrument Method that was used to collect the data with any chromatogram, even when it is subsequently modified.
- The Acquisition Log displays a record of instrument errors and details of data acquisition.
- If a chromatographic system allows interactive changes during acquisition (through either an unlocked front panel, separate controller, or console software) and users have the permission to perform interactive changes during a run, those changes are recorded in the Acquisition Log which is permanently linked to the raw data.

Most chromatographic hardware does not allow such interactive changes, even for privileged users.

- The Acquisition Log is available to view using an Empower Report.
- In Empower 3 Feature Release 2 and higher versions, Acquisition Logs are also displayed with other audit trails in the Result History tab of the Result Audit Viewer.

POST RUN REPORT

Project Window > Preview/Publisher > Report Groups > Post Run Reports

- For some specific Empower Software-controlled instruments a Post Run Report is available to verify the actual acquisition settings, statuses and experimental conditions during acquisition, *e.g.*, MS data acquisition and Waters ACQUITY™ UPLC™ Systems.
- The Post Run Report is available to view using an Empower Report.

METHOD HISTORY

Project Window > Methods tab > Right Click > Method Properties... > Method History > Revision History

- Empower Software methods are never overwritten and are automatically versioned.
- Methods are assigned unique IDs (within the Project) at the time of creation, with all versions available for review, and permanently linked to results generated and associated with a specific method version.
- Methods can be locked, assuring that modifications can no longer be made.
- While an indication of changes to any Empower Software method exists in the Project Audit Trail, more details of the change are stored in Method History, including the reason for change.
- Previous versions of methods can be "made current" allowing users, if permissioned, to restore an earlier version into use.

METHOD DIFFERENCES

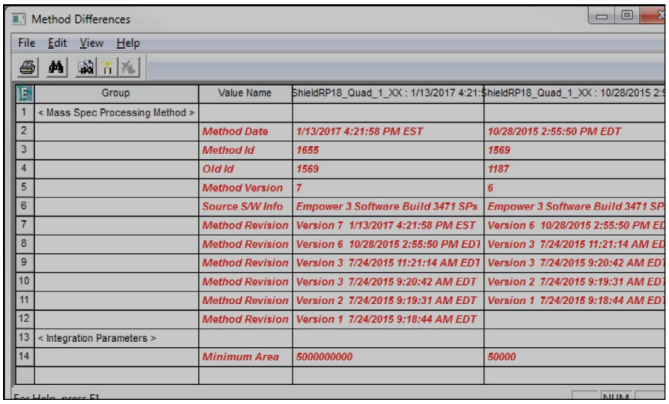
Project Window > Methods tab > Right Click > Method Properties > Method History > Differences

Project Window > Methods tab > Select two methods > Right Click > Method Differences

While audit trails provide a history of modifications made to a method, at times it may be necessary to compare two different methods or two versions of the same method to view the details of the change, including the 'before and after' values.

This can be useful to determine if all changes adhere to any standard operating procedure (SOP)-mandated allowable changes or to retrace the steps an analyst performed when working with chromatographic data.

- The Empower Method Differences feature may be used to compare two methods with different names or two versions (either historical or current) of the same method.
- Method Differences can be used for Instrument Methods, Sample Set Methods, Sample Set Method templates, Method Sets, Processing Methods, Report Methods and Export Methods.
- The Method Differences table may be searched to look for key parameter alterations.
- Documenting and reviewing method IDs, limiting permissions allowing method modification or providing the ability to and procedurally locking methods may negate the need to examine method histories in detail, given method changes would be easily observed, restricted or prohibited.



	Group	Value Name	ShieldRP18_Quad_1_XX : 1/13/2017 4:21:	ShieldRP18_Quad_1_XX : 10/28/2015 2:
1	< Mass Spec Processing Method >			
2		Method Date	1/13/2017 4:21:58 PM EST	10/28/2015 2:55:50 PM EDT
3		Method Id	1655	1569
4		Old Id	1569	1187
5		Method Version	7	6
6		Source S/W Info	Empower 3 Software Build 3471 SPs	Empower 3 Software Build 3471 SP
7		Method Revision	Version 7 1/13/2017 4:21:58 PM EST	Version 6 10/28/2015 2:55:50 PM ED
8		Method Revision	Version 6 10/28/2015 2:55:50 PM ED	Version 3 7/24/2015 11:21:14 AM ED
9		Method Revision	Version 3 7/24/2015 11:21:14 AM EDT	Version 3 7/24/2015 9:20:42 AM ED
10		Method Revision	Version 3 7/24/2015 9:20:42 AM EDT	Version 2 7/24/2015 9:19:31 AM ED
11		Method Revision	Version 2 7/24/2015 9:19:31 AM EDT	Version 1 7/24/2015 9:18:44 AM ED
12		Method Revision	Version 1 7/24/2015 9:18:44 AM EDT	
13	< Integration Parameters >			
14		Minimum Area	5000000000	50000

Figure 7. The Method Differences functionality highlights the differences between methods and method versions.

SAMPLE AND SAMPLE SET METHOD HISTORY

Project Window > Sample Set / Injections / Channels > Tools > Alter Sample > Edit > View Sample History

Project Window > Sample Set / Injections / Channels > Tools > Alter Sample > Edit > View Sample Set Method History

Changes to sample metadata are often required. Metadata may be as simple as a sample name or other descriptive text field but may also be a critical value that is required to calculate the final results. Modification of metadata may be needed, either pre- or post- acquisition to complete missing metadata or to correct incorrectly entered metadata.

Metadata changes will often be simple corrections or may indicate an attempt to influence the final results. Changes to sample metadata are therefore audit trailed, with the 'before' and 'after' values recorded automatically so that previous values are not obscured and are associated with an acceptable justification.

Records where the metadata has been altered are flagged, indicating that a deeper review is needed as part of a risk-based quality management system.

- Changes to sample metadata are tracked – who, what, when, and why.
- Raw data and records, where the sample metadata has been altered, are permanently flagged.
- Existing Results, generated with the original data, remain unchanged. Data must be reprocessed to incorporate new values; this creates new and distinct Results.
- Sample metadata changes are audit trailed in Empower Software through the Project Audit Trail and Sample and Sample Set Method Histories.
- Sample and Sample Set Method Histories are available in the Alter Sample tool and the Result Audit Viewer (Empower 3 Feature Release 2 and higher versions) and display both the original and new values.
- Sample and Sample Set Method History may be included in Reports. However, the level of detail provided may fill dozens of pages for a single run. Review is more typically performed on the original electronic record within the Empower application, under a risk-based approach based on the Altered flag and other indicators.

MESSAGE CENTER

The Message Center is a troubleshooting log that allows Empower Software and programs that interact with the Empower Software application such as Oracle, Windows, and instrument drivers to communicate informational messages, warning messages, and error messages to users and administrators for informational, troubleshooting, and monitoring purposes. The Message Center helps users monitor and troubleshoot the system by providing details about various events, such as instrument and processing errors. The Message Center can be leveraged to resolve technical issues which may or may not have an impact on your chromatographic data.

The Message Center typically displays only the messages relating to the currently logged in user. However, with appropriate privileges, messages relating to all users in the system are displayed. In Empower 3 Feature Release 4 Service Release 3 and higher versions, the Message Center allows long term storage of all messages and is searchable with Empower View Filters.

The Message Center is not intended as a replacement for, or a component of the audit trail. Any critical messages related to user creation, modification, or deletion of data are always permanently saved into the associated audit trail along with the user's justification when appropriate. Message Center messages commonly describe an action or activity which could not be completed as expected. These messages can be instrumental in the determination of root cause analysis of OOT/OOS and other issues.

Performing a trend analysis of messages occurring in the Message Center relative to users, methods, systems and other parameters may indicate:

- Deficiencies in a method's reliability or lack of fit for intended use
- A need for maintenance, repair, or calibration of specific instrumentation
- Troubleshooting and resolution to issues that arise with a frequency higher than expected is necessary
- Improper configuration of environment
- Gaps in user comprehension and adherence to processes and procedures, and the need for additional training for specific individuals

Based on regulations and CGMPs, Message Center messages that occur in your environment should be risk assessed and rated in a matrix for frequency, detectability, and severity. This information should subsequently be used to mitigate any data integrity issues or issues that may impact patient safety. A process for appropriate message monitoring should be implemented. It is recommended to incorporate a review of these messages in your procedures for data review as part of your risk mitigation strategy.

Note: The Waters Knowledge Base contains troubleshooting information on many Message Center messages.

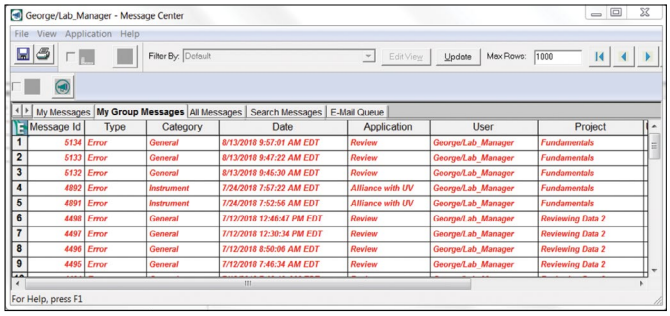


Figure 8. The Empower Message Center displays error messages from instruments, third party applications, Oracle, and Empower Software for troubleshooting purposes.

OTHER NON-AUDIT TRAIL LOGS

Within the overall Empower Software application, instrument control consoles may also include their own cache of error logs. For instance, the ACQUITY UPLC PDA Detector has its own log tab in its console.

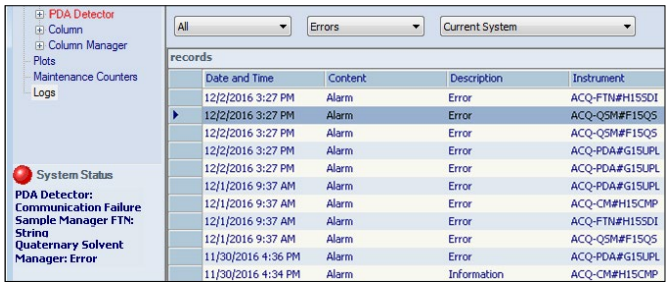


Figure 9. Additional Logs may exist in specific instrument console pages.

The Message Center and other available logs and messages are intended to aid in user level monitoring and/or troubleshooting in the laboratory, either independently or with the assistance of Waters or third-party technical support.

REVIEWING AUDIT TRAILS, MESSAGE CENTER MESSAGES AND LOGS AS PART OF ROUTINE AND PERIODIC DATA REVIEW

It is the expectation of both European[6] (GMP Annex 11) and US regulations[7] that audit trails and other appropriate records are regularly reviewed. Even though there is no formal mention of this in 21 CFR Part 11, companies that fail to have a formal process to review audit trails and error logs have had this omission cited in official observations or warning letters. Review of the original and complete electronic record is expected.[8]

Most regulated companies include audit trails and logs relating directly to data and results as an integral part of the metadata needing to be reviewed based on a risk-based approach before batch or study release. A risk-based approach is appropriate for organizations with mature Quality Management Systems.

The *WHO TRS 996 Annex 05*[4] states:

"A risk-based approach to reviewing data requires process understanding and knowledge of the key quality risks in the given process that may impact patients, products, compliance and the overall accuracy, consistency and reliability of GXP decision-making. When original records are electronic, a risk-based approach to reviewing original electronic data also requires an understanding of the computerized system, the data and metadata, and the data flows."[4]

And

"The risk-based review of electronic data and metadata, such as audit trails, requires an understanding of the system and the scientific process governing the data life cycle so that the meaningful metadata are subject to review, regardless of the naming conventions used by the software developer."[4]

Regardless of your approach, Empower Software contains functionality that can assist.

EMPOWER TOOLS FOR EFFICIENT DATA REVIEW

The Empower Relational Database

Because Empower Software uses an Oracle relational database as its central data repository, all chromatographic data is permanently linked to its associated metadata (sample identifiers, methods, results, *etc.*) thus aiding in ALCOA++ principles, CGxP and regulatory compliance, and data review.

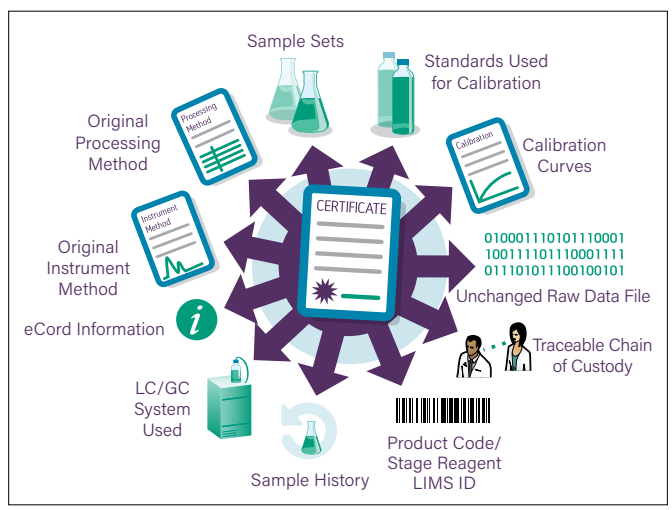


Figure 10. The Oracle database underlying Empower Software creates permanent linking relations between methods, dynamic electronic data, and metadata which cannot be broken, permitting easy query and review of related data.

Within the Empower Database, objects are date/time stamped and assigned unique IDs. When a method is modified, a new version is created rather than overwriting the original method. This provides assurance that your data is traceable, original and contemporaneous, and ensures that previous content remains available for review and for compliance purposes. When data is viewed in Empower Software, it can be mined and efficiently displayed to locate and view related metadata in a meaningful way. This functionality is crucial for CGxP and 21 CFR Part 11 compliance and supports routine and periodic data review.

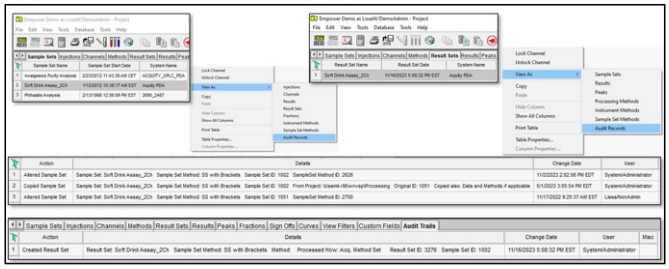


Figure 11: The View As functionality leverages the power of a relational database

The Review Window

Project Window > select data > Tools > Review

Empower software provides privilege-controlled access to methods, chromatographic data, Result information, and metadata within the Review window.

Result Audit Viewer

Project Window > select Results or Result Sets > Tools > Review > Tools > Result Audit Viewer

The Result Audit Viewer (Empower 3 Feature Release 2 and higher versions) brings audit records from the Project Audit Trail, Acquisition Log, Method, and Sample Histories together into a single window, and permits easy comparison of methods and Results.

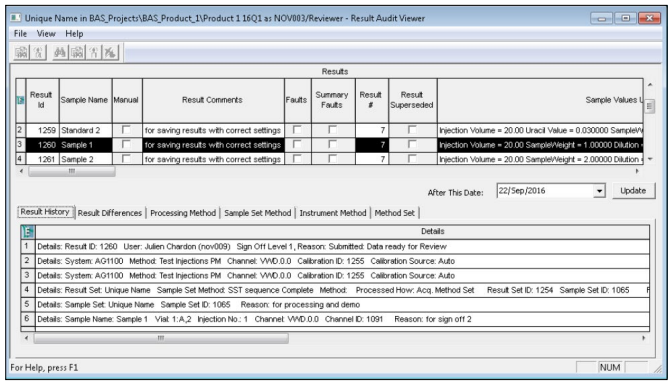


Figure 12. The Review window and the Result Audit Viewer facilitate a reviewer in interrogating the data, methods, peak results, calibration curves, and audit records. The Results can then be taken directly to Preview/Report Publisher for electronic sign-off.

View Filters

Edit View button

Empower View Filters can be leveraged to sort, search, and quickly locate information, including unprocessed data, manually processed data, unsigned Results, Results signed off more times than expected, aborted acquisition, re-processed data, re-acquired data and so on.

- Empower System Audit Trail, Project Audit Trail, and Message Center (Empower Feature Release 4 Service Release 3 and higher versions) provide View Filters to search for specific events which may indicate improper use of the system at the administration level and the Project level.
- Specific views can be created to display only the information needed for review.
- Just in Time View Functionality allows an ad hoc approach to searching.
- View Filters used within the multi-Project view allow searching across multiple Projects simultaneously to find data of interest across your entire laboratory, site, or enterprise.

Here is a small subset of items that View Filters can help you monitor during data review:

- Have all Channels been locked to prevent further processing?
- Have all Results been electronically Signed appropriately?
- Are the Injection Status / Channel Status as expected?
- Have all injections been processed?
- Were sample information changes made after the injection was acquired?
- Are there any unexpected Peak or Result Processing Codes?

- How many times was the Channel reprocessed?
- Did the Result fail any System Suitability check
- Was the Result manually processed?
- Does the Result contain any manual integration?
- Is there any unusual audit trail activity?
- Are there any unusual messages in the Message Center that need to be investigated?

System Suitability

Suitability, Limits, and Noise and Drift tabs within processing method. System Suitability Option must be enabled within the project.

System Suitability limits automatically flag 'suspect' data that is out of (or almost out of) your specification (OOS). System Suitability reports with control charts also expose data that is OOS or trending in that direction

Custom Fields

Project Properties > Custom Fields tab

Custom Fields provide innumerable ways to automatically determine and display data that fits your desired risk criteria. Custom Fields can:

- Show when manual integration is used
- Determine if a Result passes or fails all collective specification criteria
- Reveal data that was aborted
- Determine if a Result is the most recent Result
- Confirm the correct method used for acquisition and processing
- Determine whether all of the samples processed are from the same Sample Set

Project Integrity Test

Project Properties > Integrity tab > Test Project Integrity

Empower Software provides checksum and cyclic redundancy check (CRC) verification for all human-readable and machine-readable data to protect against data being altered by external access to the system. This check is part of the Project Integrity verification process, ensuring that the data file has not been modified or damaged since it was acquired. Project Integrity testing also provides an additional level of confidence that the information contained in a Project may be reliably and completely retrieved.

waters_connect™ Data Intelligence Software

The waters_connect Data Intelligence Software is a Waters Informatics Software product that works with Empower Software and provides detailed dashboards that help your lab visualize and derive insights from your Empower Software data. Data is extracted from Empower Software and pre-built dashboards are published as read-only versions of your Empower Software analyses. Custom dashboards can also be created to mine Empower Software data, including the audit trails. In particular, the Data Integrity dashboard provides insights on a number of key areas focused on key data integrity metrics in your Empower Software database. These insights help you quickly identify areas of concern and ensure that the use of your Empower Software instances aligns with procedural implementation.

The Data Integrity dashboard includes information on:

- Aborted Single Injections
- Aborted Sample Sets
- Unprocessed Channels
- Reprocessed Channels
- Single Injection Details
- Manually Integrated Peaks

For more information regarding waters_connect Data Intelligence Software, visit waters.com/dataintelligence and connect with your local Waters Informatics Sales Specialist.

DOCUMENTING DATA REVIEW INCLUDING AUDIT TRAIL REVIEW

Documentation of data review should be performed in a similar way to documentation of any review process. Typically, this is done by signing results as 'reviewed' or 'approved', following a data review SOP which outlines how the review process should be performed, including how and when to review audit trails and other logs.

The *WHO Guidance*[4], notes that data review, whether paper or electronic, is typically signified by signing the records that have been reviewed. Written procedures should clarify the meaning of 'review' and 'approval' signatures to ensure that the responsibility of the signature is understood.

Empower provides the ability to electronically sign chromatographic results together with functionality to ensure adherence to 21 CFR Part 11 electronic records and electronic signatures. Additionally, in Empower version 3.8.0 and higher versions, during a 'Sign Off 2', users can electronically certify that they have reviewed the audit trails associated with the Result(s) which they are signing.

After sign off, the audit trail certification information is available in the Project window and on Empower reports. Audit trails can also be 'printed to PDF' if that is something that your procedure requires.

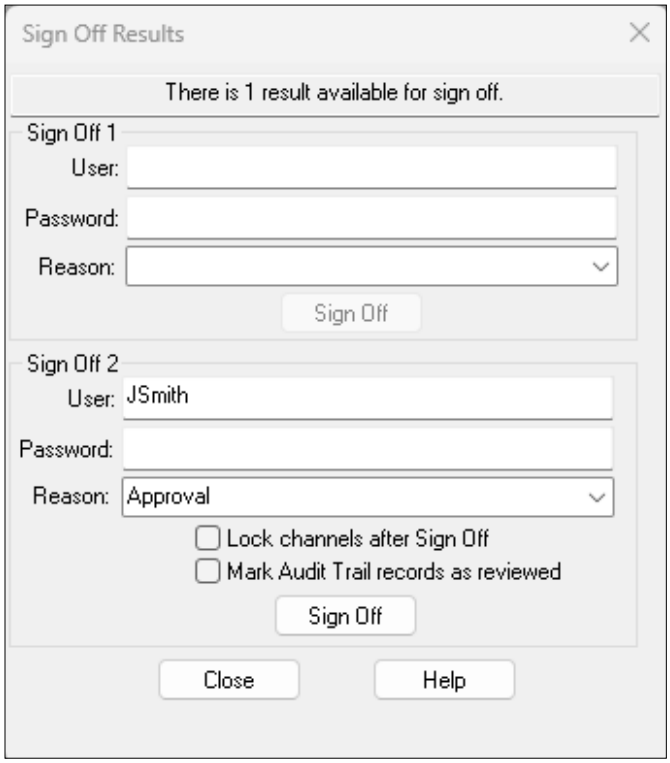


Figure 13. During electronic sign off, users can confirm they have reviewed the audit trails associated with the Result(s) which they are signing.

SUMMARY

Empower Software provides tools to capture user actions as they relate to data creation, modification, and deletion in addition to instrument errors, Oracle errors, and other errors. The unique way Empower Software utilizes the Oracle database ensures that the links between various records can never be broken, including the links between audit trails and Results or methods.

Reviewing audit trails and logs makes the most sense as an integrated part of the data review process, so it is essential that the reviewers have a good knowledge of the information and tools available within Empower Software. The extent of audit trail review should be considered, along with the extent of any other critical metadata which should be included in peer review and approval review. A clear SOP to identify the frequency, roles, responsibilities, and approach to a risk-based review of data and metadata including audit trails and logs (as well as documentation that this is adhered to) should be developed and followed. Periodic monitoring should investigate the effectiveness of the data review SOP.

Waters can partner with you in this process. If you need assistance with your workflows, procedures, and understanding the information available to you in Empower Software, please contact your local Waters Professional Services Representative.

References

1. FDA Title 21 Chapter 1 Subchapter A Part 11 (21 CFR Part 11) Electronic Records; Electronic Signatures; www.ecfr.gov.
2. PIC/S Guidance: GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED GMP/GDP ENVIRONMENTS; https://picscheme.org/docview/4234.
3. OECD Series Number 17: Advisory Document of the Working Party on Good Laboratory Practice Application of GLP Principles to Computerised Systems 2016; http://www.oecd.org.
4. WHO_TRS_996 Annex05; https://www.gmp-compliance.org/files/guidemgr/WHO_TRS_996_annex05.pdf.
5. PIC/S INSPECTION OF PHARMACEUTICAL QUALITY CONTROL LABORATORIES, Aide-Memoire; https://picscheme.org/docview/3455.
6. PIC/S GMP Guide: Concept Paper on the revision of Annex 11 of the guidelines on Good Manufacturing Practice for medicinal products – Computerised Systems; https://picscheme.org/docview/4967.
7. Data Integrity and Compliance With Drug CGMP Questions and Answers Guidance for Industry, Section III: QUESTIONS AND ANSWERS, question 8; https://www.fda.gov/media/119267/download.
8. Questions and Answers on Current Good Manufacturing Practices, Good Guidance Practices, Level 2 Guidance – Records and Reports; http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/ucm124787.htm.

For your local sales office, please visit waters.com/contact

Waters™

Waters, ACQUITY, UPLC, Empower, and waters_connect are trademarks of Waters Technologies Corporation. All other trademarks are the property of their respective owners.

©2025 Waters Corporation. March 25-13793 720005904EN Rev. B

Waters Corporation
34 Maple Street
Milford, MA 01757 U.S.A.
T: 1 508 478 2000
F: 1 508 872 1990
waters.com