Electronic Records and Data Storage Overview

DE44494.1656828704

Table of Contents

Introduction

This document provides summary information for Agilent Dissolution Workstation software. Dissolution Workstation is the preferred solution for organizations that perform dissolution testing in an electronic records environment. This document provides information on how the software implements the essential technical requirements of 21 CFR Part 11 to facilitate 21 CFR Part 11 compliance. It is important to note that no piece of software or equipment can ensure compliance since 21 CFR Part 11 compliance requires both technical and procedural controls.

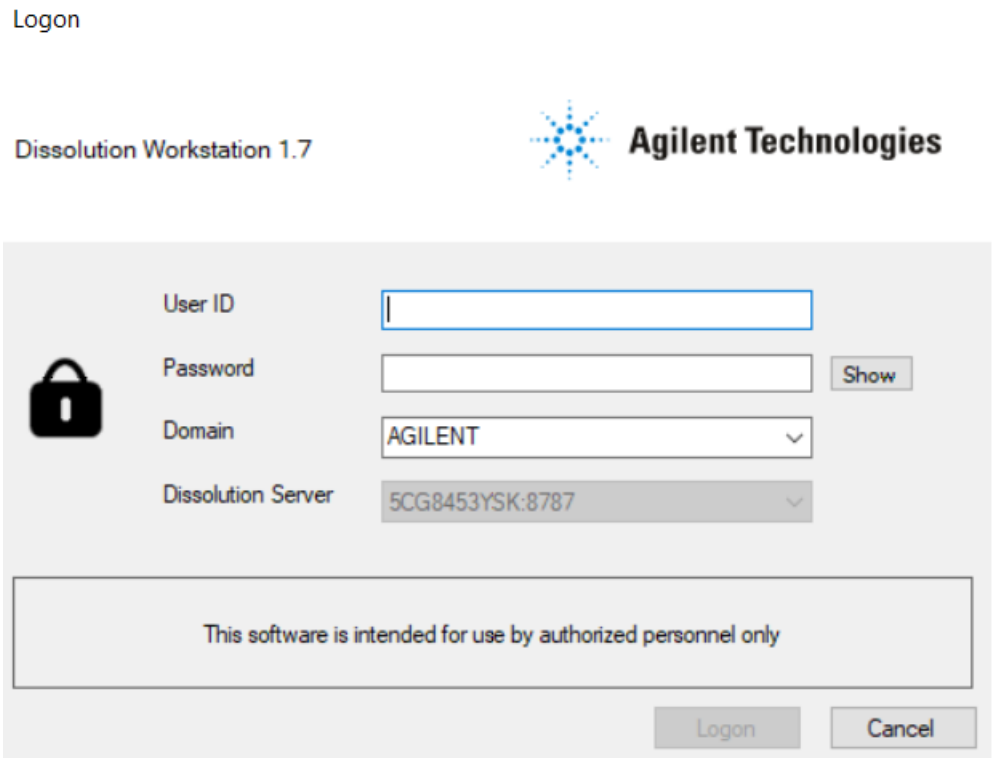
This document also provides guidelines for the deployment of the software in a laboratory.

This document makes frequent references to Windows™. This is used as a generic reference to Microsoft Windows™ operating systems. The Dissolution Workstation leverages the security capabilities of the Windows™ operating system. The current version (1.7) has been validated for use on Windows™ 10.

User Administration

For the purposes of 21 CFR Part 11, the Dissolution Workstation software is a closed system. Section 11.3 defines a closed system to be “an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system”. Access control is therefore an important feature of the software and extensive use is made of Windows™ security.

Each time the software is started, the user is prompted to logon. Logon credentials are tested against the Windows™ security database before the user can gain access to the system. The user cannot access any features of the software until the logon is complete.

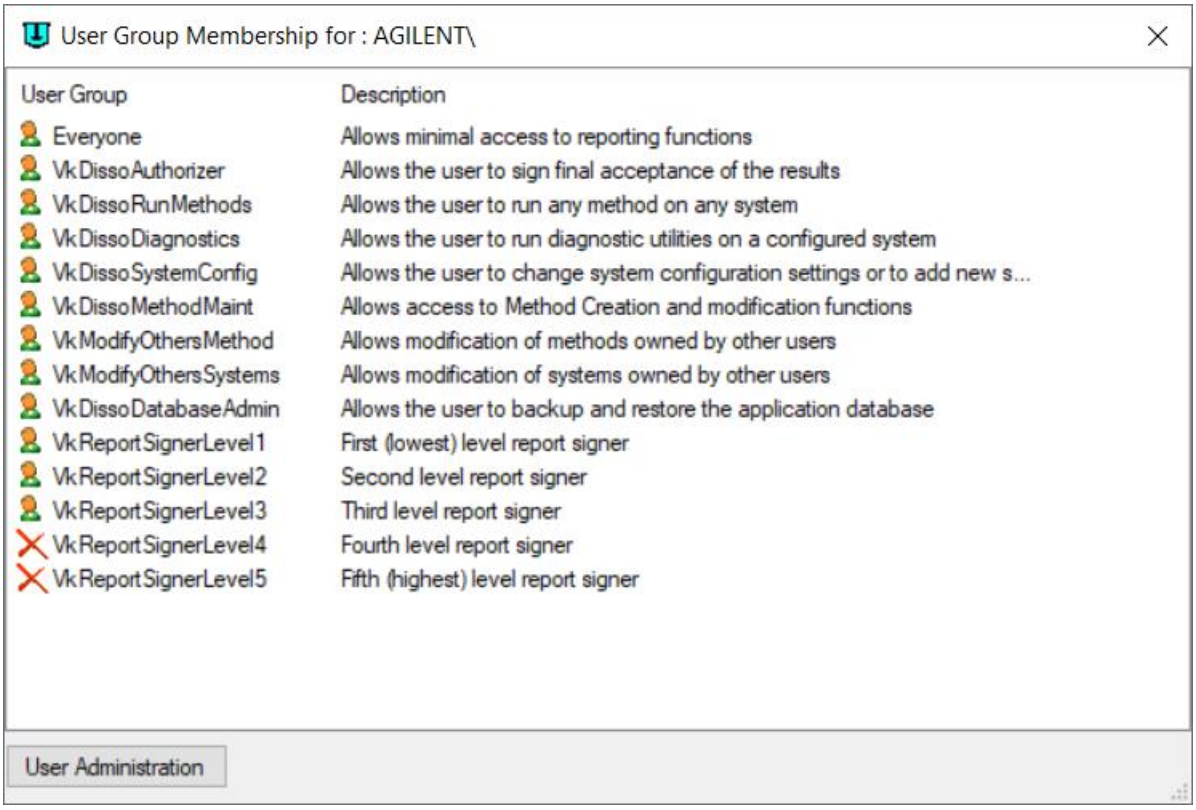


After three unsuccessful logon attempts, the login failure is recorded to the dissolution database. To provide a secure environment, the Windows™ Local Security Policy needs to be set to audit logins, ensure minimum password requirements, and to disable login accounts after three unsuccessful login attempts have been made. Since Domain policy can override Local System Policy, it is important that for Windows™ Domain/Active Directory environments, the Domain/Active Directory policies are set up correctly.

Several user groups are added to the local computer when the software is installed. These user groups define the functionality that can be assigned to a user. It is possible to add these groups to the Windows Domain Controller providing centralized management of group membership.

To provide a user with the permission to use any given functional area of the software, the user must be added to the appropriate group using the built-in Windows user administration functions. Users can be added from multiple Windows™ NT domains on the user’s network, or

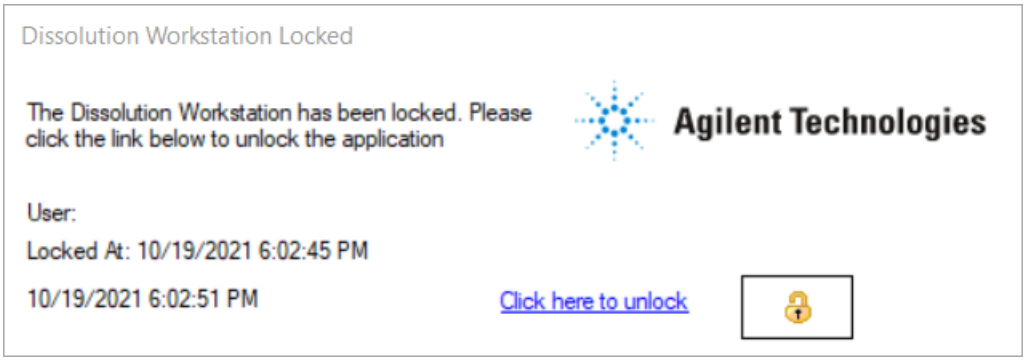
from the Windows™ local security database on the PC running the software. It is important to note that the Dissolution Workstation Software does not store any user passwords or group configuration information—this information is maintained by the Windows™ operating system in a secure and encrypted manner.



Once a user's group membership has been defined, features of the software will be enabled or disabled according to group membership. Where a user is not allowed access to a feature of the software by virtue of permissions, the feature will be grayed out as per Windows™ standards.

For 21 CFR Part 11 compliance purposes, the software employs Windows™ features to ensure that:

- **Access is limited to authorized individuals (11.10(d)).**
- **No two individuals have the same combination of identification code and password. (11.300(a)).** This is a fundamental feature of the Windows™ security database. Furthermore, to ensure user identification when logon IDs are duplicated across Windows™ domains, the full **Domain\UserID** form of the user ID is used for all signature and audit trail events.
- **Password issuances are periodically checked, recalled, or revised (11.300 (b)). Dissolution Workstation Software does not contain specific features of its own to enable this.** It is instead the responsibility of the system administrator to ensure that the password aging feature of the Windows™ operating system is properly set for each domain and local computer.
- **Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes (11.300 (d)).** An entry is made in the Windows™ system audit log when the account is disabled, and also when the account is re-enabled. The end user is responsible for ensuring that the Windows™ Local Security Policy and Windows™ Domain Security Policy has been appropriately set up. The software can be programmed to automatically "lock" after a defined period of time or can be manually locked at any time by using the "Lock Application" function. This prevents unauthorized access to the system when the PC is unattended.



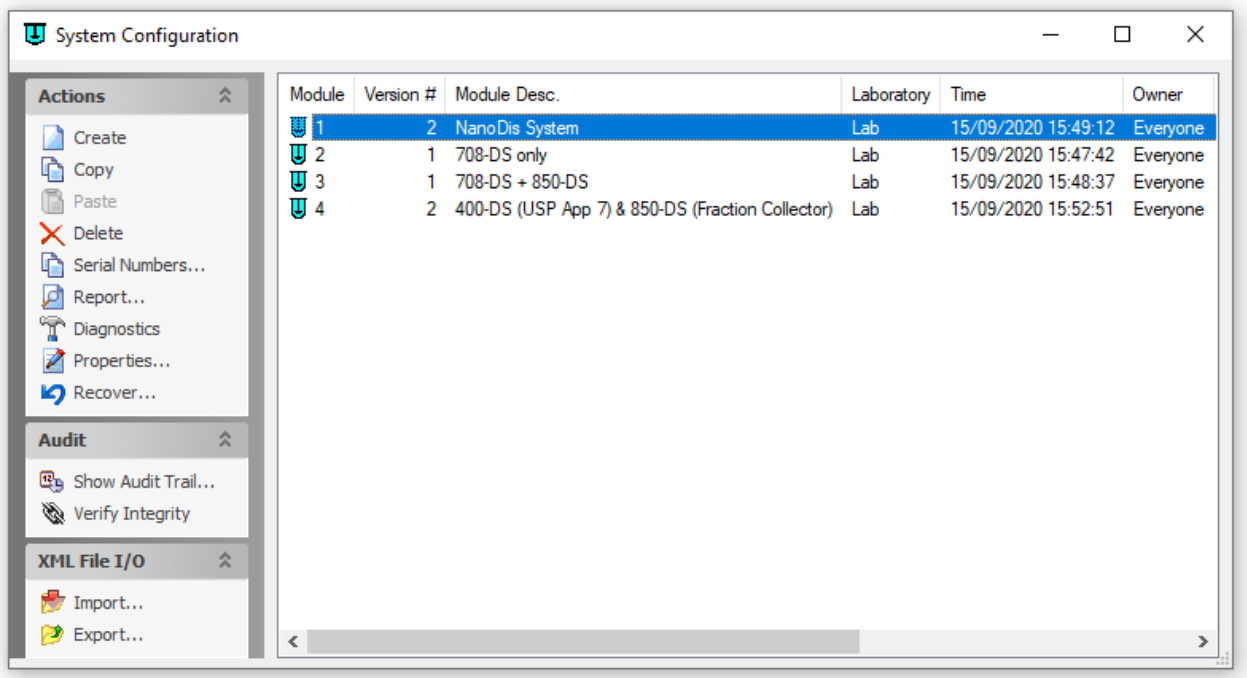
The locked system can then be unlocked by an authorized user. If a program is actively running, it can only be stopped by a user with VkDissoRunMethods group membership. All user logons are recorded to the workstation database.

System Administration

The Dissolution Workstation software has the capability of automating dissolution tests using the following Agilent Technologies instruments:

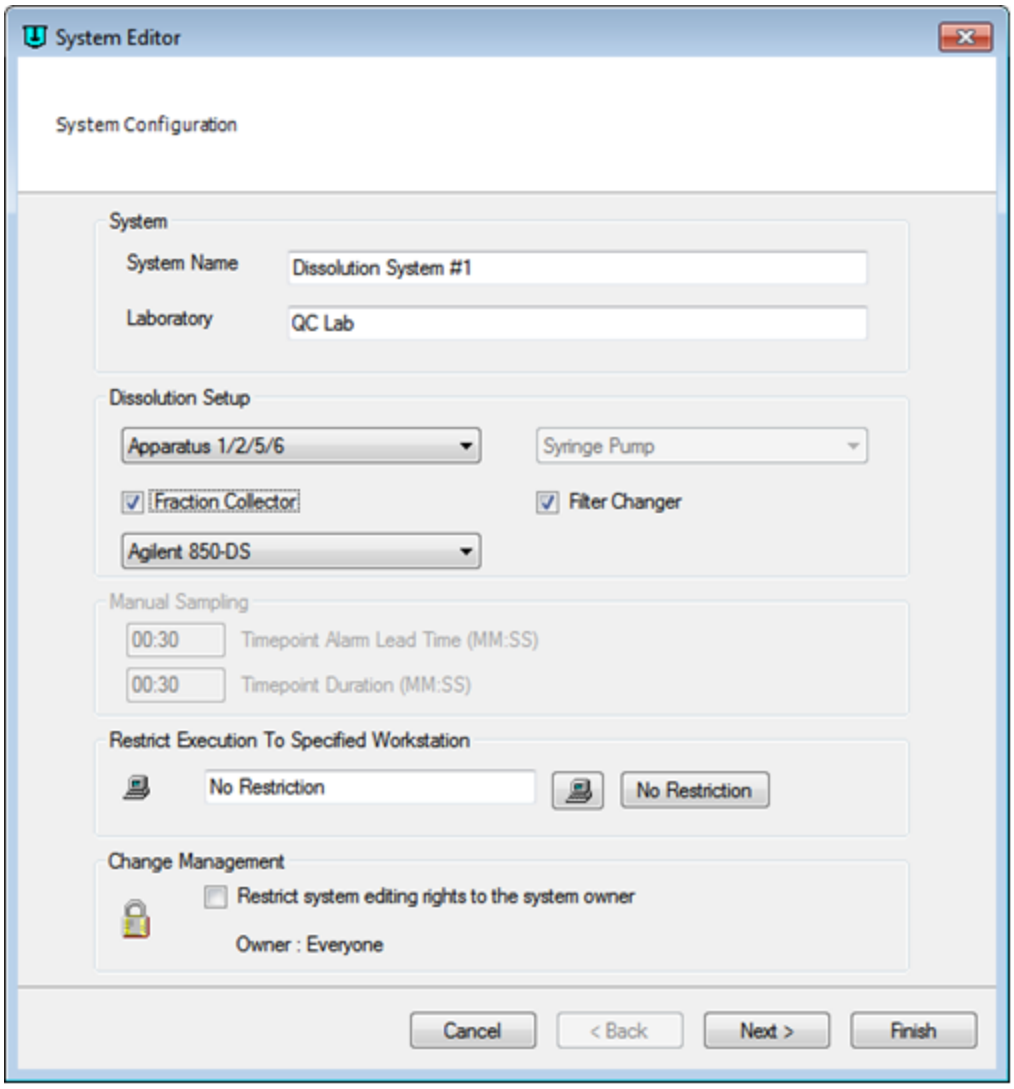
- USP Dissolution Apparatus 1, 2, 5 and 6 (e.g., 708-DS)
- USP Dissolution Apparatus 3 and 7 (e.g., Bio-Dis)
- Fraction Collector / Sampling Station (e.g., 850-DS)
- NanoDis System
- 400-DS (small-volume USP Apparatus 7)
- 280-DS Mechanical Qualification System (MQS)

System administration is required to configure the components that will be used for a dissolution test. Systems can be added, modified, and removed from the database.

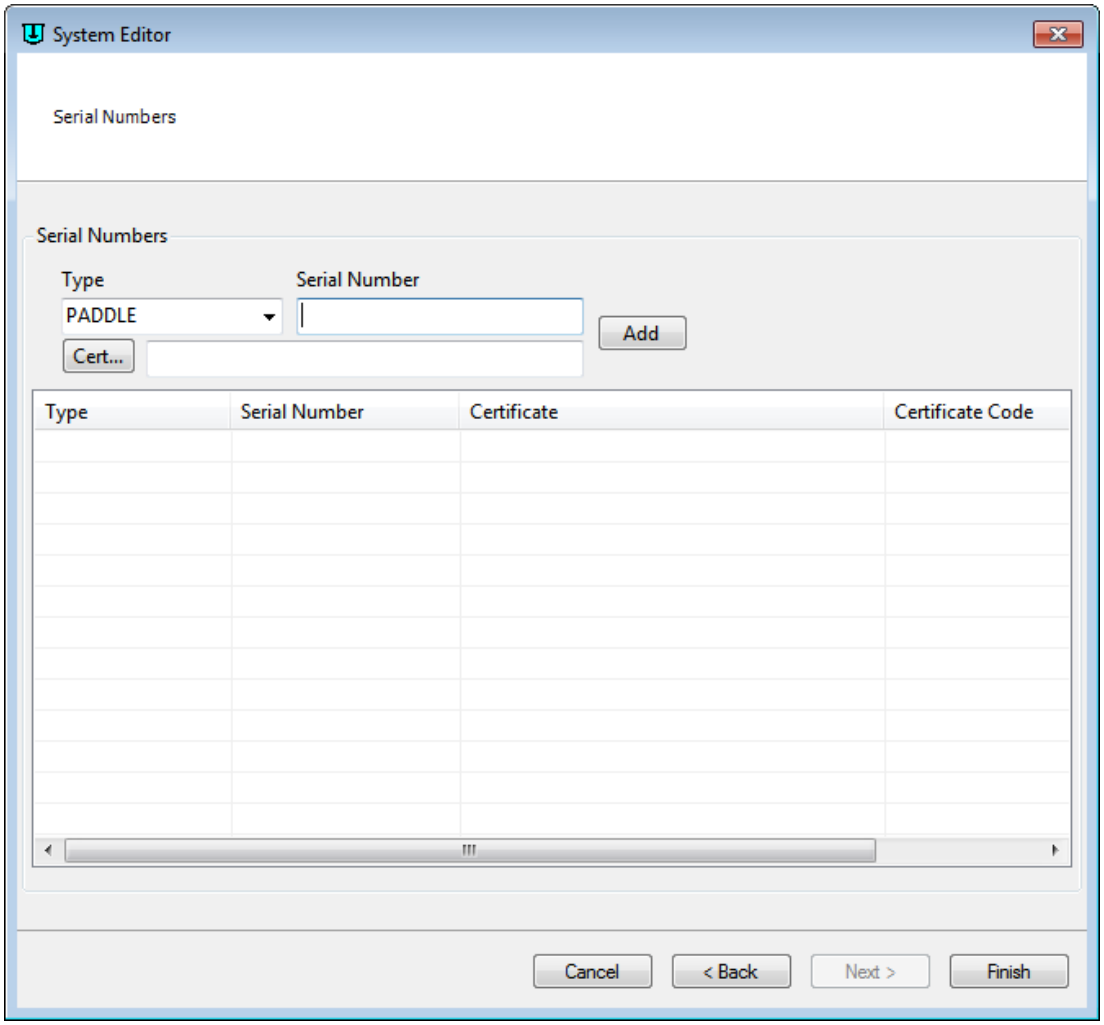


The software allows the configuration of multiple systems. System configuration entails selecting the equipment that will be physically configured in your lab and setting the appropriate communication and physical properties of the system. Serial numbers are stored for each system to allow tracking of physical system changes (e.g., vessel, shaft replacements).

Four systems can be configured and accessed at one time on a single computer. No restrictions are placed on the number of configured systems in the database.



Since it is possible to use a centralized database, the software provides features that limit the execution of a system method to a specific workstation and can prevent changes to the system configuration by anyone else other than the “System Owner” and users that have the VkModifyOthersSystems permissions.

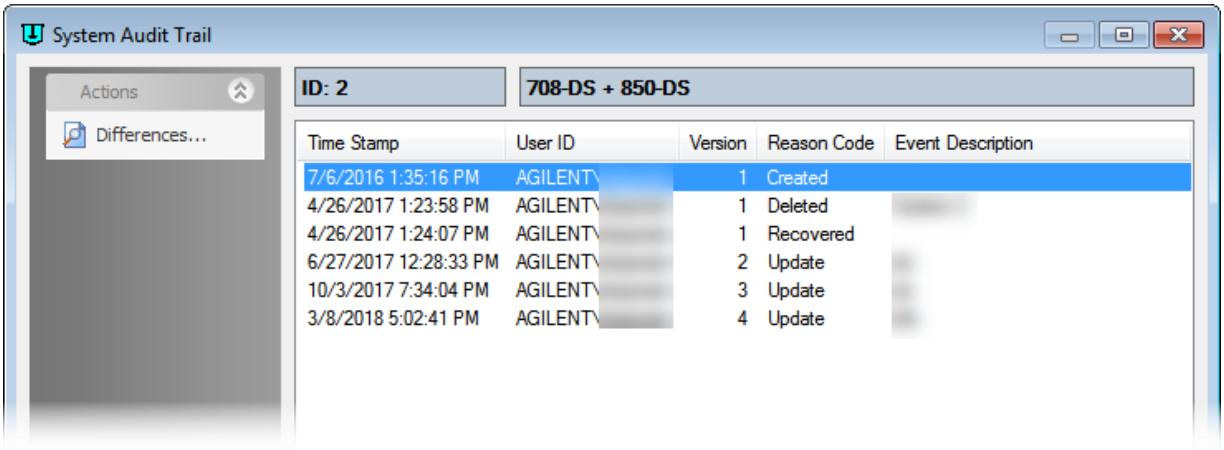


Use of system serial numbers is optional. The path of a certificate that corresponds to an individual accessory may be stored as part of the system information. If system serial numbers are used, they are managed and versioned along with changes to system configuration.

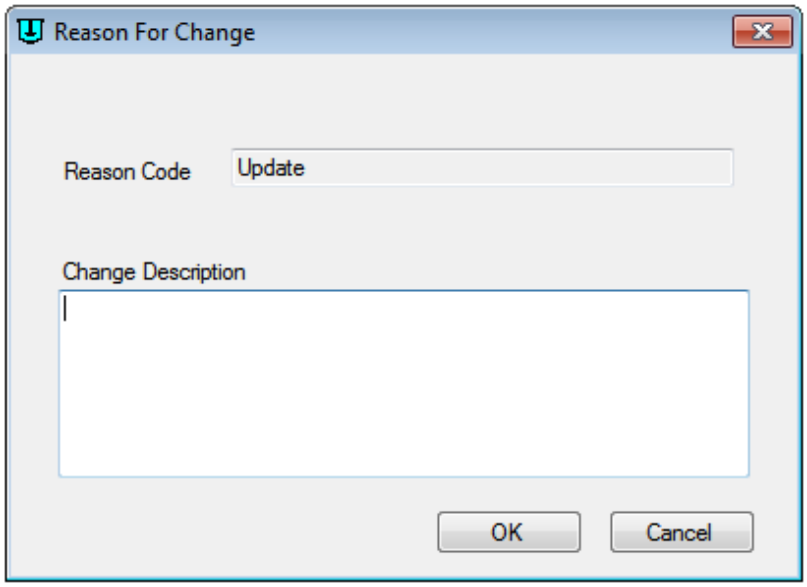
System Audit Trails

An important aspect of system configuration is the audit trail. Whenever a system configuration entry is changed, a new version of the system configuration is saved in the database. This allows the user to determine the differences between two or more versions of the same system to determine what changes were made. Reports are easily created to summarize specific changes between versions. This feature is common to method management as well, satisfying the audit trail requirements of 21 CFR 11 Sec 11.10(e).

- **Use of secure, computer generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail information shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. (11.10(e)).**

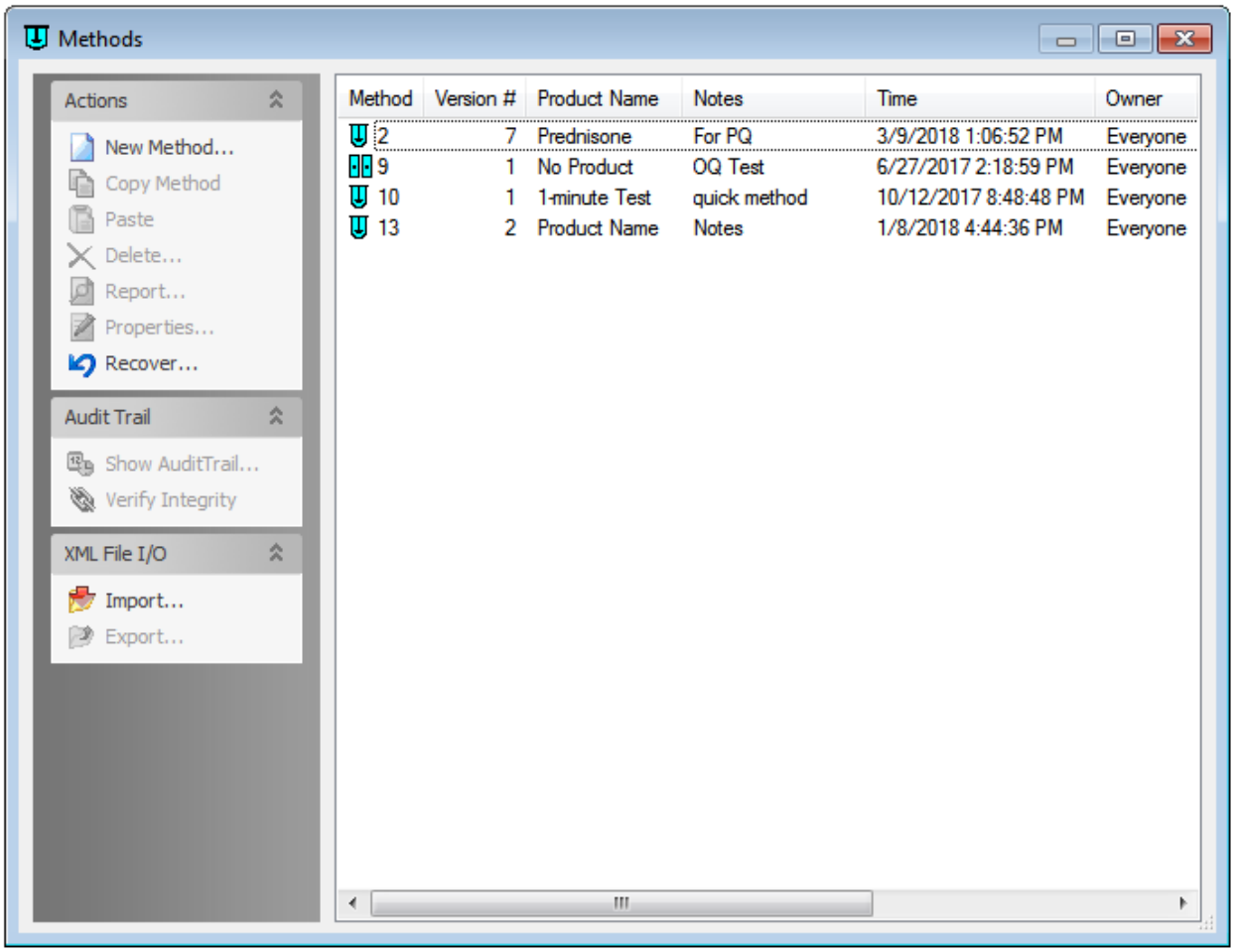


Whenever a change to a system or method is made, the current user is required to document the reason for the change by making an entry in the following dialog box:



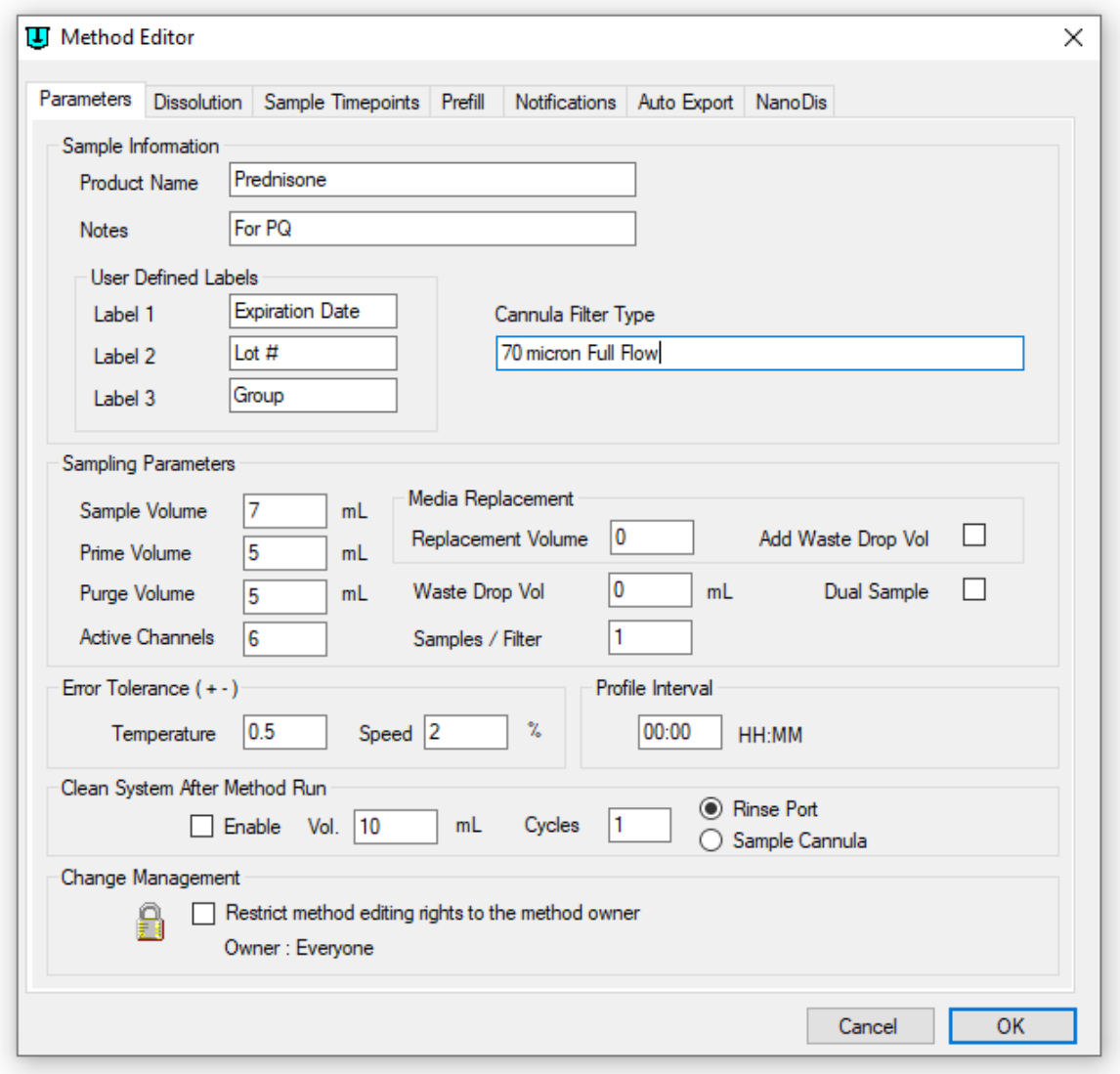
Method Management

The Dissolution Workstation software can store and manage multiple methods. The software does not limit the number of methods. A method in DWS is a collection of sample time points, dissolution tester properties and other necessary information about the test to be performed.



Methods can be created, deleted, modified, or executed by appropriate context menu item selection. Any change made to a method results in a new version. The audit trail feature dynamically determines the differences between two or more versions of the same method.

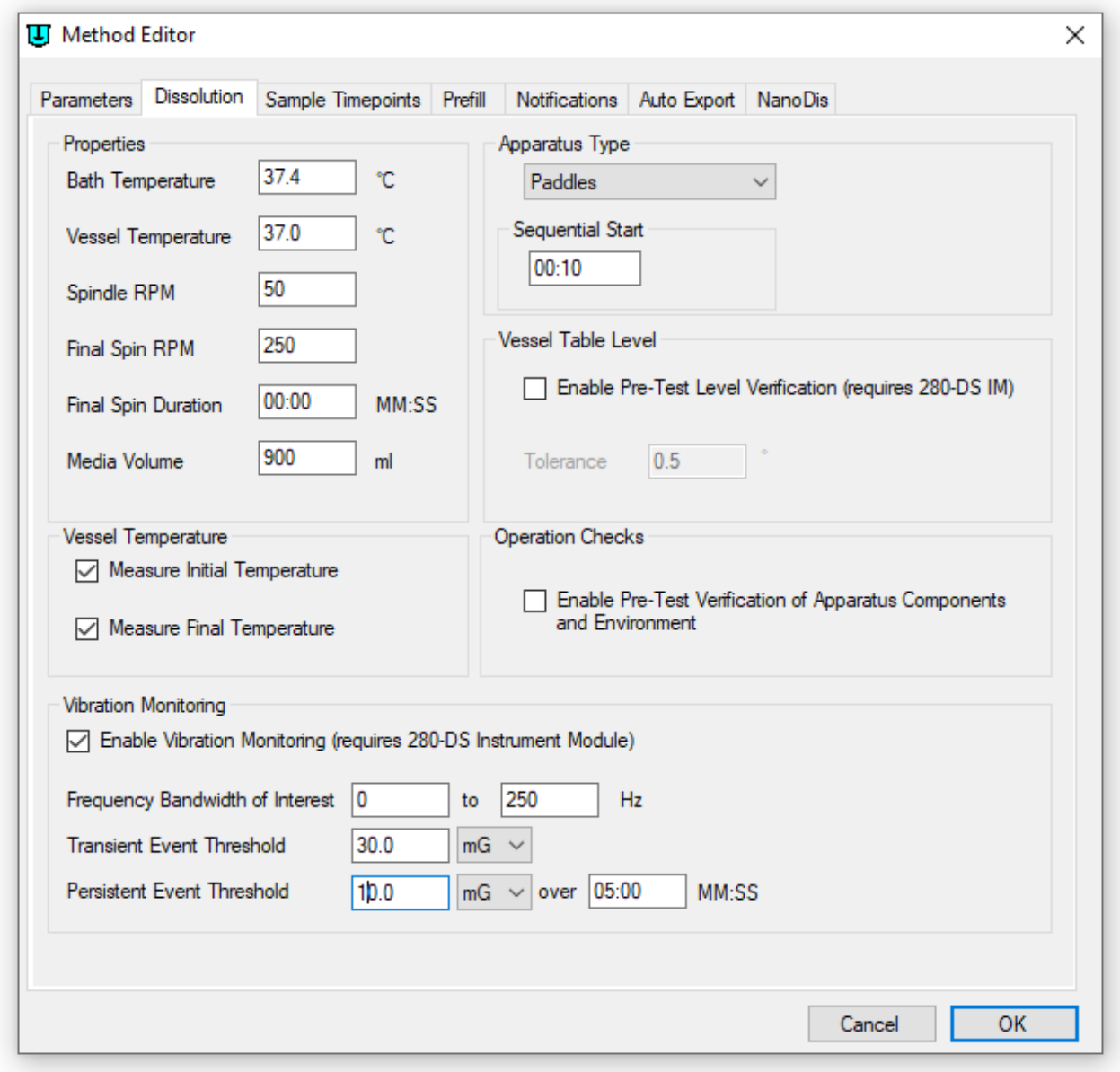
Note that a **method or system is never purged from the database** when it is “deleted”. Its attributes are changed to simply prevent it from being shown in the on-screen browser.



A method consists of the parameters required for a dissolution test. Changes to the parameters are audit trailed using the dynamic audit trail features of the software.

The method includes three user defined labels (15 characters each). These labels are presented to the user when a method is run to allow the user to enter test specific data (e.g., Lot/Batch information) at the start of the test that are relevant to the protocols of the user's environment. This allows users without method editing rights to document the relevant information for each dissolution test.

Dissolution tester properties determine the RPM and temperature at which the test will be run. For dissolution testers that have AutoTemp, the temperature tolerance is calculated at each sample point.

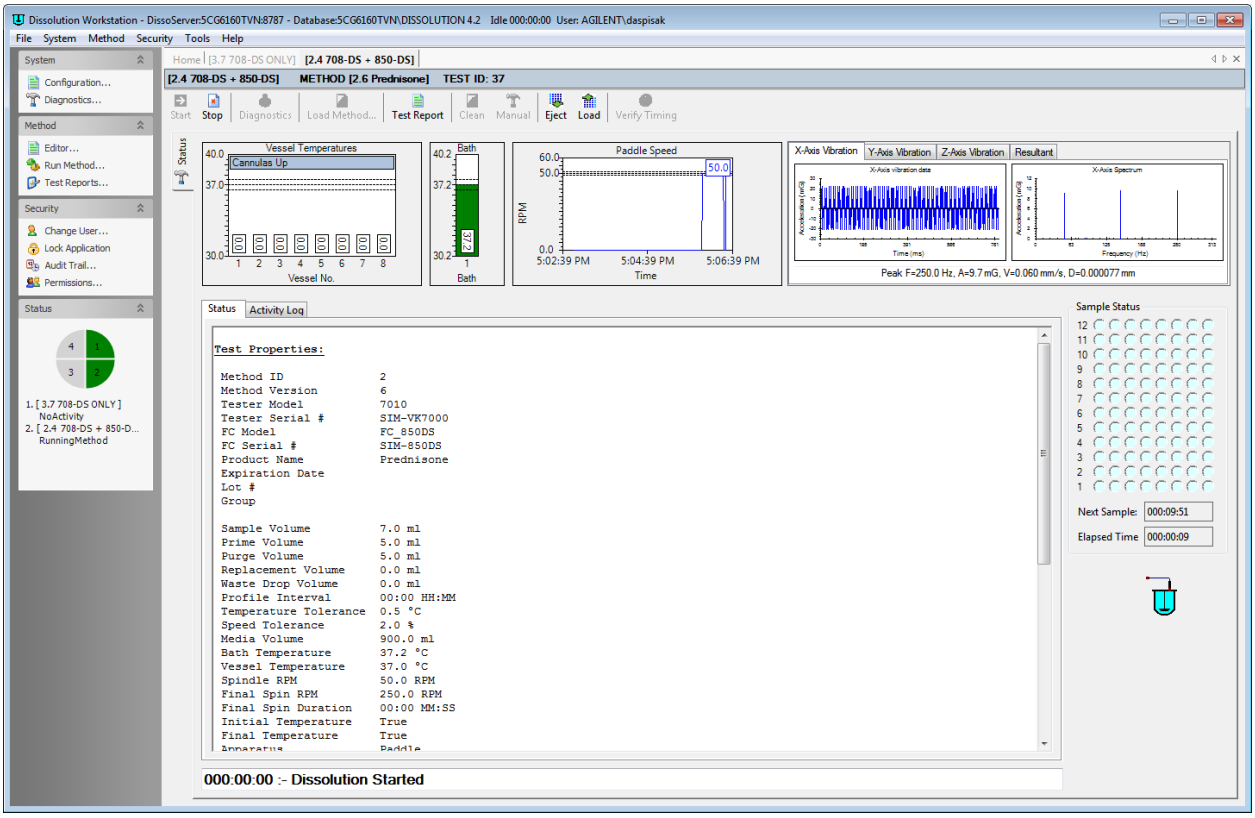


Time points specify the intervals at which samples will be drawn from the dissolution vessels. Each sample time point corresponds to a single row in the fraction collector, starting at the first row and moving through to the last row.

A special type of time point, Sample + Media Change, causes the system to pause after the Media Change time point to allow the user to change media. A distinction may be made between Media Addition and Full Media Replacement – this alerts the software as to whether the dosage form has remained in the dissolution media or temporarily removed. The elapsed time of the dissolution test will be adjusted accordingly based on this selection. The duration of the media change event is recorded to the database during a run.

Method Execution

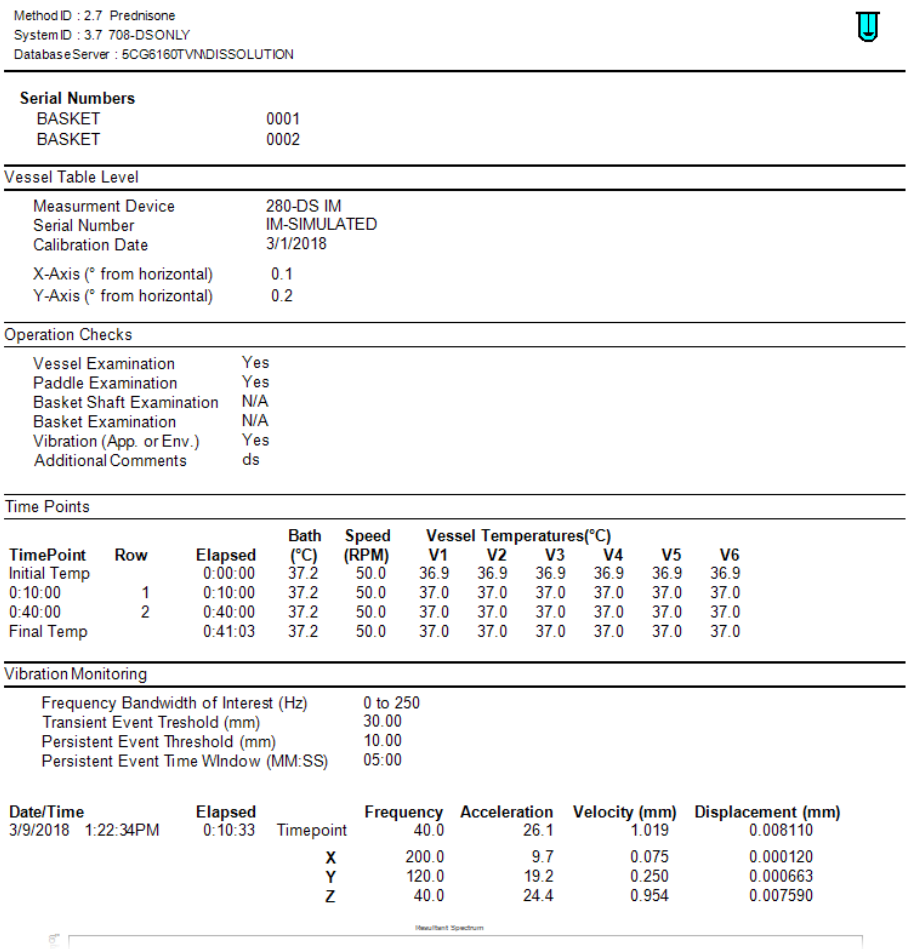
When a method is executed on a particular dissolution system, the software records the method parameters used as well as instrument information (e.g., RPM, temperatures) and the times at which samples are drawn. The entire process is automatically recorded to the software database and the user is shown real-time status information as the software progresses through each time point.



Test Reports

Once a program has completed, the results are available for review, and electronic signature. The software maintains complete history for all runs executed on the system, and satisfies the following technical requirements of 21 CFR 11:

- **Ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency (11.10(b))**. Data is physically stored in a protected database and can be exported as .PDF files. A report viewer facility is incorporated into the software to allow printing and previewing of results generated by a run.
- **Protection of records to enable their accurate and ready retrieval throughout the records retention period (11.10 (c)).** Records are protected by limiting access to the database to individuals authorized to manage results and methods.



Method ID : 2.7 Prednisone
System ID : 3.7 708-DSONLY
Database Server : 5CG6160TVN\DISSOLUTION

Serial Numbers

BASKET	0001
BASKET	0002

Vessel Table Level

Measurment Device	280-DS IM
Serial Number	IM-SIMULATED
Calibration Date	3/1/2018
X-Axis (° from horizontal)	0.1
Y-Axis (° from horizontal)	0.2

Operation Checks

Vessel Examination	Yes
Paddle Examination	Yes
Basket Shaft Examination	N/A
Basket Examination	N/A
Vibration (App. or Env.)	Yes
Additional Comments	ds

Time Points

TimePoint	Row	Elapsed	Bath (°C)	Speed (RPM)	Vessel Temperatures(°C) V1	V2	V3	V4	V5	V6
Initial Temp		0:00:00	37.2	50.0	36.9	36.9	36.9	36.9	36.9	36.9
0:10:00	1	0:10:00	37.2	50.0	37.0	37.0	37.0	37.0	37.0	37.0
0:40:00	2	0:40:00	37.2	50.0	37.0	37.0	37.0	37.0	37.0	37.0
Final Temp		0:41:03	37.2	50.0	37.0	37.0	37.0	37.0	37.0	37.0

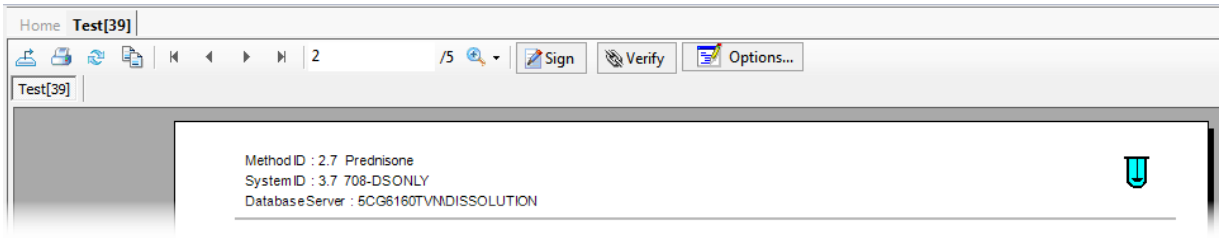
Vibration Monitoring

Frequency Bandwidth of Interest (Hz)	0 to 250
Transient Event Treshold (mm)	30.00
Persistent Event Threshold (mm)	10.00
Persistent Event Time Window (MM:SS)	05:00

Date/Time	Elapsed		Frequency	Acceleration	Velocity (mm)	Displacement (mm)
3/9/2018 1:22:34PM	0:10:33	Timepoint	40.0	26.1	1.019	0.008110
		X	200.0	9.7	0.075	0.000120
		Y	120.0	19.2	0.250	0.000663
		Z	40.0	24.4	0.954	0.007590

Results can be previewed, exported, electronically signed, and printed. A document ID is affixed to each report. The document ID is generated using a Hashing algorithm that ensures an extremely high probability of uniqueness of the document. Small changes in the document, result in large unpredictable changes in the hash code. The integrity of the documents stored in

the database can be determined for methods, systems and reports using the “Verify Integrity” function.



If an application other than the Dissolution Workstation software modifies the database, then this function will fail, and the user will be notified. Adding the document ID provides a first pass check to see if printed documentation or exported PDF files match the data in the database. A second pass, visually comparing every data element, is required to guarantee a match.

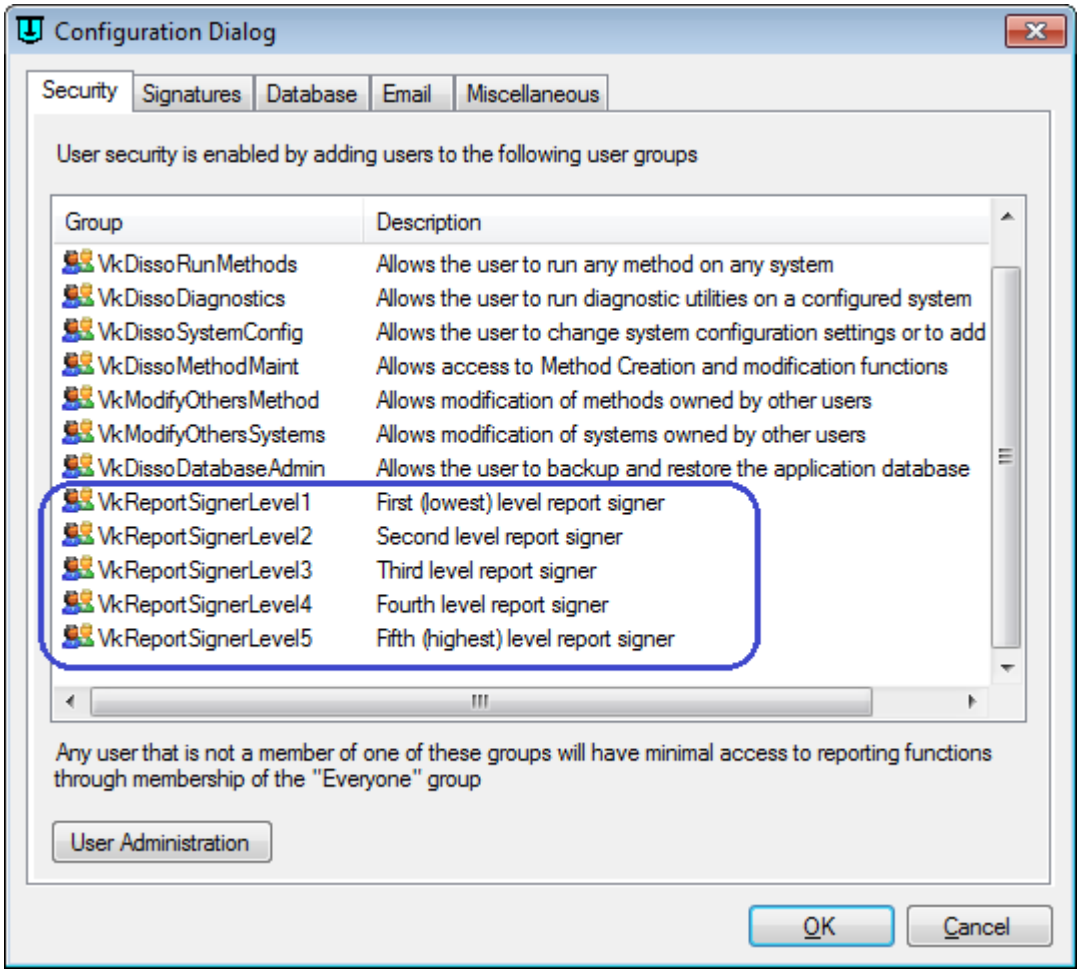
Electronic Signatures

When the user is satisfied with the results, the results can be electronically signed. An electronic signature is defined by 21 CFR 11 to mean "*a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.*"

The Dissolution Workstation software allows multiple electronic signings of a set of results. Each signing is accomplished using the signature dialog box shown. The user authenticity is determined by testing the user ID and password against the Windows™ security database.

Signature Levels

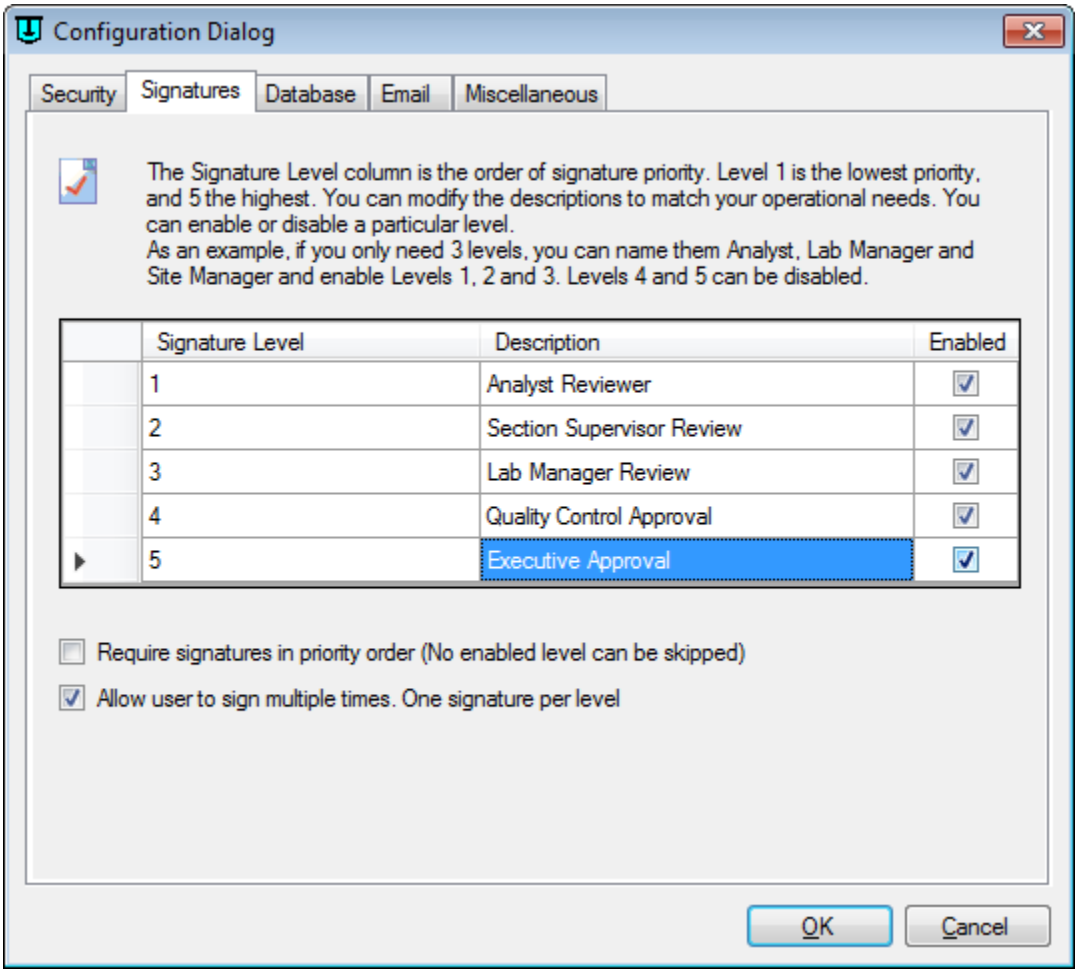
A total of 5 signature levels are possible. These levels are enabled for a specific user by membership of a signature level group. These groups are shown below



The naming of the groups at this point are not important, and only convey the possible levels from lowest to highest that the system supports. These are normal Windows groups that can be defined locally to the computer or at a domain level. This is the common approach for existing DWS/400-DS/280-DS groups.

Configuration of the levels is performed from within the DWS 1.7 software using the Tools/Options dialog under the **Signatures** tab. The description at each level is user defined and is for informational purposes, it does not control behavior. Behavior is controlled by the level number only.

For details on how to define each signature level refer to the Dissolution Workstation operating manual.



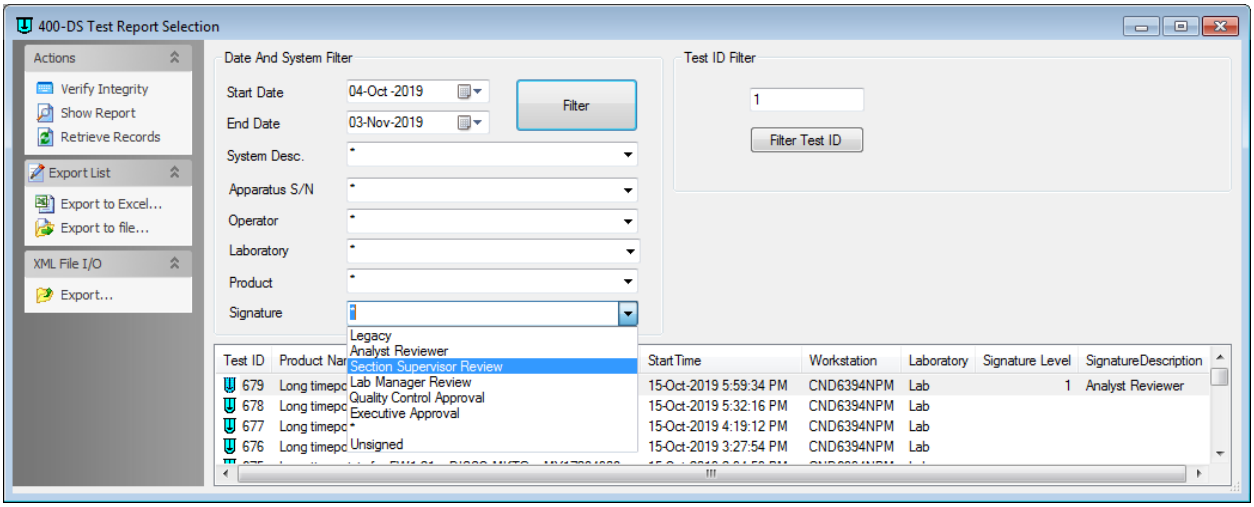
Signing Reports

When signatures are applied to a report for the first time, all enabled levels will be shown.

Once a report has been signed, the signature dialog will display the signatures that have already been applied to the report. It is not possible to sign at a level that has been previously signed. Each level is signed once, and the software will ensure the correct sequence is followed. Additionally, each signature requires a reason to be applied

Report Selection

A signature column has now been to the Report Selection Dialog



The report signature section displays the level, user ID and comment

Signatures

Time	Level	Reason	UserID
03-Nov-2019 12:36:10PM	1	Reviewed	Agilent\UserID

Once a signature has been added to a set of results, "*the signature cannot be excised, copied or otherwise falsified by ordinary means"* as required by section 11.70. Electronic signatures are permanently linked to the results.

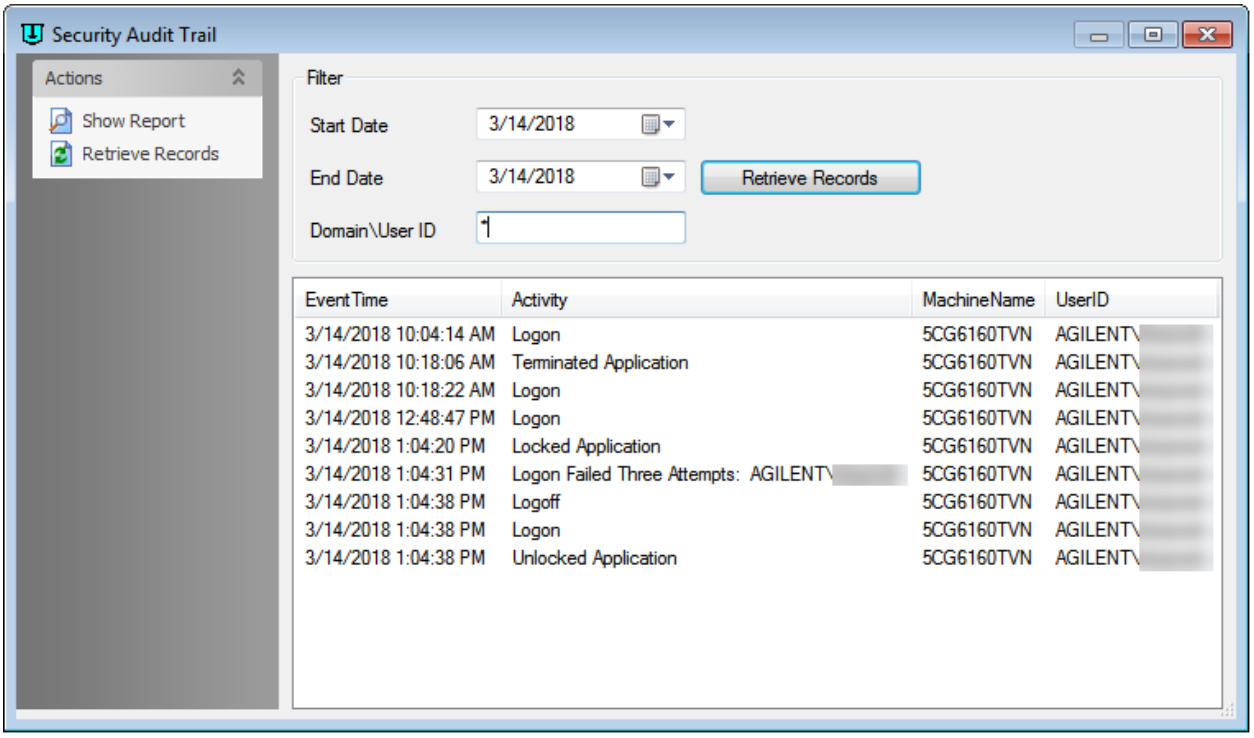
Security Audit Trail

To simplify access to security audit trail information, the Dissolution Workstation software records certain events in its own database independently of the Windows audit log. For security related events, it is very necessary to check the Windows security log at regular intervals.

The internal Dissolution Workstation log records the following events:

- Dissolution Workstation logon/logoff events
- Data verification errors
- More than three successive ID/password logon failures

NOTE: The Windows security log should always be consulted since this is the primary source for information when the Security Policy has been set correctly.

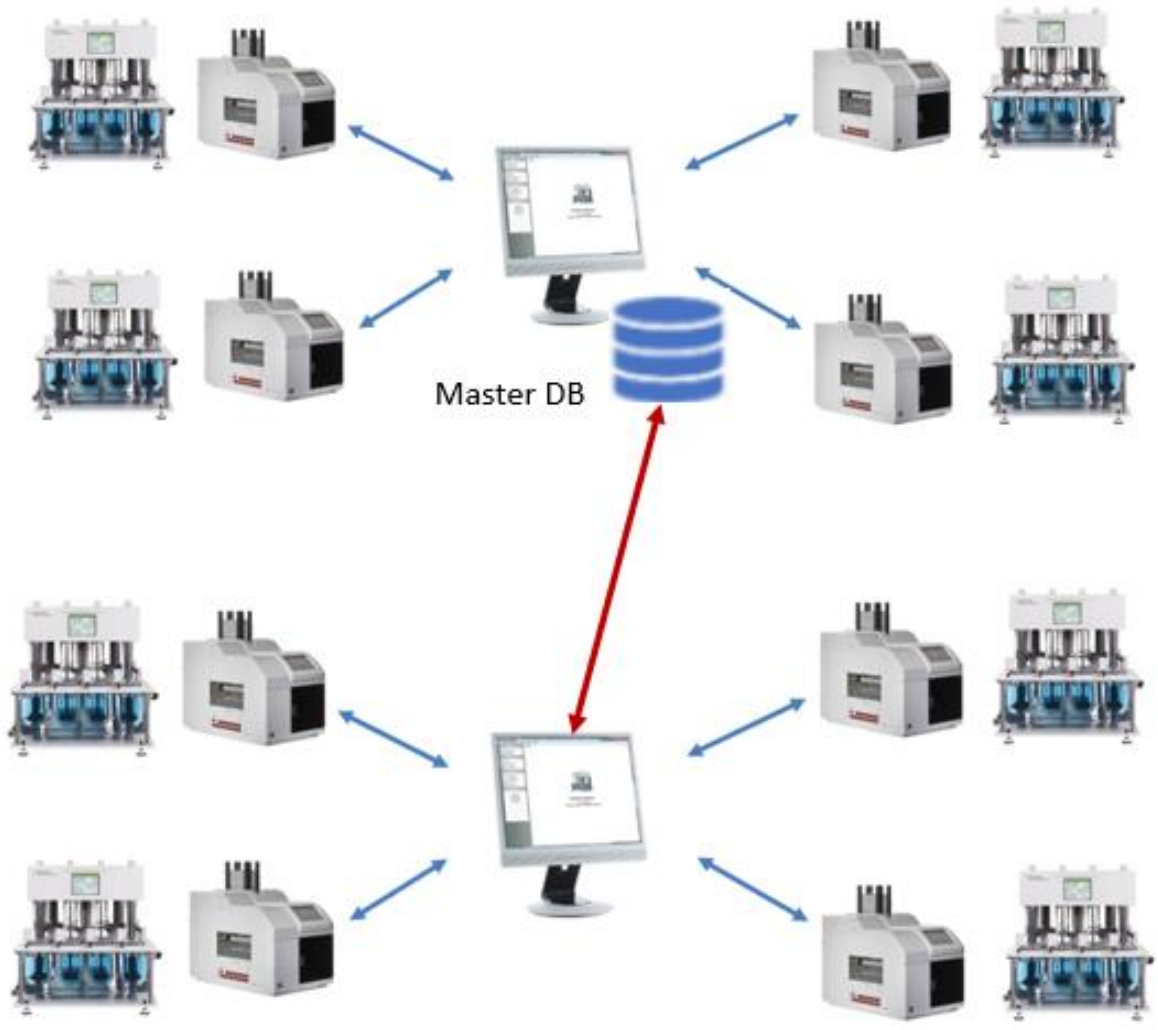


Database Configuration Options

The Dissolution Workstation installation automatically creates a local instance of Microsoft SQL Server Express. This database is the default selection for a workstation. Each workstation installation can support up to 4 sets of dissolution hardware as shown

It is possible, to designate another database on the network as the master for storing methods, systems, and test results.

The client-server architecture facilitates having multiple workstations served by a single database instance. This allows a single set of methods to be maintained for a laboratory that can be executed on any system within the laboratory. This architecture further facilitates remote access to the database from any LAN connected PC within an organization, for access to test reports.



All data generated by a workstation connected to a central database has the originating PC name attached to the data to be able to differentiate the source of data from multiple workstations. Further, the database connection name is used to uniquely identify the database from which test reports have been generated.

Any of the workstations can be designated as the Master DB if data centralization is required.

Managing Multiple Dissolution Systems from a Single Workstation

The Dissolution Workstation was designed to simultaneously control up to four (4) dissolution systems (apparatus + sampling station) from a single workstation (PC). Equipment can be connected in any number of different ways. While the PC can only run 4 tests concurrently, it can be connected to a shared database that manages the test data from multiple workstations. Since instruments are connected via RS232, it is unlikely that a standard PC will have sufficient ports to connect 4 complete systems. A serial-to-USB port extender by Edgeport is the recommended way to expand the PC's connectivity.

USB Dongle

The software is license-protected by a USB dongle. This dongle prevents the running of a test from an unlicensed computer. Each license purchased from Agilent, provides the capability of running up to 4 concurrent dissolution tests from the computer to which the dongle is connected. The software can be copied and installed on other computers but will not be able to run dissolution methods. Access to reporting via the software is enabled by default to allow remote administrative access to completed runs.