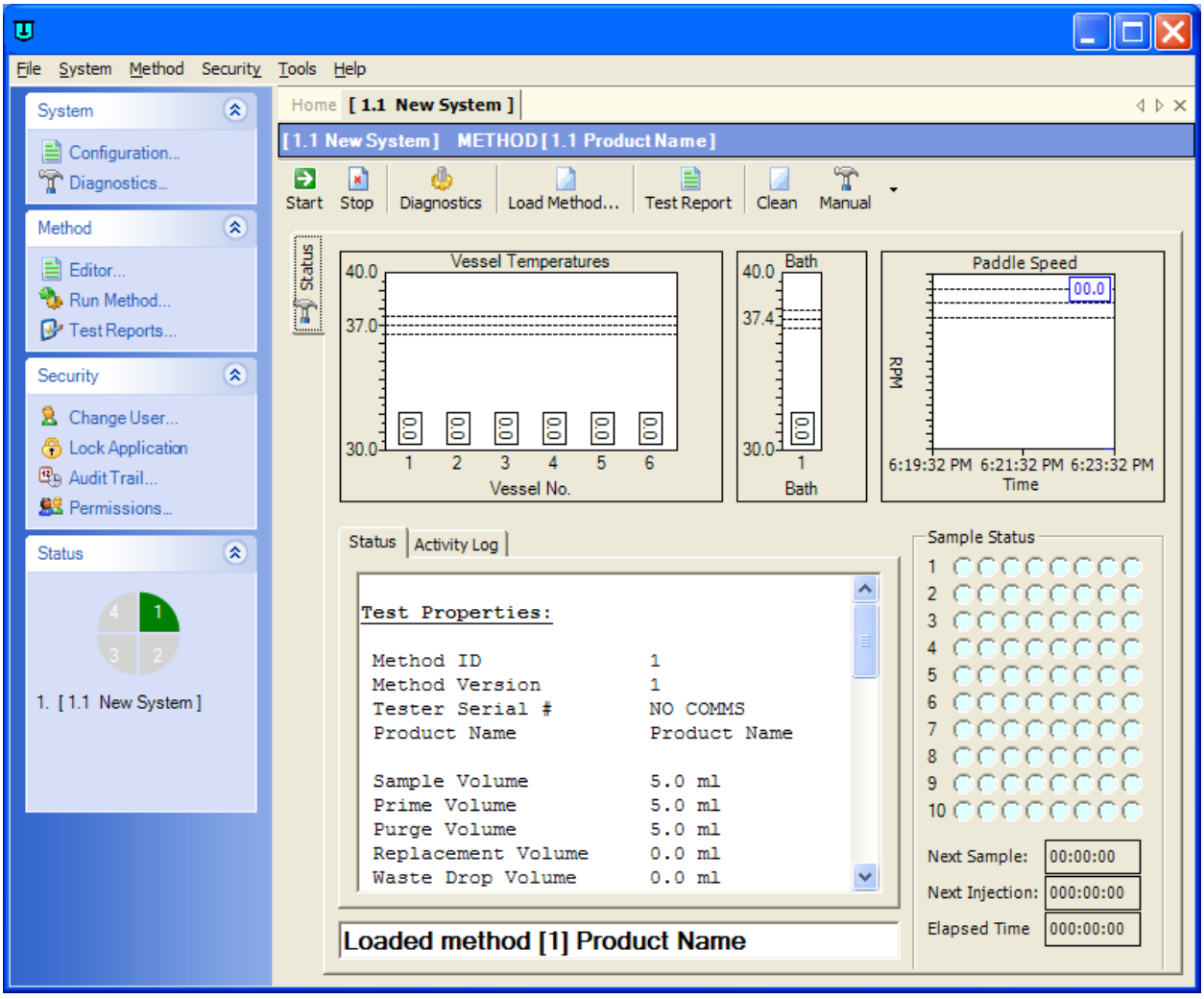
Agilent Technologies
Dissolution Workstation Software
Electronic Records and Data Storage Background

Table of Contents

Introduction

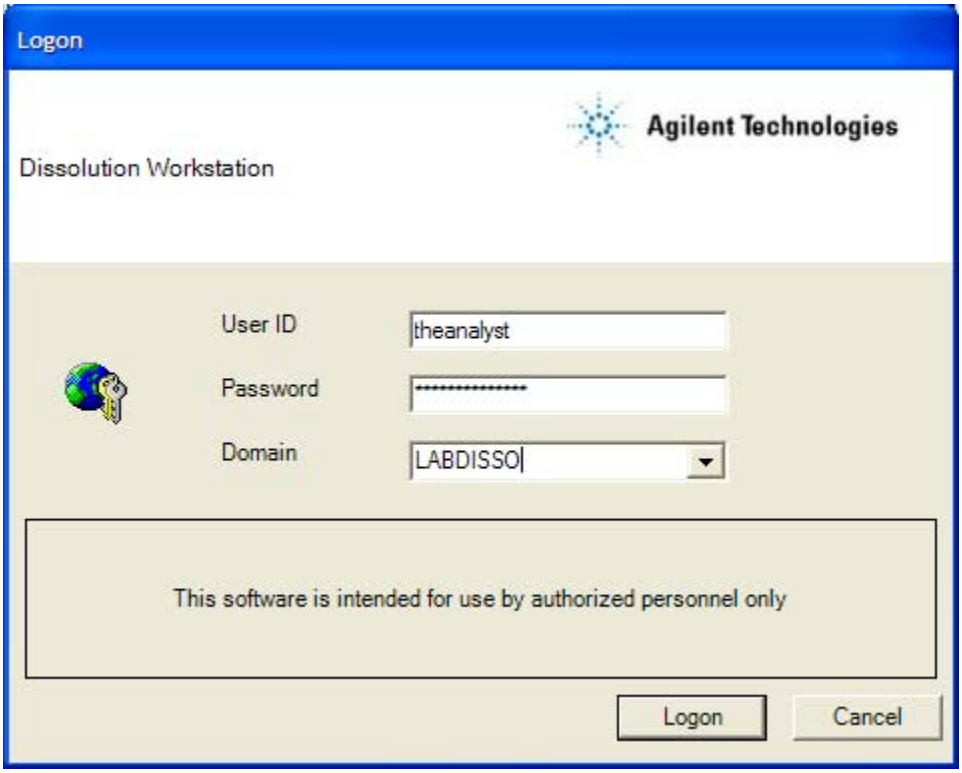
This document provides summary information for Agilent Technologies Dissolution Workstation software. The Dissolution Workstation is the preferred solution for organizations that perform dissolution testing in an electronic records environment. This document provides information on how the software implements the essential technical requirements of 21 CFR Part 11 in order 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™ 7 or Microsoft Windows™ XP. The Dissolution Workstation leverages the security capabilities of the Windows™ operating system.

User Administration

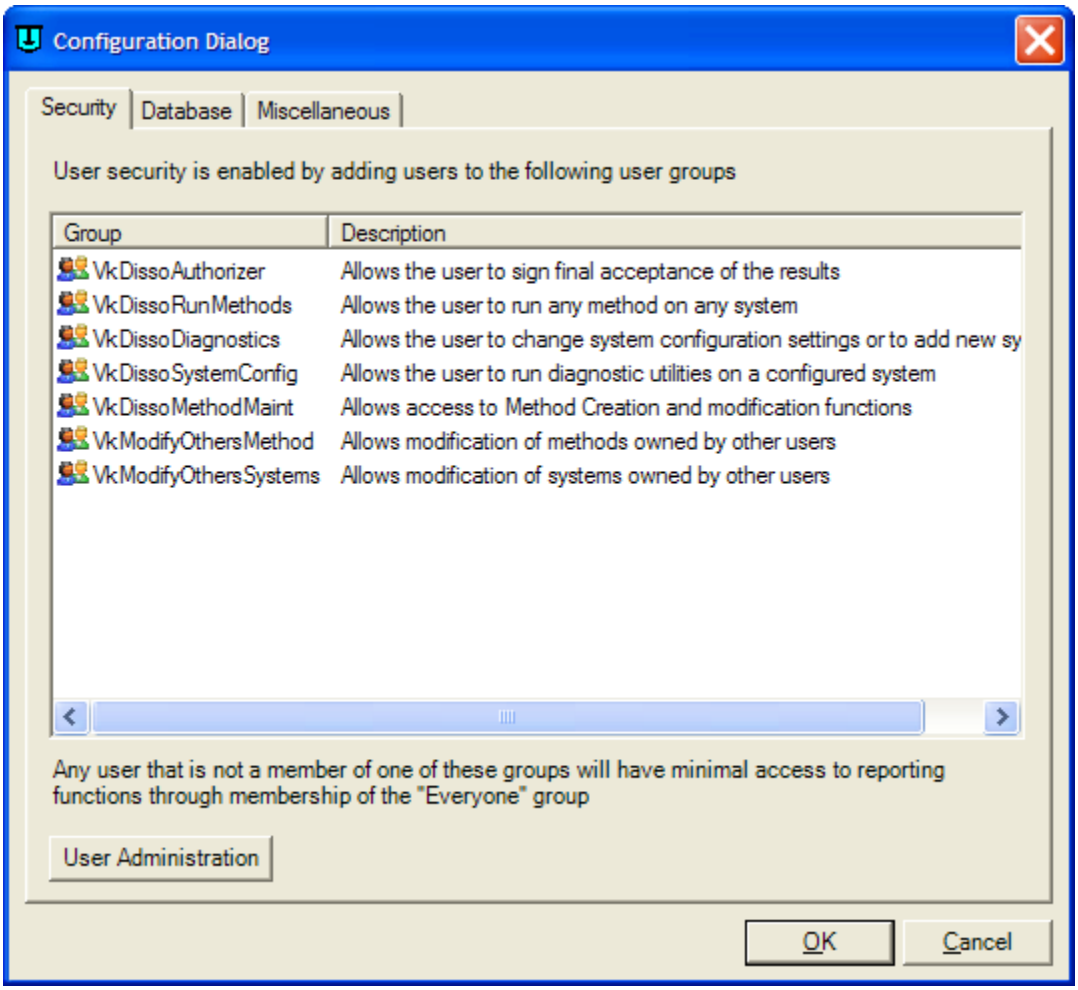
For the purposes of 21 CFR Part 11, the Dissolution Workstation software is considered to be a closed system. Section 11.3 defines a closed system to be *"an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system".* Access control is therefore an important feature of the software and extensive use is made of Windows™ 2000/XP 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 is able to gain access to the system. The user cannot access any features of the software until the logon is complete.

After 3 unsuccessful logon attempts, the login failure is recorded to the dissolution database. In order 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 3 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 be setup correctly.

A number of 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.

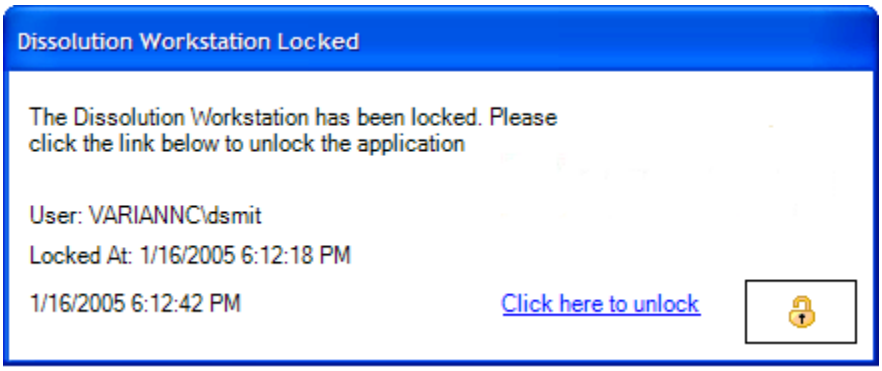


In order to provide a user with the permission to use any given functional area of the software, the user needs to be added to the appropriate group using the built-in Windows user administration functions. Users can be added from multiple Windows™ NT domains on the user's network, or from the Windows™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

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. Further, 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))**
  No specific features of the Dissolution Workstation software exist to ensure this. It is 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 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 setup appropriately. The software can be set to automatically “lock” after a defined period of time or be locked at any time by using the “Lock Application” function. This prevents unauthorized access to the system when the PC is unattended.



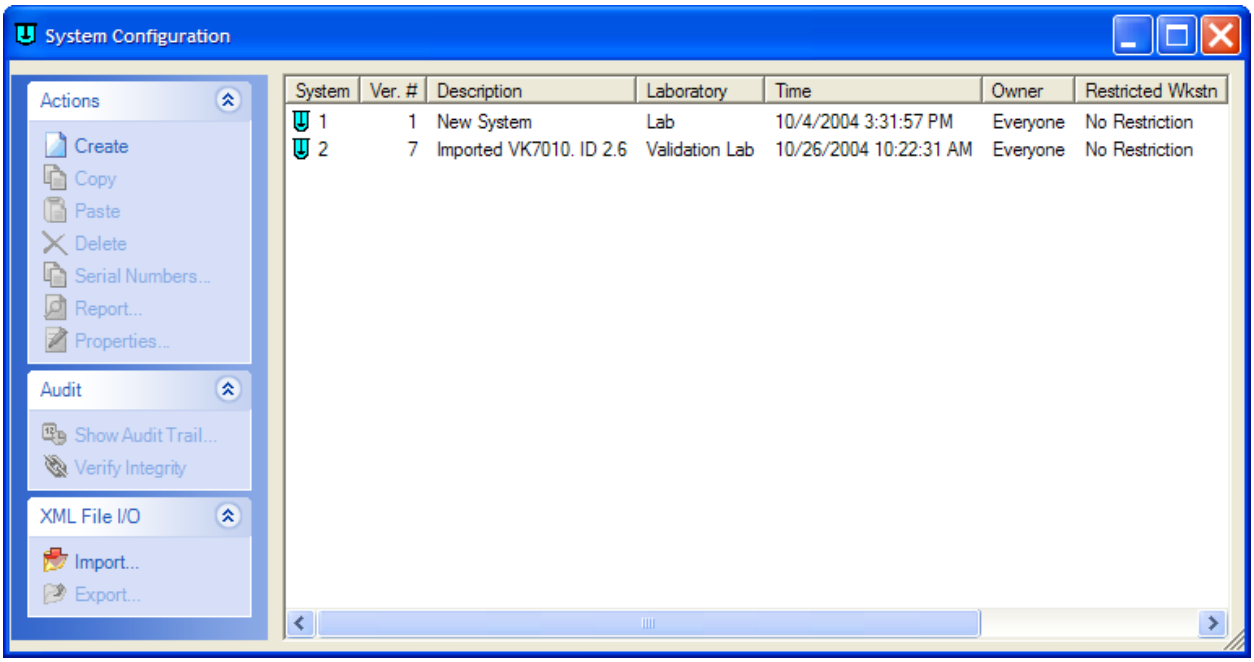
The system can be unlocked by an authorized user. If a method is running, the method can only be stopped by a user with VkDissoRunMethods group membership. User logon is recorded to the workstation database.

System Administration

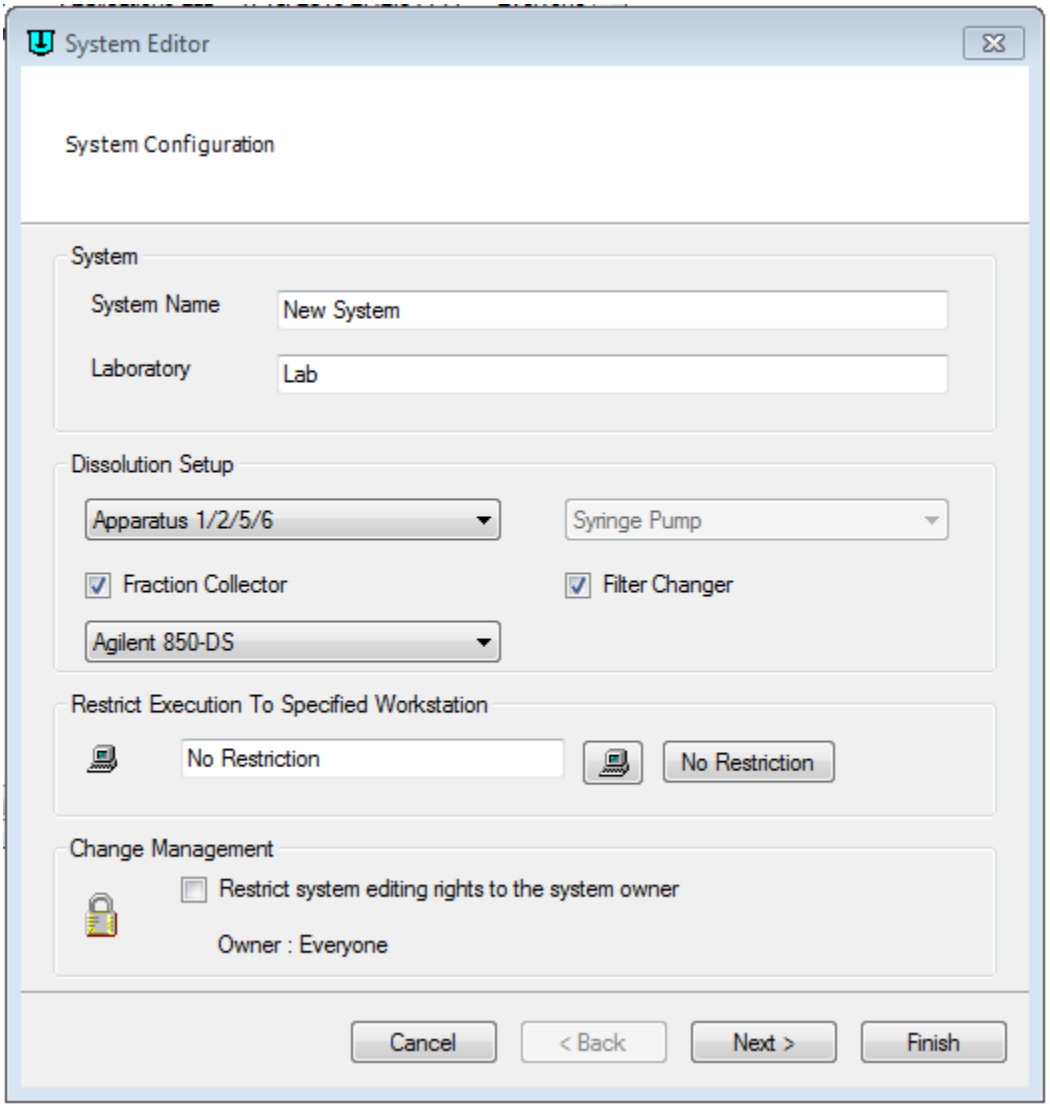
The Dissolution Workstation software has the capability of automating dissolution tests using the following Agilent Technologies instruments:

- Apparatus 1, 2, 5 and 6 Dissolution Testers (7000/7010, 7025/7030, 705-DS, 708-DS, 709-DS)
- Apparatus 3 and 7 (Bio-Dis Reciprocating Cylinder, App 7 Reciprocating Holder)
- 8000 and 850-DS Sampling Stations
- 806 Syringe Pump
- 808 Filter Changer
- 810 Peristaltic Pump

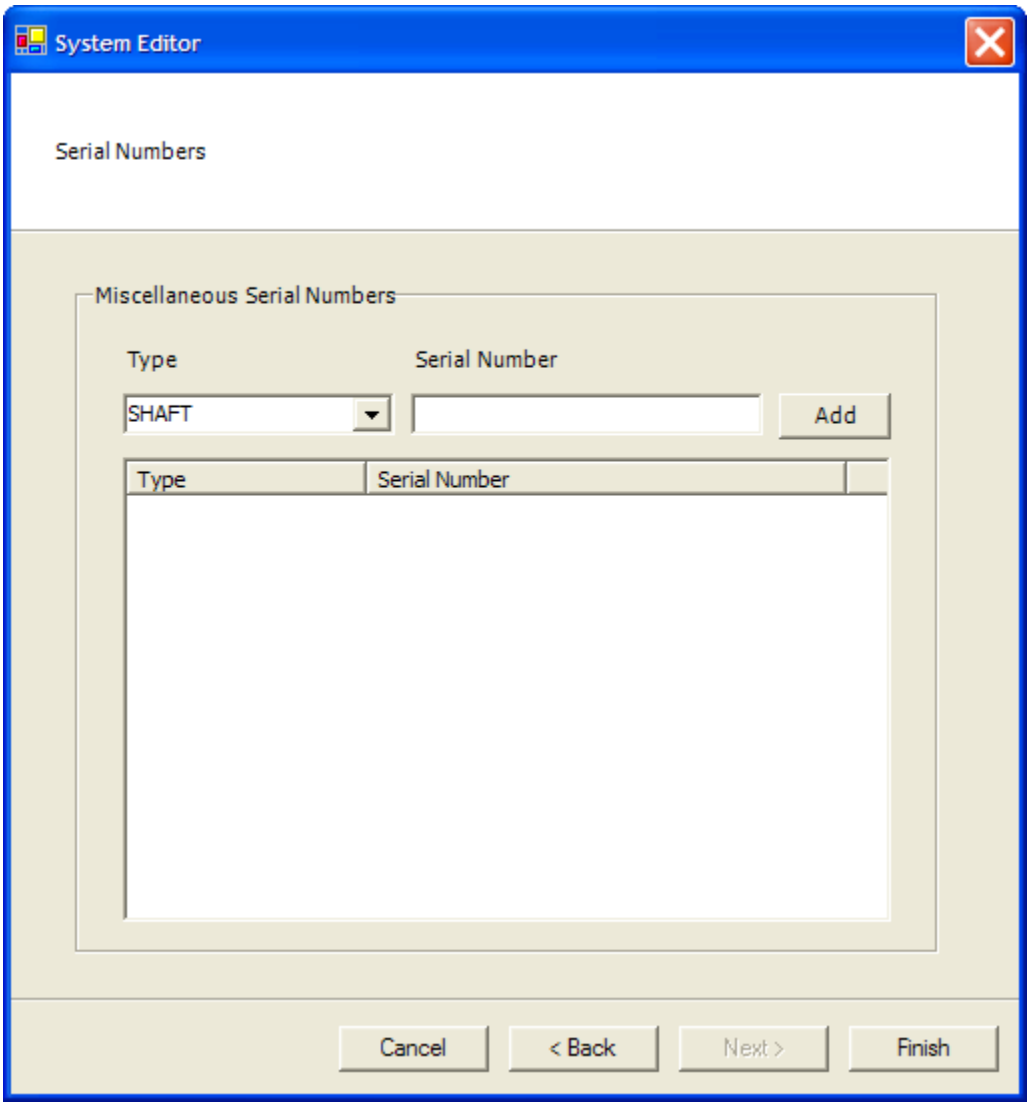
System administration is required to configure the components that will be used for a dissolution test. Systems can be added, modified and removed from the database.



The software allows the configuration of multiple systems. System configuration entails selecting the equipment that will be physically deployed in your lab, and setting the appropriate communication and other physical properties of the system. Serial numbers are stored for each system to allow tracking of physical system changes (e.g. Vessel, Shaft replacements). Only 4 systems can be 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.

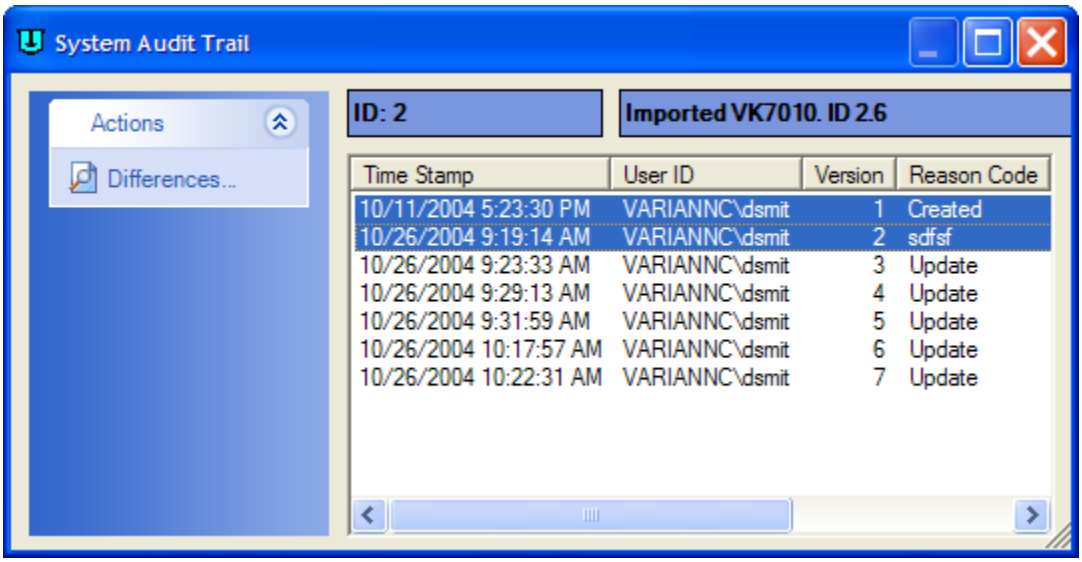


Use of system serial numbers is optional. If system serial numbers are used, they are managed and versioned along with changes to system configuration.

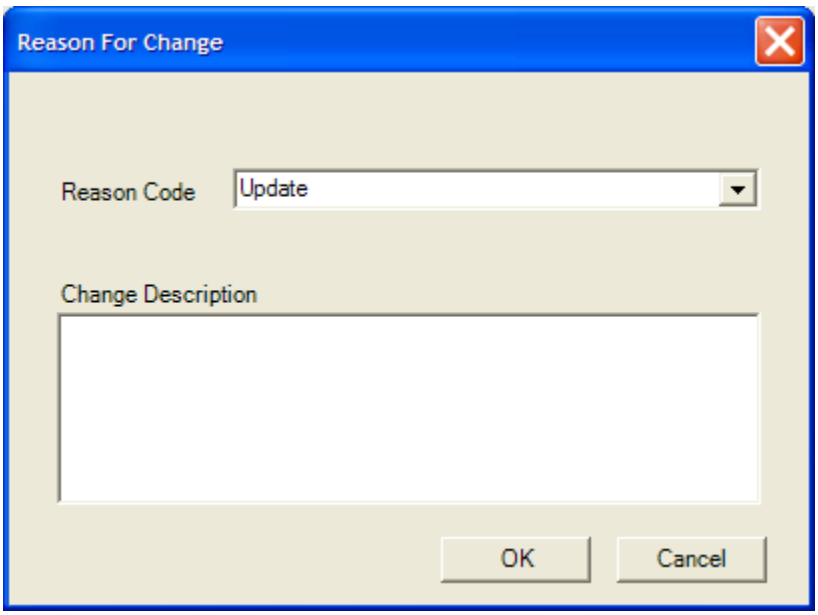
An important aspect of system configuration is the audit trail. Whenever a system configuration entry is changed, a new version of the system configuration is saved in the database. This allows the user to determine the differences between 2 or more versions of the same system to determine what changes were made. This feature is common to method management as well, satisfying the audit trail requirements of 21 CFR Part 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))

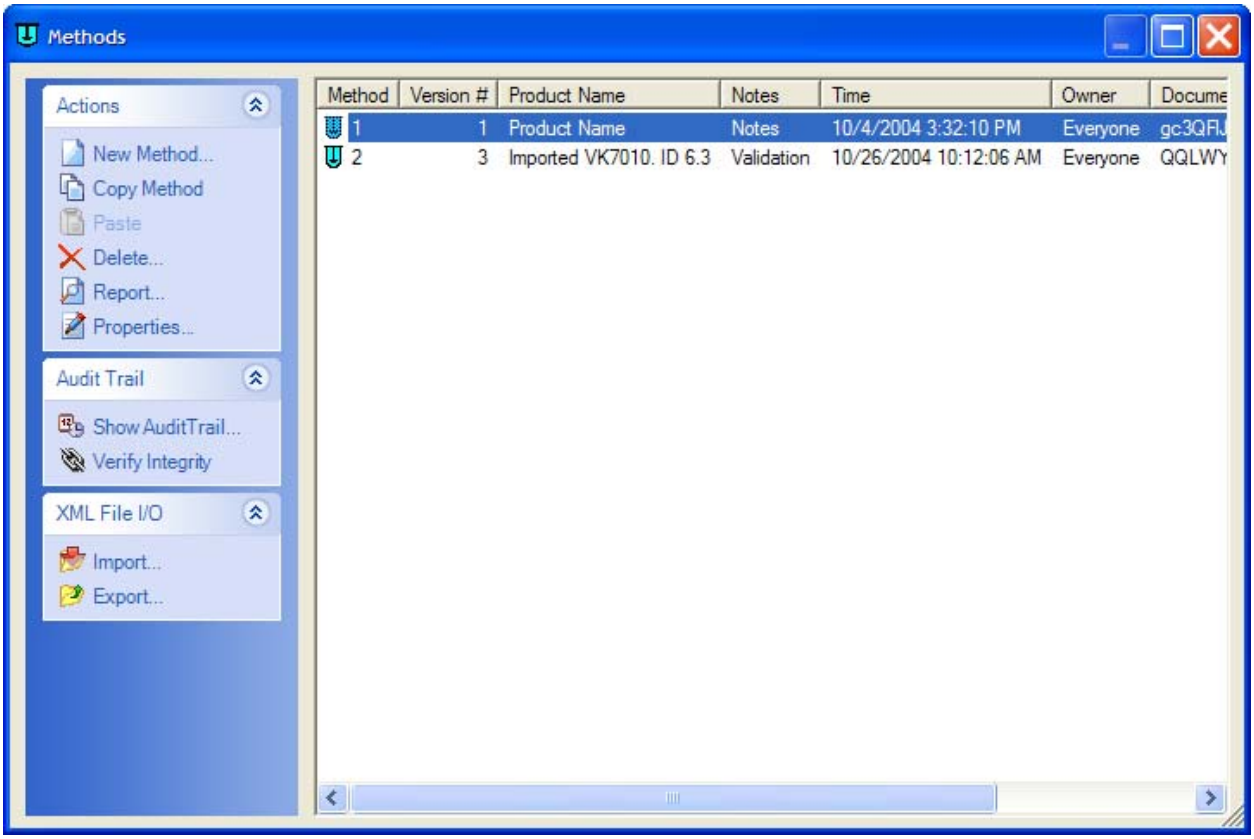


Whenever a change to a system or method is made, the current user is required to document the reason for the change, by making an entry in the following dialog box:



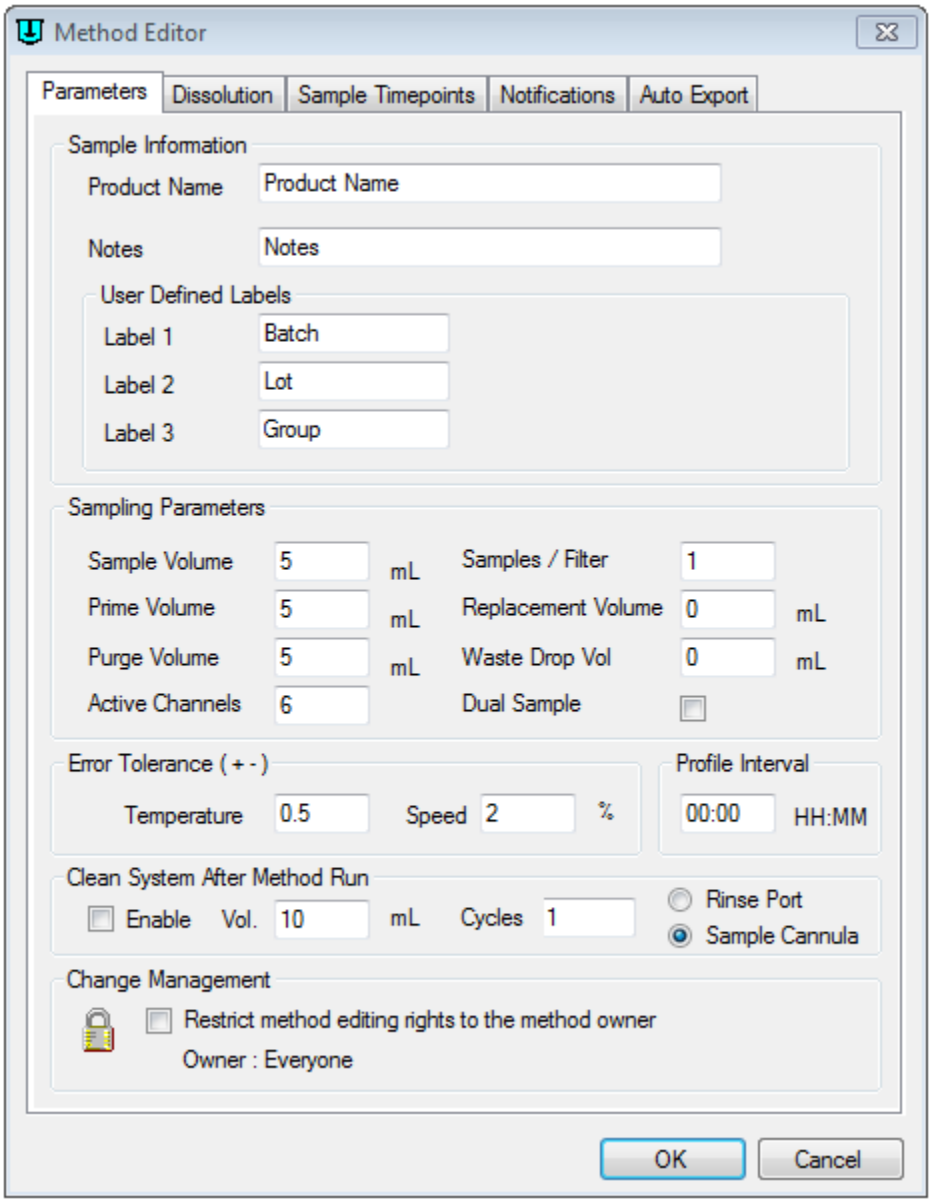
Method Management

The software can store and manage multiple methods. The software does not limit the number of methods. A method is essentially a collection of sample time points, dissolution tester properties and; if configured by the system type; HPLC injection properties.



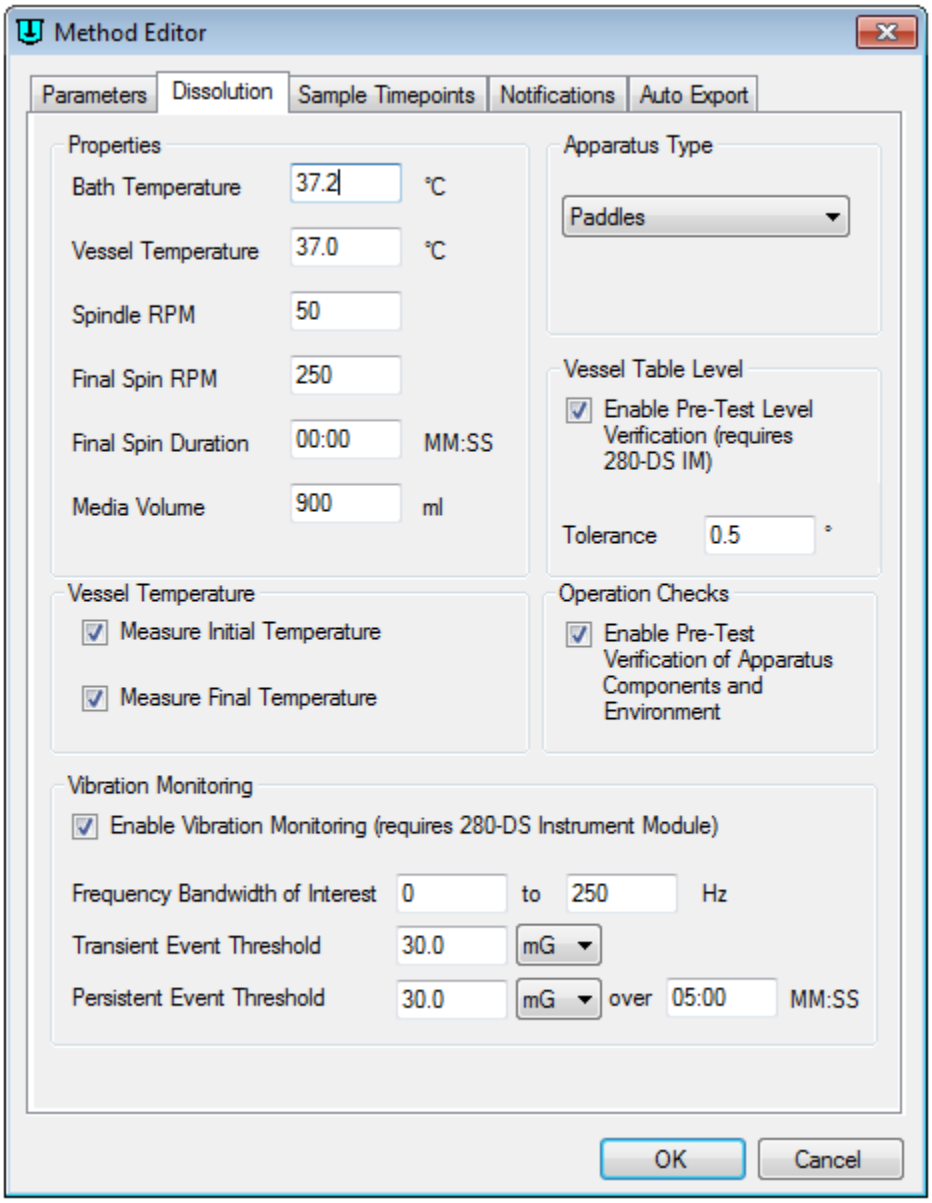
Methods can be created, deleted, modified, or executed by appropriate context menu item selection. Any change made to a method results in a new version. The audit trail feature dynamically determines the differences between 2 or more versions of the same method.

It should be noted that a method or system is never purged from the database when it is "deleted". Its attributes are changed to prevent it from being shown in the method browser.

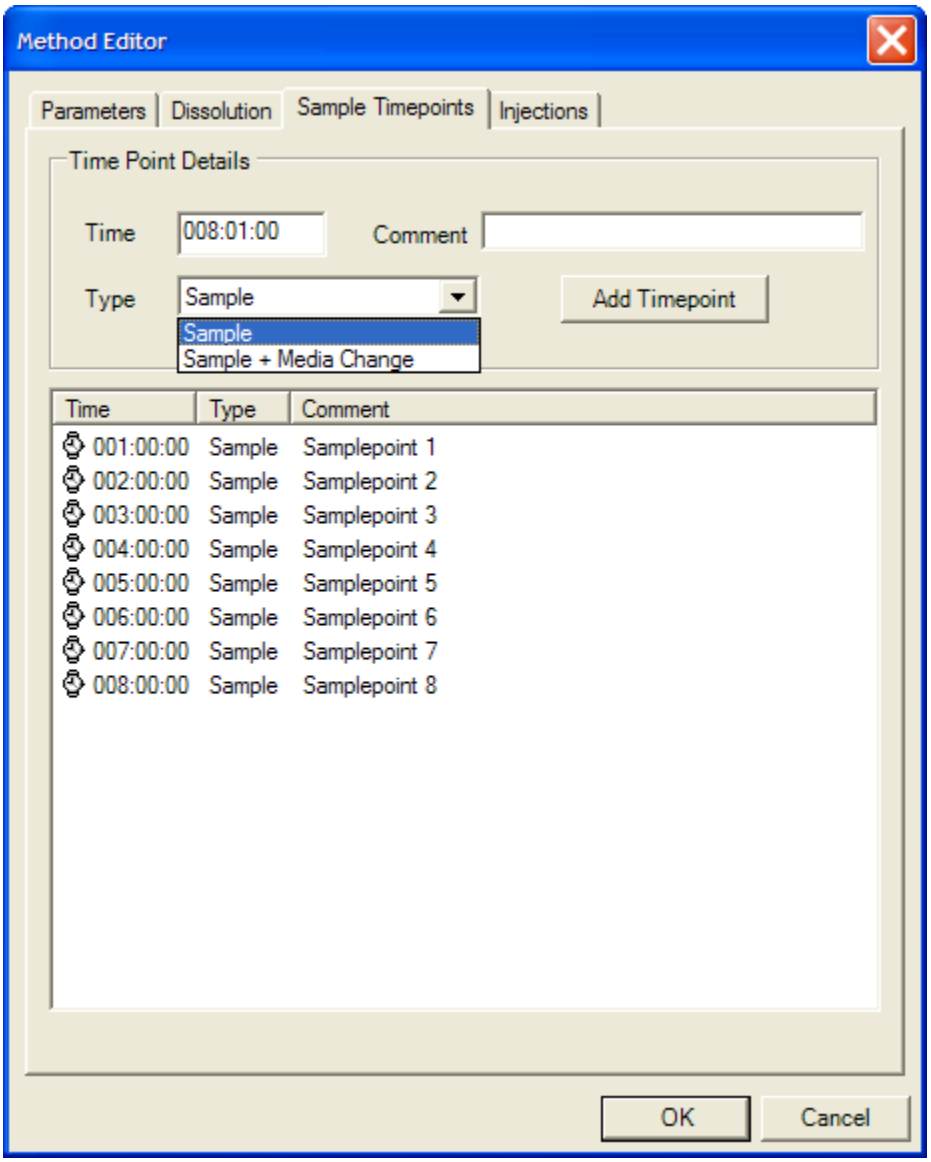


A method consists of the parameters required for a dissolution test. Changes to the parameters are audit trailed using the dynamic audit trail features of the software. The method includes 3 user defined labels (15 characters each). These labels are presented to the user when a method is run to allow the user to enter test specific data at the start of the test that are relevant to the protocols of the user's environment.

Dissolution tester properties essentially 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.

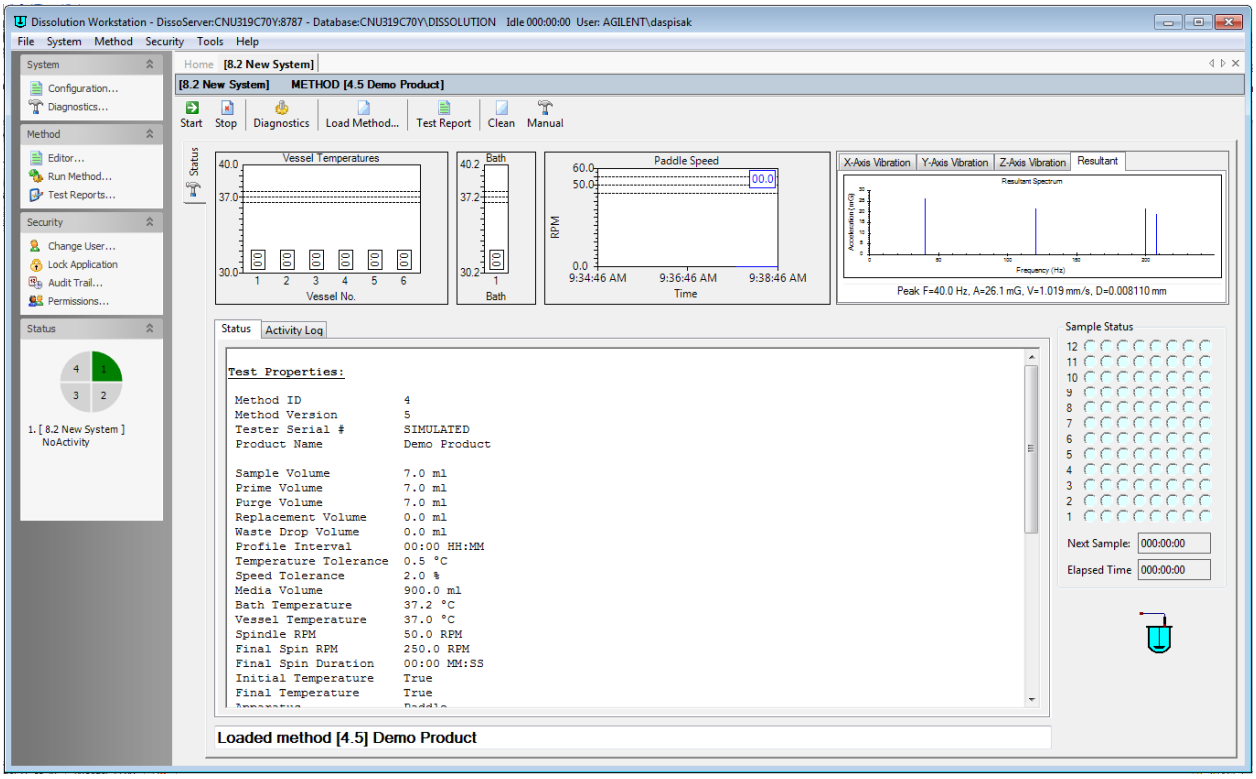


Time points specify the intervals at which samples will be drawn from the dissolution tester. Each sample time point corresponds to a single row in the fraction collector, starting at the first row and moving through to the last row. A special type of time point, Sample + Media Change, causes the system to pause after the Media Change time point to allow the user to change media. The duration of the media change event is recorded to the database during a run.


Method Editor
Parameters
Dissolution
Sample Timepoints
Injections
Time Point Details
Time
008:01:00
Comment
Type
Sample
Add Timepoint
Sample
Sample + Media Change
Time
Type
Comment
001:00:00 Sample Samplepoint 1
002:00:00 Sample Samplepoint 2
003:00:00 Sample Samplepoint 3
004:00:00 Sample Samplepoint 4
005:00:00 Sample Samplepoint 5
006:00:00 Sample Samplepoint 6
007:00:00 Sample Samplepoint 7
008:00:00 Sample Samplepoint 8
OK
Cancel

Method Execution

When a method is run on a particular dissolution system, the software records the method parameters used as well as temperature measurements and the times at which samples are drawn. The entire process is automatically recorded to the software database and the user is shown status information as the software progresses through each time point.

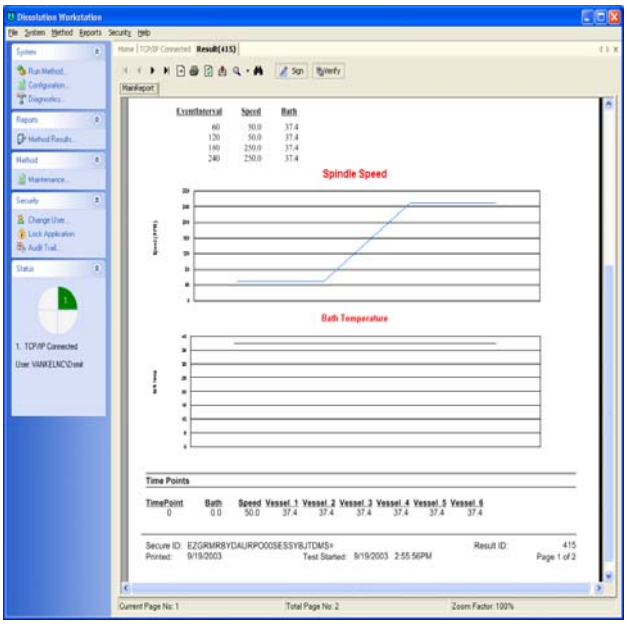


Test Reports

Once a method 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 Part 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.

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.



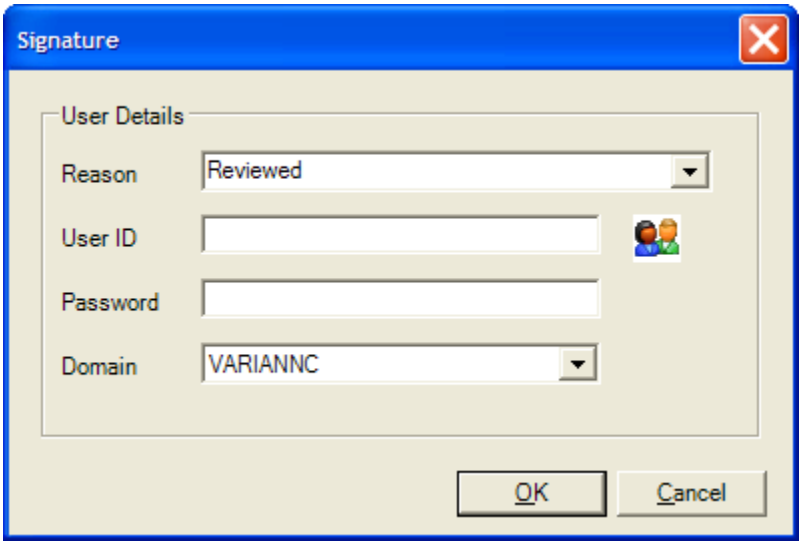
If an application other than the Dissolution Workstation software modifies the database, then this function will fail and the user will be notified.

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 Part 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.



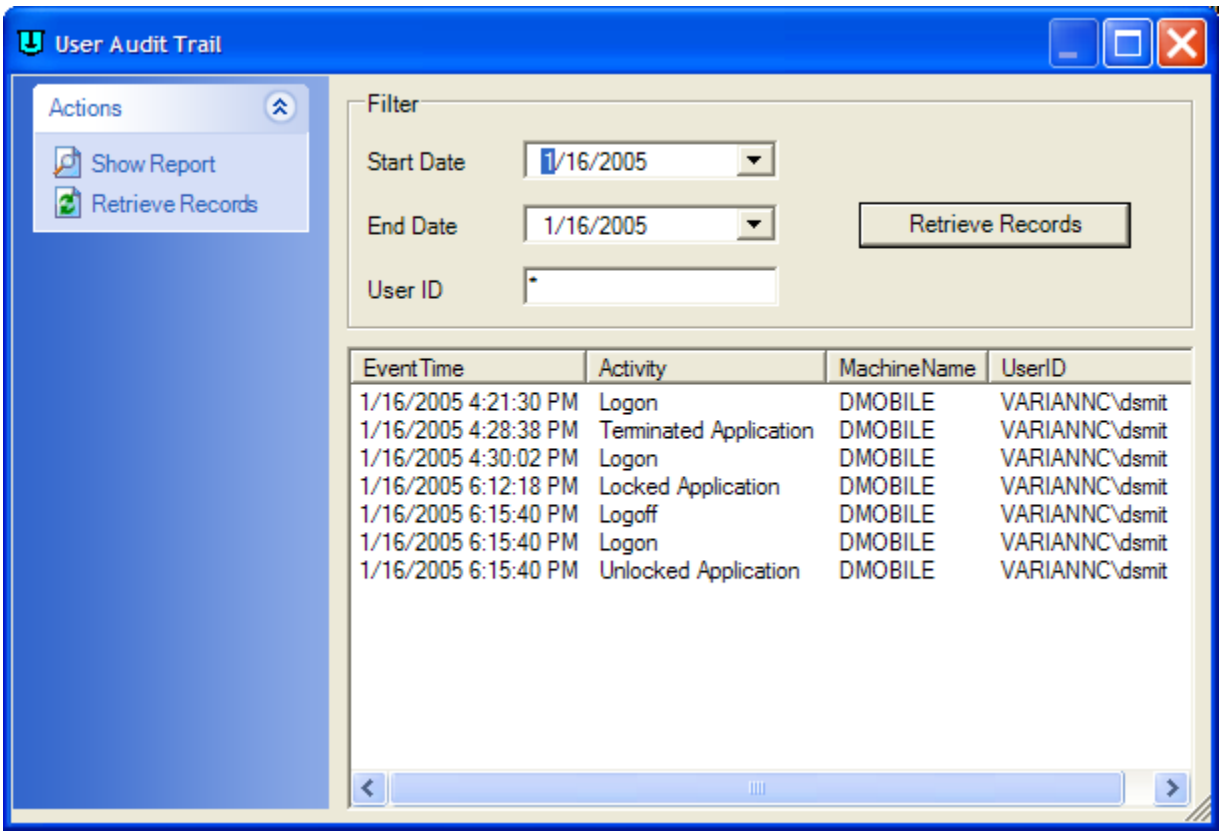
Once a signature has been added to a set of results, "*the signature cannot be excised, copied or otherwise falsified by ordinary means"* as required by section 11.70. Electronic signatures are permanently linked to the results. The Dissolution Workstation software always requires the signature to be executed using all the signature components.

Any attempts to sign a set of results using an invalid user ID, password or any combination thereof that is incorrect is automatically recorded to the system audit trail.

Security Audit Trail

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

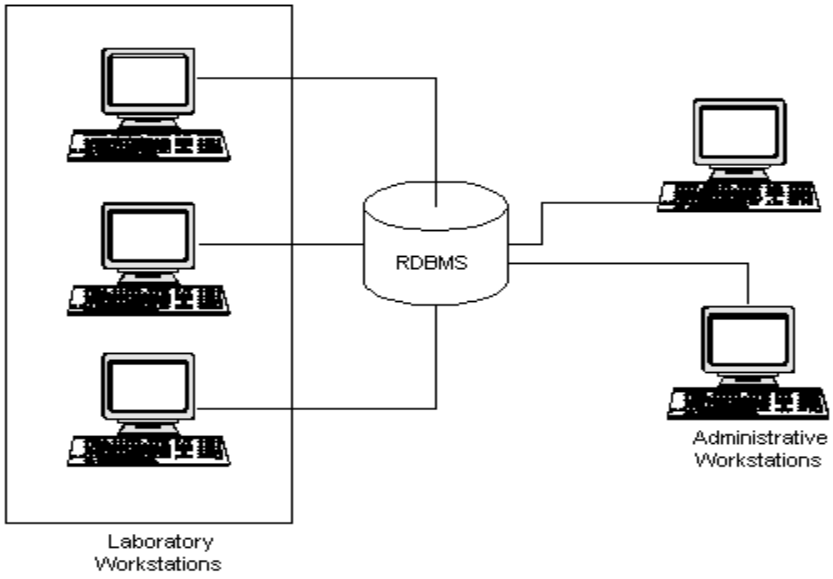
- Dissolution Workstation Logon/Logoff events
- Data verification errors
- More than 3 successive password/ID failures. (NOTE: the Windows security log should always be consulted since this is the primary source for this information when the Security Policy has been set correctly).



Database Configuration Options

The Dissolution Workstation installation automatically creates a local instance of the Microsoft Data Engine (MSDE). This database is the default selection for a workstation. However, it is possible to designate another database on the network has the source for method and system configurations, and for storing 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 in order 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.

If a single MSDE database is designated as the central database for a number of workstations, please keep in mind that the MSDE database becomes significantly slower when multiple concurrent connections are active (this is by Microsoft design). This can be overcome by purchasing Microsoft SQL Server with the appropriate number of connection licenses.

Managing Multiple Dissolution Systems from a Single WS

The dissolution workstation was designed to simultaneously control up to 4 sets of dissolution and injection equipment from a single workstation. Equipment can be connected in a variety 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 USB port extender by Edgeport is the recommended way to extend the PC's connectivity.

USB Dongle

The software is 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 interface to instruments without the dongle.