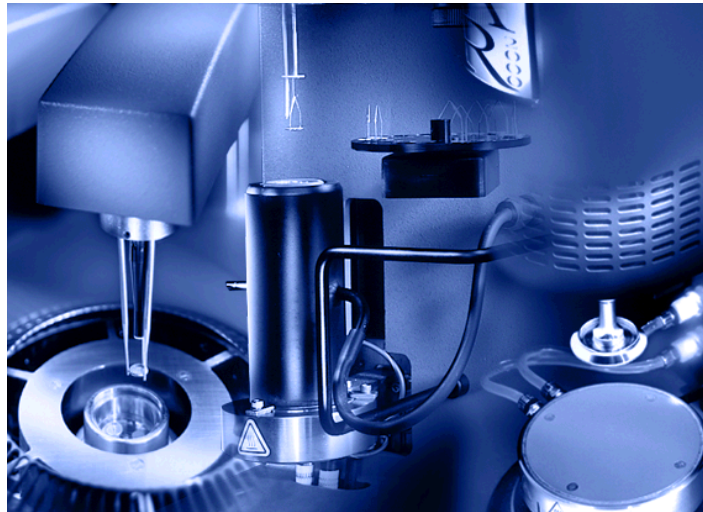


Advantage Integrity™



Getting Started Guide

Revision E
Issued February 2004



Notice

The material contained in this manual, and in the online help for the software used to support this instrument, is believed adequate for the intended use of the instrument. If the instrument or procedures are used for purposes other than those specified herein, confirmation of their suitability must be obtained from TA Instruments. Otherwise, TA Instruments does not guarantee any results and assumes no obligation or liability. TA Instruments also reserves the right to revise this document and to make changes without notice.

TA Instruments may have patents, patent applications, trademarks, copyrights, or other intellectual property covering subject matter in this document. Except as expressly provided in written license agreement from TA Instrument, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

TA Instruments Operating Software, as well as Module, Data Analysis, and Utility Software and their associated manuals and online help, are proprietary and copyrighted by TA Instruments. Purchasers are granted a license to use these software programs on the module and controller with which they were purchased. These programs may not be duplicated by the purchaser without the prior written consent of TA Instruments. Each licensed program shall remain the exclusive property of TA Instruments, and no rights or licenses are granted to the purchaser other than as specified above.

Important: TA Instruments Manual Supplement

Please click on the links below to access important information supplemental to this Getting Started Guide:

- [TA Instruments Trademarks](#)
- [TA Instruments Patents](#)
- [Other Trademarks](#)
- [TA Instruments End-User License Agreement](#)
- [TA Instruments Offices](#)

Table of Contents

Important: TA Instruments Manual Supplement	3
Table of Contents	4
Notes, Cautions, and Warnings	6
Chapter 1: Introducing Advantage Integrity™	7
Overview	7
Parts of the Advantage Integrity System	7
What Constitutes an Electronic Record?	7
Responsibilities of the TA System Manager	8
Accessing the System	9
Logging In	9
Changing Your Password	9
Introducing the TA System Manager	10
Initial Setup of the System Manager	11
Creating New User Accounts	12
Setting Up Groups	14
Assigning Multiple Users to a Group	15
Assigning a Group to an Individual User	16
Assigning Privileges	17
Assigning Privileges to a Group	17
Assigning Groups to Privileges	18
Defining System Projects	20
Assigning Multiple Users to Projects	21
Assigning Projects to an Individual User	22
Defining System Modules	23
Assigning Multiple Users to a Module	24
Assigning Modules to an Individual User	25
System Settings Options	26
Server and Database Information	26
Changing the TA System Options	26
Activities and System Logs	28
Showing Audit Event Properties	28
Overview	29
General Changes	29
Chapter 2: Using the Integrity™ System	29
Using an Integrity-Licensed Instrument	30
Handling Multiple Users for a Single Instrument	32

Using an Integrity-Licensed Universal Analysis	33
Using an Integrity-Licensed Rheology Data Analysis	35
Using the Database Viewer	36
Browsing for Data in Tree View	37
Customizing the Sort Order	38
Viewing Audit Trail Events	39
What Events are Recorded?	39
Instrument Control Events	39
Universal Analysis Events	40
Rheology Data Analysis Events	40
TA System Manager Events	40
Adding Audit Trail Comments	41
Adding a Comment to an Existing Audit Trail Entry	41
Adding a New Audit Trail Entry	41
Viewing an Audit Trail Entry Report	42
Chapter 3: Backing Up & Archiving the Database	43
Overview	43
Built-in Oracle® Facilities	43
Additional Backup Utilities	44
Archiving Data	44
Index.....	45

Notes, Cautions, and Warnings

The following conventions are used throughout this guide to point out items of importance to you as you read through the instructions.

A NOTE highlights important information about equipment or procedures.



A CAUTION emphasizes a procedure that may damage equipment or cause loss of data if not followed correctly.



A WARNING indicates a procedure that may be hazardous to the operator or to the environment if not followed correctly.

Chapter 1

Introducing Advantage Integrity™

Overview

The Electronic Records and Electronic Signatures Rule (21 CFR Part 11) was established by the United States Food and Drug Administration (FDA) to define the requirements for submitting documentation in electronic form. TA Instruments understands the importance of this rule and has developed software with this regulatory compliance in mind. Section 11.3 defines a *closed system* as "an environment in which the system access is controlled by persons who are responsible for the content of electronic records that are on the system." TA Instruments' Advantage Integrity software is a closed system. To fully comply with the rule, it is important for an organization that uses electronic records and electronic signatures to have Standard Operating Procedures (SOPs) that support and complement the Advantage Integrity software functionality.

The 21 CFR Part 11 rule specifies that electronic signature capabilities are optional. The Advantage Integrity software does not provide electronic signatures. Therefore, sections 11.50, 11.70, 11.100, 11.200, and 11.300 do not apply to this software.

Parts of the Advantage Integrity System

The basic TA Instruments' Advantage Integrity system consists of licensed software that is installed on an instrument control computer (referred to as a "controller") and on one or more instruments, which all communicate with a dedicated Oracle database server. The instruments may consist of a Q Series™ DSC and/or TGA or an AR series rheometer. The server may be connected locally or through the company network. For detailed information see the online help in each program.

What Constitutes an Electronic Record?

Electronic records are defined as "any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system." For the TA Instruments Advantage Integrity system, these electronic records consist of the following:

- Raw experimental data (thermal analysis and rheology)
- Saved analyzed data files (thermal analysis and rheology)
- Saved data analysis session files (thermal analysis and rheology)

Thermal Analysis Only:

- Saved Universal Analysis bitmap (.bmp) image files
- Saved data analysis Acrobat PDF files
- Saved Universal Analysis text files

Rheology Only:

- Instrument control geometry files
- Instrument control procedure files
- Instrument control session files
- Data analysis graph styles
- Data analysis polymer library
- Data analysis report templates
- Data analysis user-defined models
- Data analysis user-defined variables
- Data analysis report templates and settings
- Data analysis committed reports
- Data analysis options*

* Stored in data base, but not accessible.

Responsibilities of the TA System Manager

The TA System Manager plays a very important role in this system. Each Integrity system will need at least one appointed person to act in this role. It is best if this person is already familiar with the Advantage Q Series software. The TA System Manager is responsible for the following items:

- Defining the components of the system (users, projects, groups, and modules).
- Assigning each user account to their designated groups, projects and modules.
- Defining user access rights. Within each group, the TA System Manager can define the access rights (privileges) for instruments and data analysis functions whereby restricting access to functions which are not in accordance with the company's standard operating procedures (SOP).
- Setting up password policies. The database system relies on password protection to maintain the integrity of the system.
- Database archival.

The System Manager must log in appropriately as described in the next section before user accounts, projects, instruments, and the database system can be set up.

NOTE: In order to protect the integrity of the database system, a user who is a member of the System Manager Group can **ONLY** perform those functions assigned to a System Manager. Therefore, any projects, modules, or other groups cannot be assigned to a member of the System Manager Group.

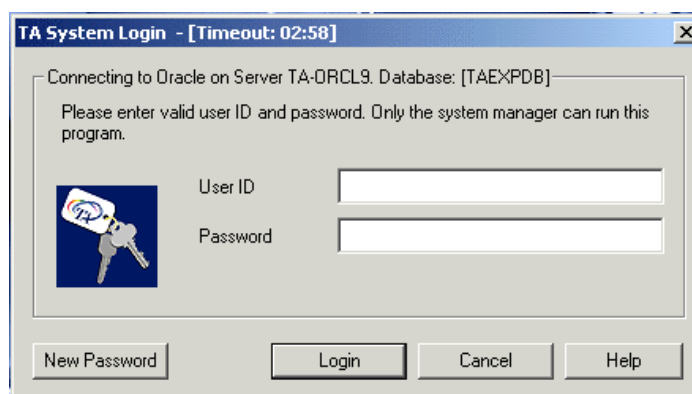
Accessing the System

Logging In

When you open any software component of the database system, either the TA System Manager Program, an Instrument Control program, or the Data Analysis program, the **Log In** window (shown below) is displayed. User access (logging in) is based upon a **User ID** (or log-in name) and **Password**. The User ID and/or password may be case-sensitive if this option is selected by your TA System Manager.

The first time that you use the program you will be required to enter your User ID and default password, as defined by the TA System Manager. This process requires the first-time user to immediately change their password upon initial log in.

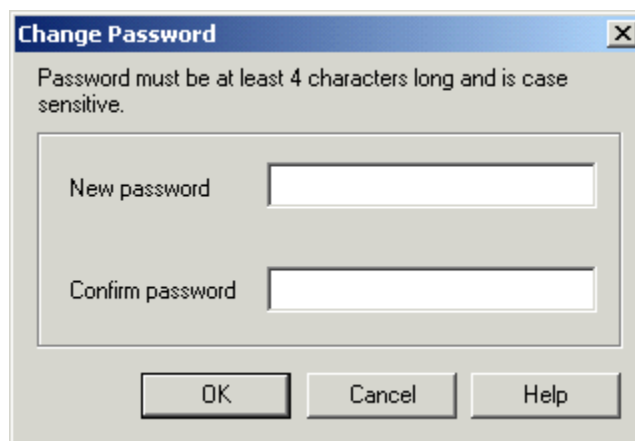
After a period of inactivity the system will automatically log you out. This time period (referred to as the "log-in session timeout") is defined by the TA System Manager. However, it is recommended that you log out of the system when you leave the system.



Changing Your Password

The database system relies on password protection to maintain the integrity of the system and the audit trail. Your log-in password may be changed at any time and must be changed when it expires. The expiration date is set by your TA System Manager. Shortly before your password expires, you will begin to receive "password expiration" notices each time you log in. To change your password, follow these instructions:

1. Open the desired program. Once the Log in window is displayed, type in your User ID and old password, then select **New Password**. The figure shown to the right is displayed.
2. Type in the **New Password**. All passwords must follow these rules:
 - The password must contain the minimum number of characters defined by the TA System Manager. Any combination of numbers, symbols, or letters is allowed.
 - Passwords cannot contain spaces.
 - The User ID and/or password may be case-sensitive, if this option is selected by your TA System Manager.
 - Passwords cannot be reused for a specific user account.
3. Type the new password again to confirm the previous entry.
4. Click the **OK** button.



Introducing the TA System Manager

After the TA System Manager has successfully logged in, the opening window shown below is displayed. The TA System Manager program is used to create and edit user accounts, groups, projects, and modules.








On the left-hand side of the opening window is a set of tools that are used in this program. Click on the desired tool to display the related System Manager options. Each option has a relationship to the other options allowing many functions to be conducted in two places. (For example, assigning a group to a user versus assigning a user to a group can be accomplished using two different dialogs.)

This manual provides basic information about the tools and how to perform the initial setup of the system. For more detailed information, see the online help.

After the system has been successfully installed, the System Manager will need to create user accounts for each user requiring access to the database. Follow the step-by-step instructions in the next section to perform the various operations.

Initial Setup of the System Manager

Follow these basic steps to set up the components of this system:

1. Create new user accounts for each person requiring access to the database system using the **User Account Manager** . Once user accounts have been created, use this tool to manage these accounts and create any additional accounts. NOTE: The information needed on the **General Page** must be entered first. See page 12 for more details.
2. Define user groups and their privileges using the **Group Manager** . Once the groups have been created, use this tool to manage the groups, define their module privilege's list, and create additional user groups. The user accounts can be assigned to one or more of the various user groups. See page 14 for more details.
3. Define new projects using the **Project Manager** . Once the projects have been created, use this tool to manage the projects and create additional projects. A user account can be assigned to one or more of the various projects. See page 20 for more details.
4. Verify that all the modules have been added to the system using the **Module Manager** . Once the modules have been added, use this tool to manage the modules and add any additional modules. Users can be assigned rights or privileges to one or more of the various modules. See page 23 for more details.
5. View and manage the system settings defaults using the **System Settings Manager** . See page 26 for more details.
6. Review your selections.

Creating New User Accounts

A *user* is defined as those accounts having access rights to this system. To create new user accounts, follow the instructions listed below:

1. Log into the TA System Manager, click the **User Accounts** icon, , to open the **User Account Manager**.

2. Select the **General Page** (shown to the right). This window displays the general information regarding a new user account.

The User Account Manager creates new user accounts and assigns project and instrument privileges for each of these accounts.

General Groups Projects Modules

User Log-in IDs

- BDC
- ben
- dean
- DMW
- ina
- jay
- jian
- jz-service
- RLB
- searl
- TAService
- TASystem
- test
- tina
- tina2

User Account Information

User ID: BDC Password: xxxxxx

Full Name: Brian Curran

Department: R & D

Company: TA Instruments, Inc.

Account Information

Pwd. Expires: 5/31/2002

Status: Change Password First


Note: TA Instruments user account.

New Copy to Reload Apply

3. Click the **New** button. The appropriate fields will be cleared.

4. Enter the new **User ID**. This ID may be up to 20 characters in length. The user account information (excluding password) cannot be modified once the account has been created.

5. Enter a default **Password** that follows the password rules found on page 9. This default password, as defined by the system manager, will need to be changed by the user at the first log in.

6. Enter user's **Full Name**. A maximum of 50 characters may be entered.
7. Select the **Department** name from the list or enter a new one. New entries will be retained and added to the list. A maximum of 50 characters may be entered.
8. Select the **Company** name from the list or enter a new one. New entries will be retained and added to the list. A maximum of 50 characters may be entered.
9. Modify the password expiration date, **Pwd. Expire**, if desired. This date is based on the creation of the user account. The default password expiration time is set using the System Settings Manager .
10. The **Status** of the new account will be automatically changed to "Change Password First." Once the **Apply** button is selected the status cannot be changed until the user defines their own password.
11. Enter any desired **Notes** regarding user account. A maximum of 256 characters may be entered.

12. Select the **Apply** button to add new user account. You will be prompted with a message to verify the entered password. (If you change your mind after starting a new account, you can select the **Reload** button to cancel the operation.)

NOTE: The System Manager controls when the user account's password expires and whether the account is enabled or disabled. Once a user account is created it can not be deleted, only enabled or disabled.

13. Repeat steps 1 through 12 for each additional user account.

Once the user accounts have been created, set up the user groups, projects, and modules. Follow the instructions on the next several pages. Once all of the items have been initially set up, assign the user accounts to each of these items as directed.

Setting Up Groups

A *Group* defines a set of privileges associated with the modules (*e.g.*, instruments and data analysis program) within the system. These groups are then assigned to user accounts to restrict actions to defined privileges.

One or more groups can be assigned to each user account. When multiple groups are assigned to a user account, the allowable "actions" are defined by the superset of these combined groups. In other words, if you belong to a group (*e.g.*, Group A) that allows you access to a certain action, that access will be available for you when you log in, even if you belong to a second group (*e.g.*, Group 2) that does not allow access to that action.

Three default groups are available by default when the Advantage Integrity system is initially installed:

- **System Manager:** This group has access to the TA System Manager program only and cannot be used to access any other modules in the system (such as instruments and data).
- **TA Service:** This group is used by the TA Service personnel to service the equipment when needed.
- **Operator:** This group allows access to data analysis and instrument modules, however the privileges list must be defined by the TA System Manager before the operator group is used. See page 26 for information.

The System Manager and TA Service groups cannot be assigned in combination with any other group.

Follow these instructions to set up the groups:

1. Log into the TA System Manager.

2. Select Groups by clicking on the



The **Group Manager/General Page** will be displayed as seen in the figure to the right.

3. Click the **New** button.

4. Enter the **Name** of the group you want to create.

5. Choose **Enabled** from the drop-down **Status** list. (This function allows you to disable a group at a later time when it is no longer needed.)

6. Enter information that identifies the group and/or its functions in the **Description** field.

7. Click the **Apply** button to add the new group. (If you change your mind after starting a new group, you can select the **Reload** button to cancel the operation.)

8. Repeat steps 3 through 7 for each new group you wish to add.


After the groups have been set up they can be assigned to user accounts through either the **Group Manager** or **User Manager** functions.

- Use the **Group Manager** when first setting up a user group since it allows multiple users to be assigned at once (see the next section for information).
- Use the **User Manager** to assign groups to an individual user account (see page 16 for information).



Once the group is defined you can assign privileges to the group. See "Assigning Privileges" on page 17 for information.

Assigning Multiple Users to a Group

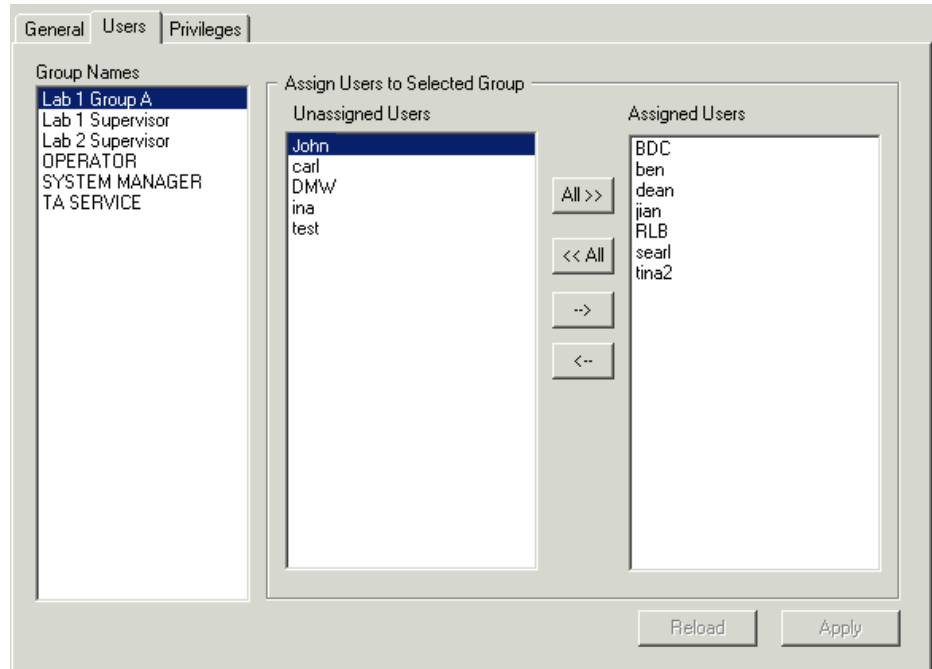
The System Manager can assign one or more users to each group by following the instructions below:

1. Select the **Group Manager** by clicking on the  icon in the left-hand pane.

2. Click the **Users Page**.
The figure shown to the right is displayed.

3. Assign the users to a group by selecting the **Group Name** from the list, then selecting the desired User(s) from the **Unassigned Users** list and then clicking the  button to move the User(s) to the **Assigned Users** list. Alternatively, you could use the  button to assign all Users to the selected group.

4. Select **Apply** to save these changes.



Assigning a Group to an Individual User

NOTE: If you are assigning multiple user accounts to a group, access the Group Manager





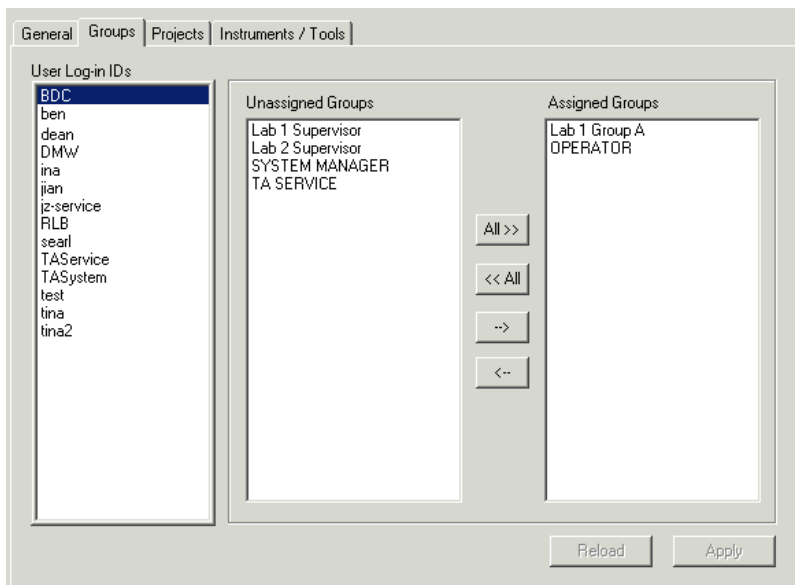
, then select the User Page.

The System Manager can assign one or more groups to each user account by following the instructions below.

1. Click the **User Accounts** icon, , to open the **User Account Manager**.

2. Select the **Groups Page**. The figure shown to the right is displayed.

3. Assign the groups to the user account by selecting the **User ID** from the list, then selecting the desired group(s) from the **Unassigned Groups** list and then clicking the  button to move the project to the **Assigned Groups** list. Alternatively, you could use the  button to assign all available groups to the selected user account. Note that each user must be assigned to the "Operator" group at a minimum. The System Manager and TA Service groups cannot be assigned in conjunction with any other group.



4. Click the **Apply** button.

Assigning Privileges

Each user assigned to a group is restricted to only those actions that are defined by the group's *privilege* list. Privileges may be defined for an individual instrument (*e.g.*, 0100–0123) or globally for the instrument type (*e.g.*, all DSC's or all AR's). In addition, one group defines privileges for all items in the module list. If privileges are not specified for each of these items, then no rights will be granted for that item.

Privileges may be set up through the **Group Manager** or using the **Module Manager**. Either option displays the same information but shows the items in a different relationship to each other.

- Use the **Group Manager** to define the privileges by group. See page 17, "Assigning Privileges to a Group."
- Use the **Module Manager** to assign groups to individual controls (privileges list) for each module. See page 18, "Assigning Groups to Privileges."

Assigning Privileges to a Group

The System Manager can assign privileges to each group by following the instructions below:

1. Log into the TA System Manager.

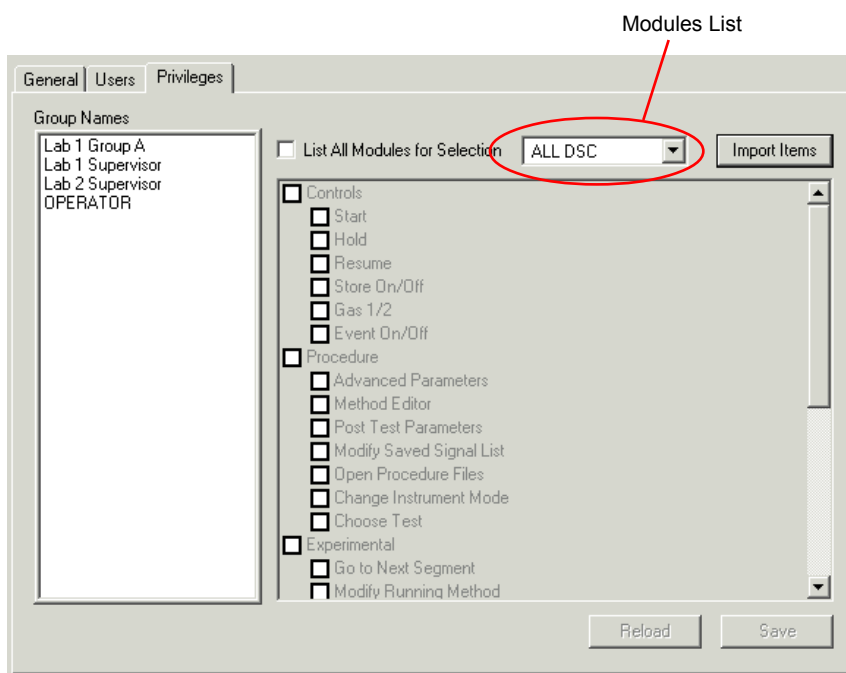
2. Select the **Group Manager** by

clicking on the  icon in the left-hand pane.

3. Select the **Privileges Page**. The window shown in the figure to the right will be displayed.

4. Select the desired group from the **Group Name** list.

5. Uncheck the **List All Modules for Selection** box, if you want to assign privileges for this group by module type (*e.g.*, DSC, TGA, AR) rather than individually for each specific module (*e.g.*, 0100 – 0123, 0500 – 0050).



6. Select a module from the drop-down list. (In our example, ALL DSC's will have the same set of privileges for the selected group.)

7. Check each control item in the list that the members of this group will have the right to access. Any item not selected will be restricted (inaccessible) for that group.

8. Select **Save** to save the selections.

- Repeat steps 6 through 8 for each module in the drop-down list. (For example, you can set up DSC privileges, then TGA, then AR, then data analysis, etc.)

NOTE: You can also view the privilege list per module using the **Module Manager**.


- Repeat steps 3 through 8 to grant privileges for any other group(s).

NOTE: Click the **Import Items** button to update the scripts that are used to generate the list of privileges for each of the system module types. This option may be needed when a new version of instrument software is installed.

Assigning Groups to Privileges

The System Manager can assign individual controls (privileges) to one or more groups by following the instructions below:

- Log into the TA System Manager.

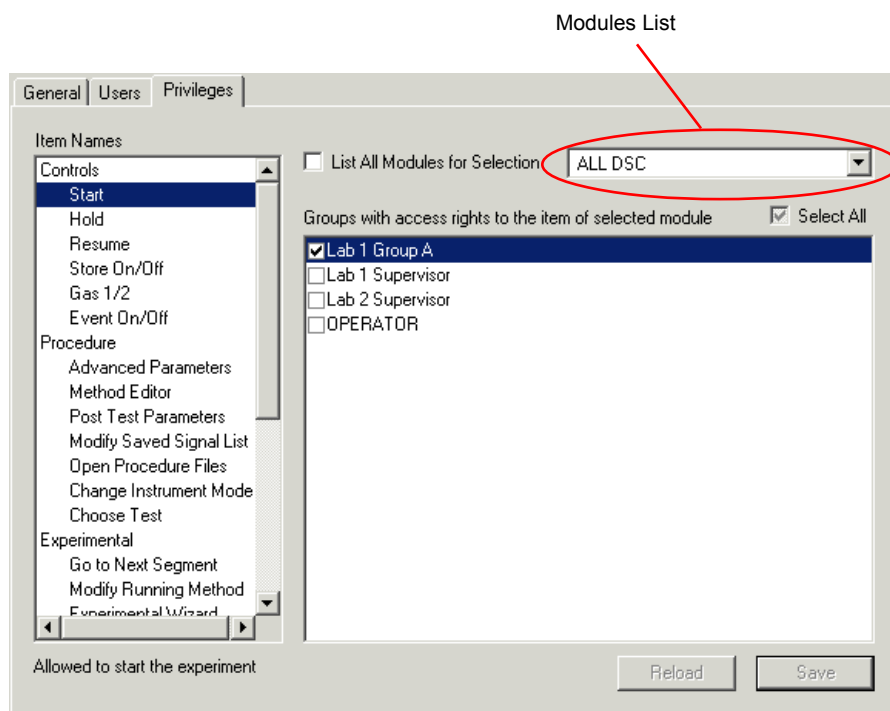
- Select the **Module Manager** by clicking on the  icon in the left-hand pane.

- Access the **Privileges Page**.
The window shown in the figure to the right is displayed.

- Uncheck the **List All Modules for Selection** box, if you want to assign privileges for this group by module type (e.g., DSC, TGA, AR) rather than individually for each specific module (e.g., 0100 – 0123, 0500 – 0050).

- Select a module from the drop-down list. (All DSC's are chosen in our example.)

- Select the first control item in the list from the **Item Name** list. (Such as the **Control/Start** function shown in our example.)




- Using the list of groups displayed in the left-hand pane, check those groups that will be granted access to this control for the selected module. Any groups that are not selected (left blank) will be restricted from having access to that item. (Alternatively, you can check **Select All** to assign all of the groups to the selected control or uncheck **Select All** to unassign all of the groups to the selected control.)

- Repeat steps 5 through 7 for each item in the control list.

9. Select **Save** to save the selections.
10. Repeat steps 4 through 9 to grant access privileges to each item in the module drop-down list. [For example, you can now set up access to the specific module items (TGA, DSC, AR), then WinUA (Universal Analysis) or RADATA (Rheology Data Analysis).]

Defining System Projects

A *Project* is defined as a way to categorize a series of data (or tests). These projects are set up using the **Project Manager**, . Setting up a new project is a permission only granted to the TA System Manager.

1. Log into the TA System Manager.

2. Select Projects by clicking

on the  icon in the

left-hand pane. The **Project Manager/General Page** will be displayed as seen in the figure to the right.

3. Click the **New** button.

4. Enter the desired **Project** name. A maximum of 50 characters may be entered.

5. Select the **Company** name from the list or enter a new one. New entries will be retained and added to the list. A maximum of 50 characters may be entered.

6. Select the **Department** name from the list or enter a new one. New entries will be retained and added to the list. A maximum of 50 characters may be entered.

7. Choose **Enabled** from the drop-down **Status** list. (This function allows you to disable a project that is no longer needed and prevents its assignment to newly-created data.)

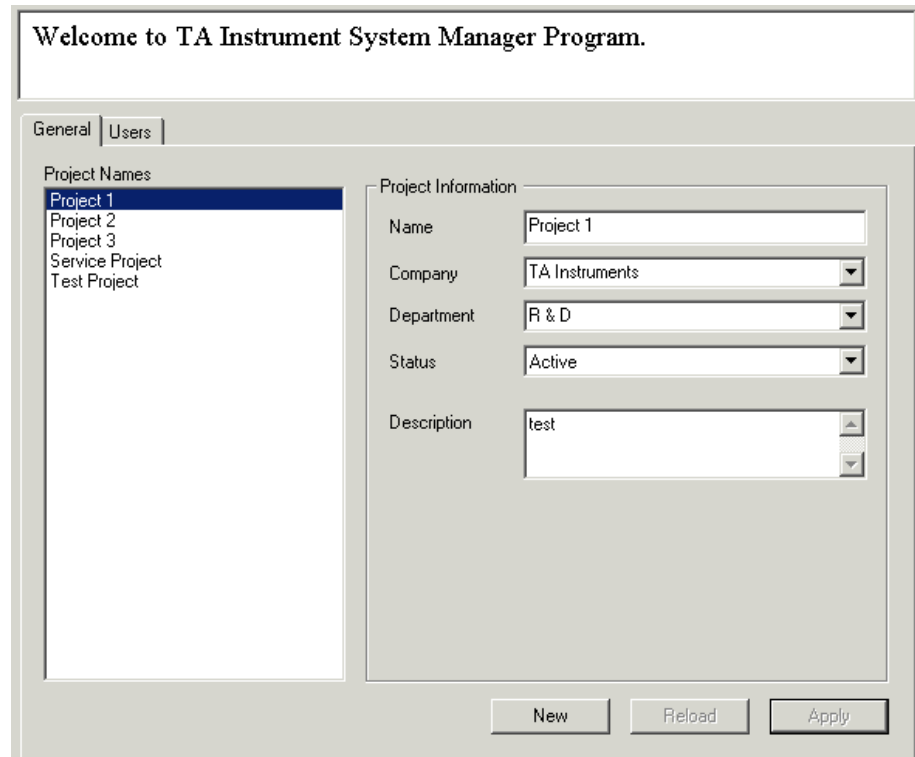
8. Enter any desired information regarding the new project into the **Description** field. A maximum of 256 characters may be entered.

9. Select **Apply** to add the new project. (If you change your mind after starting a new project, you can select the **Reload** button to cancel the operation.)

10. Repeat steps 3 through 9 to add additional projects.


After you have set up the projects desired, you can assign projects to user accounts through either the **Project Manager** or **User Manager** functions.

- Use the **Project Manager** when first setting up a project since it allows multiple users to be assigned at once (see the next section for information).
- Use the **User Manager** to assign projects to an individual user account (see page 22 for information).





Assigning Multiple Users to Projects

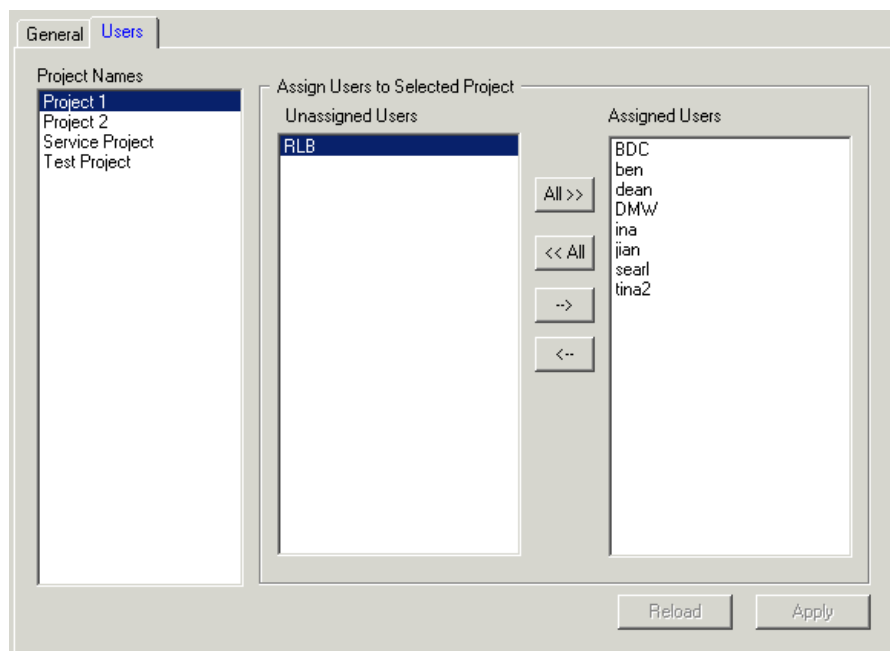
The System Manager can assign one or more users to each project by following the instructions below:

1. Log into the TA System Manager.
2. Select the **Project Manager** by clicking on the  icon in the left-hand pane.

3. Access the **Users** page. The figure shown to the right is displayed.

4. Assign the users to a project by selecting the **Project Name** from the list, then selecting the desired User(s) from the **Unassigned Users** list and then clicking the  button to move the User(s) to the **Assigned Users** list. Alternatively, you could use the  button to assign all Users to the selected project.

5. Select **Apply** to save these changes.



Assigning Projects to an Individual User

NOTE: If you are assigning multiple user accounts to a project, access the Project Manager



, then select the User page.

The System Manager can assign one or more projects to each user account by following the instructions below.

1. Click the **User Accounts** icon, , to open the **User Account Manager**.

2. Select the **Projects Page**.

The figure shown to the right is displayed.

3. Assign the desired projects to the new user account by selecting the User ID from the list, then selecting the desired Project(s) from the **Unassigned Projects** list and then clicking the

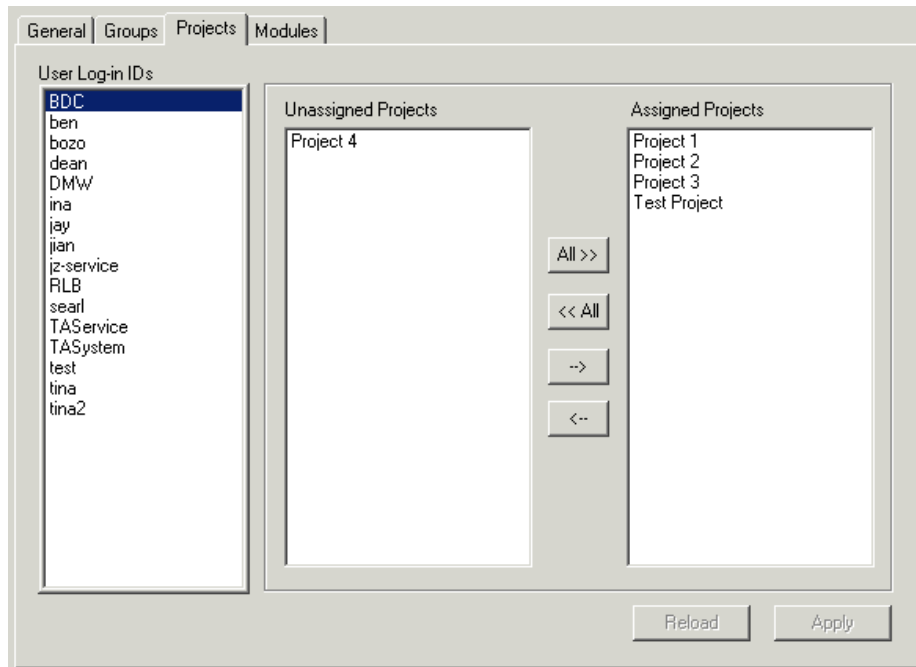


button to move the project to the **Assigned Projects** list. Alternatively, you could use the



button to assign all projects to the selected user account.

4. Select **Apply** to save these changes.



The screenshot shows the 'User Account Manager' window with the 'Projects' tab selected. The window has four tabs: 'General', 'Groups', 'Projects', and 'Modules'. The 'Projects' tab is active, displaying a list of 'User Log-in IDs' on the left, including 'BDC', 'ben', 'bozo', 'dean', 'DMW', 'ina', 'jay', 'jian', 'jz-service', 'RLB', 'searl', 'TASservice', 'TASystem', 'test', 'tina', and 'tina2'. The 'BDC' user is selected. To the right of the user list are two lists: 'Unassigned Projects' (containing 'Project 4') and 'Assigned Projects' (containing 'Project 1', 'Project 2', 'Project 3', and 'Test Project'). Between these lists are four buttons: 'All >>', '<< All', '-->', and '<--'. At the bottom right of the window are 'Reload' and 'Apply' buttons.


Defining System Modules

System modules include all instruments and the data analysis program. For Thermal Advantage Q Series™ these components are the DSC and TGA instruments, and Universal Analysis. For Rheology Advantage these components are the AR rheometers and Rheology Advantage™ Data Analysis. Each DSC, TGA, and AR instrument is represented by a unique instrument serial number (e.g., 0100 – 0123, 0500 – 0050). Access rights for these instruments may be granted based on either the individual instrument serial number or globally by instrument type (e.g., all DSC, all TGA, or all AR).

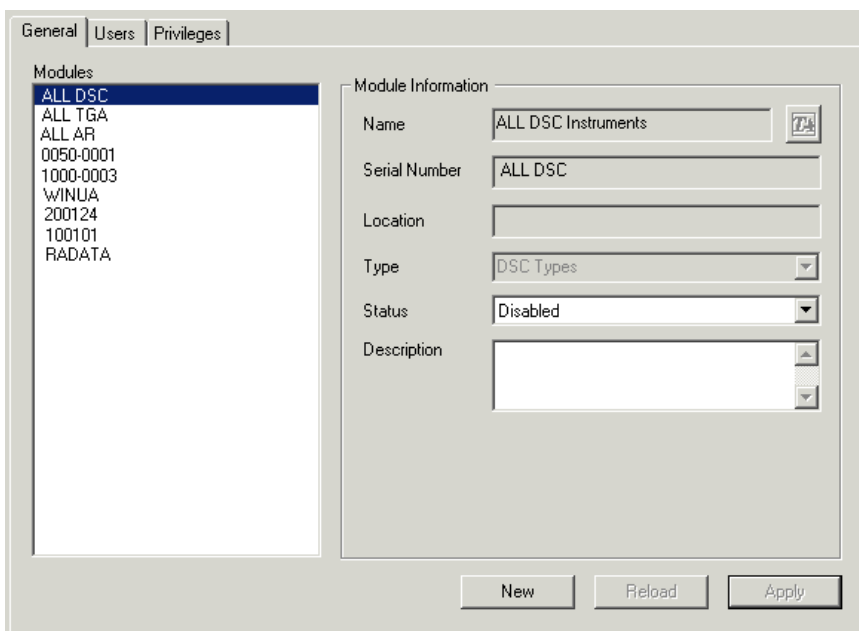
Access the TA System Manager to verify if these components have been imported into the System Manager program as follows:

1. Log into the TA System Manager.

2. Select Modules by clicking on

the  icon in the left-hand pane. The **Module Manager/General Page** will be displayed as seen in the figure to the right.

During the Integrity installation all modules (both instrument and data analysis) are imported into the system. Verify that all the instruments of the system are listed. If an instrument is missing from the list, proceed to step 3.



3. Click the **New** button.

4. Click the TA button to display the list of Integrity-licensed instruments visible from this controller. (In other words, to use this function you must perform the operation from a controller that has Advantage Q Series™ installed.) Select the instrument of interest and click **OK**. The module and the information for this instrument will be automatically imported.

5. Choose **Enabled** from the drop-down **Status** list. (This function allows you to disable a project that is no longer needed and prevents its assignment to newly-created data.)

6. Enter any desired notes regarding the new module into the **Description** field. A maximum of 256 characters may be entered.

7. Select **Apply** to add this new module. (If you change your mind after starting a new module, you can select the **Reload** button to cancel the operation.)


8. Repeat steps 3 through 7 for each module to be added.

After you have verified/set up the modules desired, you can assign modules to user accounts through either the **Module Manager** or **User Manager** functions.



- Use the **Module Manager** when first setting up a module since it allows multiple users to be assigned at once (see the next section for information).
- Use the **User Manager** to assign modules to an individual user account (see page 25 for information).

Assigning Multiple Users to a Module

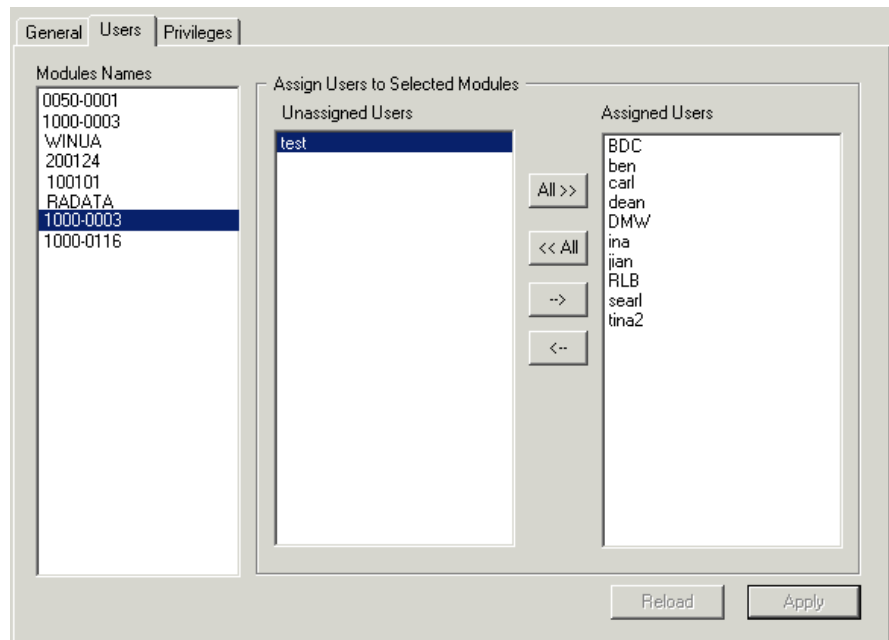
The System Manager can assign one or more users to each project by following the instructions below:

1. Log into the TA System Manager.
2. Select the **Module Manager** by clicking on the  icon in the left-hand pane.

3. Access the **Users** page. The figure shown to the right is displayed.

4. Assign the users to a module by selecting the **Modules Name** from the list, then selecting the desired User(s) from the **Unassigned Users** list and then clicking the  button to move the User(s) to the **Assigned Users** list. Alternatively, you could use the  button to assign all Users to the selected module.

5. Select **Apply** to save these changes.



Assigning Modules to an Individual User

NOTE: If you are assigning multiple user accounts to a module, access the Module Manager





, then select the User page.

The System Manager can assign one or more modules to each user account by following the instructions below.

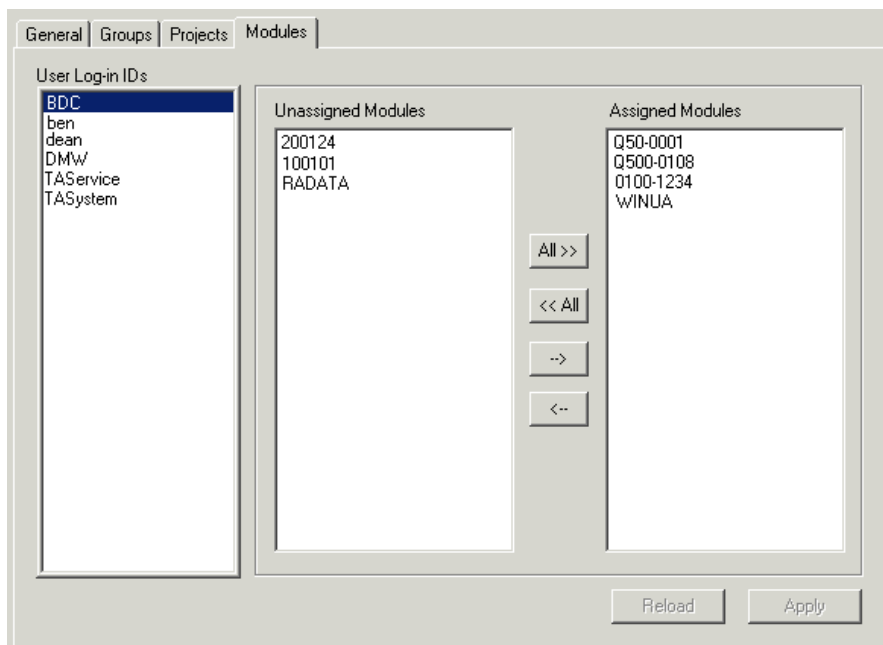
1. Click the **User Accounts** icon, , to open the **User Account Manager**.

2. Select the **Modules Page**.

The figure shown to the right is displayed.


3. Assign the desired modules to the new user account by selecting the **User ID** from the list, then selecting the desired module(s) from the **Unassigned Modules** list and then clicking the  button to move the project to the **Assigned Modules** list. Alternatively, you could use the  button to assign all modules to the selected user account.

4. Select **Apply** to save these changes.



User Login IDs	Unassigned Modules	Assigned Modules
BDC	200124	Q50-0001
ben	100101	Q500-0108
dean	RADATA	0100-1234
DMW		WINUA
TAService		
TASystem		

System Settings Options


Select the System Settings icon,  , to access the system settings and event logs. Some of these settings—such as the server and database information—were established when the system was installed.

Server and Database Information

The server and database information displayed on the **General Page** shown in the figure to the right is obtained during set up and creation of the database.

Changing the TA System Options

The **System Settings Manager** displays a list of the available options related to password log-in policies as well as the way changes are saved within this program.

1. Log into the TA System Manager.
2. Click on the **System Settings**,  , icon in the left-hand pane.
3. Select the **Settings** Page. The **System Settings Manager/ Settings Page** will be displayed as seen in the figure to the right.

A description of each parameter is listed below:

- **Maximum # of Log-in Attempts:** The number of times that you want to allow a user to try logging into the system before it becomes inaccessible (disabled). If the system becomes inaccessible, the system manager must re-enable the account. The default number of attempts is three.

The TA System Help Manager provides online help for operating the System Manager program.

General | Settings | Activities | System Log

Server Information

Name:	TA-ORCL9
Product:	Oracle9i
Product Version:	9.0.1.1.1
Installation Date:	05/08/2002 13:52:08
Provider:	ORAOLEDB.Oracle

Database Information

Database Name:	TAEXPDB
Creation Date:	08/12/2002 10:53:11

General | Settings | Activities | System Log

TA Instrument Database System Options

Maximum # of Log-in Attempts	4	
Minimum Password Length	4	char.
Log-in Session Timeout	15	min.
Password Expiration Time	24	Months

☒ TAsystem Password Never Expires ☐ Case Sensitive User IDs

☒ TAservice Password Never Expires ☒ Case Sensitive Passwords

TA System Manager Options

☒ Automatically apply changes when switching between pages

☒ Automatically apply changes when switching between list items.

Reload Save

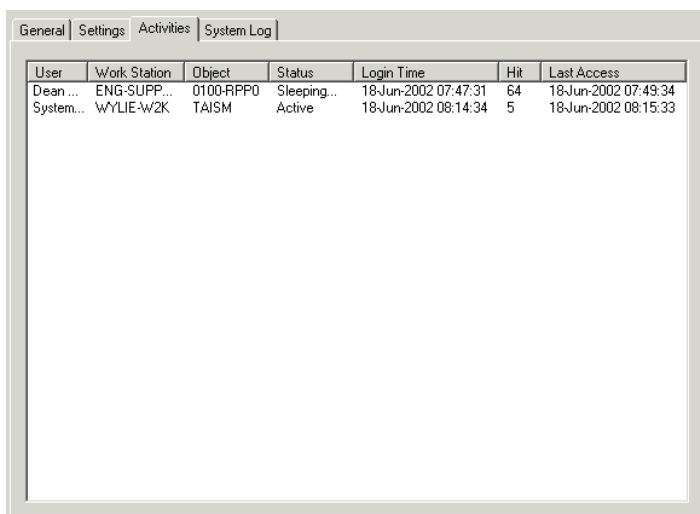
- **Minimum Password Length:** The minimum number of characters that a user must enter when defining their password. This setting will be enforced when creating new user accounts or the next time the user is required to change their password. A maximum of 20 characters is allowed. The default setting is four characters.
 - **Login Session Timeout:** The amount of inactivity time (e.g., no user interaction with program) before the user will be automatically logged out. The default time out is 15 minutes.
 - **Password Expiration Time:** The default password expiration time from the time of creation of the user account. The default password expiration time is three months from today's date. This time can be customized through the User Account information.
 - Account never expires options:
 - Check the box, **The password of TAsystem account never expires**, if you do not want to apply the password expiration time to this account.
 - Check the box, **The password for TAservice account never expires**, if you do not want to apply the password expiration time to this account. It is recommended that you enable this option to allow easier access by the TA Service Representative, if needed.
 - Case sensitive options:
 - Check the box, **Case Sensitive User ID**, if you want to enforce case sensitivity for the User ID.
 - Check the box, **Case Sensitive Passwords**, if you want to enforce case sensitivity for the passwords.
 - TA System Manager options: These options define how you want to apply changes within the TA System Manager. (Changes made to these options take effect immediately and do not require you to select **Apply**.)
 - Check **Automatically apply changes when switching between pages**, if you want the changes to take effect immediately when you switch to a different page (you will not have to click the **Apply** button).
 - Check **Automatically apply changes when switching between list items**, if you want the changes to take effect immediately upon switching to a different item listed on the left-hand side of the page (you will not have to click the **Apply** button).
4. Choose the desired options, then click the **Save** button.

NOTE: Use the Reload button to set the system defaults back to their saved state.

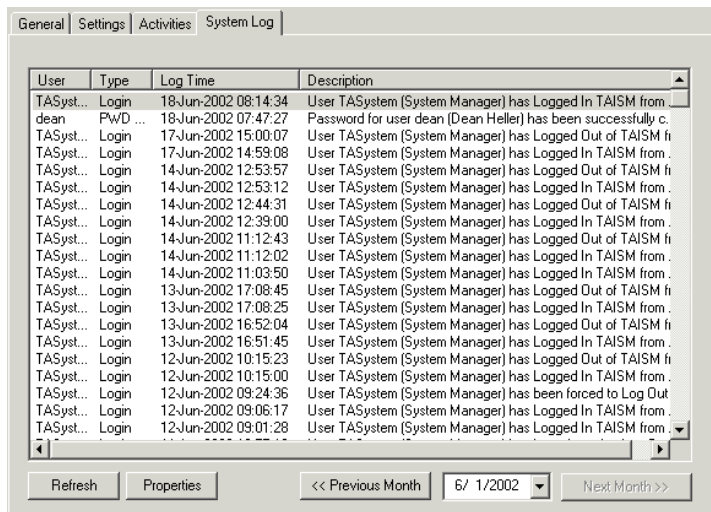
Activities and System Logs

The system settings option within the TA System Manager can be accessed to display the activities and system log information.

Click the **Activities Page** to display the Activities Log as seen in the figure to the right. This is a view-only report that gives you an overview of who is logged into the modules of this system.



User	Work Station	Object	Status	Login Time	Hit	Last Access
Dean ...	ENG-SUPP...	0100-RPP0	Sleeping...	18-Jun-2002 07:47:31	64	18-Jun-2002 07:49:34
System...	WYLIE-WZK	TAISM	Active	18-Jun-2002 08:14:34	5	18-Jun-2002 08:15:33



User	Type	Log Time	Description
TASyst...	Login	18-Jun-2002 08:14:34	User TASystem (System Manager) has Logged In TAISM from ...
dean	PWD ...	18-Jun-2002 07:47:27	Password for user dean (Dean Heller) has been successfully c...
TASyst...	Login	17-Jun-2002 15:00:07	User TASystem (System Manager) has Logged Out of TAISM fr...
TASyst...	Login	17-Jun-2002 14:59:08	User TASystem (System Manager) has Logged In TAISM from .
TASyst...	Login	14-Jun-2002 12:53:57	User TASystem (System Manager) has Logged Out of TAISM fr...
TASyst...	Login	14-Jun-2002 12:53:12	User TASystem (System Manager) has Logged In TAISM from .
TASyst...	Login	14-Jun-2002 12:44:31	User TASystem (System Manager) has Logged Out of TAISM fr...
TASyst...	Login	14-Jun-2002 12:39:00	User TASystem (System Manager) has Logged In TAISM from .
TASyst...	Login	14-Jun-2002 11:12:43	User TASystem (System Manager) has Logged Out of TAISM fr...
TASyst...	Login	14-Jun-2002 11:12:02	User TASystem (System Manager) has Logged In TAISM from .
TASyst...	Login	14-Jun-2002 11:03:50	User TASystem (System Manager) has Logged In TAISM from .
TASyst...	Login	13-Jun-2002 17:08:45	User TASystem (System Manager) has Logged Out of TAISM fr...
TASyst...	Login	13-Jun-2002 17:08:25	User TASystem (System Manager) has Logged In TAISM from .
TASyst...	Login	13-Jun-2002 16:52:04	User TASystem (System Manager) has Logged Out of TAISM fr...
TASyst...	Login	13-Jun-2002 16:51:45	User TASystem (System Manager) has Logged In TAISM from .
TASyst...	Login	12-Jun-2002 10:15:23	User TASystem (System Manager) has Logged Out of TAISM fr...
TASyst...	Login	12-Jun-2002 10:15:00	User TASystem (System Manager) has Logged In TAISM from .
TASyst...	Login	12-Jun-2002 09:24:36	User TASystem (System Manager) has been forced to Log Out
TASyst...	Login	12-Jun-2002 09:06:17	User TASystem (System Manager) has Logged In TAISM from .
TASyst...	Login	12-Jun-2002 09:01:28	User TASystem (System Manager) has Logged In TAISM from .

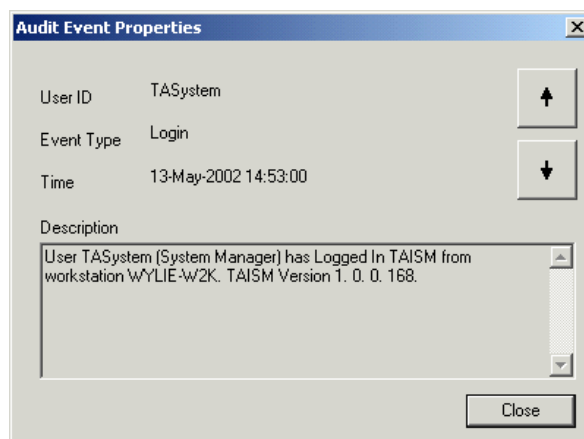
Click the **System Log Page** to display the System Log as seen in the figure to the left. This is a view-only report that records audit events associated with the TA System Manager (TAISM) program. The report contains items such as logins and logouts, as well as user, projects, and group changes.



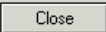
Showing Audit Event Properties

Each audit event contained in the Systems Log is associated with a particular TA System Group account and is classified according to its type and logged with a time of creation. Access this information by clicking the **Properties** button on the **System Settings Manager/System Log Page**. The **Audit Event Properties** window (shown in the figure to the right) is displayed.

You can step forward or backward through the System Log events, displaying each event's properties, by clicking on

the  and  buttons.



User ID	TASystem	
Event Type	Login	
Time	13-May-2002 14:53:00	
Description	User TASystem (System Manager) has Logged In TAISM from workstation WYLIE-WZK. TAISM Version 1. 0. 0. 168.	
		

Chapter 2

Using the Integrity™ System

Overview

The TA Instruments Advantage Q Series™ Instrument Control and Universal Analysis programs, with the Integrity option, are functionally the same as their non-Integrity counterparts. This chapter deals with the differences for each of these components.

General Changes

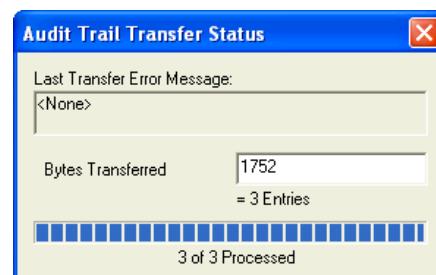
- Logging in is required to access the licensed instruments and data analysis software. The TA System Manager is responsible for creating user accounts, for assigning instruments and data analysis access rights (modules), and for assigning groups and their privileges. The logging-in and System Manager functions are described in Chapter 1.
- A secure Oracle® database is used to store and retrieve data.
- A computer-generated, time-stamped audit trail is part of the system.

Using an Integrity-Licensed Instrument

Once an instrument has been set up with an Advantage Integrity license, it will become part of the Advantage Integrity system. Access will be controlled, data will be stored in the Oracle® database, and an audit trail will record events. Once you are logged in to the instrument, the basic operation of an Integrity instrument is the same as its non-Integrity (standard) counterpart for calibrating, setting up experiments, and starting runs.

The few differences are noted here.

- **Audit Trail Transfer (applies to thermal analysis only):** When the instrument control window is first opened, the **Audit Trail Transfer Status** window (shown here) is displayed, if there are instrument audit trail messages to be transferred. During the audit trail transfer do not close the instrument control window. You may also see this window when closing the instrument control window.




- **SUID# (applies to thermal analysis only):** Instead of defining the data storage path, the database will automatically assign a SUID# to the original, raw data record. This number can be seen on the **Summary Page** of the **Experimental View** (shown in the figure to the right).

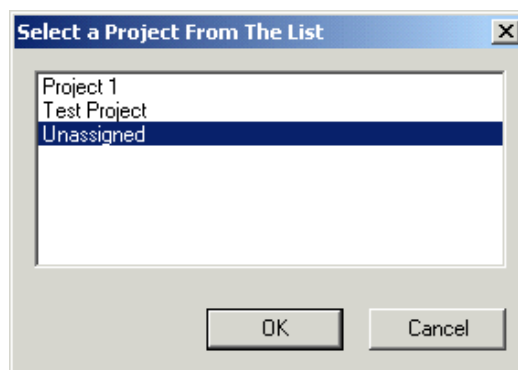
NOTE: Each saved data record within the database will also be assigned a Record ID #, which is displayed on any saved images that are created.

- **Project Name:** Each experiment is assigned to a Project. Project assignment provides a means to category the data in the database, and then later uses that assignment to sort the records in the database for easier retrieval. The available projects are those assigned to you by the TA System Manager (see page 20). The TA System Manager is also responsible for defining the projects available in this system.

Summary Page for Integrity-Licensed Instrument Control

To assign a project to a run follow these steps:

1. Click on the  button to the right of the **Project Name** field. The window shown here will be displayed.
 2. Select a project from those displayed and click **OK**.
- **Operator:** The **Operator** field on the **Notes Page** will automatically display the User ID of the person creating the run and can not be changed. See the section "Handling Multiple Users for a Single Instrument" on page 32 for rules that apply when there is more then one instrument operator.



- **Restricted or Unavailable Functions:** Within the Advantage Integrity system the TA System Manager can define privileges (*e.g.*, restrict actions) within each module of the system (see page 17).

Within the instrument control programs (thermal analysis and rheology) this list of controllable privileges includes items such as access to calibration parameters and analysis, modifying a run, etc. Therefore, typical functions may not be available depending on the access groups(s) assigned to you. Consult with your TA System Manager to learn about your privilege list for instrument control.

- **Unavailable Instrument Control functions:**

Thermal Analysis: A set of functions that are available in the standard version of Q Series™ instrument control, are *not* available when logged into the Integrity system. These functions include:

- Run Reject
- Archive Enable
- Autoanalysis.

Rheology: A set of functions that are available in the standard version of Rheology Advantage instrument control and data analysis, are *not* available when logged into the Integrity system. These functions include:

- Load/Save notes, Load/Save options
- Instrument new and select
- Navigator
- Switch to Data Analysis with an active run.

- **Thermal Analysis Q Series Method, Procedures and Sequence Files:** These files are *not* saved in the database, nor are the changes audited for these files in this system. They continue to be saved at the designated file location specified by the operator. However, file open and save for these file types are recorded in the audit trail. Moreover, the saved data record contains the details of the experimental conditions (*e.g.*, method, calibration, and instrument parameters) within the parameter block of the saved data record. This information can be viewed in the Universal Analysis program by selecting **View/Parameter Block**.
- **Thermal Analysis Q Series Active Experiments:** An experiment which is currently in progress may be viewed in Universal Analysis, but until the experiment is complete you can not save any results (*e.g.*, saved analyses, pdf generation).
- **Rheology Active Experiments:** An experiment which is currently in progress cannot be viewed in Rheology Advantage Data Analysis until the experiment is complete and saved.

Handling Multiple Users for a Single Instrument

When there is more than one user accessing a single instrument, the following rules apply depending upon the type of Integrity™ program you are using.

Using Thermal Analysis Integrity:

- You can *alter another user's run* only when assigned access rights to the project associated with that run. You will receive a message asking if you wish to "take ownership" of that run. Select Yes to take ownership. Your name will now be assigned as the **Operator** on the **Notes Page**. Select No to deny ownership of that run, then you can click the **Append** button to create a new run.
- You can still *start another user's run*, even if you do not have access rights to the project assigned to that run. In this case, your User ID will be recorded as the **Run Operator** in the data record's parameter block, which can be viewed through the Universal Analysis program's **View/Parameter Block** function. The operator name will remain as the User ID of the original owner.
- You may *delete any runs* regardless of their assigned projects.
- If you do not have access rights to the assigned run's project, you will get an **Access Not Allowed** message. In this case, you will need to select the **Append** button to create a new run.
- When you load a saved sequence, the currently logged in user is designated as "Operator" for all runs. The project specified for the current run will then be applied to all runs in the sequence. If the user does not have access rights (privileges) to that project, the project for each run will be set to "Unassigned."

Using Rheology Integrity:


- You can alter another user's run only when assigned access rights to the project associated with the run. When you log on you will receive a message asking if you wish to take ownership of that run. Select Yes to take ownership. Your name will now be assigned as the operator on the notes page, and you will be able to perform any action that your privileges allow. If you do not take ownership then the run will continue and you will not be able to log on.

Using an Integrity-Licensed Universal Analysis

Universal Analysis can access and analyze data stored in the Integrity database system, as well as data stored in traditional data files (historical data), but not both at the same time. When logged into the Integrity system, only database records can be accessed. A secure **Audit Trail** is generated for all actions performed while logged into the database, including the logging in/logging out process. There is no Audit Trail while viewing historical (disk based) data.

Most of the functions available in the Integrity-licensed Universal Analysis program are the same as those provided in its non-Integrity (standard) counterpart.


The differences between the programs are noted below:

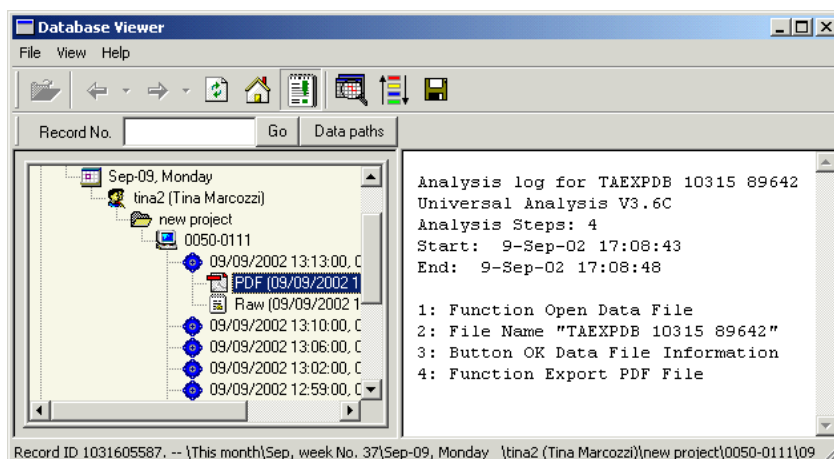
- **Logging In:** Before accessing records in the Integrity database you must log into the database using a valid user name and password (see page 18 for details). Any traditional data files that are open must be closed before logging in.
- **Opening Files:** After logging into the database you will need to locate the data from your experiment. Select **File/Open**. The **Database Viewer** will be displayed. (See page 36 for more information on the Database Viewer.) Use the searching and sorting functions of the Database Viewer to locate and highlight the desired record. The only records displayed in the viewer will be those assigned to projects to which you have access rights. To open the file, click the  button or select **File/Open**, and the data file will be opened in Universal Analysis. See the remainder of this chapter for information on using the Database Viewer and Audit Trail.
- **Restricted or Unavailable Functions:** The system administrator can use the TA System Manager program to define privileges (allowed functions) within each module of the Integrity system (see page 17). For Universal Analysis, this list of controllable functions includes most of the menu items in the program. The functions that are available to you depend on your assigned access group(s).

Some functions available in standard mode are *never* available when logged into the Integrity database. These functions include:

- Automatically reopening records (**File/Reopen**)
 - Removing saved analysis information (**File/Remove Saved Analysis**)
 - Editing raw data parameters (**File/Edit Param Block**)
 - Excluding data (**Edit/Exclude Data**)
 - Editing cells within the spreadsheet view of the data (**Edit/Modify, Cut, Paste**)
 - Editing textual reports (**View** menu)
 - Creating an autoanalysis queue (**Macros/Autoqueue, View/Autoqueue Report, Log**)
- **Analysis Log:** Each action performed within Universal Analysis is recorded in an analysis log for the currently open data record. When an analysis or report is saved in the database (*e.g.*, using the **Save Analysis** or **Export PDF File** functions), the associated analysis log is stored in the database along with the new record.

The analysis log for *reports* is viewed directly through the Database Viewer (**File/Open**). Select the desired record in the viewer and click on the **More**

Information button, , on the tool bar. If available, the analysis log will be displayed in the right pane of the Database Viewer as shown in the figure to the right.

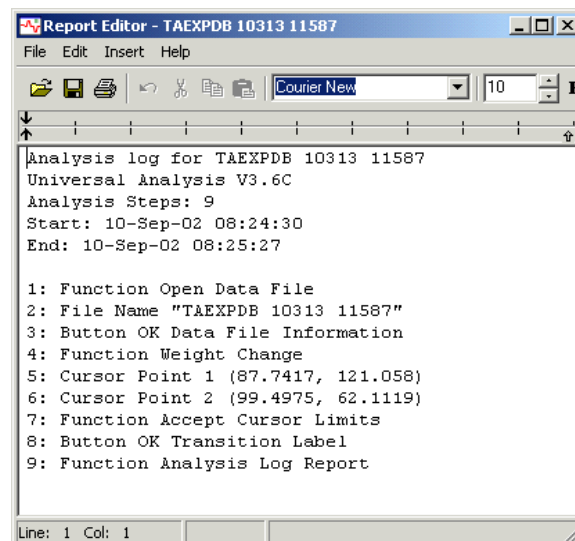


Analysis Log Displayed in the Database

You can also view the analysis log for a *saved analysis* by opening the saved analysis record in Universal Analysis and select **View/Analysis Log**. The window shown below is displayed in the Report Editor.

- **Saving Results:** To save the analysis performed on an original (raw) data file, you can select the **File/Save Analysis** and/or **File/Export PDF File** functions.
 - **Save Analysis Only** saves the analysis results generated thus far for the current data record.
 - **Save Analysis and Data** saves the analysis results plus a complete copy of the original raw data.
 - **Export PDF File** saves a copy of the analyzed graph in Portable Document Format.

In each case a new database record is created. Records generated from the raw (original) data are saved in the database under the date of the original data record. An analysis log, detailing the functions performed, is stored with the saved record. Integrity database records are protected from modification or deletion.



Analysis Log for Saved Analyses


- **Macro (mac), Initialization (ini), and Custom Report Template (uat) Files:** These files are not saved in the database. Changes to these files are not audited by the system. The files are saved at the file location specified by the operator. However, file open and file save functions for these files are recorded in the audit trail, and in the analysis log for the currently open database record.

Using an Integrity-Licensed Rheology Data Analysis

Rheology Advantage™ can access and analyze data stored in the Integrity database system as well as data stored in traditional data files (historical data). A secure audit trail is generated for all actions performed while logged into the database that results in a committed report. No audit trail is generated while accessing historical data.

Most of the functions available in the Integrity-licensed Rheology Advantage program are the same as those provided in its non-Integrity counterpart.

The differences between the programs are noted below:

- **Logging In:** Before accessing records in the Integrity database you must log into the database using a valid user name and password (see page 9 for details). Selecting **Cancel** on the Log-in window will open the non-Integrity version of Rheology Advantage Data Analysis.
- **Opening Files:** After logging into the database you will need to locate the data from your experiment. Select **File/Open**. The **Database Viewer** will be displayed. (See page 36 for more information on the Database Viewer.) Use the searching and sorting functions of the Database Viewer to locate and highlight the desired record. The only records displayed in the viewer will be those assigned to projects to which you have access rights. To open the file, click the  button or select **File/Open**. See the remainder of this chapter for information on using the Database Viewer and Audit Trail.
- **Restricted or Unavailable Functions:** The system administrator can use the TA System Manager program to define privileges (allowed functions) within each module of the Integrity system (see page 17). For Rheology Data Analysis, this list of controllable functions includes most of the menu items in the program. The functions that are available to you depend on your assigned access group(s).

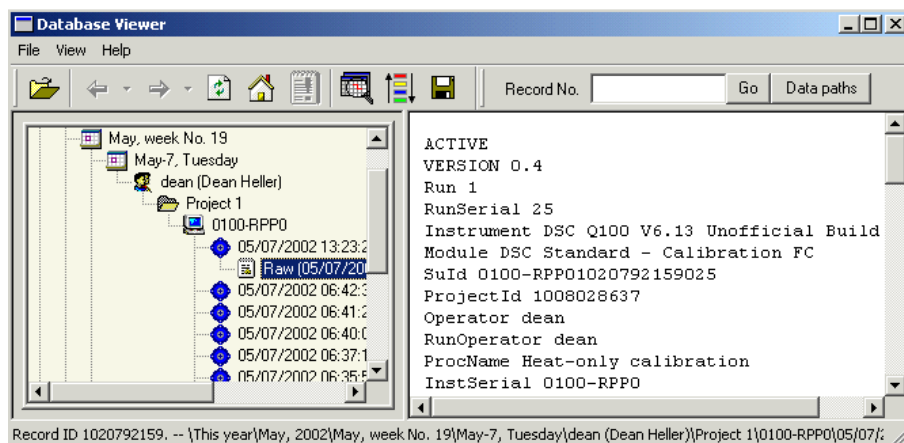
Some features available in standard mode are *never* available when logged onto the Integrity database. These are:

- Rheology Advantage Navigator
 - Making any changes to the raw data and overwriting the original file
 - Analyzing running data
 - Undo/Redo functions.
- **Analysis Session:** Each action performed within Rheology Advantage data analysis is recorded in an analysis log. When a session is committed to a report the associated log is stored in the database along with the report. The analysis log for reports is viewed through the database viewer.
 - **Print and Commit:** This produces a hard copy report with a unique record ID#, and a saved analysis session in the database.
 - **Save to Disk:** Data stored in the database can be extracted (as a copy) and saved to disk so that it can be read by the non-Integrity version of the data analysis software.
 - **Database and Disk-Based Files in Same Session:** If you have privileges set up to allow both secure and non-secure files to be opened in the same session, the following rules apply:
 - If the filename is displayed or printed, it will have text added to indicate it is from a non-secure source.

- If the session is saved, the file will be saved to the database. Text will be added to the name to indicate that it was from a non-secure source and there will be an import entry in the audit log.
- If a hard copy is produced by performing a print and commit, the footer will include a note to indicate that the report contains non-secure data.

Using the Database Viewer

Part of the Advantage Integrity system includes a secure Oracle database. Depending on whether you are using Thermal or Rheology Integrity, this data can include raw (original) data, saved analysis, saved session, Tzero calibration, saved Adobe PDF (Portable Document Format) files, and saved BMP (Bitmap) images. Data contained in this database can be displayed, sorted, and exported using the **Database Viewer** (shown below).




To open a saved data record from an Integrity-licensed data analysis program select **File/Open** from the menu after logging into the system. The Database Viewer will be displayed. Follow the instructions in the section beginning on the next page to locate and open data records.


The Database Viewer can also be displayed from a thermal analysis Q Series™ Integrity-licensed instrument control program by selecting **View/Experimental Data in Database** from the menu after logging into the system. However, files cannot be opened except through the Universal Analysis program.

Browsing for Data in Tree View

The left-hand pane of the **Database Viewer** window (shown on the previous page) can be used to locate data in tree view. Click on each item to open the items below it until you come to the desired record. The order of these

items may be customized using the  button on the tool bar. See "Customizing the Sort Order" on the next page for information.


The items displayed in the left-hand pane are used to designate a specific file, document, or piece of information as seen in the list to the right.

- **Dates, User, Project, Instrument, Run Number:** When you click on one of these icons, the records that apply are displayed in the right-hand pane. See the figure on the previous page for an example of this.
- **Raw Data files, Tzero Calibration files, Text files** (saved Universal Analysis report), **Saved Analysis Session files:** When you select the data file record, the data file parameter block information is displayed in the right-hand pane. To open the file, click the  button or select **File/Open**, and the data file will be opened in Universal Analysis.
- **PDF files (thermal analysis only):** When you select an Acrobat PDF file, the Acrobat Reader program will open and the file will displayed.
- **BMP files (thermal analysis only):** When you select a bitmap image file the image will open in the right-hand pane.

NOTE: Records generated from the raw (original) data (such as saved analysis pdf files) are saved under the date of the original record.

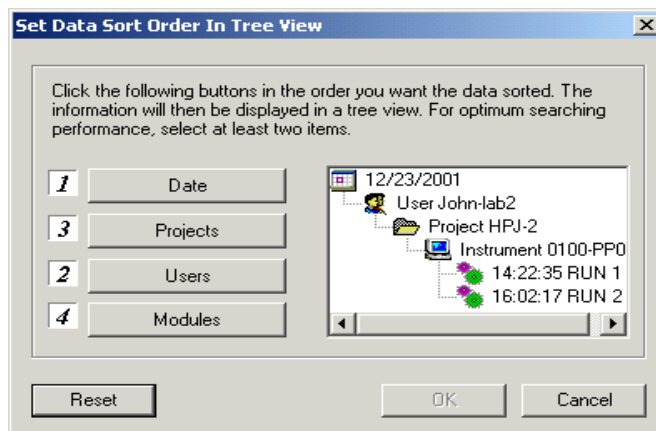


Customizing the Sort Order

You can change the way the database information is arranged, or sorted, in the left-hand pane's tree view by clicking the  button on the **Database Viewer** or **Audit Trail Viewer** tool bar to open the window shown here.

The numbers shown on the left indicate the order set for the tree view display. To change the order, follow these steps:


1. Click the **Reset** button to clear the order.
2. Click the classification buttons in the order you wish to display the hierarchy. A number is displayed next to the button indicating the level in the tree view. (At least two items should be selected to optimize searching performance.) For example, you may wish the data to be sorted primarily by **Date**. In that case, click the **Date** button first. To continue setting up the hierarchy as seen in the figure above, you would click the **Users** button second, **Projects** button third, and **Modules** button last.
3. Click **OK** when finished. The **Database Viewer/Audit Trail Viewer** will arrange the information according to the selected hierarchy.

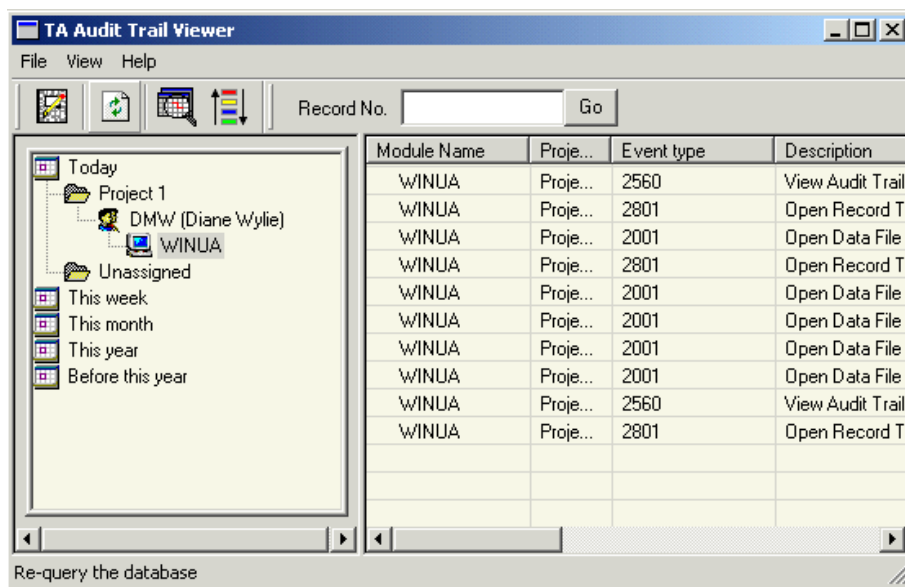


Viewing Audit Trail Events

The TA Instruments' Integrity system provides secure, computer-generated, time-stamped audit trails to independently record events. Each record identifies the person, time /date, and a description of the event. Comments may be added, if desired, by the user.

The Audit Trail can be viewed from either the Advantage Instrument Control program or Universal Analysis program by selecting **View/Audit Trail** from the menu. This window (shown to the right) can be used to view audit trail events and add comments to an audit trail. The events shown in this window can be sorted to enhance locating records using

the **Set Sort Order**, , functions (see page 38 for information).



What Events are Recorded?

Various events are recorded in the **Audit Trail** depending upon which Integrity program is in use. This section provides a description of the recorded events available through the Audit Trail Viewer.

Instrument Control Events

The recorded events include:

- Logging in/logging out of the programs (including automatic log outs)
- All instrument messages
- Calibration changes (including rheology zero gap and rheology temperature system changes)
- Run start and completion events
- Rheology run override (temperature, equilibration, etc.) and abort
- Rheology run results stored
- Thermal Analysis Q Series Autosampler pan load/unloads
- Modifications to the running experiment (e.g., method or gas changes and add or modify step)
- Procedures (file open and save)
- Q Series method or sequence file open and save
- Rheology geometry, session open, and save
- Software version changes
- Rheology firmware updates.

Details of the experimental conditions (e.g., Thermal analysis method, calibration, and instrument parameters or rheology procedure, geometry, and instrument options) are stored with each saved data record. This information can be viewed in the Universal Analysis program by selecting **View/Parameter Block** or viewed in the Rheology Advantage Data Analysis program as you normally view data.

Universal Analysis Events

The recorded events for the Universal Analysis program include:

- Logging in/logging out of the programs (including automatic logouts)
- Data record open and exports (e.g., printing, PDF generation)
- Saved analysis open and save
- Results and data report open and save
- PDF open and save
- Software version changes

Details of the analyses are recorded in the analysis log within the saved analysis, PDF, or BMP image generated from Universal Analysis. After opening a data record in Universal Analysis, all actions are recorded within the analysis log. Once your analysis is complete, you can save this record, along with the associated analysis log, back to the database by selecting **File/Save Analysis** and/or **File/Export PDF File**. If the data is not saved, the analysis log is not recorded. Saved analysis logs can be viewed through the Database Viewer window.

Rheology Data Analysis Events

The recorded events for the Rheology Data Analysis program include:

- Logging in and out
- Data record export to disk
- Session open and saved
- Report print and commit
- Software version changes

TA System Manager Events

The recorded events for the TA System Manager program include:

- Logging in/logging out of the programs (including automatic logouts)
- Creation and modification to User Accounts, Projects, System Objects, and Groups
- Modifications to system settings
- Archiving



The audit trail for the TA System Manager is only accessed through the TA System Manager by selecting **System Settings**, then selecting the System Log page. See the Advantage Integrity online help for further information.

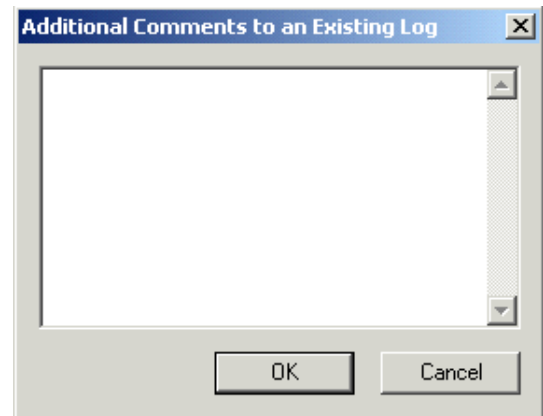
Adding Audit Trail Comments

You can add a comment to an existing audit trail entry or to add a new audit trail entry to further explain an action or event. There are several different places in the system that can be accessed to add an audit trail comment.

- You can add a new comment from the Universal Analysis program or from the instrument control program (see next page).
- You can add a comment to an existing audit trail entry from the **Audit Trail Viewer** window in either program (see the section below).

Adding a Comment to an Existing Audit Trail Entry

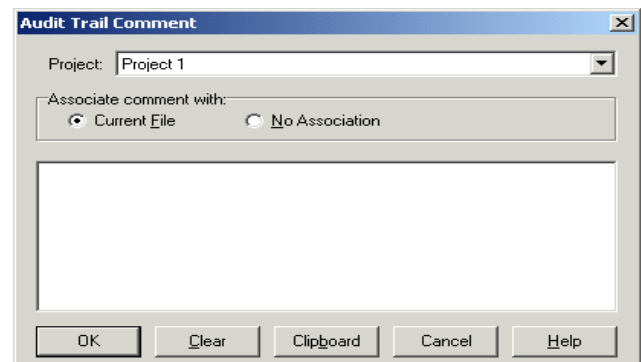
1. Open the **Audit Trail Viewer** by selecting **View/Audit Trail** from either the Advantage Instrument Control or Universal Analysis program.
2. Browse the audit trail to find the desired entry for the additional comment. Once the audit entry  is highlighted, click on the  button on the tool bar or double click on the audit entry to display the **Additional Comments to an Existing Log** window.
3. Type the desired comment to be added to the comments section for this audit trail entry.
4. Select **OK** when finished.



Adding a New Audit Trail Entry

To add a new audit trail entry ["User Comment"] to the audit trail, follow these steps:

1. Open the desired program. From an instrument control program, select **View/Add an Audit Comment** or from Universal Analysis select **Edit/Audit Trail Comment**. The appropriate window will be displayed.
2. Select the desired project association from the drop-down list.
3. *Universal Analysis:* Select to associate this comment entry with the **Current File** or to have **No Association**.



Universal Analysis Add Audit Trail Comment


Instrument Control: Select to associate this comment entry with the **Selected Run** (e.g., same Record ID) or to have **No Association**.

4. Type in the desired comment.
5. Select **Add** (within Instrument Control) or **OK** (within Universal Analysis) when finished.


Instrument Control Add Audit Trail Comment

Viewing an Audit Trail Entry Report

Comments can be seen in the Comment column within the **Audit Trail Viewer**, along with the data and time of entry, and user name (see the figure below). Multiple comments may be entered for any entry. You may need to

refresh () the viewer to see it after immediately adding the entry.

Added by	Record ID	Comments
Diane Wylie	1017235023	15-Jul-2002 13:2...
Diane Wylie	1017235023	
Diane Wylie	1020291034	
Diane Wylie	1020291034	
Diane Wylie	1020291034	
Diane Wylie	1020291034	
Diane Wylie	1020291034	
Diane Wylie	1020291034	
Diane Wylie	1020792159	
Diane Wylie	1020792159	
Diane Wylie	1017235023	

To view any audit entry in textual format, browse the tree-view to the lowest level and highlight the desired Audit Entry  . A textual report for this entry will be displayed in the right-hand table view pane.

Chapter 3

Backing Up & Archiving the Database

Overview

It is extremely important to regularly back up the information in the Oracle® database. **Daily backup** to a reliable utility is recommended to best maintain the integrity of the system and allow retrieval of data, if necessary.

When looking to purchase a backup utility you may want to consider the following minimum attributes:

- Ability to backup a live (active) database
- Job scheduling capability
- Record sorting functions
- Administration from a computer networked to the server (if desirable).

In many cases, the backup operation may start and/or restart the database. Therefore we recommend scheduling your backup operation during times when the database has the least amount of use.

In addition to backing up the files to specified hard-disk drive folder, the utility used for backup should include a method to transfer the backup files to a longer-term media such as tape, CD-R, or DVD-R.

There are many ways to backup and recover information contained in Oracle databases. This section provides information that you can use to determine the type of system best suited for your needs.

Built-in Oracle® Facilities

Oracle's Enterprise Manager supplies a backup utility and associated documentation that can be accessed through the Oracle 9i server CD-ROMs. To access this utility, Oracle Management Server (OMS) must be installed on at least one of your Oracle servers. This is installed from the Oracle 9i Server CD set.

For more information on the Oracle backup utility, access the following website: <http://www.orafaq.com/faqdbabr.htm>.

In addition to the utility described above, a command-line based utility is automatically installed on all Oracle servers in the %OraHome%\bin folder named Ocopy.exe. The syntax is similar to the standard copy command (*i.e.*, 'copy x:\databasefiles.dbf y:\backupdir'). This command will copy active database files, but it will stop the database before performing the backup. Refer to your Oracle documentation for further information.

Additional Backup Utilities

As an alternative to the built-in Oracle backup system, you may want to consider one of the following:

- The DDS/4 Tape drive option offered by TA Instruments includes an evaluation version of Veritas Backup Exec, which includes an Oracle agent.

For more information, a fairly comprehensive list of Oracle Backup Solutions Program partners (BSP) is available at <http://technet.oracle.com/deploy/availability/htdocs/bsp.htm>.

- There are several Graphical User Interface (GUI)-based, basic functionality programs available. One of the more widely used utilities is the DBBackup package available at <http://www.kiesoft.com/oraback>. This utility features such the ability to backup a live database, direct support for tape devices, support for CD-R/RW & DVD-R, etc.

Should you require more information than we have presented here regarding backup utilities, please contact your TA Instruments representative at the office nearest your location (see the next section).

Archiving Data

As your database begins to fill with records, you may find the need to archive data from the database. Archiving allows records, based on a time criteria, to be remove (archived and purged) from the active database to free space for future data records. The archive records are saved to an external media (*e.g.*, CD-R/W or DVD+RW) or to a shared hard drive location for future recall by the Integrity software. The Advantage Integrity software provides it own Archive Utility program to perform this operation. For more detailed instructions, consult the DBArchive Help documentation by selecting the Help menu in the software.

Symbols

21 CFR Part 11 7

A

access

- licensed instruments 29
- not allowed 32
- TA System Manager 29

accounts

- creating new user accounts 12 to 13

Activities Log

- displaying 28

Advantage Integrity. *See* system

Advantage Integrity system. *See* system

analysis log 40

- for reports 34
- for saved analyses 33
- viewing 34
- for saved reports
- viewing 34

AR Rheometers

- defining system modules 23

AR series rheometer 7

archiving data 44

audit event 28

- properties 28

Audit Trail 33, 39

- adding new entry 41
- existing record
 - adding comments to 41
- recorded events 39
 - for Instrument Control 39
- viewing 39, 42

Audit Trail Viewer 42

B

backup 43

- desired attributes of 43

C

- closed system
 - definition 7
- comments
 - adding to Audit Trail 41
- components 7

D

- database
 - archiving 44
 - backing up 43
 - backing up while live 44
 - built-in Oracle backup utility 43
 - command line based 43
 - media used for backup 43
- database information
 - changing for system 26
- Database Viewer 36
 - displaying from data analysis 36
 - displaying from instrument control 36
 - sorting 38
 - tree view 37
- DBBackup 44
- DDS/4 Tape drive 44

E

- Electronic Records and Electronic Signatures Rule 7. *See also* 21 CFR Part 11
- Enterprise Manager
 - backup utility 43
- event
 - adding new to Audit Trail 41
- events
 - adding comments to 41
 - recorded for Rheology Data Analysis 40
 - recorded for TA System Manager 40
 - recorded for Universal Analysis 40
 - recorded in the Audit Trail 39
- experiments 31
- expiration of password 9, 12

F

files

- Acrobat PDF 7
- bitmap 7
- custom report template 34
- data 7
- initialization 34
- macro 34
- method 31
- not saved in database 34
- opening 33, 35
- procedures 31
- sequence 31
- session 7
- text 7

functions

- unavailable with Integrity 31, 33, 35

G

group

- definition 14
- status 14

Group Manager

- assigning privileges 17
- setting up new groups 14

groups

- assigning to individual users 16
- assigning to multiple users 15
- assigning to privileges 18
- creating new user groups 14
- default groups available 14

I

instrument

- handling multiple users 32
- licensed for Integrity 30

instruments

- defining as system modules 23

L

licenses

- using instruments with Integrity 30

logging in 9, 33

- changing password 9

logging out
automatic 9

M

media used for backup 43

method files 31

Module Manager

assigning groups to privileges 18

assigning privileges 17

modules

assigning to individual users 25

assigning to multiple users 24

N

Notes, Cautions, and Warnings 6

O

Ocopy.exe 43

operator 30

Oracle

built-in backup utility 43

Oracle Backup Solutions Program partners (BSP) 44

Oracle database 29

P

password 9

case sensitivity 27

changing 9

expiration 9

rules 9

setting expiration date 12

privileges

assigning 17

assigning to a group 17, 18

procedure files 31

project 30

assigning to a run 30

Project Manager

creating new projects 20

- projects
 - assigning to individual users 22
 - assigning to multiple users 21
 - definition 20
 - status 20, 23

Q

- Q Series 7
 - defining system modules 23

R

- record
 - viewing 34

- Record ID # 30

- records 40
 - bmp files 37
 - dates 37
 - definition 7
 - instrument 37
 - locating 33, 35
 - project 37
 - raw data files 37
 - run number 37
 - saved analysis session files 37
 - text files 37
 - types 7
 - Tzero calibration files 37
 - user 37

- remote key. *See also* system key

- results
 - saving 34

- Rheology Data Analysis
 - defining as system module 23
 - using with Integrity 35

- rules for passwords 9

- run
 - starting 32

- run ownership 32

S

- sequence files 31

- sorting the database 38

- status
 - user account 12

SUID# 30

system

- accesssing 9
- automatic log out 9
- changing password 9
- components 7
- Database Viewer 36
- default groups 14
- defining modules 23
- defining projects 20
- defining settings 26
- icons 37
- logging in 33
- logging into 9
- password 9
- password expiration 9
- restricted functions 31, 33, 35
- User ID 9
- using Rheology Data Analysis with Integrity 35
- using Universal Analysis with Integrity 33

System Log

- displaying 28

System Manager. *See* TA System Manager

System Settings Manager

- changing system options 26

T

TA System Manager

- Activities Log 28
- assigning privileges 17
- automatic log out 9
- creating groups 14
- creating new projects 20
- creating new user accounts 12
- default groups 14
- defining settings 26
- first login 9
- initial setup 11
- introduction 10
- options 27
- setting password expiration date 12
- System Log Page 28

time

- password expiration 27

tree view 37

U

Universal Analysis

- defining as system module 23
- using with Integrity 33

user

- definition 12
- status 12

User Account Manager

- assigning modules to a user account 25
- assigning projects to a user account 22
- creating new user accounts 12 to 13

User ID 9, 30, 32

- case sensitivity 27
- creating new 12

users

- assigning individual user to a module 25
- assigning individual user to a project 22
- assigning individual user to one or more groups 16
- assigning multiple users to a group 15
- assigning multiple users to a module 24
- assigning multiple users to a project 21

