NOTICE: This document contains references to Varian. Please note that Varian, Inc. is now part of Agilent Technologies. For more information, go to **www.agilent.com/chem.**

Agilent Technologies

Varian, Inc.
2700 Mitchell Drive
Walnut Creek, CA 94598-1675/USA

Access Control and Audit Trail Software

Operation Manual

QUALITY SYSTEM
ISO 9001
CERTIFIED

03-914941-00:3

Table of Contents

Figures

Introduction

Access Control and Audit Trail software documentation

The optional Access Control and Audit trail software for Star workstation version 6.0 and above is designed to help the customer meet the requirements of 21 CFR 11. The documentation for this software is divided into three main parts.

1. This manual, the operator's manual, presents all of the features, which relate to access control and audit trail software. This manual will be useful mainly for those who act as administrators for the Star software and those who are tasked with writing SOPs for the proper compliance with 21 CFR 11. It contains detailed information about the software.

2. The electronic manual on the Star CD has been updated to include all of the changes to Star 6.0 and above that would normally be seen by someone who does not have the optional software.

3. The Setup and Documentation manual contains information about installation and initial start up of the Access Control and Audit Trail software, typical SOPs that could be used with the software, information on how we validated the software, how a customer can perform a limited on site validation and training material to help an administrator learn the software.

Software System Description

Overview of the Access Control and Audit Trail Software

The Varian MS Workstation is based on the Varian Star Workstation Software. In this document, 'Star' is used as a generic term to refer to either set of software.

The Access Control and Audit Trail software is available as an option for Star and MS Workstation Software. The features of this software are designed to help a user meet the requirements of the 21 CFR 11 regulations. This manual applies to Star versions 6.30 and above.

Software Organization

Star Access Control and Audit Trail software is divided into two parts. The first part is the security administration software. This software allows an administrator to identify users of the Star workstation software and designate what capabilities they will have when using the software. The Workstation Software has been modified to limit access to various functions as set by the system administrator.

The second part of the Access Control and Audit Trail software is modifications to the standard Star software to create a system audit trail, applications locking, file security and versioning capability for methods and data files. These capabilities are fully integrated with Star 6.0 and above software.

Star 6.0 and above software addresses electronic signatures using Adobe Acrobat or some other third party software. Acrobat can be installed with Star and reports can be printed to

Acrobat Distiller. Once in .PDF format, the capabilities of Acrobat can be used to electronically sign documents.

Definition of Terms

The following terms are used in the Star software and the Star manuals. Although most of these terms are common to other software, it is best to review the individual terms to make sure that their exact meaning is understood in the context of Star 6.0 and above software.

Rights: Rights are permissions that are assigned to a particular individual to do specific actions. They are assigned to a particular user or a group of users in the context of a specific project. For example, an individual can be assigned the right to run methods in a particular project and the right to modify methods in a different project. Rights are additive. If a user is assigned the right to build a method in one project and is assigned the right to run methods in that project based on their membership in a group, then they have the right to do both.

Implied Rights: The application of one right may also imply the application of other rights. For example, if a user is allowed to *modify a method* then it is implied that the user has the right to *view a method*.

Users: A user is a specific individual who has been identified in the system.

Groups: A group is a collection of individuals who, after being individually defined, are grouped together for the purpose of assigning rights. For example, several users can be grouped together as chemists and given the right to run methods in a particular project. Assigning rights by groups speeds up the process and provides consistency. One user can be part of several different groups.

Administrators: Administrators are a specific group of users who have the right to access the Security Administration program. There is always a default administrator with a login of admin, which cannot be deleted. Users who are assigned to the group Administrators can be assigned to other groups as appropriate. Users can be assigned as administrators themselves without being assigned to the group “administrators”.

Projects: Projects are the key element connecting users and instrumentation. Any number of projects can be created on the security system. Users or groups of users are assigned rights based on projects. Instruments and workstations are assigned to projects. This allows users to run the instruments associated with their projects.

Global Project: The global project is a special project, which is associated with all of the instruments on the security system. When a user has rights on the global project, these rights apply to all instruments in individual projects WITH WHICH THE USER HAS BEEN ASSIGNED. For example, if a user has the right to run standards and samples on the global project, they will have this right on any project to which they are associated. Users are associated with a project by "applying rights" to them on that project from the user or group screen.

Workstation: A workstation is a computer which has Star workstation software running on it. This workstation can be named. In addition it has an ID as part of the system. Identifying hardware on the PC itself generates the ID number.

Instrument: An instrument is a single module or a set of modules configured onto one of the instrument configuration screens of each workstation. The Star workstation can have either a one-instrument or a four-instrument configuration. Not all of the instruments on a workstation must be configured. An instrument is identified by a combination of its position on the configuration screen and the workstation on which it is configured.

Private and Public Locks: The system is locked when anyone who wishes to interact with the system must enter a login name and a password. When the Star system is first started or when the Security server is first started, they are public locked.

A public lock is a lock that anyone with permission to use that function of the system can open. For example, if you have the right to run a sample, then you have the right to open and run system control. If no one had previously started system control, it is public locked and you must login with a valid login and password to run it. The purpose of a public lock is general system security.

A private lock is a lock that only the person who has previously logged in and someone with a special right to convert a private lock to a public lock, can open.

The purpose of a private lock is to make sure that no one else modifies the work that you are doing. If you have started an automated run on instrument 2 on a particular workstation, you can private lock this instrument. Then, if anyone else comes up to the system, they will not be able to access that instrument even if they have the rights to run that instrument.

If someone private locks a system and then leaves, there must be some way to unlock the system so that someone else can use it. Either an administrator or someone who is given the right to open private locks can do this. This may be all of the lab supervisors or some other designated persons. That person can convert a private lock to a public lock. Once the application is public locked, anyone who has rights on the system can log in and use the system within the limit of their rights.

Security Database: The security database contains all information about users, groups, projects, workstations and instruments. In addition, it contains all of the reasons which the administrator has built using the security administration software.

Security Audit Log: The security log is the audit trail for the security database and the Administrative software.

Security Server: When Access Control and Audit Trail software is loaded with Star version 6.0 or above, security can be controlled either through the workstation on which the software was loaded or through a workstation on the network. The point of control is determined by the location of the security server. The security server is the workstation on which the security database is located.

Flow of rights in the Star Software

The organization of the administration software can be visualized as shown in Figure 1.

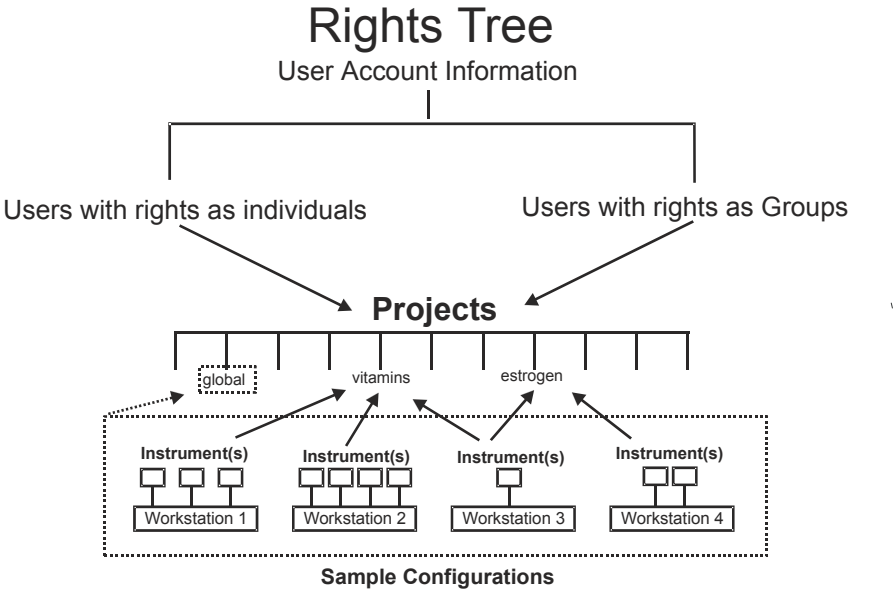

Figure 1 The relationship of users, group and their rights with instrument and workstations through projects.

The general flow of work in the security software is as follows:

1. Projects are created
2. Individual users are identified through user account information
3. Users are assigned rights either individually or through their inclusion in groups FOR A PARTICULAR PROJECT
4. Workstations are identified and they are associated with the instruments that are attached to them.
5. Instruments are assigned to one or more projects. Users given rights on those projects (and the global project) will get rights on those instruments.

Security Administration software

Overview of the Security Administration software

Scope and Purpose

The purposes of the security administration software are as follows:

The software allows the system administrator to create projects to connect users to instruments.

The software allows the administrator to identify workstations and the instruments associated with them.

The software allows the system administrator to create and delete system users

The software allows the system administrator to assign each user an individual set of rights.

The software allows the administrator to associated individual users with instruments through projects.

The software allows the system administrator to customize the system characteristics relative to system security

The software alerts the system administrator to any attempted breach of security, whether intentional, accidental or due to a lack of system understanding

The software, in conjunction with appropriate SOPs, helps the system administrator maintain compliance with 21 CFR 11 and other regulations.

Software organization and preliminary activities

The security administration software is a separate and distinct software package from Star software. Only a person designated as an administrator can access it. All changes to the security administration software are logged into a separate audit trail, which is visible only to an administrator. It does, however, set the rights that individuals have to access all parts of the Star workstation version 6.0 software.

Loading the Star Access Control and Audit Trail software is covered in a separate document. Before the software is initially installed, one or more individuals should be designated to perform the task of being an administrator for the system. If the Star security server is on a single machine, the Star administrators should be identified as at least a power user on that machine. If the security server is on a network computer, the administrators must be at least a power user on the network. Note, for Windows 2000 and Windows NT, the individual who installs that software will have to be designated as an administrator.

Figure 2 Security Administration Software Icon

To initially access the security program, click on the security icon on the Star menu bar. When you do this, a dialog box will appear as shown in Figure 3.

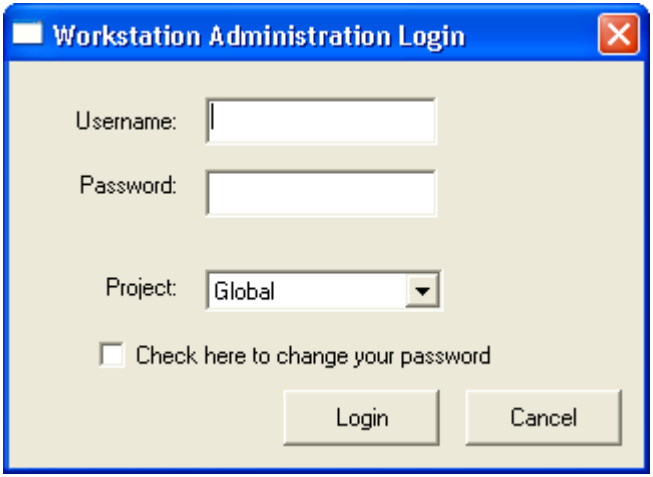

Figure 3 Logging into the Security Administration Software.

The default username is **admin** and the default password is **chrom**. You should leave the project as global project. **Once you have logged on as the default administrator, you should change the password for the default login and preserve that information in a secure place.**

If the Star security database provides security for more than one workstation, you will automatically be connected to the database when you log into the security administration software on any workstation attached to the database.

The Security Administration software

Once you have logged onto the security administration software you will see the following screen. Note that entries have been made on this screen to show examples of what could be entered. Entries on individual screens will either come up with a preset or blank as described in the tables listed below.

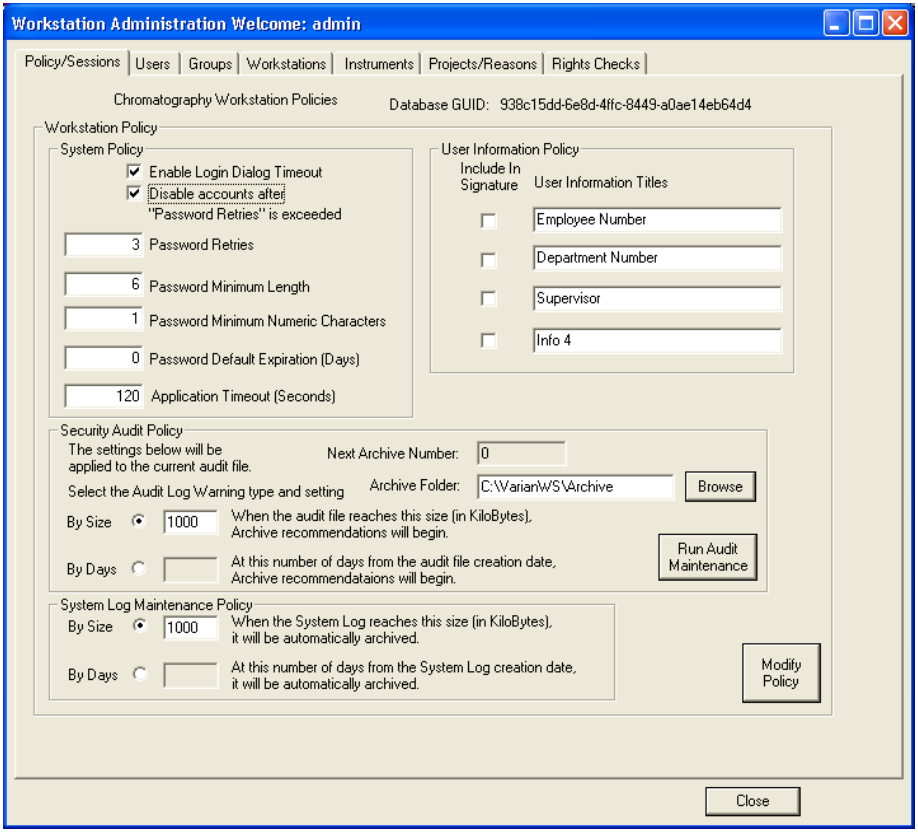

Figure 4 Policy/Session Screen of the Security Administration Screen

There are seven different sections included in the security administration software.

Policy/Sessions

This section allows an administrator to set the general policies for administering the security system. The values used should be set in the organization SOPs.

This section allows an administrator to see who is using the system at the present time

This section also allows the administrator to query the Administrative audit trail to determine what has been done on the system previously.

Users

This section is where user identification is created. The user login, password and user name are all entered here. This is also the place where users are given individual rights. Each user login creation is given a unique large number for positive identification.

Groups

In order to make the assignment of rights easier for a large number of users of a network based system, the group page lets an administrator create groups, which have a set of rights. Then individuals can be assigned to one or more groups and get the rights that are assigned to that group(s).

Workstations

Each workstation can be named and individually identified, and the location where it is getting the security information can be specified.

Instruments

Each workstation can have 1 to 4 instruments associated with it. Each instrument is numbered based on the number in the workstation. Each instrument is associated with one or more projects.

Projects/Reasons

Any number of projects can be created. These projects form the basis for the assignment of rights.

Also preset reasons for actions can be entered. These will be available throughout the software for entry into audit trails making it easy to enter a reason for individual actions.

Rights Checks

The rights check section allows an administrator to check what rights any particular user has and to find out how they got those rights.

Overall, this software allows the administrator to assign rights to individuals and groups of individuals based on projects. It also allows the administrator to assign particular workstations and their associated instruments to different projects**. Careful management of projects is key to having the Security Administration Software provide the appropriate access and security for your laboratory.**

Note: In all cases, entries into a particular field will not automatically change the value of that field. A second button must be depressed (such as the modify policy button on the screen above) to have the system accept the entries. Also, for most entries, a reason will be required when an entry is changed. This is explained in detail on the workstation/reason screen.

Note: When an entry has been changed but the user has not yet accepted the change, an entry in the upper right hand corner of the screen or section of screen will read, “Changed”. These changes can be accepted by pressing the appropriate buttons. They can be rejected by exiting the screen and not accepting the changes.

Entering Reasons for Changes

Every time that you make a change to any entry in the Administration software, you will be asked for a reason. An example of this is shown in Figure 5.

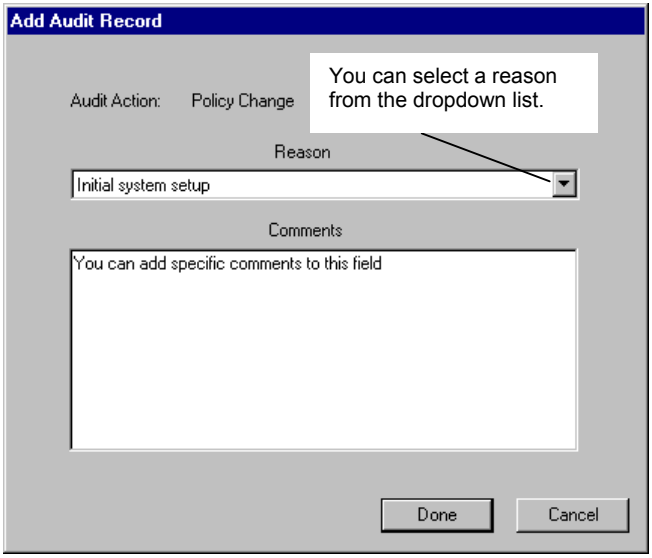

Figure 5 Request for reason for making changes.

You must select one of the predefined reasons from the dropdown list, or enter a comment, or both.

Policy/Session Screen Entries

Overview

The Policy and Sessions screen (Figure 4) lets you set global policies for all of the Star workstations attached to the Star security database. These policies apply to all workstations and instruments, which are configured from this software. The sessions screen applies ONLY to the workstation on which you are current working.

Individual Entries

Entry	Range of values	Meaning
Enable Login Dialog Timeout	Check/Uncheck	If this is checked, there is a timeout set on the login screen. When a user tries to access a function on the Star system, which requires a login, the login screen will stay up for only 2 minutes. If a login has not been attempted in this time, the screen will automatically close. This will not be considered a failed login even if the user name has been entered.
Disable accounts after "Password Retries" is exceeded	Check/Uncheck	If checked, when someone has tried to login on a particular account and failed consecutively greater than the number of times listed in the Password Retries entry below, the account will be disabled. It will not respond to an attempted login even with the proper name and password. This occurrence will be recorded in the audit log for the administration software and an Alarm will be activated. An administrator can reactivate an account without having to create a new account. If a successful login has been accomplished on that account before the limit is reached, the count will be reset.
Password Retries	1 to 99	This is the number of consecutive incorrect login attempts that can occur before the account is disabled. These login attempts can be separated in time. If a correct login is accomplished, the count is reset.
Password Minimum Length	0 to 20	This is the minimum length of password that will be accepted when a new account is created or when a new password is entered for an old account. The minimum length of password should be set by corporate SOPs. Passwords greater than 5 characters are recommended. If this number is changed, all previously recorded passwords will be accepted but all new passwords will have to meet these requirements.
Password Minimum Numeric Characters	0 to 20	This is the minimum number of numeric characters that must be in a password. If this exceeds the minimum password length, then by default, this will become the minimum password length.
Password Default Expiration (Days)	0 and 1 to 999	This is the number of days from the day that a new password was created, that it is valid. Entering 0 means that passwords will always be

Entry	Range of values	Meaning
		valid. Entering a number will cause the system to begin to prompt the user to change their password 5 days before the expiration date of the password. After a password has expired, the system will not let a user log in until their password has been changed. This entry can be modified for each individual system user on the User screen.
Application Timeout (Seconds)	0 and 1 to 999	This is the length of time that an application will remain open without any activity from the user before it is public locked. If a user mistakenly leaves a workstation without logging out or private locking the system, whatever application they were using will automatically become public locked so that no one else can use the application under a false login name.
User information Titles	31 characters	These titles are used on the Users page to remind the administrator what information should be added to the user profile.
Include in Signatures (Up to four entries can be checked)	(Check)	When this is checked off, the particular information about the individual user will be displayed whenever the users name is displayed. This includes such things as electronic signatures etc. **At present, internal electronic signatures are not implemented.**
Audit Log warning by size	Check and 1 to 9999 Kbytes	This is the size of the administrative audit log file that will cause the system to give an administrator a warning that they should archive the audit log file. The file size is indefinite but it is easier to manage the files if they are archived periodically. This warning will occur without concern for the number of days since the last audit file was archived. This is not the number of entries in the log but the actual file size. The Audit log will NOT archive automatically. An administrator must archive it.
Audit log warning by days	Check and 1 to 999 days	This is the number of days since the last administrative audit log file was archived when reminders will begin to occur to archive the present file. These are reminders only. They will not require the administrator to archive the file. The Audit log will NOT archive automatically. An administrator must archive it.

Entry	Range of values	Meaning
Next archive number	0 – 999	This is number of the next security archive. The archives are numbered consecutively from 1. The number cannot be entered or changed.
Archive Folder	(Any location on the PC or an attached network)	This is the location in which the security archive will be stored.
System log maintenance policy - Size	Check and 1 to 2550 Kbytes	This is the size at which the system log on this workstation will automatically create an archive of the present file and create a new system log. This is automatic. The administrator does not have to manually archive the system log.
System log maintenance policy - Days	Check and 1 to 255 days	This is the number of days that will elapse before the system log on this workstation will automatically create an archive of the present file and create a new system log. This is automatic. The administrator does not have to manually archive the system log.
Modify Policy	(Press)	The policies that have changed will not take effect unless you click this button. After you press the button, you will be asked for a reason for this change. You can cancel policy modification if you want. You can always tell whether any policies on the screen have changed by looking in the upper right hand corner of the screen. It will display the word “Changed” if any policy has been changed and not already accepted.
Run Audit Maintenance	(Press)	Clicking this button will allow you to examine the administrative audit log Once you have done this; you can search the audit log for particular entries, archive the audit log or print a copy of the audit trail. You will also clear any Alarms from this screen. This is described in more detail in the section on the administration audit log.

User Screen Entries

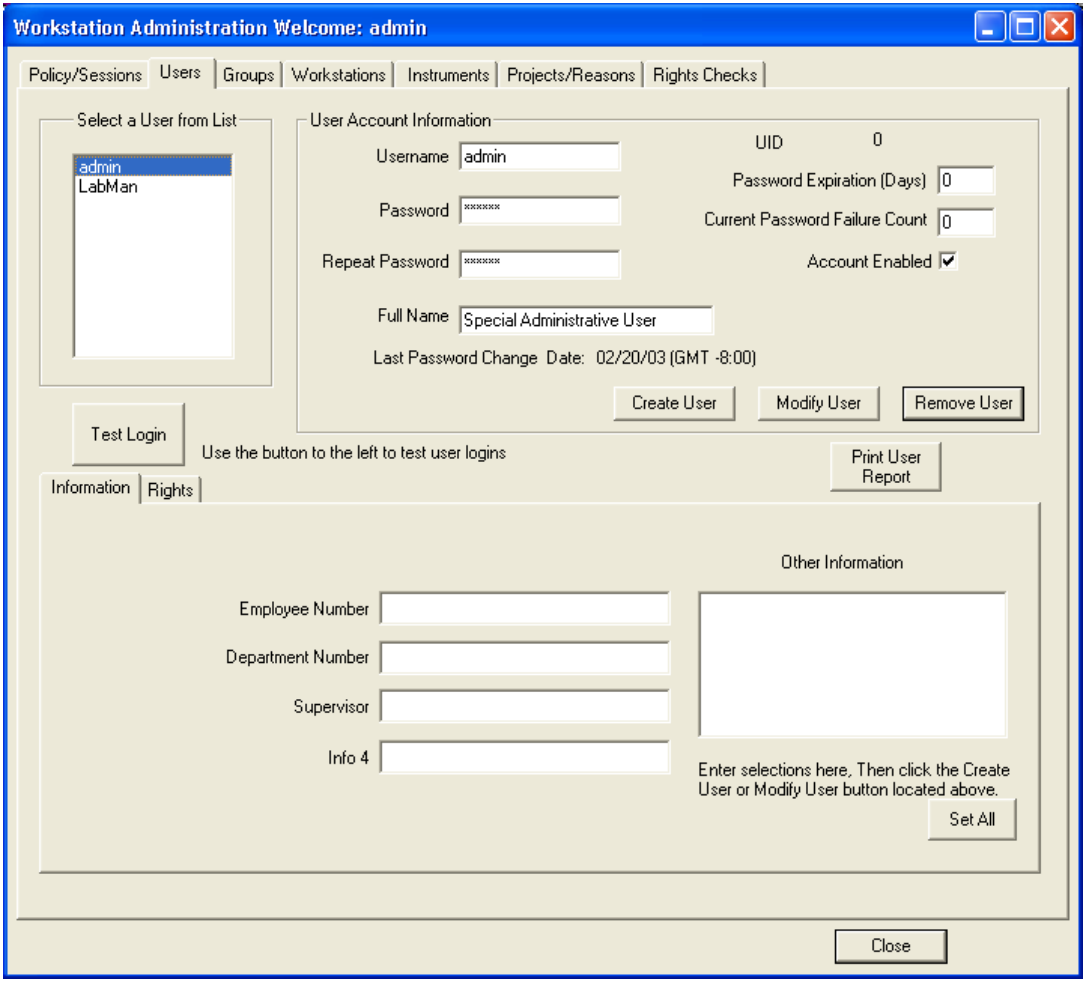

Figure 6 Users screen – User Information Displayed

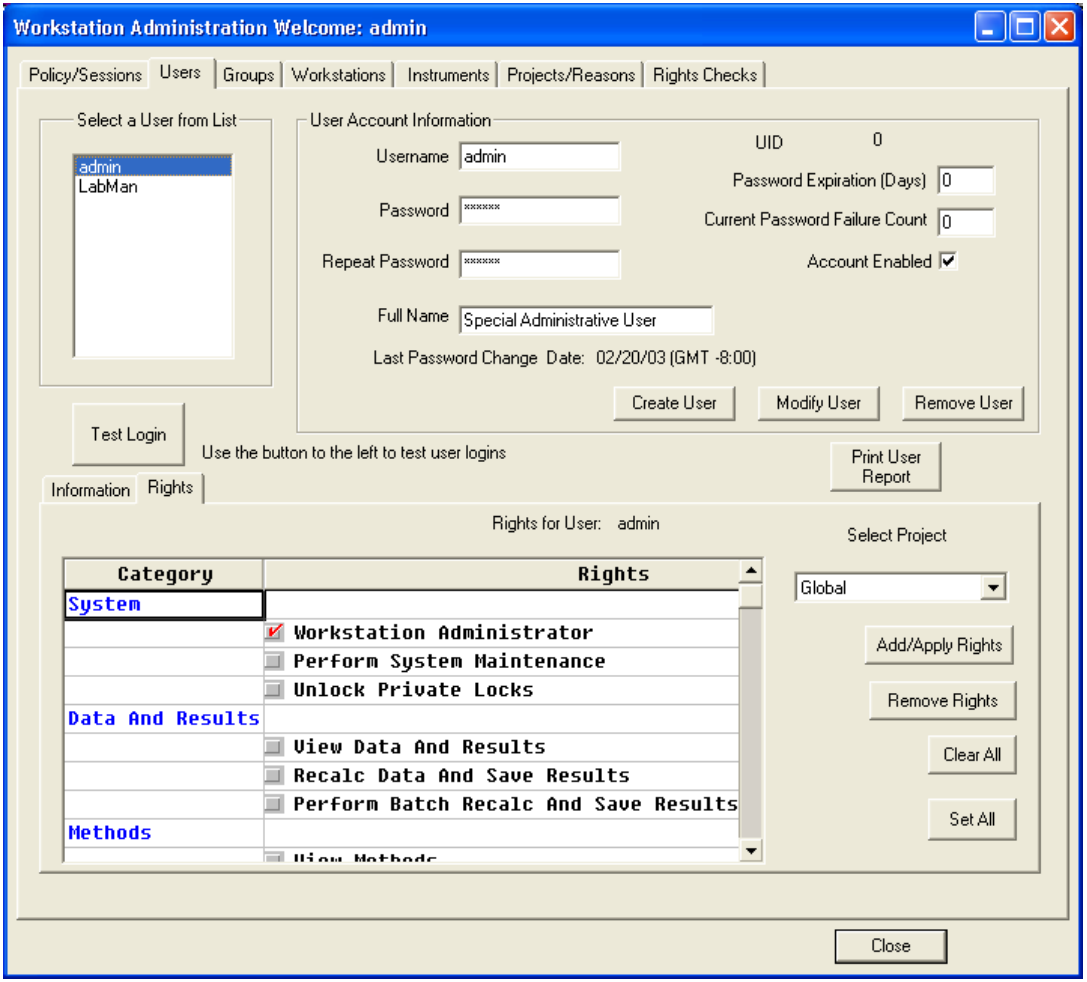

Figure 7 Users screen – User Rights Displayed

Overview

The users screen allows the administrator to enter information about an individual user. It also allows the administrator to give rights to a particular individual on any of the projects.

New users can be created here by filling all the entries in the User Account Information, then pressing the Create User button.

Individual Entries

Entry	Range of Values	Meaning
Select a user from List	Any previously entered user	This will allow you to select an existing user whose individual information or rights you can modify.
Username	1 to 15 characters	Log in name for the user. This can be anything that follows company policy. To add a new user, you type in a new name here.
Password	1 – 20 characters, must meet previously set policy for minimum characters and numbers.	This is the password that a user will enter in order to log in to the Star system.
Repeat Password	Same as password	This allows a user to confirm their password.
Full Name	0 to 18 characters	This should be the full name of the user, as he or she would sign their name.
Last password Changed Date	(Date)	This is the last date a particular user changed their password.
UID		The user ID is a large alphanumeric string that is automatically created whenever a new user is created. This number cannot be changed. It can be used to distinguish two users who have the same name or other information.
Expiration (Days)	0 and 1 to 999	When a new user is created, the password expiration period set in the policy screen will automatically be entered in this field. If the administrator wants to change the value for a particular user, it can be changed here using the modify user button. A zero value means the password will never expire.

Entry	Range of Values	Meaning
Current password failure count	0 to 99	This is the current number of times a particular user has tried to log in and failed.
Account enabled	(Check)	The administrator can enable or disable accounts as necessary. If an attempt has been made to access an account with the wrong password more than the consecutive number of times set in the policy section, the account will automatically become disabled.
Create/Modify/Remove User	(Press)	All entries must be validated before they are accepted.
Test Login	(Press)	When a new user has been created, this can be used to test that the user is active in the database.
Print User Report	(Press)	This can be used to print a report documenting the rights of the selected user in existing projects.
Information tab Fig. 4		
Specific information	31 characters	These four entries have prompts that were set in the policy section. This will help the administrator remember what information about the user should be put into these sections. This permanently attaches the information to the user in the security database.
Other information	127 characters	This is other information about the individual user. All of this will help the administrator positively identify the user in case of later question.
Rights tab – figure 5		
Select Project	Project names	This specifies which projects are associated with these rights for this individual. An individual can have different rights on different projects. Rights assigned under the global project apply to ALL projects with which the user is associated. It is necessary to associate an individual with a project even if their rights are going to be generated through the Global project. Selecting Add/Apply rights with the appropriate project selected will do this.

Entry	Range of Values	Meaning
Add/Apply Rights	(Press)	This will adjust the rights for an individual on a particular project to those selected in the rights table. This can both add and remove rights depending on what is checked.
Remove rights	(Press)	This will remove ALL rights from the selected account for the selected project. This will not remove rights from the Global project.
Clear all	(Press)	This will remove the checks from all of the boxes in the rights table. It does NOT apply the change.
Set All	(Press)	This checks all the boxes in the rights table. It does NOT apply the change.
System	N/A	Rights Category – **Note that the rights in this Category can only be granted in the Global Project.**
Workstation Administrator	Yes/No check	This allows the user access to the security administration software to perform all tasks associated with the software. An administrator can also unlock private locks. This right can only be assigned to a user on the global project. Note, this is not the same as being an administrator on the Windows NT or 2000 system.
Perform system maintenance	Yes/No check	It will also allow the user to add software to the Star system, update software or remove the software. This right will also allow the user to “repair” files. For example, if a method has been used with an older version of an instrument driver, and a newer version is installed, the method will be automatically updated the next time it is opened in method editor or run in system control. However, this modified method will no longer have the proper check sum attached. The user will be notified of this. If the user has the right to perform system maintenance, they can correct this. This right can only be assigned to a user on the global project.
Unlock private Locks	Yes/No check	This will allow the user to unlock a private lock. A user creates a private lock when they do not want anyone modifying what they have done on the system. The same user can login again. No one else can login.

Entry	Range of Values	Meaning
		However, someone with this right can turn a private lock into a public lock and then allow anyone with the right to access the software, to do so. Note, this right does not assume that the user can access any particular part of the software. This right can only be assigned to a user on the global project. **All administrators have this right. See the section on private locks for more information.**
Data and Results	N/A	Rights Category
View Data and Results	Yes/No check	This gives the user the ability to run any report application completely or to load a data file into IG, zoom the screen and print the resultant chromatogram. This right allows you to open and use all of the features of Aurora, Star Report Writer and Star Finder. This right allows you to open PolyView 2000.
Recalc Data and Save Results	Yes/No check	This allows the user to recalculate data in interactive graphics and PolyView 2000 and save the new results. If the user has this right, they also have the rights to view the data files (Implied rights.)
Perform Batch Recalc and Save Results	Yes/No check	This right allows the user to perform batch recalculations on a series of files. If a user has this right, they also have the rights to View data.
Methods	N/A	Rights Category
View Methods	Yes/No check	The user has the right to display a method either through method editor or through system control.
Modify Methods	Yes/No check	The user has the right to make any modifications they want to a method. (Note, all changes are archived into the method in a new version and the old method parameters can be accessed and restored.) Methods which are password protected will require that the user know the password when they modify the method.

Entry	Range of Values	Meaning
		Having this right implies that the user has the right to view a method.
Delete Methods	Yes/No	
MS Instrument	N/A	Rights Category – **These rights are only shown for an MS Workstation.**
Autotune an MS	Yes/No check	This allows the User to exercise the Automatic tuning capabilities of an MS.
Manually Tune an MS	Yes/No check	This allows the User to exercise the Manual tuning features. This right should only be granted to experienced users.
Execute a 1200 MS Macro	Yes/No check	For the 1200 MS Software, right to manually execute a Paw Macro Language Script (PML).
Edit a 1200 MS Macro		For MS 1200 Users. Right to create/modify PMLs
Instrument	N/A	Rights Category
View Instrument Status	Yes/No check	This allows the user to click on one of the instrument boxes on the system control screen and display the status of that instrument. They cannot; however, make any changes to the instrument parameters and they cannot run a method.
Change and Configure Instruments	Yes/No check	This allows the user to change the instrument identification and configuration.
Run with Standards	Yes/No check	This allows the user to run both standards and samples through all mechanisms including Quick Start, sample lists and sequences. As part of this right, a user can change the instrument parameters for the particular run that they are making.
Run without Standards	Yes/No check	This allows the user to run samples only through all mechanisms including Quick Start, sample lists and sequences. The results will be generated and stored in the run file. However, the user cannot run a Calibration type run; therefore the response factors and coefficients for the calibration

Entry	Range of Values	Meaning
		curve cannot be changed. If the user tries to run a calibration run, the system will default to an Analysis (A) type run. Later someone with the proper rights could recalculate the chromatogram as a calibration run. As part of this right, the user can change the instrument conditions for the runs that they are making.

Groups screen entries

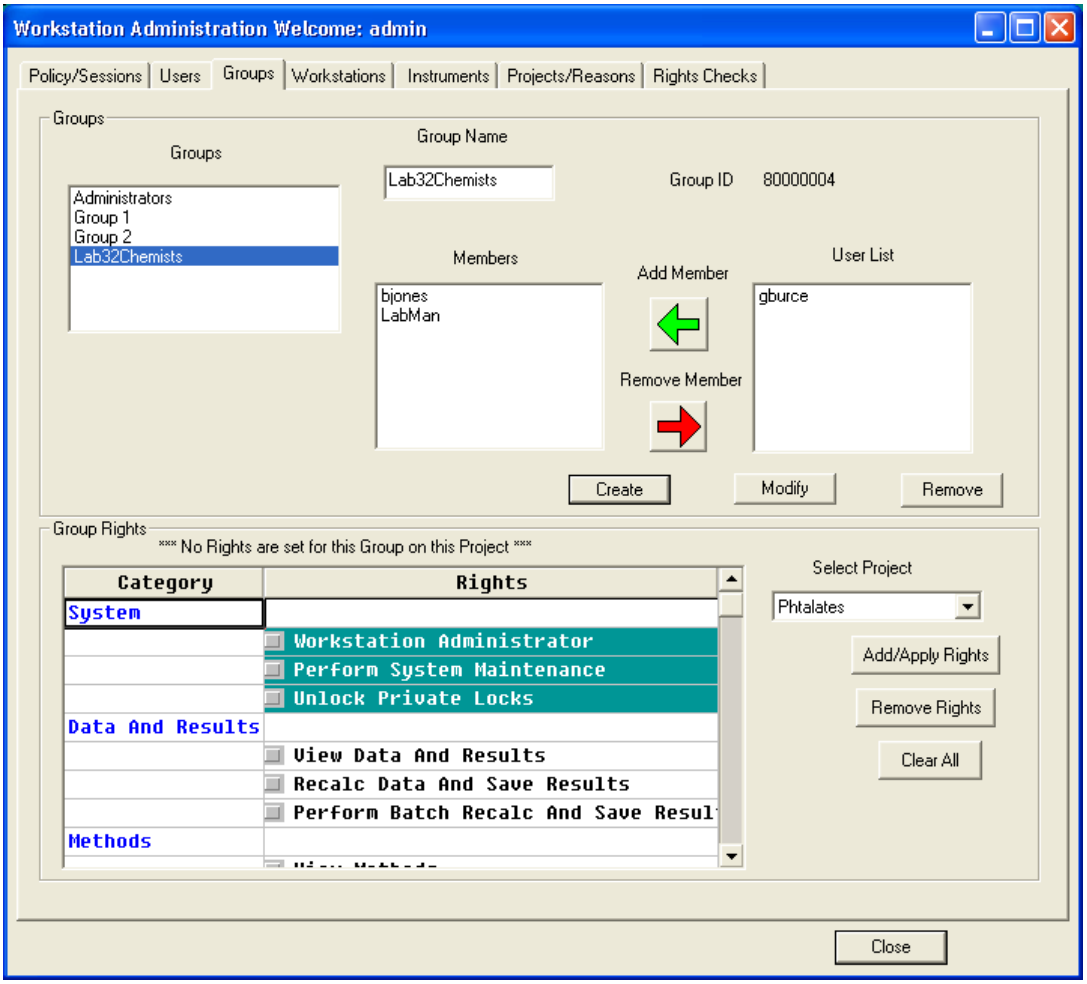

Figure 8 Group Entry Screen

Overview

The Groups screen allows individual users to be grouped to make the assignment of rights easier. If several people who will be using the instrumentation have exactly the same duties and rights, making them a group and assigning their rights in that manner is easier than doing this for each individual.

Groups can be given any name. Once a name is given, individuals are assigned to the group.

The group called Administrators cannot be removed. Users who will perform the function of administrators could be put in this group. However, users can be given administrative rights directly without being made part of the group.

Being designated an administrator in this software does not make the individual an administrator in the Windows NT, Windows 2000, or Windows XP software. That must be done through the Windows software itself.

Individual Entries

Entry	Range of Values	Meaning
Group Name	1 to 15 characters	This is the name of the group that some user will belong to. New groups are created by typing in the name of a new group and pressing the Create key.
Groups		This is a list of all of the groups that have already been created.
Group ID		This is a number given to a particular group to be able to uniquely identify that group. It is assigned consecutively.
User list		This is a list of all of the users currently configured on the system with the exception of those users who are part of the current highlighted group. Note, a user must be created on the users page before they are assigned to a group.
Members		This is a list of all of the users currently configured on the system who are part of the group that is highlighted in the Groups box.
Add Member	(Press)	This adds the highlighted member in the users list to the group.
Remove member		This removes the currently highlighted member in the members list from the group.
Create	(Press)	This button creates a new group.
Modify	(Press)	This button will validate the newly changed group.
Remove	(Press)	This button will remove a group from the list of groups.

All of the remaining entries on this screen are the same as those on the users screen.

Workstation Screen Entries

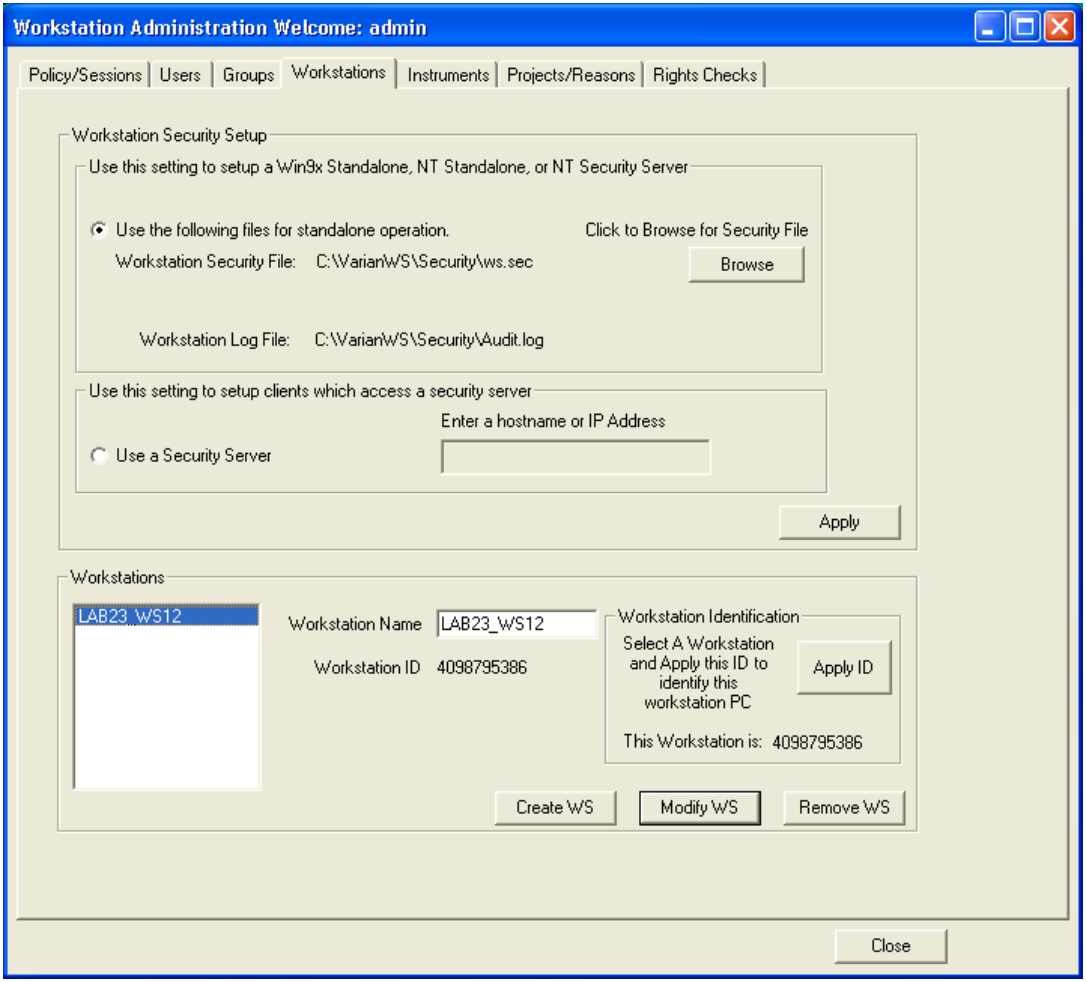

Figure 9 Workstation Entry Screen

Overview

This screen allows the administrator to choose between using the security database on the local PC and using the security database on a networked PC.

Using the security database on a local PC is convenient for very small labs where there are only one or two workstations. However, larger labs will want to use one security database for all of their workstations. By putting the security database on the network, user information can be entered once and applied to all of the workstations and instruments. Also, an administrator will be able to access the security system from any PC attached to the network which has Access Control and Audit Trail software on it.

Having a variety of workstations share one security database requires that you create one Workstation configured for standalone operation. Then all of the other workstations should be configured to use the standalone workstation as the security server.

This screen allows the administrator to create workstations. A workstation is any PC on which the Access Control and Audit Trail software is installed. All of the planned workstations can be named from a single workstation. However, to identify the workstation, the administrator will have to log on to each workstation and press the Apply ID while selecting the appropriate workstation name.

Individual Entries

Entry	Range	Meaning
Use the following files for Standalone Operation	On / Off	When this is checked, the workstation will use its own security database and audit log file. This needs to be checked if this particular workstation will be used as a security server for other workstations.
Workstation Security File	Full file path	This displays where the security file for this system is located (for standalone operation)
Workstation Log File	Full file path	This displays where the security audit log for this system is located (for standalone operation).
Browse (Click to Browse for Security File)	Press	This allows the user to select the security database that will be used with this particular workstation. The file can be located anywhere accessible to the local workstation.
Use a security Server	On / Off	If the security database is on a different workstation, this is checked and the workstation is identified either by its name on the network (not its name in the Star software) or by its IP address. Note the workstation acting as the security server must be configured for standalone operation.
Enter a hostname or IP address	Any networked PC or an IP address	This is the server name or IP address.
Workstation Name	1 to 15 characters	The name of a workstation can be created here. The name should be something that identifies the workstation to the operators. This is not designed for network use. Multiple workstation names can be created from any individual workstation
Workstation ID (Apply ID)	(Press)	This number is read from the workstation hardware and uniquely identifies the workstation. In order to apply the ID the administrator must log on to each individual workstation, select the name used to designate the local workstation and press the Apply ID button. This will give a unique ID to that workstation. Applying an ID to each workstation is critical. If you do not apply an ID, no one will be able to log into any of the Star software on the workstation.
Create Modify Remove		Same as other screens

Instrument Screen Entries

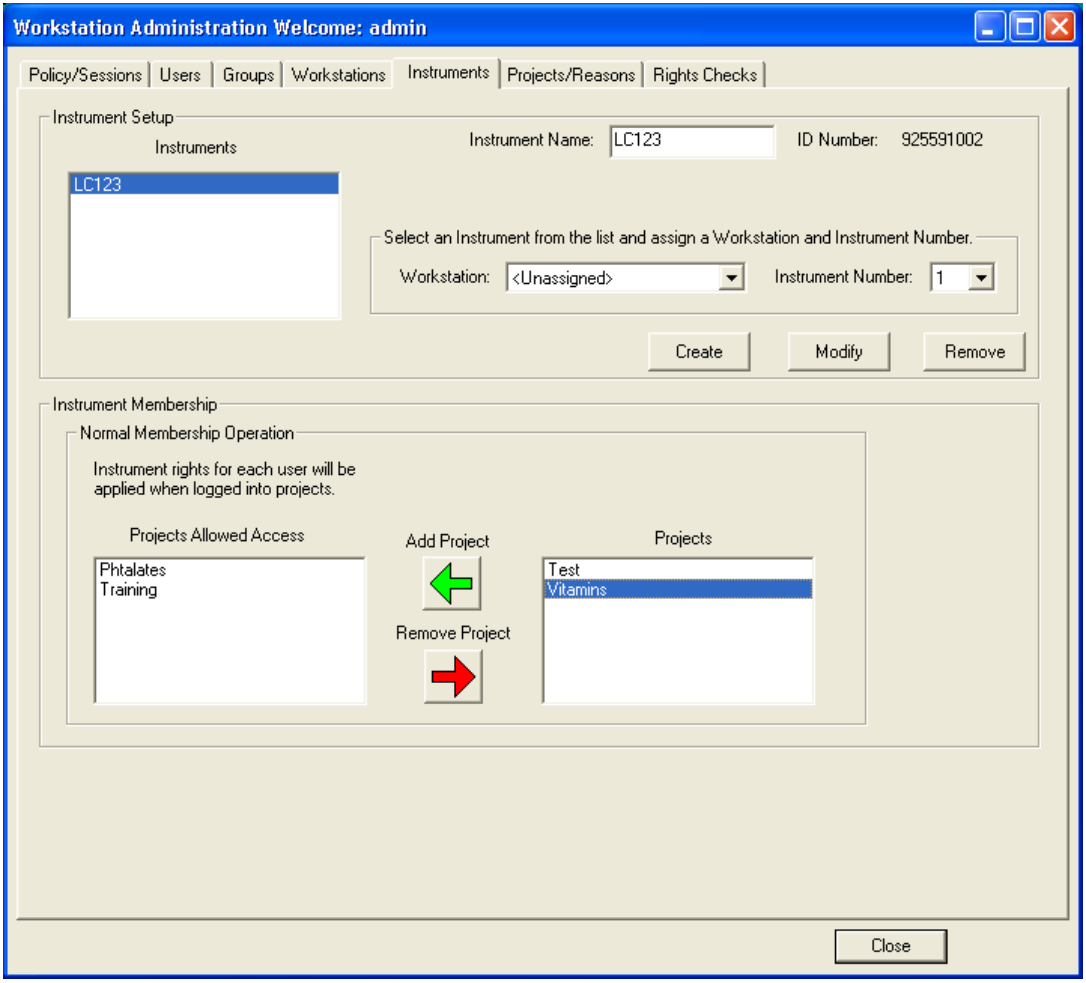

Figure 10 Instruments Entry Screen

Overview

The instruments screen allows an administrator to coordinate an instrument with a workstation. In the Star workstation, there can be anywhere between 1 and 4 instruments. The instruments are numbered 1 through 4 on the Star workstation configuration screen. These correspond to the instrument number values.

This screen also includes the table which associates individual instruments with projects. This is the connection between the rights of an individual or group and the instruments on which they have these rights.

Individual Entries

Entry	Range of Values	Meaning
Instruments		This is the list of instruments that have already been configured.
Instrument name	1 to 15 characters	This is the name that you will use to designate an instrument. A default name is given to all instruments attached to a particular workstation. The default name is “workstation name”_1 to 4. The administrator can change this name to any other name here.
Instrument ID number		This is a number created when an instrument is created. (All instruments are created automatically when a workstation is created on the previously page.) This number uniquely identifies the instrument.
Workstation		This is the workstation name (which you have already created on the previous screen) to which this instrument is attached.
Instrument number	1 to 4	This is the number of the area on the workstation configuration screen that you are going to identify with the above name. When a name is assigned to a workstation as described in the previous screen, either 1 or 4 default instruments are created. These default instruments have names the same as the workstation to which they are attached with a _1 through -_4 after the workstation name. The administrator can change the names to whatever they want.

Entry	Range of Values	Meaning
Create Modify Remove		Same as on all of the screens
Projects		This is the list of projects which have been configured on the system
Projects Allowed Access		This is a list of the projects which have access to the instrument selected above. The projects are specific for each instrument selected above. The default project has access to all instruments.
Add Project		When this is pressed, the project highlighted in the projects box will be associated with the instrument highlighted in the instruments box above
Remove Project		When this is pressed, the project highlighted in the Projects Allowed Access box will be disassociated with the instrument highlighted in the instruments box.

Projects/Reasons Screen Entries

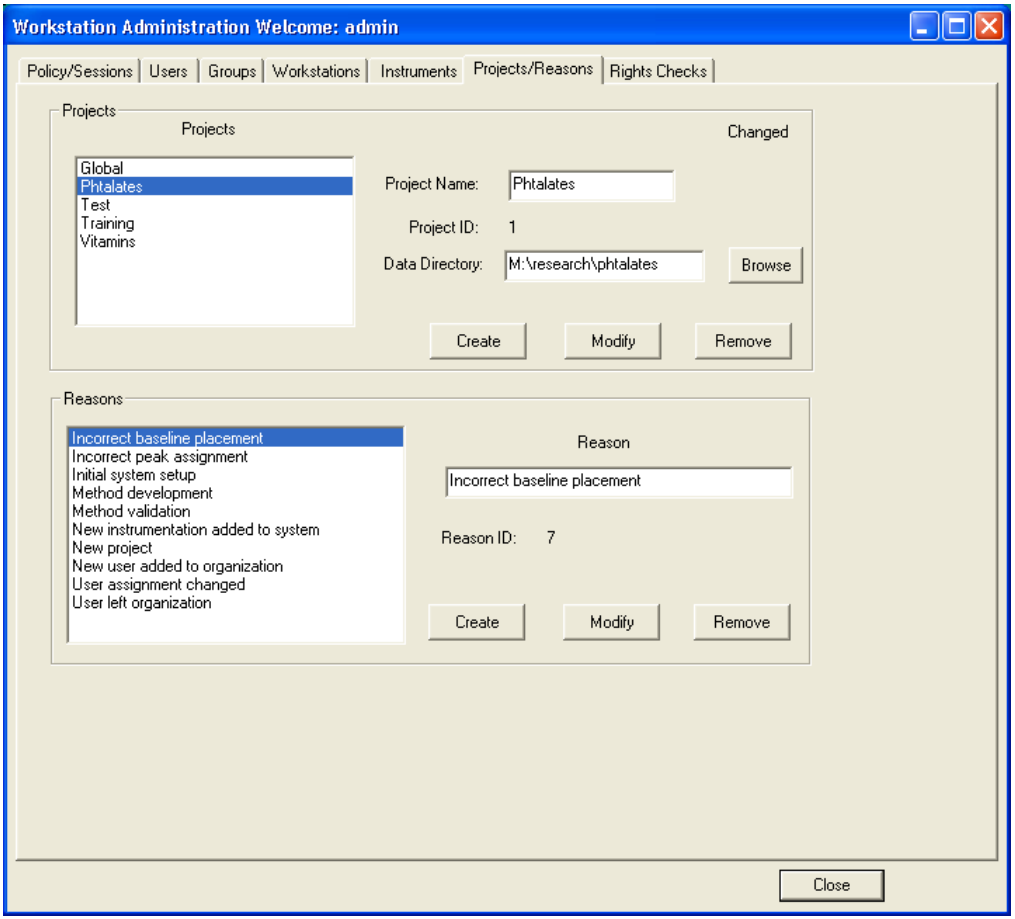

Figure 11 Project/Reason Entry Screen

Overview

Projects are the key element in linking workstation and instruments to users or groups of users. Users have rights based on projects. Instruments and their corresponding workstations are assigned to one or more projects. This links the two together.

The global project is a project with which all instruments are associated. Rights assigned to an individual or group for the global project allow them to perform those actions on all instruments.

The reason section allows an administrator to develop a list of reasons that can be easily selected when someone using the workstation is requested to enter a reason. There are 10 preset reasons already in the software. They can be deleted or modified if desired.

Individual Entries

Entry	Range of Values	Meaning
Projects		This is a list of the projects which have been created.
Project Name	1 to 15 characters	This is the name of a project that you want to create. Typing in a new name and pressing create will create a new project.
Project ID		This is a number that is created when a project is created to help identify the project within the workstation. They are created sequentially. Note, the global project always has a 0 value for ID.
Data Directory (Browse)	Any valid name or press browse.	This is the directory that is preset for data storage for each project. When a user logs in with a specific project, this directory will become the preset in all places which specify where data is stored. This directory will be relative to the workstation on which the user is logged in. Therefore, if a directory on the C drive is used, it will always be a local directory. Also, if using a networked location, each workstation and user will need permission on the network to access that location. When the user goes to actually save data, the user will always be able to save data to any other directory. This does not force a user to save data in a particular directory.
Reasons	1 to 78 characters	These are preset explanations that can be used whenever a user is prompted to enter a reason for an action or a change in the software. A user can always enter a freeform entry (with or without a preset reason) when prompted for a reason. But some reason must always be entered. The preset reasons can be removed.

Rights Checks Screen Entries

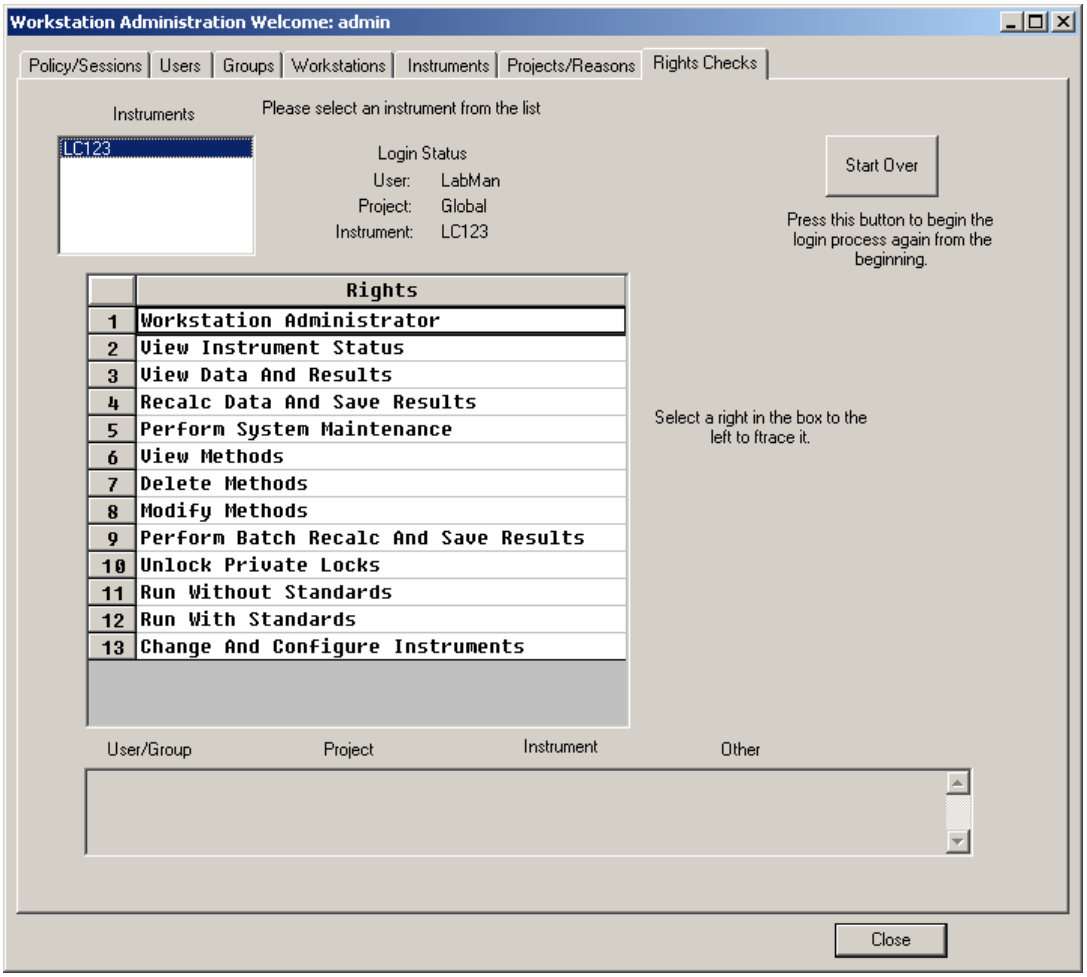

Figure 12 Rights Check Screen

Overview

This rights check screen is designed for an administrator to find why a user has a particular set of rights on a project. To find what rights they have, project-by-project, it is easier to go to the users or groups screens. However, when it is not clear how a user got certain rights, this screen can be used to trace the source of the rights.

Individual Entries

Entry	Range of Values	Meaning
Users / Projects / Instruments	List of Users List of Projects List of Instruments	Select the User, Project, and Instrument combination for which you want to assess the rights. Once you select a user , the list shows the projects this user is associated with. Once you select a project, the list shows the instruments in that project. Once you select an instrument, the Rights table is updated.
Rights		The Rights table shows the rights available to the selected Use/Project/Instrument. The administrator can click on each right and the listbox at the bottom of the screen shows how that right is derived.
Trace		This button will allow the administrator to find out how a particular user got the right. The result of a trace is displayed in the lower screen (see Fig 12b)

Workstation Software

File Security

Scope and Purpose

In the Star Workstation system, files integrity is preserved using two mechanisms.

1. An individual who has the rights to make changes to a file must authorize any changes intentionally made to a file. When authorized changes are made, an internal version of the file is created or an audit log entry is made. This identifies who made the changes and why they were made. This functions throughout Star software.

2. Star software uses checksums to assure that files have not changed since they were last opened by a Star application.

File Integrity Tests

Whenever a Star application opens a file, it checks that the file checksum is correct. If it is correct, the process will proceed. If it is not correct, the user will be notified that there is a problem and asked if they want to update the checksums. Only someone with maintenance rights can update the checksums.

A file will have incorrect checksums when information has been added to or removed from the file outside of the Access Control and Audit Trail software. This could happen in three ways.

The first way is for the file to be opened in a Star application, which is not under Access Control and Audit Trail software. This could be an older version of Star or Star 6.0 and above without Access control and Audit Trail software installed. In either case,

access to the file would not have been controlled and therefore the checksum would be incorrect.

The second reason is that the File was opened and modified in some other software. In this case, the checksum would not be recalculated and would be incorrect.

The third reason would be that the Star software updated the file automatically. When a new instrument driver with new capabilities is installed, it will automatically update any file which uses this driver. This update procedure will occur the first time the file is opened in either System Control or Method Editor. This is only done for method files. It is done so that the method can use the updated driver to control the instrument.

In any of these cases, Star software allows a user with rights to do system maintenance to fix the file so that it has the proper checksum. This is automatic when you select a request to update files.

Overview of the Logs and Audit Trails in Access Control and Audit Trail Software

Scope and Purpose

The purposes of the logs and audit trails in Access Control and Audit Trail software are as follows:

The software will track all changes to calculated results, methods, and the security database.

The software will track all “significant activities” which happen on the Star system.

The software will record detailed information about the changes.

The software will require that a reason for the change be entered, either from a list of preset reasons or as a freeform entry.

The software will allow the display, printing and archiving of this information.

Outline of the Access Control and Audit Trail Software Audit Trails and Logs

There are four separate logs or audit trails in the software. Two of these are internal audit trails - the information about what happened to a file is stored in the file itself. Two of these are external logs – all of the information is stored in a separate file, which can be archived at periodic times.

Method files (.MTH) have an internal audit trail

Data files (.RUN) have an internal audit trail

The Security server and database has an audit trail that is a separate file

The entire system has an audit trail that is a separate file.

Method File Audit trail

Scope and Purpose

A method is used to collect data and therefore affects the data and results. For this reason, it is necessary to control changes to a method and note when parts of a method have changed. To do this, the method has an internal log or versioning scheme. When a method is changed, a new version of the method is created within the method file itself. The method versions are consecutively numbered, 1 being the earliest version.

New Method File Structure

The new method file structure is essentially the same as the old file structure with the addition of a new entry called version. See Figure 13.

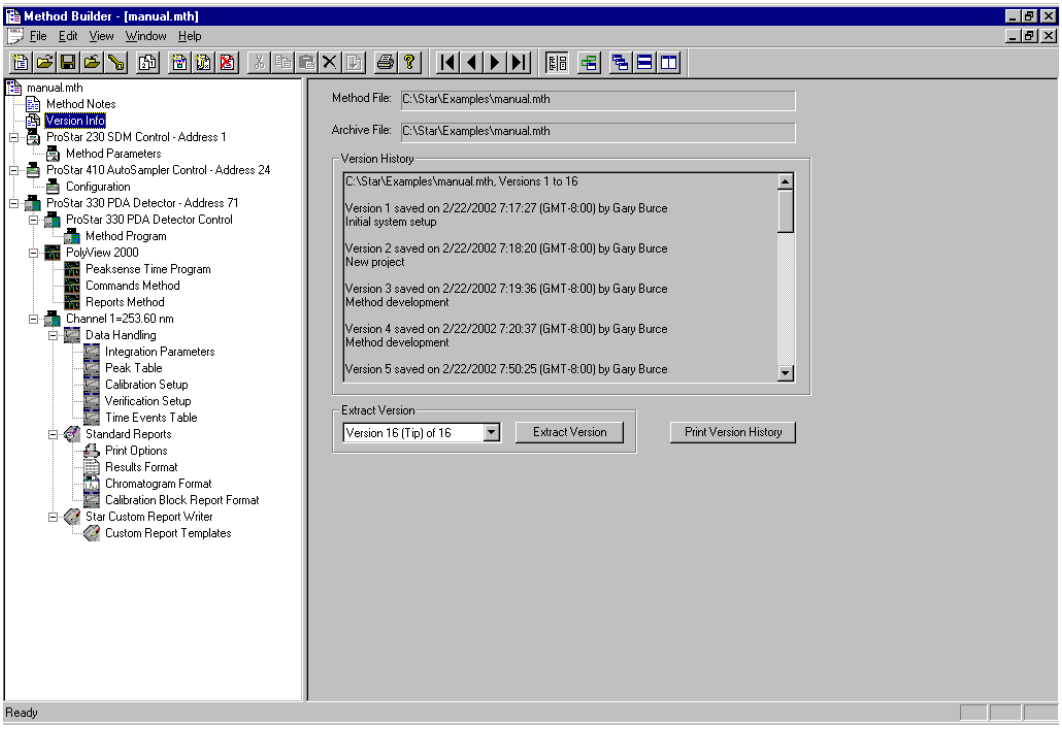

Figure 13 Method Editor Screen Showing Version Information

The version information section is located directly below the Method notes entry. You can also go to the version information by clicking on the version button in the tool bar. When the version information section is selected, the history of the method is displayed in the Version History table. Below this section, a drop down menu allows the user to select the version that they wish to extract and use. The version history screen contains information including the date and time when the version was created, the person who created the version and the reason for the change. The exact nature of the change can always be exactly discerned by comparing that version with the previous version.

The latest version is label as the TIP. This version is the version that would normally be active when you opened a method file to edit or run samples and standards. If you want to run or edit an earlier version of a method, you select the version that you want

to work with and press the Extract button. The dialog box is shown in Figure 14.

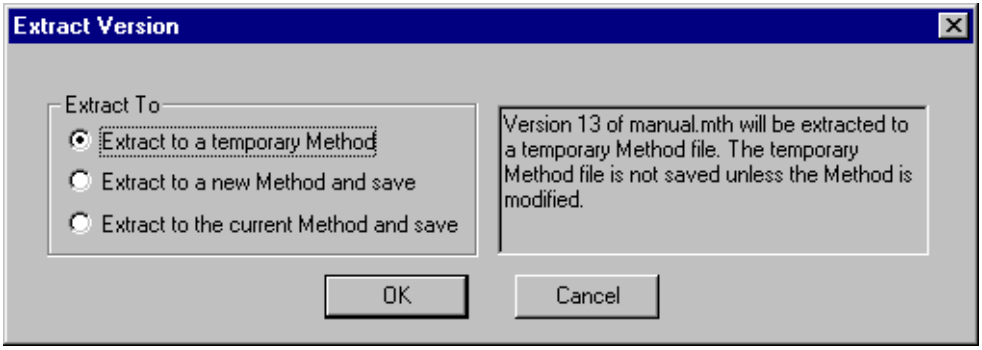

Figure 14 Dialog Box for Extracting Versions of a Method.

If you extract a version to a new name, it will appear as a new method with that name and no version history. This method can be used as any other method.

If you extract to the current method and save, it will become the new TIP for that method. This can then be used as any other method.

If you extract to a temporary method, it will give a temporary name to the method as shown in Figure 15. This file can be used for comparison between it and another version of the file but it cannot be used to run an analysis.

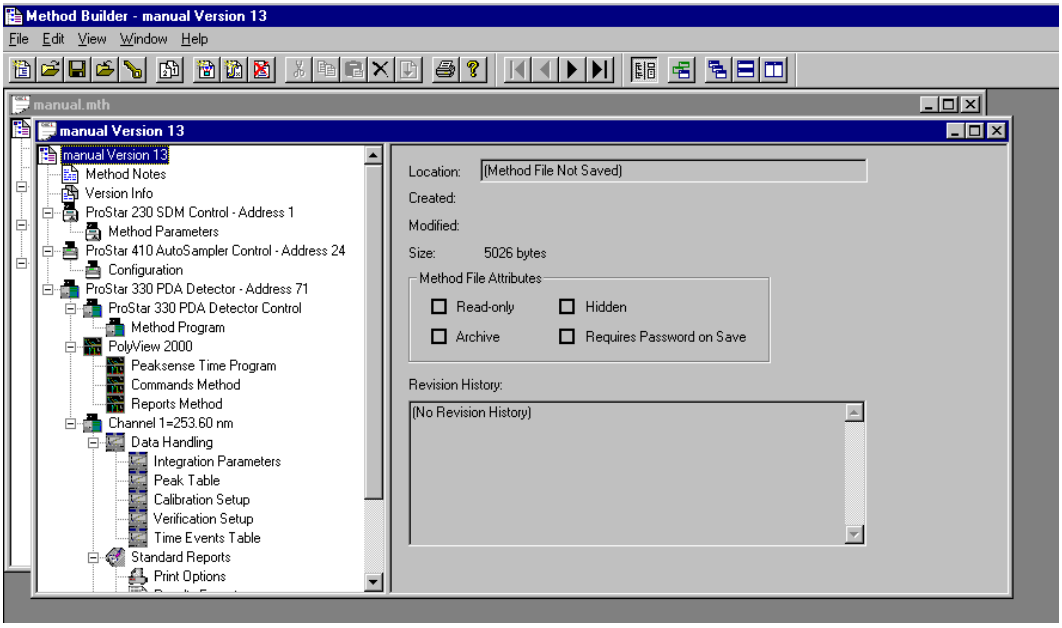

Figure 15 Version 2 of the Method Test

Method Rights

There are three method rights: view method, modify method, and delete method. The right to “view a method” allows the user to open a method file and review the contents. This can be done from the Method Editor Icon on the Tool Bar, through System Control or any other way that a method can be opened. However, a user who does not have the right to modify a method, will not be able to save any modifications, and will not be able to build a new method.

Users with the right to modify a method can either build a new method or modify an exiting method. If a new method is built, they can save it as any name except for that of a previously existing method. If they have modified a method, they can either “save” it with the same name or “save (it) as” a new name.

With the right to delete a method, the method editor function that deletes methods sections will offer the option to delete the whole method if all sections are selected for deletion.

Save vs. Save As

Once modifications to a method are finished, the method can either be “saved” as the same name or “saved as” a different name. These are two very different functions, which have two very different results.

The purpose of the “Save As” function is to create a new method with a new name. If the user is allowed to modify a method, they can always save the method as a different name whether it was a newly created method or a method modified from an existing method.

When the “Save As” command is used to save a method, there will only be one version of the method, the one newly created. This is the mechanism of removing versions from a method.

The purpose of the “Save” function is to modify an existing method. There could be many reasons for modifying a method. When modifying an existing method, the Star workstation creates a new version of the method while preserving the older method (See Figure 15). The older version of the method can be accessed for review, modification and use.

Password Protecting Methods

To protect a method from unauthorized modification you can password protect it. Pressing the key Icon in the method editor tool bar accesses password protection. (If a message is displayed saying that a new password cannot be created because that function has been disabled, you can go to the Star Tool Bar, select the Security Administration (Key) icon and unselect the “Disable creation of new passwords” function in file revision settings.) This will prompt you to set a password for a method. When someone tries to “save” the method, they will be asked for the password. In this way, changes to validated methods can be restricted.

Password protection does not prevent the method from being “saved as” another name. Therefore, the user can make a copy of a password-protected method for use in methods development or method modification without knowing the password. This will help prevent methods from being accidentally modified.

Reasons for Changes

When you attempt to save a method that has been modified, you will see a screen which asks for the reason for the change. This screen is shown in Figure 16.

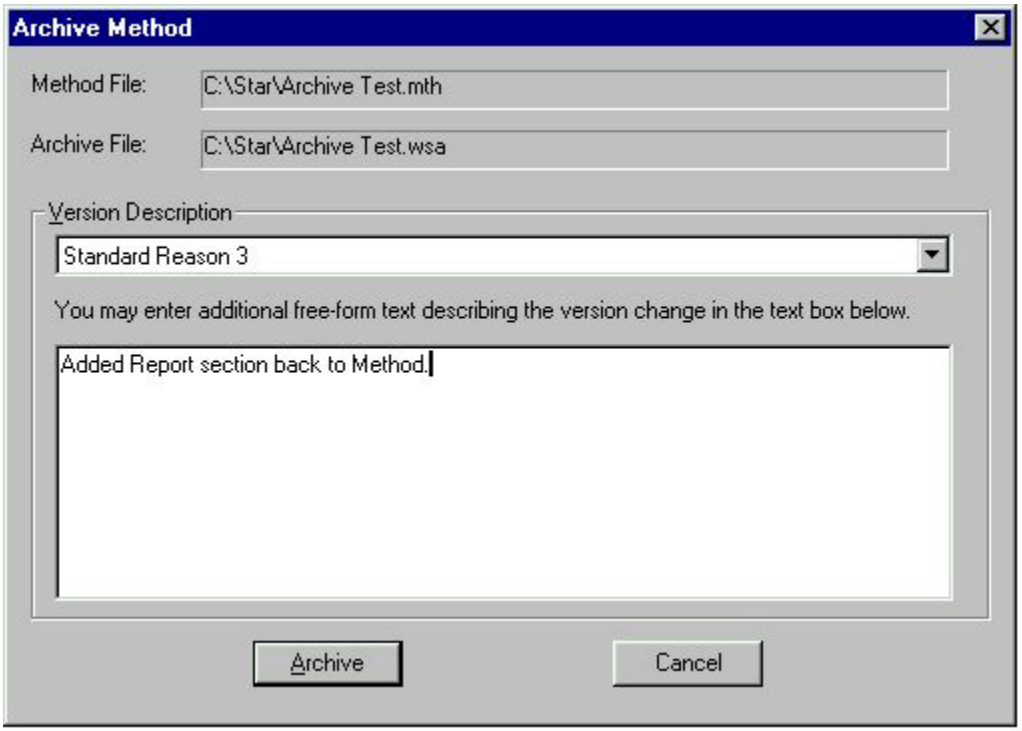

Figure 16 Dialog for Entering Reasons for the Change in the Method.

Data File Audit Trail

Scope and Purpose

When an analytical run is made, the calculation of results may not always be correct. At times, the system might assign inappropriate baselines under part of the chromatogram, misidentify a peak or measure a noise inappropriately.

Also, after a run has been made, other calculations may be desired. One of the standards could have been made up incorrectly and the results may need to be recalculated without that standard. A researcher may want to know the effect of using peak height to calculate results instead of peak area.

Whenever any of these changes to the results are made, the older results, and how they were determined, must be saved. This is done with an internal archive in a similar manner to the internal archive of the method file.

Note: *The following section describes concepts and functionality for the Interactive Graphics Application dealing with Standard Chromatography Data Files (.RUN). The same concepts apply to .SMS / .XMS Mass Spectrometry Data Files, and equivalent functionality is available in the MS Data Review Application.*

Contents of the Modified Data files

When a recalculation is done, either manually through Interactive Graphics or automatically through System Control or batch recalculation, the .RUN file will have 3 additions to it. These 3 additions will constitute a new version of the file, which will be accessible similarly to the way in which different versions of the .MTH file are accessed.

A new set of results will be added to the file. These results will be appended to the file while the original results will be preserved.

A new set of data handling parameters will be added to the file. These are the parameters that were used to create the results.

The standard information about who made the change, when it was made and why it was made are added to the file.

This information will only be saved in the .RUN file when the .RUN file is closed, or when exiting Interactive graphic. (When using batch reprocessing either through System Control or the Batch Recalculation function, the changes will be made automatically.) While the .RUN file is open, any changes made are only temporary. They do not affect the data in the file. Therefore, even if several different baseline assignments or different sets of data handling parameters are applied to the

data, only the final results and corresponding data handling parameters are saved.

Accessing Different Versions of Results in a Data File

When a .RUN file, which has several versions, is opened in Interactive Graphics the user will be able to select which version to display.

To see a different version of the results in a .RUN file, you select a file in the normal manner. After a file has been selected and the chromatogram displayed, either pull down the File menu and select version or use the version button on the tool bar. The screen shown in Figure 17 will be displayed. The reason why each version was created will be listed.

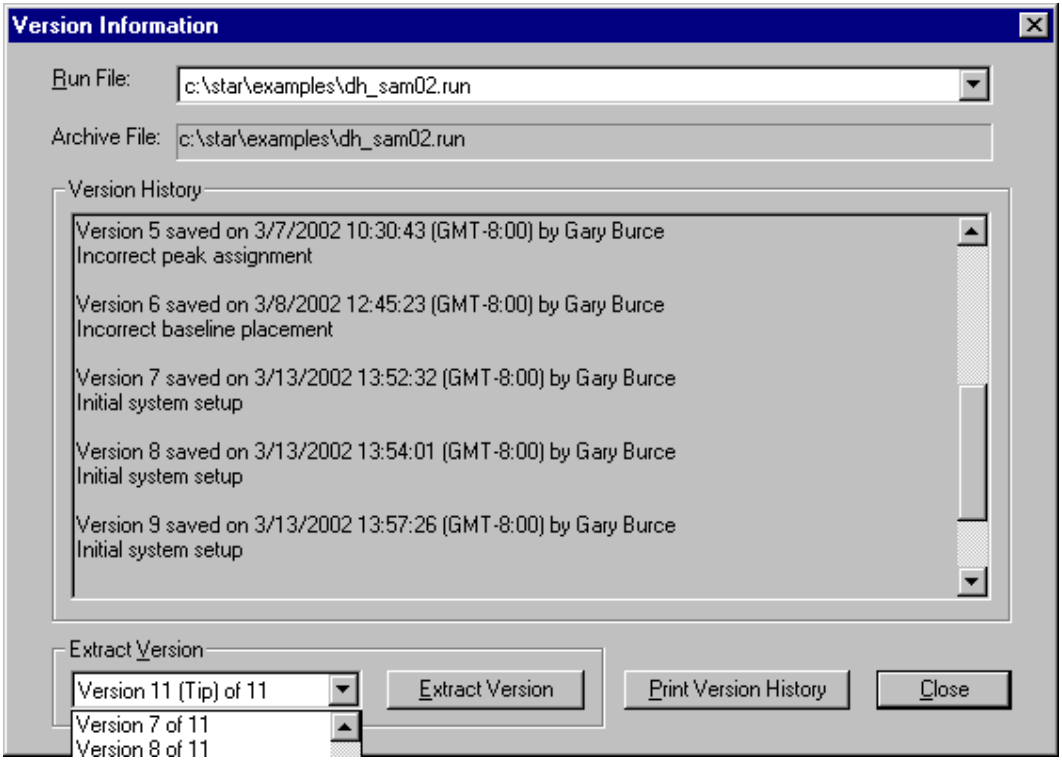

Figure 17 Version Information Screen

To see one particular version, select the version from the pull down menu on the bottom and push the button that says “Extract Version”. When the ‘Extract Version” dialog box appears, you will have three choices:

1. Extract the .RUN file to a temporary file. This will allow you to view the results of older calculations without changing, or permanently storing the results.

2. Extract to new run file and save. This will allow you to create a new .RUN file with an earlier version of calculations.

3. Extract to the current run file. . This will make the selected version of the data the TIP.

Once you have extracted a version of the results in the .RUN file, you can proceed to do the normal .RUN file actions.

You can also print the History of all of the Versions from that screen.

Automated Recalculations

When an automated recalculation in System Control is done, all of the files will have a new version added to them. The identity of the individual doing the recalculation, the time and date of the recalculation and the reason for the recalculation will all be the same.

Manual Recalculations Using Interactive Graphics

When a .RUN file is opened in Interactive graphics, a temporary file will be created. As changes are made to the results due to several recalculations, the changes will be stored in this temporary file. If another recalculation is done, the results will overwrite the previous results in the temporary .RUN file. This will continue for as long as recalculations on a file are being done.

In order to perform recalculations, a method will also be opened. By default, a temporary method will be created with the data handling parameters which were stored in the .RUN file as the TIP. This temporary method can then be modified and trial recalculations performed. This can be done an unlimited number of times.

Alternatively, any other method can be opened by selecting the appropriate method from the File menu. Once opened, this method can be used for recalculations.

At any time, the user can choose to save the results of a recalculation either by closing Interactive Graphics or by removing the chromatogram from the IG display. When this is done, the user will be asked whether they wish to save the results of the recalculation as a new version of the file. If they choose to do this, the corresponding data handling parameters and header information will be added to the .Run file. The user will be asked to enter a reason for the change and the user's identification and the time and date will be stored.

In addition, the user will be asked if they want to save the changes made to the separate method used for recalculation.

If several files were changed during one interactive graphics session, the user will be asked whether they want to change each file respectively.

This design allows the user to try different trial recalculations without having to save the results each time. They only have to save the final results when they are happy with the recalculated results.

Security Server Activity Log

Scope and Purpose

One of the two continuing logs in the system is the security server log. This log records changes to the entries in the security server database. There is one log for each security server.

Creating and Adding Entries to the Security Server Activity Log

When Star 6.0 and above with Access Control and Audit Trail software is installed on a PC, a security server log is created at the same time that the security server database is created. When a change to the database is made by pushing the modify, add, or delete button; the log will be automatically updated. Information indicating who changed the database, when it was changed and what was changed is entered.

In addition, two other types of entries are made in the database. When an administrator logs onto the security server, even if they do not make any alterations to the database, a record is created.

If there has been an administrator alert generated by the system this is also entered into the log. One way to generate an alert would be for someone to try to log onto the system with an incorrect password more than the consecutive number of times set in the policy section of the security server. This occurrence will be entered into the log and, when the next administrator logs into the system, the security server log will record that he was informed about the occurrence.

The security audit log can be accessed by pressing the “Run Audit Maintenance” button on the Policy screen of the administration software. The security audit log is shown in Figure 18 below. In the security audit log, the information about the actions taken in the administrative software is displayed. On the first line is the information about log creation. In this case, the old log was archived and the new log was automatically created. All other lines refer to either actions taken or alarms.

If an Alarm has been generated, there will be a red A next to one of the lines. This line represents the cause of the alarm. When any administrator logs into any part of the Star system on any workstation or the administration software on any PC, they will be notified if there is an alarm. If there is an alarm, they will be able to access the Audit log from the Policy screen of the Administration software and be able to see what caused the alarm. They can then take appropriate action. Once action has been taken, they can clear the alarm. The log of the action that caused the alarm will be preserved in the audit log itself. The two actions that cause an alarm are: too many retires for a log in with an incorrect password, and when someone unlocks a private lock.

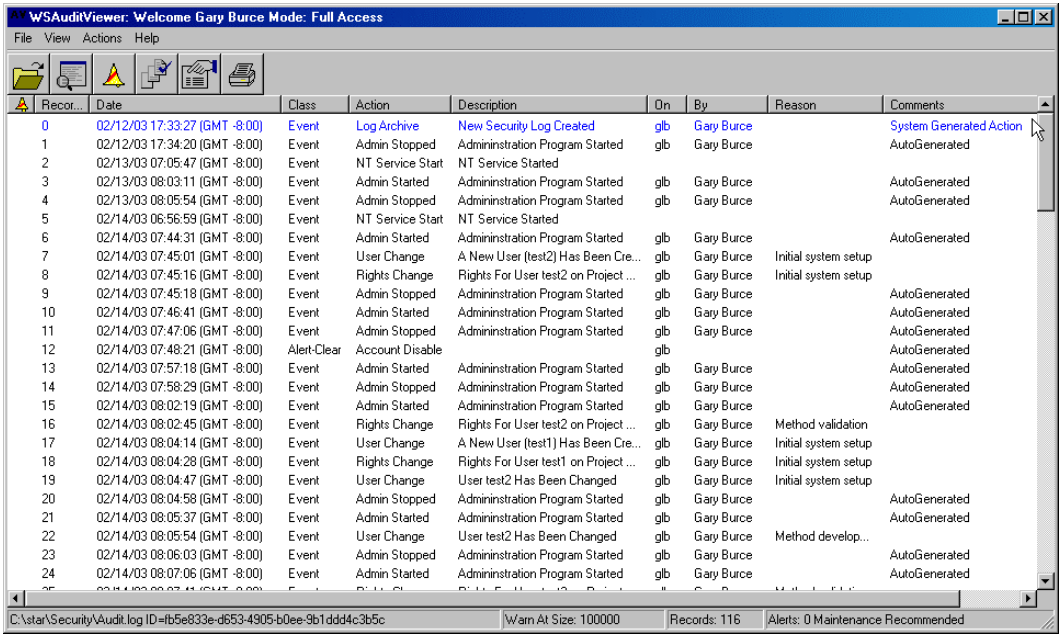

Figure 18 Security Audit log

Once the Security audit log viewer is open, the pull down menus allow the administrator to open older logs and print logs (on the file menu), View details of each entry on the View menu, and Clear Alert, archive the log and change the log setting on the Action menu. Each of these functions has a corresponding icon on the tool bar.

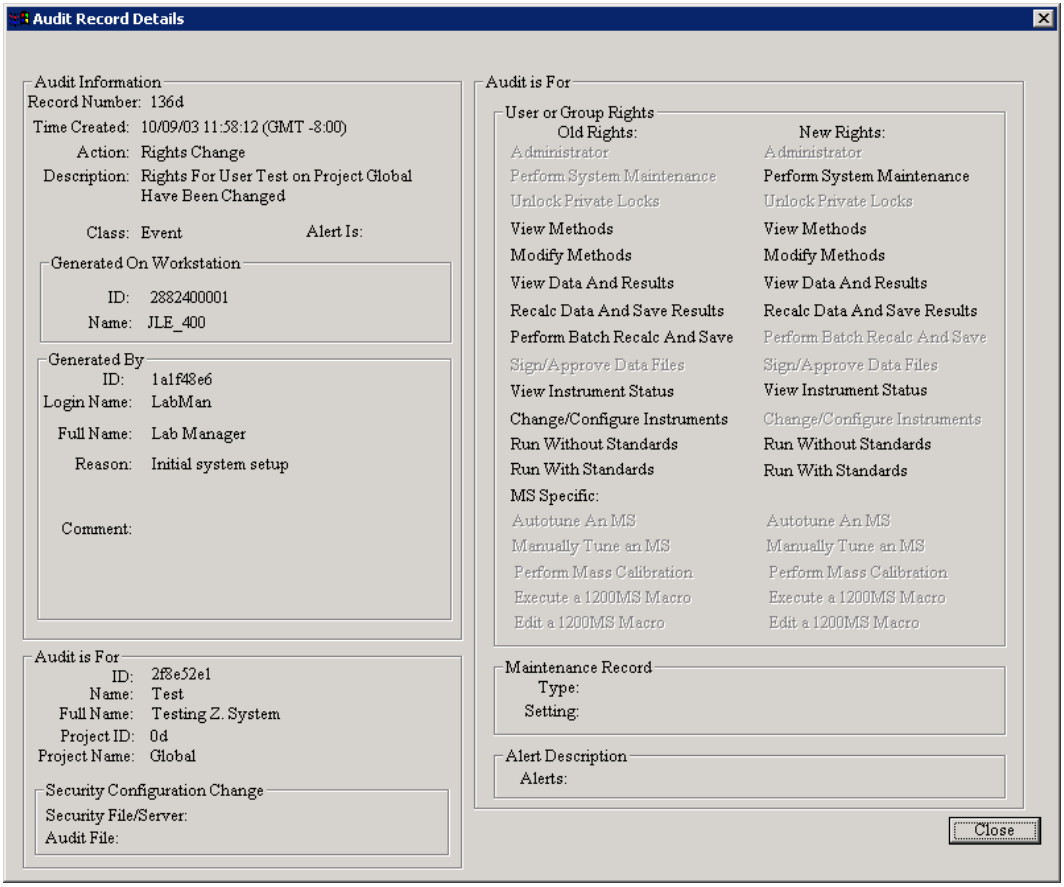

Figure 19 Security Server Log Example

Figure 19 shows an example of the details of an audit log entry. This entry was for the modification of rights for a user on the global project.

When a log is archived, it is permanently closed, given a name and stored in a permanent archive file on the same workstation as the security server. It has a sequentially numbered name. When the log is archived, a new log is automatically created as shown in the first line in Figure 18.

A hardcopy printout of the details of the audit log can be created. This is shown in Figure 20 below.

```
Created: 09/28/2001 20:55:53 (GMT), Signature: 762398541, Version: 1,
GUID: dfd2800a-7e8a-430c-a8ac-8fa516297cde
Properties: 0, Database Type: "Global", Number of Records: 6
Maintenance type: By Size: Current Size is: 2276, Warnings begin at size: 100000

 Record ID: 0 Type: Event At: 09/28/2001 20:55:55 (GMT)
 Reason:
 Comment:Auto
 Generated By: GAry Burce (login name 1, ID 473525078)
 Workstation: KMHOME(ID=-1997310232)
 Type NONE Action: "Admin Program Started"

 Record ID: 1 Type: Event At: 09/28/2001 20:56:16 (GMT)
 Reason: Standard User actions
 Comment:
 Generated By: GAry Burce (login name 1, ID 473525078)
 Workstation: KMHOME(ID=-1997310232)
 Type 1 Action: "User Change"
 Generated For: Kevin Myers (login name kmyers, ID 1660092969)

 Record ID: 2 Type: Event At: 09/28/2001 20:56:33 (GMT)
 Reason:
 Comment:removed 2 as admin
 Generated By: GAry Burce (login name 1, ID 473525078)
 Workstation: KMHOME(ID=-1997310232)
 Type 1 Action: "Rights Change"
 Generated For: 2 2 (login name 2, ID 272837187) on Project Global (ID 0)
 Old Rights: 1 New Rights: 0

 Record ID: 3 Type: Event At: 09/28/2001 20:56:46 (GMT)
 Reason:
 Comment:oops added user 2 again
 Generated By: GAry Burce (login name 1, ID 473525078)
 Workstation: KMHOME(ID=-1997310232)
 Type 1 Action: "Rights Change"
```

Figure 20 Audit Log Printout

System Log

Scope and Purpose

The system log is an external log, which keeps track of things that happen on the individual workstation. There is one log per workstation. The major use of the system log is to allow someone to determine what actually happened on a workstation at a particular time. If there were unusual results generated, the system configuration was changed or any other occurrences; they can be traced through looking at who logged onto the system, who ran samples and when these actions happened. This can be determined using the combination of the system log and the message log.

Creating and Adding Entries to the System Log

Entries to the system log are created automatically. There is no interaction that a user needs to do except when prompted for a reason for a particular entry.

Entries are made into the log when some action on the system is taken. Some of the different types of entries that are logged are listed below:

1. Logging in and out of the system or a particular application
2. Private locking and unlocking the system
3. Changing an instrument configuration in system control
4. Instruments going off line
5. Starting a manual run or an automatic series of runs.
6. Suspending, Resuming or aborting an automated run

Not all of the actual events that will be logged are listed here. Anything that materially affects the system or data generated by the system will be logged. Running a system without injecting samples in order to condition a column or flush out old solvent is not something that has to be recorded in the system log.

Accessing the System Log

The system log is accessed using the message log viewer. This is located in the Start menu under the Varian Star Workstation directory and labeled “Log Viewer”. (A shortcut to this can be created and put on the desktop if desired.) When this program is started, the log will be displayed as in Figure 21.

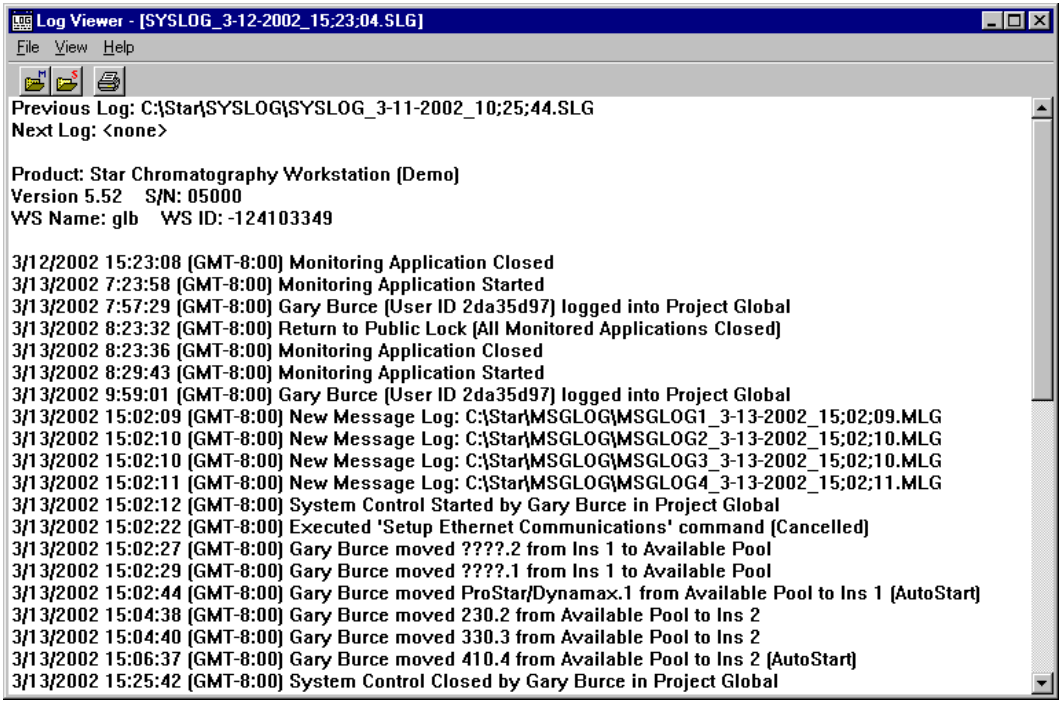

Figure 21 System Log

On the top of the log is the previous and next log entries (Since the log shown above is the current system log, there is no entry for Next Log. When this log is archived, the name of the next log will be entered.

The menu items in the system and message log viewer allow the user to display any of the system or message logs and print them. You can also access any message log listed in the system log by clicking on the message log name in the system log.

The logs are named with the date and time that they were initially created as well as the workstation name on which they were created. This allows the identity of a log to be determined even if it has been archived off of the original workstation.

Archiving the System Log

The system log is automatically archived whenever it exceeds the limits set on the Policy screen of the administrative software. When it is archived a new log is immediately created and starts to log actions on the system. The log cannot be manually archived.

The New Message Log

Scope and Purpose

The message log is the main mechanism that the Star system uses to record what actually happens in system control. The message log records everything that happens on a particular instrument during a series of injections. This includes sample information, instrument status, user intervention etc.

When system control is initially opened, a message log is opened for each of the instruments on the system even if there are no modules in the instruments. The message log will continue to log information about the instruments on each of the 4 instruments. This will include information from manual runs or other actions.

When an automated series of runs is started using either a sample list or a sequence, the message log will be archived and a new message log will be started. This new message log will record everything that happened during that automated series of samples.

Changes to the Message Log from Star 5.52 and Earlier

Unlike the message log in previous versions of Star software before version 6.0, when a new message log is started, the old message log is archived. The message log will be stored as a separate permanent file with a message log name. When an automated run is completed, the message log will be given a

name. When a new automation run is started, a new message log will be created with a different name.

The message log will be stored not only as a separate file but also as part of the system log. This will allow the user to know everything about what has gone on in the system for every automated run.

An example of the message log is shown below in Figure 22

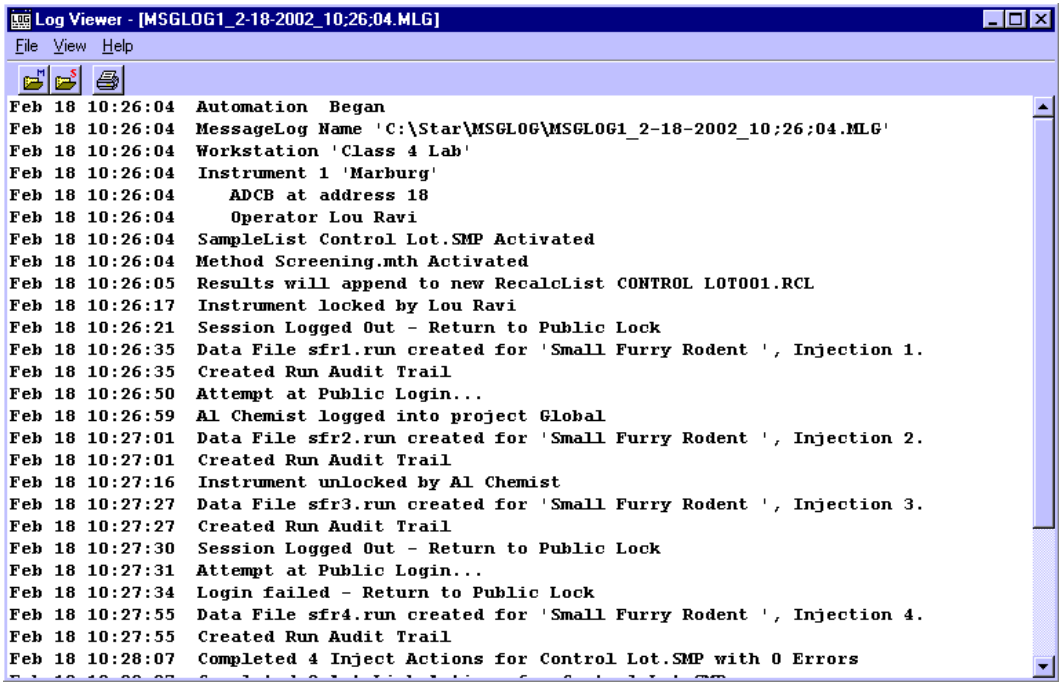

Figure 22 Message Log

Application Locks and Logging Out of the System

Scope and Purpose

The Access Control and Audit Trail software manages access to different areas of Star software. Because several different users can use Star software on the same workstation at the same time, there are application locks, which control access between

applications. These locks allow one users to start an automated process and lock the application so that another user can log in and perform other functions.

Logging in to Applications and Public Locks

Initially, the Access Control and Audit Trail software blocks access to Star 6.0 and above software. A login screen appears whenever any application is activated. Note, the Star Tool Bar application is started automatically or can be started manually without any login because it only provides access to the applications and does not provide access to data or methods.

To log into the Star system, click on the Star toolbar or select an entry from the menu. The Login screen will appear. Once you have logged in, select the application that you wish to start. Logging in does not start an application.

Once someone logs in, they will be able to launch any application to which they have access rights but logging in does not launch an application. If they do not have the right to launch that application, a screen appears referencing them to their system administrator to obtain the necessary rights. This type of lock is called a **Public lock**. A Public lock is one that anyone with the right to log into that application on the Star workstation can open.

Once the user successfully logs onto the system, he or she can freely move between applications without logging in again, so long as they have the appropriate rights. Because rights are project dependent, successfully accessing various applications will depend on the project that the user specified in their log in. If the user does not have the rights needed in the particular project they are trying to access or in the global project, the access will fail.

When the Star system is locked, any process that has already been started will continue to run. Automated analyses, batch reprocessing etc. can be done while the system is locked.

Applications Timeout and Public locks

There is an application timeout, which is set for all applications on the Policy screen of the administrative software. If there has

been no activity on the system for more than the specified length of time, the system will create a **public lock**. This public lock acts like any other public lock. Anyone with the right to log into the system will be able to do so.

Private Locks

The purpose of a private lock is to allow someone to interrupt his or her activities on the workstation and make sure that no one else can use the workstation until they return. A private lock is one that only the original user and someone specifically designated to have the right to open private locks, can open. A private lock, like a public lock, applies to the entire system. The one exception to this is in system control as described below. Therefore when the system is private locked, no one else will be able to use any of the Star applications although any analyses that are presently running will continue.

One of the rights of a system administrator is to be able to unlock a private lock. Also, other users can be designated to have the right to unlock a private lock. A user can create a private lock only in system control or through the monitor application as described below.

Locking and Logging Out of the System

The state of the Star software relative to locks and who is logged in can be determined using the Star 6.0 and above Monitor program. This programs runs continuously in background on any workstation that has Access Control and Audit Trail loaded on it. It can be accessed through the "lock" icon in the lower right hand corner of the Windows screen (see Figure 23).

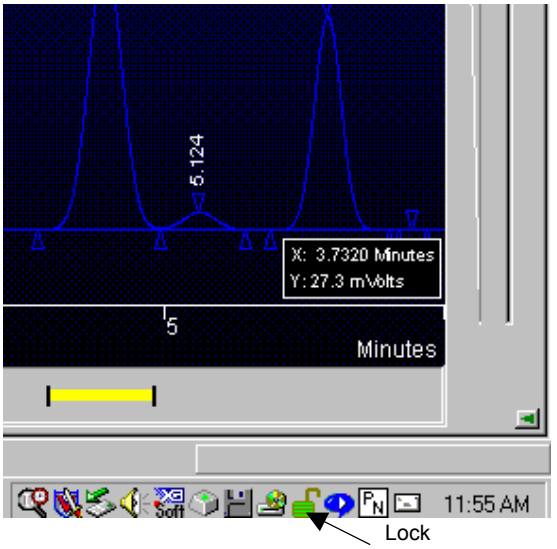

Figure 23 Lock Icon

When you restore this application by double clicking on the icon, the screen in Figure 24 will be displayed.

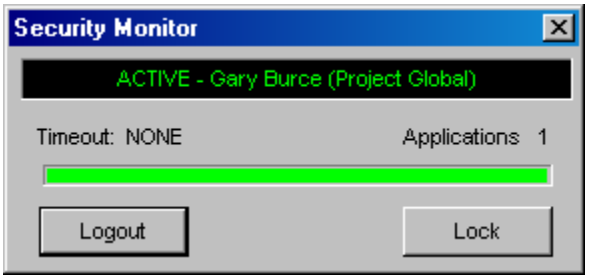

Figure 24 Access Monitor Screen

From this screen, the user can log out or private lock the system. If they have finished all of their activities, they can logout and the system will be Public locked. If they want to temporarily leave the system and assure themselves that no one will make changes while they are gone, they can Lock the system.

The horizontal green bar above the Logout and Lock buttons measures the amount of time that remains until the system times out. The shorter the length of the green, the sooner the system will time out. The length of the time out period is controlled by the settings in the Policy page of the administrative software.

Private Locks in System Control

System control is the Star application which uses private locks most frequently. When a user has set up an automated sequence of injections and started automation on one of the four instruments associated with a workstation, they can private lock the instrument and log out of the system. In this way, anyone else can log on to the system and use any part of it except for the instrument that is already in use. The person who private locked the instrument and anyone given specific rights to unlock private locks are the only ones who can access this instrument.

When you are logged into an instrument in system control, you can private lock the instrument by selecting the Lock Instrument command on the instrument pull down menu. When an instrument is already locked, the command changes to “Unlock Instrument" and is located in the same menu, (see Figure 25). If the instrument was locked by another user, the command will be rejected unless you have the right to override the lock, in which case you will asked if you want to proceed with the unlocking.

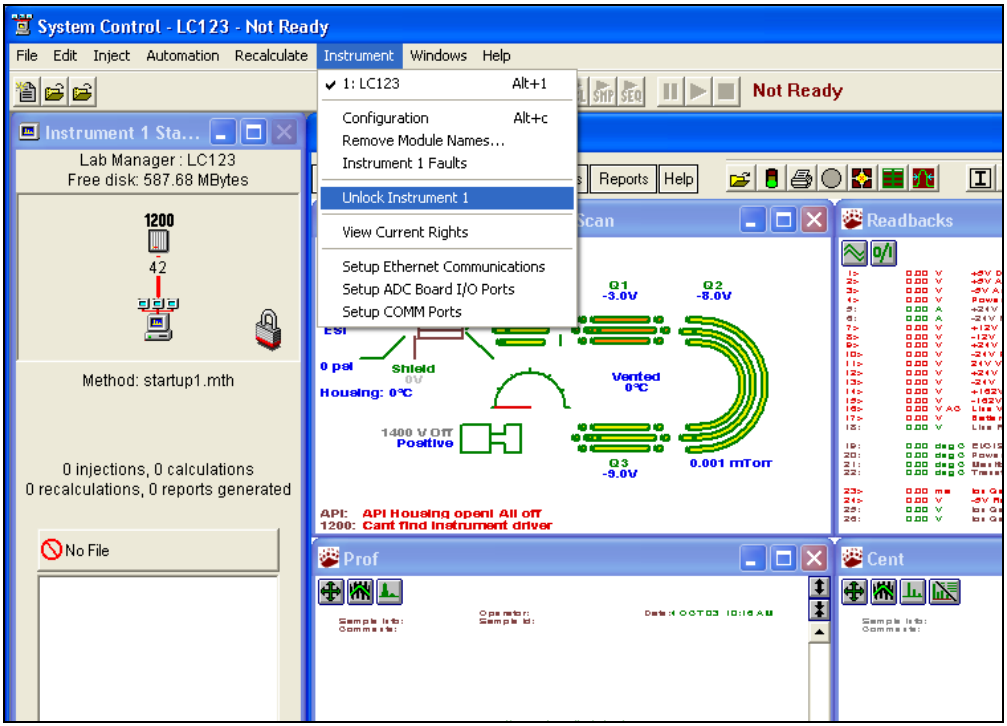

Figure 25 The Instrument Pull-down Menu Showing the "Unlock Instrument 1" Command

You can see when an instrument is locked by looking at the Instrument Status screen (observe the lock icon in Fig 25). If you try to access an instrument that is locked, a message box will indicate that it is locked and who locked it.

Figure 26 Notification that Instrument is Locked

When you lock an instrument, you will be asked if you want to log out of the system. If you do, then the system will be ready

for someone else to log in and work with it. When an instrument is private locked, all of the instruments that are not locked are available for use by anyone with the rights to use them. In this way, no one can modify instrument or automation parameters of instrument 1 except the person who started the automation and someone with the right to unlock private locks. If a private lock is unlocked, then anyone with the right to use this instrument can use it. Also, if a private lock is unlocked, an Alert is created and the next user with administrative rights who logs onto the system will be informed of the alert.