

## AA and ICP-OES

## Key Capabilities

- Multiple user levels
- Login/password support provided by Microsoft® Windows®
- Method (and IEC or MSF files in the case of ICP) saved with the data in the results database
- Reprocessing doesn't change stored data
- Master event log records all significant actions performed by each user
- Files and data objects are automatically assigned version numbers and changes between versions are recorded
- Old versions of files or data objects are automatically moved to a history directory

## WinLab32 for AA and ICP – Enhanced Security Option

### Introduction

WinLab32™ for AA and ICP redefined the software standard for high-performance instrumentation for inorganic analyses. Now an Enhanced Security™ version is available which meets the special needs of highly regulated labs such as those that must comply with the U.S. FDA's 21 CFR Part 11 regulations.

### Basic WinLab32

The basic WinLab32 package includes a number of features designed to help today's laboratories cope with regulations mandated by government agencies or quality protocols. Features for this purpose included in this version of WinLab32 include the following:

- WinLab32 leverages the powerful security features of Microsoft® Windows® to provide the protection your laboratory needs. Personnel can be divided into groups with each group assigned a level of permission. The "administrator" group can install and configure the software and perform any WinLab32 task while other groups may be restricted from performing certain tasks. With WinLab32 software you define the groups and permissions assigned to each – passwords control access (Figure 1).

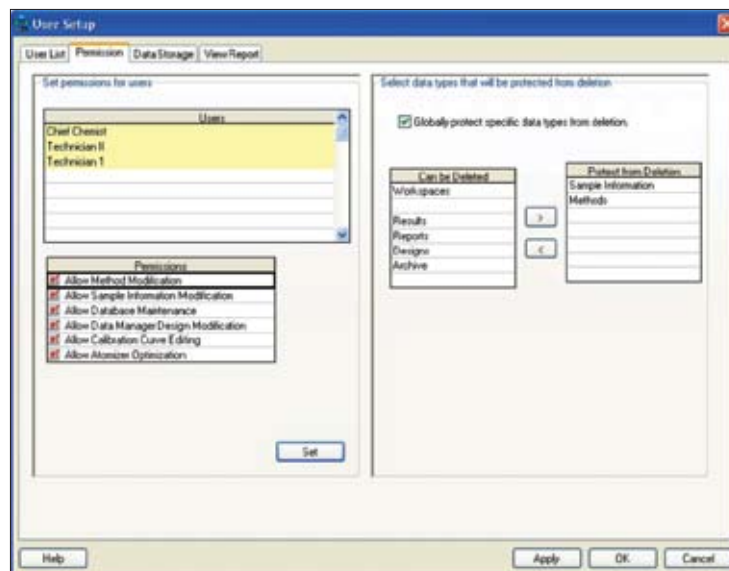


Figure 1. WinLab32 User Setup utility.

- Different users can access the same or different files such as method databases or sample information files as determined by the system administrator. Files can be located on the instrument controller or on other computers connected to the controller across the network.
- WinLab32 “signs” its data. When data are saved from an analysis, a proprietary check sum is also computed and stored in the database – all transparent to the user. If anyone alters the data after it is saved, for example by altering the analysis time or changing the concentration value, this alteration is readily detected using a command in the Data Manager.
- WinLab32 saves a copy of the method (and IEC or MSF files in the case of ICP) used to acquire the data along with the data in the results library. This provides an audit trail of the conditions used to perform the analyses.
- Reprocessing doesn’t change the data stored, but rather new data are written to the results library along with a notation stating that the data represent reprocessed data rather than original data.
- WinLab32 software meets 21 CFR Part 11 requirements for a closed system.

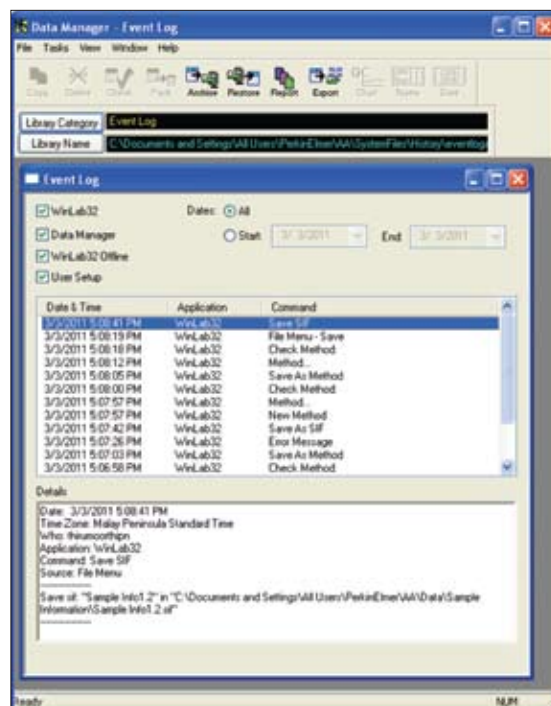


Figure 2. Viewer for the Master Event Log.

### Enhanced Security option

The Enhanced Security option adds the additional capabilities needed by highly regulated laboratories, such as those operating under the rules of 21 CFR Part 11. These additional capabilities supplement the features in the basic WinLab32 package and include the following:

- The software maintains a Master Event Log that records all significant actions performed by the user. Each entry includes the date and time of the action, what was done, the name of the user, and, in many cases, the reason the action was performed. This event log can be viewed or printed using the Data Manager (Figure 2).
- The software automatically adds version numbers to all files and data sets, records the changes between versions, and automatically moves old versions to a history directory. Changes can be viewed using the Data Manager (Figure 3). The software restricts all users to choosing file names from a common pool. In this way, files are uniquely identified across the system, regardless of the analyst creating or using them.
- The software includes options to prevent analyses from being performed without saving data and to allow analyses only with saved methods. These restrictions ensure that a proper audit trail is maintained for all activities.

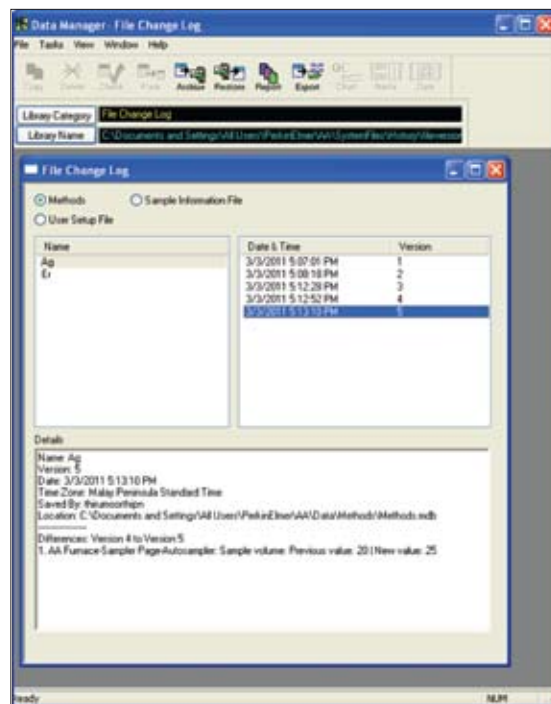


Figure 3. Viewer for the File Change Log where differences between versions of files and data objects are displayed.