

Analyst[®] 1.6 Software

Laboratory Director's Guide



This document is provided to customers who have purchased AB SCIEX equipment to use in the operation of such AB SCIEX equipment. This document is copyright protected and any reproduction of this document or any part of this document is strictly prohibited, except as AB SCIEX may authorize in writing.

Software that may be described in this document is furnished under a license agreement. It is against the law to copy, modify, or distribute the software on any medium, except as specifically allowed in the license agreement. Furthermore, the license agreement may prohibit the software from being disassembled, reverse engineered, or decompiled for any purpose.

Portions of this document may make reference to other manufacturers and/or their products, which may contain parts whose names are registered as trademarks and/or function as trademarks of their respective owners. Any such usage is intended only to designate those manufacturers' products as supplied by AB SCIEX for incorporation into its equipment and does not imply any right and/or license to use or permit others to use such manufacturers' and/or their product names as trademarks.

AB SCIEX makes no warranties or representations as to the fitness of this equipment for any particular purpose and assumes no responsibility or contingent liability, including indirect or consequential damages, for any use to which the purchaser may put the equipment described herein, or for any adverse circumstances arising therefrom.

For research use only. Not for use in diagnostic procedures.

The trademarks mentioned herein are the property of AB Sciex Pte. Ltd. or their respective owners.
AB SCIEX™ is being used under license.



AB SCIEX

71 Four Valley Dr., Concord, Ontario, Canada. L4K 4V8.

AB SCIEX LP is ISO 9001 registered.

© 2011 AB SCIEX.

Printed in Canada.

Contents

Foreword	7
Related Documentation	7
Technical Support	7
Chapter 1 Security Configuration Overview	9
Security and Regulatory Compliance	9
Security Requirements	9
Analyst Software and Windows Security: Working Together	9
Audit Trails within the Analyst Software and Windows	10
Audit Trails in the MultiQuant Software	10
21 CFR Part 11	11
System Configuration	11
Windows Security Configuration	11
Users and Groups	11
Active Directory Support	12
Windows File System	12
System Audits	12
File and Folder Permissions	13
Event Viewer	13
Alerts	13
Chapter 2 Configuring Analyst Software Security	15
Software Security Workflow	15
Analyst Software Installation	16
Verifying Software Components	17
Analyst Software Security Configuration	17
Steps for Configuring the Analyst Software	17
About Security Modes and Accounts	18
Selecting the Security Mode	19
Selecting an Acquisition Account	19
Setting up Screen Lock and Auto Log Out	20
Unlocking or Logging off from the Analyst Software	21
Access to the Analyst Software	21
About People and Roles	22
Analyst Software Access	24
MultiQuant Software Access	32
Adding a User or Group to the Analyst Software	35
Changing a Role	35
Removing People from the Analyst Software	35
Creating a Custom Role	35
Deleting a Custom Role	36
Setting Access to Projects and Project Files	37
Adding Access to a Workstation	39
Removing a Workstation	40
Printing Security Configurations	40

Chapter 3 Analyst Administrator Console	41
About the Administrator Console	41
Benefits of Using the Administrator Console	41
Console Administrators	43
Setup of Workgroups	43
Overview of Tasks	43
About Workgroups	44
Connecting the Administrator Console Client to the Server	45
Creating Roles	47
Copying a Role	47
Adding Users or Groups to the User Pool	48
About Projects and Root Directories	48
Selecting a Template Project	49
Creating a Root Folder	49
Adding an Existing Root Directory	49
Refresh a Project Root	50
Create a Project	50
Adding an Existing Project	50
About Workgroups	51
Creating a Workgroup	51
Adding Users or Groups to a Workgroup	52
Adding or Removing a Role	53
Adding Projects to a Workgroup	53
Adding Workstations to a Workgroup	54
Setting a Default Workgroup for the Analyst Logon Information dialog	55
Changing the Default Workgroup when in Integrated Mode	55
Workgroup Security Modes and Logging on to the Analyst Software	55
Audit Trails	56
Administrator Console Ongoing Tasks	56
Synchronizing the Administrator Console Client and Server	57
Changing the Attributes of the Administrator Console Client	57
Deleting Roles	57
Changing the Properties of a Role	58
Deleting Users or Groups	58
Deleting Projects	58
Deleting Workstations	59
Deleting Workgroups	59
Changing the Attributes of a Workgroup	59
Deleting Users, Projects, or Workstations from a Workgroup	60
Changing a Role	61
Reviewing Project Permissions	61
Chapter 4 Network Acquisition	63
About Network Acquisition	63
Benefits of Using Network Acquisition	63
File Security, File Formats, and Data Backup	64
Network Project Security	64
Special Acquisition Account	64
Options for Data File Formats	65

Data Backup Process	65
Deleting the Contents of the Cache Folder	66
Configuring Network Acquisition	66
Creating a Root Directory	66
Setting the root directory	66
Changing the File Format	67
Selecting an Acquisition Account	67
Chapter 5 Auditing	69
About Audit Trails	69
About Audit Maps	70
Setup of Audit Maps	70
Installed Audit Maps	71
Working with Audit Maps	72
Creating an Audit Map	72
Changing an Audit Map	74
Copying an Audit Map from Another Project	74
Applying an Audit Map	75
Viewing, Printing, and Searching Audit Trails	75
Viewing an Audit Trail	75
Viewing the Audit Configuration Embedded in a Results Table	76
Viewing Details for an Audit Record in the Instrument Audit Trail	76
Viewing an Archived Audit Trail	77
Printing an Audit Trail	77
Searching for an Audit Record	77
About using Audit Maps with Projects Created in Previous Versions of the Analyst Software	78
Appendix A Audit Trail Records	79
Audit Trail Records	79
Audit Trail Archives	79
Instrument Audit Trail	79
Project Audit Trail	81
Quantitation Audit Trail	82
Administrator Console Audit Trail	83
Appendix B Auditing Using MultiQuant Software	85
About the Audit Trail Manager	85
About Audit Maps	86
Setting up Audit Maps	86
Creating or Changing an Audit Map	86
Audit Configurations	88
Viewing Audit Configurations Embedded in the Results Table	89
Viewing, Searching, and Printing Audit Trails	89
Viewing the Audit Trail Results in the Audit Trail Viewer	89
Performing a Keyword Search	89
Filtering Audited Events	89
Printing the Audit Trail Viewer	91
Exporting the Audit Trail Viewer	91
About the Audit Trail Viewer	91

Appendix C Additional Security Customization	93
Data File Changes (Explore Processing)	93
Creating Explore Processing History Files	94
Viewing an Explore Processing History file	94
Adding an Instrument Maintenance Log entry	94
Viewing an Instrument Maintenance Log entry	94
Configuring Email Notification	95
Data File Checksum	96
Verifying Data File Checksum	96
Enabling or Disabling the Data File Checksum Feature	97
Appendix D Data System Conversion	99
MassChrom Data Files Translation	99
Translating API Files to .wiff Files	99
Generating Instrument Files	100
Converting Experiment Files	100
Index	101

The information contained in this manual is intended for two primary audiences:

- The laboratory administrator, who is concerned with the daily operation and use of the Analyst[®] software and attached instrumentation from a functional perspective.
- The system administrator, who is concerned with system security and system and data integrity.

Related Documentation

The guides and tutorials for the instrument and the Analyst software are installed automatically with the software and are available from the Start menu: All Programs > AB SCIEX > Analyst. A complete list of the available documentation can be found in the Help. To view the Analyst software Help, press F1.

Technical Support

AB SCIEX and its representatives maintain a staff of fully-trained service and technical specialists located throughout the world. They can answer questions about the instrument or any technical issues that may arise. For more information, visit the Web site at www.absciex.com.



This section describes how the Analyst[®] software access control and auditing components work in conjunction with Windows access control and auditing components. It also describes how to configure Windows security prior to installing the Analyst software.



Note: If you are using the Administrator Console to centrally manage security, see [Analyst Administrator Console on page 41](#).

Topics in this section:

- [Security and Regulatory Compliance on page 9](#)
- [System Configuration on page 11](#)

Security and Regulatory Compliance

The Analyst software provides:

- Customizable administration to meet the needs of both research and regulatory requirements.
- Security and audit tools to adhere to 21 CFR Part 11 regulations for the use of electronic record keeping.
- Flexible and effective management of access to critical instrument functions.
- Controlled and audited access to vital data and reports.
- Easy security management linking to Windows security.

Security Requirements

Security requirements range from relatively open environments, such as research or academic laboratories, to the most stringently regulated, such as forensic laboratories.

Laboratory monitoring agencies such as the FDA (Food and Drug Administration) and the EPA (Environmental Protection Agency) require adherence to GLP (Good Laboratory Practices.) The Analyst software supports regulated laboratory environments and helps you comply with GLP. In particular, the Analyst software auditing and access control components are designed to help you meet the requirements of the CFR (Code of Federal Regulations), Title 21, Chapter I, Part 11, Electronic Records; Electronic Signatures, for file and process security, validation, and data tracking.

Analyst Software and Windows Security: Working Together

The Analyst software and the NTFS (Windows New Technology File System) have security features designed to control system and data access.

Windows security provides the first level of protection by requiring users to log on to the network by means of a unique user identity and password. This makes sure that only those who are

recognized by the Windows Local or Network security settings can have access to the systems. For more information, see [Windows Security Configuration on page 11](#).

The Analyst software has three progressively more secure system access modes:

- Single
- Mixed
- Integrated

For more information on security modes and security settings, see [About Security Modes and Accounts on page 18](#).

The Analyst software project security configuration is tied to the Windows NTFS; therefore there is no need to set the NTFS object permissions externally. You can set file permissions using the Analyst software, thus managing project security directly with the Analyst software.

The Analyst software also provides completely configurable roles that are separate from the User Groups associated with Windows. Through the use of roles, the laboratory director can control access to the software and instrument on a function-by-function basis. For more information, see [Access to the Analyst Software on page 21](#).

Audit Trails within the Analyst Software and Windows

The auditing features within the Analyst software, together with the built-in Windows auditing components, are critical to the creation and management of electronic records.

The Analyst software provides a system of audit trails to meet the requirements of electronic record keeping. Separate audit trails record:

- Additions or replacements to the mass calibration table or resolution table, system configuration changes, security events, and entries in the Instrument Maintenance Log.
- Creation, modification, and deletion events for project, data, quantitation, method, batch, tuning, results table, and report template files, as well as module opening and closing and printing events.
- Creation and modification of the quantitation method embedded in the Results Table file, sample information, and peak integration parameters.

The Analyst software uses the application event log to capture information about the operation of the software. Use this log as a troubleshooting aid because instrument, device, and software interactions are recorded in detail here.

Windows maintains three audit trails, known as event logs, which capture a range of security, system, and application related events. In most cases, Windows auditing is designed to capture exceptional events, such as a log on failure. The administrator can configure this system to capture a wide range of events, such as access to specific files or Windows administrative activities. For more information, see [System Audits on page 12](#).

Audit Trails in the MultiQuant Software

The MultiQuant™ software contains its own audit trail that audits creation and modification events within the MultiQuant software. The audit trail functionality is only available with the 21 CFR Part 11 license of the MultiQuant software.

21 CFR Part 11

The Analyst software provides a secure user environment, which supports the 21 CFR Part 11 requirements for the creation of electronic records, with the implementation of:

- Mixed mode and Integrated mode security linked to Windows security.
- Controlled access to functionality through customizable roles.
- Controlled access to project data on a role-by-role or group basis.
- Audit trails for instrument operation, maintenance, data acquisition, data review, and report generation.
- Electronic signatures using a combination of user ID and password.
- Proper procedures and training in your company.

Within 21 CFR Part 11, there are requirements for the control of electronic records that extend beyond the domain of the Analyst software. These requirements include the distribution and control of records in a closed or open system.

System Configuration

System configuration is usually performed by network administrators or people with network and local administration rights.

Windows Security Configuration

The Analyst software administrator must have the ability to change permissions for the project folder and all the subfolders to use the Analyst software to manage security. If the root directory is on a local computer, the Analyst software administrator could be part of the local administrators group. Only the Analyst software user who manages security must be in the local administrators group.

For the Analyst software to work well, users should be part of the Windows local user group. If certain users need to be able to stop the AnalystService, this specific access can be set up without giving the user all the local administrator privileges and thereby compromising local security.

If you plan to use network acquisition, the network administrator must set up Windows security so that the Analyst software Administrator can change permissions for the required folders. Do not add local users on acquisition computers to a network project security folder.

Users and Groups

The Analyst software uses the user names and passwords recorded in the primary domain controller security database or Active Directory. Passwords are managed using the tools provided with Windows. For more information on setting up people and roles, see [Access to the Analyst Software on page 21](#).

Active Directory Support

Active Directory can work in either mixed or native environments. In the Analyst software security configuration window and the Analyst software security database, you can specify user accounts in UPN (user principal name) format.

Mixed Environment

The network includes Windows 2000 and Windows NT servers and Windows 2000, Windows NT, or Windows XP clients.

Native Environment

The network includes Windows 2000 servers and Windows 2000 or Windows XP clients.

If the Analyst software starts in the mixed environment, the log on window contains the user name, password, and domain fields. If you are using a Windows NT account, provide all three parameters. If you are using a Windows 2000 account, type your user name in UPN format and ignore the domain field.

If the Analyst software starts in the native environment, the domain field is not displayed, and the Analyst software accepts your user name in UPN format only. The Analyst software Status window also displays your user name in UPN format.

Windows File System

In the Analyst software, files and directories must be located on a hard-disk partition formatted as the NTFS, which can control and audit access to Analyst software files. The FAT file system cannot control or audit access to folders or files and is, therefore, not suitable for a secure environment.

System Audits

If the system is enabled for auditing, it can detect security breaches and send notification of events that pose security risks. For example, if failed attempts to log on to Windows are audited, the software detects attempts to log on to the system using random passwords. If successful log ons to the system are audited, the software detects if someone is accessing the system using stolen passwords. If successful and failed file writes are audited, the software checks for potential viruses. It may also be desirable to audit successful and failed access to sensitive files, directories, and printers.

Customize the event logs as follows:

- Set appropriate event log size.
- Set automatic overwrite of old events.
- Set Windows computer security settings.

A process of review and storage can be implemented. For more information regarding security settings and audit policies, see the Windows documentation.

File and Folder Permissions

To manage security on a network drive, the Analyst software administrator must have the right to change permissions for the Analyst Data folder and all the subfolders. Access must be set up by the network administrator.

Before selecting the events or actions for audit, set the permissions for the files and folders. The permissions for folders can apply to subfolders and files in the folder. After file and folder permissions have been set, define the events that are written to the security log.



Note: Consider the access needs of users to the drive and folder on each computer. Configure sharing and associated permissions. For more information about file sharing, see the Windows documentation.

For information on the Analyst software files and folder permissions, see [Analyst Software Security Configuration on page 17](#).

Event Viewer

Open the Event Viewer through the Analyst software or through Windows Administrative Tools. The Event Viewer records the audited events in the security log, system log, or application log.



Tip! To open the Event Viewer from the Analyst software, click **View > Event Log**.

Alerts

If a system or user problem occurs, set up the network to send an automatic message to a designated person, such as the system administrator, on the same or another computer. In the Windows Services of Control Panel, the Messenger must be started on the sending and receiving computers and the Alerter service must be started on the sending computer. For more information about creating an alert object, see the Windows documentation.



This section explains how to configure the Analyst[®] software. If you are using the Administrator Console to centrally manage security, see [Analyst Administrator Console on page 41](#).



Note: You must have local administrator privileges for the workstation on which you are installing the Analyst software.

Topics in this section:

- [Software Security Workflow on page 15](#)
- [Analyst Software Security Configuration on page 17](#)
- [Access to the Analyst Software on page 21](#)

Software Security Workflow

The Analyst software works with the security, application, and system event auditing components of the Windows Administrative Tools.

Configure security at the following levels:

- Access to Windows.
- Access to the Analyst software.
- Selective access to the Analyst software functionality.
- Access to specific projects.
- Access to instrument station status.

[Table 2-1](#) contains the list of tasks for configuring security and [Table 2-2](#) shows the options for setting the various security levels.

Table 2-1 Workflow Process for Configuring Security

	Task	Procedure
<input type="checkbox"/>	Install the Analyst software.	See the Analyst software installation guide.
<input type="checkbox"/>	Install MultiQuant™ software (if required.)	See the MultiQuant software installation guide.
<input type="checkbox"/>	Configure Analyst software security.	See Analyst Software Security Configuration on page 17 .
<input type="checkbox"/>	Configure audit trails.	See Auditing on page 69 .
<input type="checkbox"/>	Configure Windows File Security and NTFS.	See Setting Access to Projects and Project Files on page 37 .
<input type="checkbox"/>	Maintain system maintenance log for instruments, security, data, and project maintenance.	See Additional Security Customization on page 93 .
<input type="checkbox"/>	Transfer or translate existing data.	See Data System Conversion on page 99 .

Table 2-2 Security Configuration Options

		CFR	Mid-Range	Non GLP
Windows Security				
<input type="checkbox"/>	Format drives to NTFS.	Yes	Yes	Optional
<input type="checkbox"/>	Configure users and groups.	Yes	Yes	Optional
<input type="checkbox"/>	Enable Windows auditing, and file and directory auditing.	Yes	Optional	Optional
<input type="checkbox"/>	Set file permissions.	Yes	Optional	Optional
Analyst Software Installation				
<input type="checkbox"/>	Install Analyst software.	Yes	Yes	Yes
<input type="checkbox"/>	Install MultiQuant software.	Yes	Yes	Yes
<input type="checkbox"/>	Select CFR options.	Yes	Optional	No
<input type="checkbox"/>	Event Viewer (inspect install).	Yes	Yes	Yes
Analyst Software Security				
<input type="checkbox"/>	Select security mode.	Integrated or Mixed	Any	Single user
<input type="checkbox"/>	Configure Analyst software roles and people.	Yes	Yes	No
<input type="checkbox"/>	Create audit maps, configure instrument, project, and quantitation audit trails.	Yes	Optional	No
<input type="checkbox"/>	Configure email notification.	Yes	Optional	No
<input type="checkbox"/>	Activate Checksum.	Yes	Optional	No
<input type="checkbox"/>	Create audit maps in the MultiQuant software.	Yes	Optional	No
Common Tasks				
<input type="checkbox"/>	Add new projects and subprojects.	Yes	Yes	Yes
<input type="checkbox"/>	Configure project audit trail for new projects and subprojects.	Yes	Optional	No
<input type="checkbox"/>	Transfer existing data.	Yes	Yes	Yes
<input type="checkbox"/>	Create maintenance log for instrument security, data, project maintenance.	Yes	Yes	Yes

Analyst Software Installation

Before installing the Analyst software, read the software installation guide and release notes on the software installation DVD. You should also understand the difference between a processing workstation and an acquisition workstation and then complete the appropriate installation sequence.

System Requirements

For minimum installation requirements, see the software installation guide that comes with the software.

Preset Auditing Options

Depending on the software version, the preset auditing options may be unavailable. After installation, the Analyst software administrator can change the selection in the Security Configuration module or configure audit maps in the Audit Trail Manager.

Verifying Software Components

After the Analyst software is installed, a Software Component Verification procedure checks that all the software components were installed and generates an installation report. This report is an event log item from the Analyst Installer in the Event Viewer Application log. Verify that the installation was successful immediately after completion.

There is an event log for the checksum inspection of the core installed files. For more information about checksum, see [Data System Conversion on page 99](#).

1. Click **Start** and then click **Control Panel**.
2. Double-click **Administrative Tools** and then double-click **Event Viewer**.
3. In the **Tree** tab, click **Application Log**.
4. Click **Analyst Installer** event in the **Source** column. In the Event Detail message, in the **Description** field, go to **Total files verified**. Errors should read zero.

Analyst Software Security Configuration

This section describes how to configure the Analyst software security.



Note: Any changes to the Analyst software security configuration take effect after restarting the Analyst software.

Steps for Configuring the Analyst Software



Tip! If you will be performing various tasks in the Security Configuration dialog, click **Apply** on each tab to save your changes before moving to another tab.

[Table 2-3](#) contains the general tasks for configuring the Analyst software.

Table 2-3 Tasks for Configuring the Analyst Software

	Task	Procedure
<input type="checkbox"/>	Configure the security mode.	See Selecting the Security Mode on page 19 .
<input type="checkbox"/>	Configure screen lock and auto log out (Mixed mode only).	See Setting up Screen Lock and Auto Log Out on page 20 .

Table 2-3 Tasks for Configuring the Analyst Software (Continued)

	Task	Procedure
<input type="checkbox"/>	Configure project security.	See Setting Access to Projects and Project Files on page 37 .
<input type="checkbox"/>	Configure instrument stations.	See Adding Access to a Workstation on page 39 or Removing a Workstation on page 40 .

About Security Modes and Accounts

This section describes the options found on the Security tab in the Security Configuration dialog.

Single User Mode: The current user who is logged on to Windows as an Analyst software administrator has full access to all Analyst software functionality. Anyone who can successfully log on to Windows on the computer has Analyst software administrator privileges.

Integrated Mode: The current user who is logged on to Windows has access to the Analyst software, providing that the Windows user is also a valid Analyst software user. For more information on logging on in Integrated mode when using the Administrator Console, see [Workgroup Security Modes and Logging on to the Analyst Software on page 55](#).

Mixed Mode: The user who is logged on to the Analyst software can be either a different user or the same user as the current user who is logged on to Windows. The user logged on to the Analyst software can be assigned to a specified role in the same way as in Integrated mode. The difference is that the user logged on to the Analyst software may be different from the user logged on to Windows. This provides the possibility of having a group log on for Windows with a known password, while requiring the Analyst software user to log on to the Analyst software using a unique user name, password, and if required, domain.

If you select Mixed mode, then the Screen Lock and Auto Logout features are available for use.

For more information on logging on in Mixed mode when using the Administrator Console, see [Workgroup Security Modes and Logging on to the Analyst Software on page 55](#).

Acquisition Account: A network account used for reading and writing data into project folders during normal acquisition, but not during tuning. The network administrator must provide appropriate access rights for network accounts. The Acquisition Account uses the rights from either the Client Account or the Special Acquisition Administrator Account.

Client Account: Uses the same account that you use to log on to the Analyst software. In Integrated Mode, the user who has logged on to Windows is also logged on to the Analyst software. In Mixed mode, the Windows user and the Analyst software user may be different.

Special Acquisition Administrator Account: This feature is intended for use in a regulated environment. The operator must provide a user name, domain, and password for this account. After the network administrator sets up this account, it can be used to acquire data regardless of the identity of the current user of the Analyst software. Although the current user may not have rights to modify data in the Data folder, data acquisition can still occur. Account information is encrypted and stored in the registry.

Screen Lock and Auto Logout: For security purposes, you can set the computer screen to lock after a defined period of inactivity. You can also set an automatic logout time where the Analyst software client will close after a defined period of inactivity. Screen Lock and Auto Logout are available in Mixed mode only.

Selecting the Security Mode

1. On the **Navigation** bar, under **Configure**, double-click **Security Configuration**.

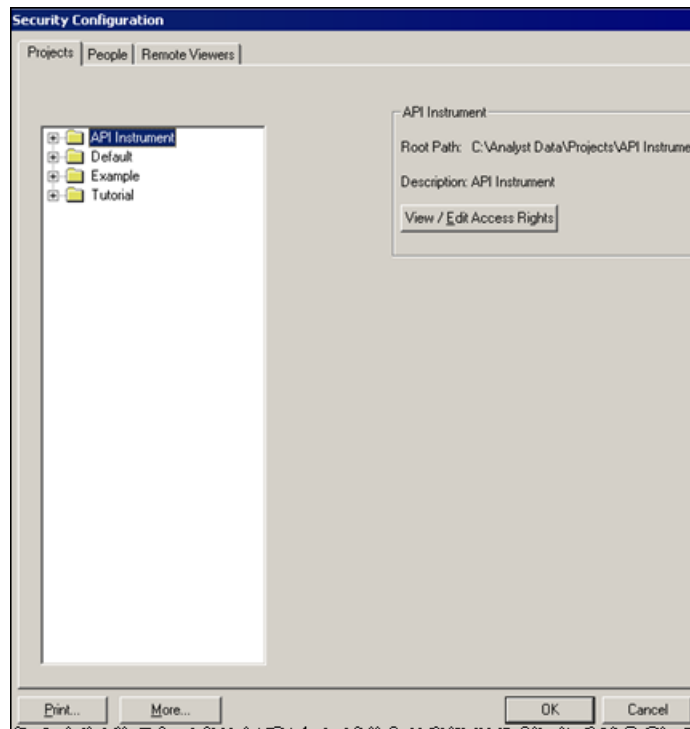


Figure 2-1 Security Configuration dialog: Projects tab

2. Click **More** and then click the **Security** tab.
3. In the **Security Mode** section, click a mode and then click **OK**.
4. Restart the Analyst software.

Selecting an Acquisition Account

1. On the **Navigation** bar, under **Configure**, double-click **Security Configuration**.
2. Click **More** and then click the **Security** tab.
3. In the **Acquisition Account** section, select an acquisition account.
4. If you click **Special Acquisition Administrator Account**:
 - i. Click **Set Acquisition Account**.
 - ii. Type the **User name**, **Password**, and if necessary, **Domain**, and then click **OK**.

If you are using Active Directory in the native environment, the domain field is not visible and you can type the user name in UPN format.

5. Click **OK**.

Setting up Screen Lock and Auto Log Out

When the screen locks, the Unlock Analyst dialog appears indicating that the system has been locked, as well as the currently logged on user name and domain. If the auto logout option is also set, then the time remaining before the Analyst software closes is also displayed. Only the currently logged on user, or users with the Administrator or the Supervisor roles, can unlock or close the Analyst software.



Note: Screen Lock and Auto Logout are available only in Mixed Mode.

1. On the **Navigation** bar, under **Configure**, double-click **Security Configuration**.
The Security Configuration dialog appears.
2. Click **More** and then click the **Security** tab.
3. Click **Mixed Mode**.



Note: MultiQuant software uses the Analyst software screen lock information. No additional setup is required for the MultiQuant software.

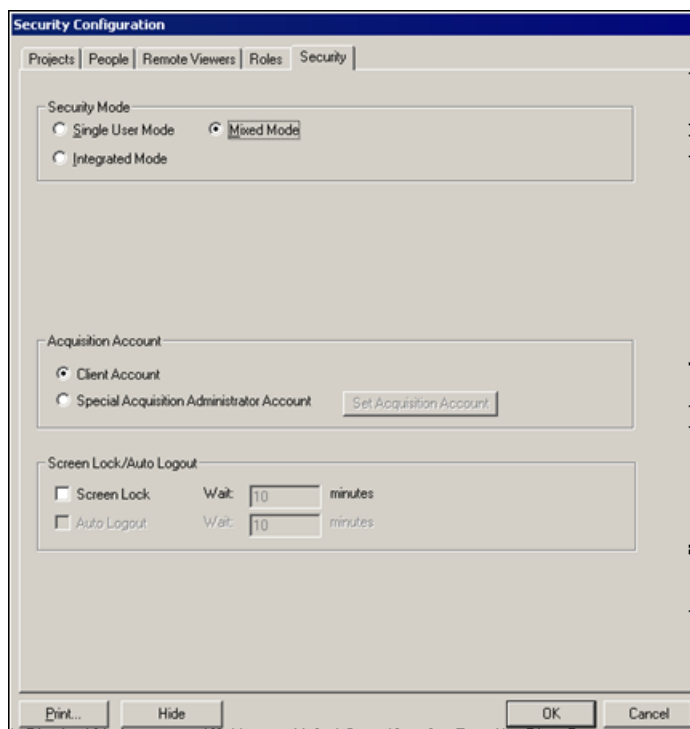


Figure 2-2 Security tab

4. Select the **Screen Lock** check box.
5. In the **Wait** field, type the number of minutes to elapse before the screen locks.



Note: If Auto Logout is enabled and the screen is not unlocked, after a defined period, the Analyst software client closes. If acquisition is taking place, it continues; however, if a Results Table, the Method Editor, or anything else is open and not saved, any changes and unsaved data are lost.

- If required, select **Auto Logout** and, in the **Wait** field, type the number of minutes to elapse before the Analyst software client closes.

You have a 10-second grace period to move the mouse or press a key to close the Unlock Analyst dialog. Only the currently logged on user, or users with the Administrator or the Supervisor roles, can unlock or close the Analyst software. The Unlock Analyst dialog also indicates the time left before you are logged out.

Unlocking or Logging off from the Analyst Software

After the Screen Lock time has elapsed, the Unlock Analyst dialog appears.

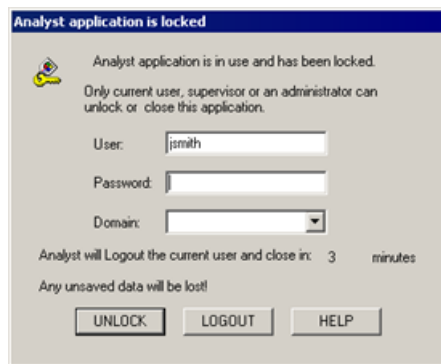


Figure 2-3 Unlock Analyst dialog

- To unlock the screen, type your user name, if necessary, and password, and then click **UNLOCK**.
- or—
- To log out, type your user name, if necessary, and password, and then click **LOGOUT**.

Access to the Analyst Software

Before configuring security requirements:

- Remove all unnecessary users and user groups such as replicator, power user, and backup operator from the local computer and the network.
- Add user groups containing groups that will hold non-administrative tasks and configure system permissions.
- Create suitable procedures and account policies for users in group policy.

See your Windows documentation for more information on the following:

- Users and groups and Active Directory users.

- Password and Account lockout policies for user accounts.
- User rights policy.

When users work in an Active Directory environment, the Active Directory group policy settings affect the workstation security. Discuss group policies with your Active Directory administrator as part of a comprehensive Analyst software deployment.

About People and Roles

The Analyst software limits access to people authorized to log on to the workstation and to the Analyst software, using their Windows user name and password for both, except when using Mixed Mode. The Analyst software does not allow multiple sessions.



Note: The People and Role tabs are not available in Single User mode.

An Analyst software administrator can add Windows users and groups to the Analyst software security database. People or groups must be assigned to one of the six predefined roles, or new roles can be create, if required. The predefined roles cannot be deleted but their rights can be modified. Only users with Analyst software roles can access Analyst software components.



Note: If the workstation is registered with the Administrator Console server, you can only add people and roles using the Administrator Console. In the Analyst software, all the buttons in the People and Roles tabs in the Security Configuration dialog are unavailable. For more information on the Administrator Console, see [Analyst Administrator Console on page 41](#).

Table 2-4 Analyst Software Roles

Role	Typical tasks	Preset access
Administrator	<ul style="list-style-type: none"> • Manages the system. • Configures security. 	<ul style="list-style-type: none"> • All Analyst software and MultiQuant software functionality
Analyst	<ul style="list-style-type: none"> • Oversees instrument operation. • Analyzes data for use by end user. 	<ul style="list-style-type: none"> • Acquisition Method • Analyst Application • Audit Trail Manager • Compound Database • Explore • Hardware Configuration • Quantitation • Report Template Editor • Sample Queue • Tune • View Status • MultiQuant

Table 2-4 Analyst Software Roles (Continued)

Role	Typical tasks	Preset access
Operator	Oversees daily use of the system, including maintenance, sample organization, data gathering, and processing.	<ul style="list-style-type: none"> • Acquisition Method • Analyst Application • Audit Trail Manager • Batch • Compound Database • Explore • ExpressView • Hardware Configuration • Report Template Editor • Sample Queue • Tune • View Status
End User	<ul style="list-style-type: none"> • Provides samples. • Receives processed results. • Integrates results with input and output from other applications. 	<ul style="list-style-type: none"> • Acquisition Method • Analyst Application • Audit Trail Manager • Compound Database • Explore • ExpressView • Report Template Editor • View Status
QA Reviewer	<ul style="list-style-type: none"> • Reviews data. • Reviews audit trails. • Reviews quantitation results. 	<ul style="list-style-type: none"> • Analyst Application • Audit Trail Manager • Quantitation • Report Template Editor • View Status • MultiQuant
Supervisor	Unlocks software or logs out user.	<ul style="list-style-type: none"> • Unlock and Logout Application and MultiQuant software

Analyst Software Access

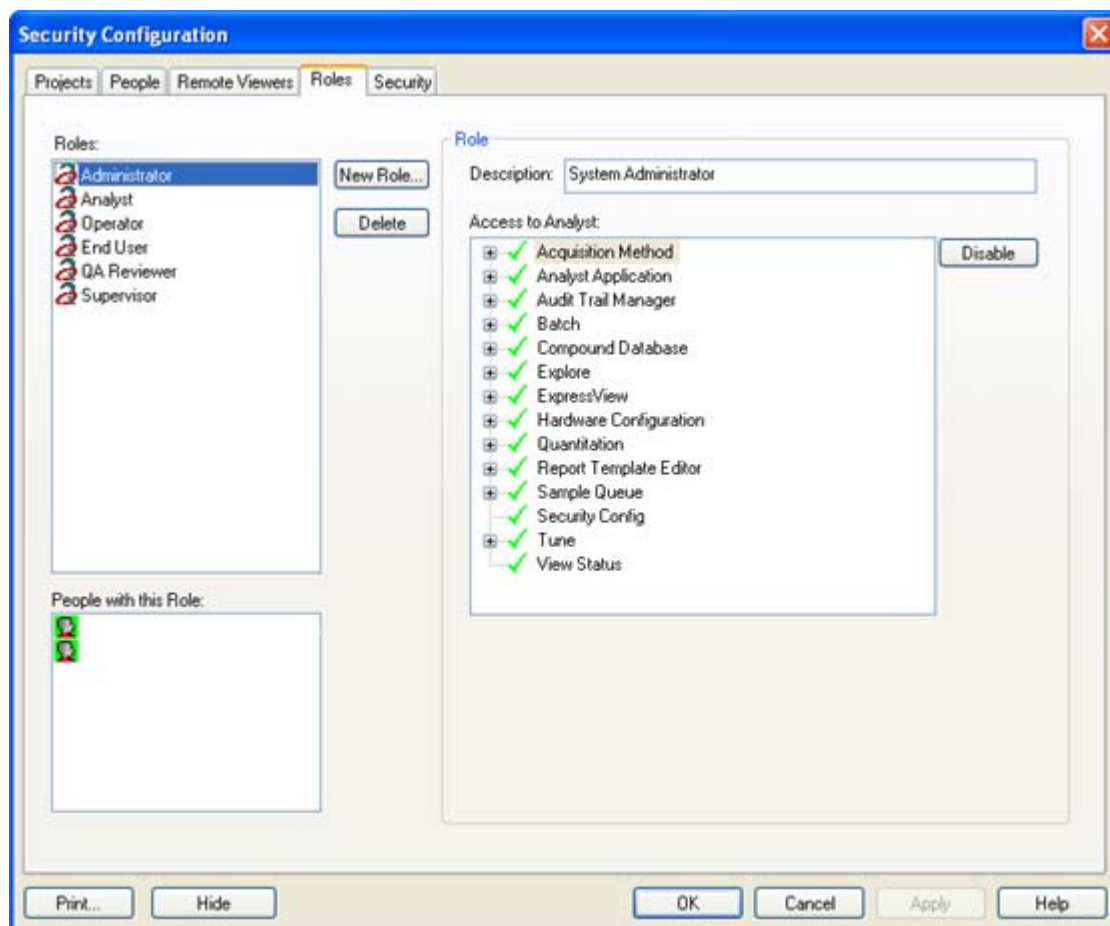


Figure 2-4 Security Configuration dialog

Table 2-5 Analyst Software Access to Acquisition Methods

Preset access	Description
Create/save acquisition methods	Allows users to create and save acquisition methods.
Open acquisition methods as read-only (acquire mode)	Allows users to open acquisition methods in read-only mode if the Create/save acquisition methods and Overwrite acquisition methods options are disabled.
Overwrite acquisition methods	Allows users to overwrite acquisition methods.

Table 2-6 Analyst Software Access to Analyst Application

Preset access	Description
Use Workspace functions	Allows users to use the Workspace functions.
Create Project	Allows users to create projects.
Copy Project	Allows users to copy projects.
Create Root Directory	Allows users to create a root directory.

Table 2-6 Analyst Software Access to Analyst Application (Continued)

Preset access	Description
Set Root Directory	Allows users to set the root directory.
Change Project	Allows users to change the project.
Load/Save Processed Data Files	Allows users to load and save processed data files.
Unlock/Logout Application	Legacy setting, now disabled.

Table 2-7 Analyst Software Access to Audit Trail Manager

Preset access	Description
View Audit Trail Data	Allows users to view audit trail data.
Change Audit Trail Settings	Allows users to modify the audit trail settings.
Maintenance Log	Allows users to view the maintenance log.
Create or Modify Audit Maps	Allows users to create or modify audit maps.

Table 2-8 Analyst Software Access to Batch

Preset access	Description
Open existing batches	Allows users to open existing batches.
Create new batches	Allows users to create batches.
Import	Allows users to import data from existing batches (.mdb or LIMS files).
Save batches	Allows users to save batches.
Use template batches	Allows user to save or open template batches.
Edit batches	Allows users to edit batches.
Submit batches	Allows users to submit batches.
Add or remove custom columns	Allows users to add or remove custom columns from the Batch Editor.
Use template acquisition methods	Allows user to use an acquisition method as a template. This option is available in the Batch Editor. Once a method is selected, the Use as template option becomes enabled.
Overwrite batches	Allows users to overwrite existing batches.
Overwrite template batches	Allows users to overwrite existing template batches.

Table 2-9 Analyst Software Access to Compound Database

Preset access	Description
Setup compound database location	Sets the compound Location and name options to ReadOnly and disables the Browse button. (In Explore mode, click Tools > Settings > Optimization Options.) Enables the Use Defaults Now button in the Optimization Options dialog only if the user has access to both the compound database location and the compound database user options.

Table 2-9 Analyst Software Access to Compound Database (Continued)

Preset access	Description
Setup user options	Allows users to set the User ID and Password options on the Optimization Options dialog. (In Explore mode, click Tools > Settings > Optimization Options.) Enables the Use Defaults Now button in the Optimization Options dialog only if the user has access to both the compound database location and the compound database user options. (Right-click in the Compound database to access these features.)
Add to compound database	Allows users to add compounds to the compound database. (Right-click in the Compound database to access this feature.)
Modify database (overrides add/delete if disabled)	Allows users to add, delete, or modify the compound database (compounds or optimization settings).
Delete compound from database	Allows users to delete compounds from the compound database. (Right-click in the Compound database to access this feature.)
Delete optimization settings from database	Allows users to delete optimization settings from the compound database. (Right-click in the Compound database to access this feature.)

Table 2-10 Analyst Software Access to Explore

Preset access	Description
Save data to text file	Allows users to save data to text files. (Right-click in a spectrum or chromatogram and then click Save to Text File.)
Setup library location	Legacy setting, now disabled.
Setup library user options	Legacy setting, now disabled.
Add library record	Allows user to add a library record. (Right-click in a spectrum or in Explore mode, click Explore > Library Search > Add.)
Add spectrum to library record	When disabled, users cannot click the Append MS button in the Library Search dialog. (In Explore mode, click Explore > Library Search > List.)
Modify library record (overrides add/delete if disabled)	Allows users to modify library records (overrides add/delete if disabled).
Delete MS spectrum	Legacy setting, now disabled.
Delete UV spectrum	Allows users to delete a UV spectrum.
Delete structure	Allows users to delete a structure.
View library	Allows users to click the List and List with Constraints features. (In Explore mode, click Explore > Library Search.)
Search library	Allows users to use the Search Library and Set Search Constraints. (To access this feature, right-click a spectrum or in Explore mode, click Explore > Library Search.)

Table 2-10 Analyst Software Access to Explore (Continued)

Preset access	Description
Select processing algorithm to retrieve peak list	Legacy setting, now disabled.

Table 2-11 Analyst Software Access to ExpressView

Preset access	Description
Start Express View dialog	Allows users to run ExpressView.
Modify options	Allows users to configure ExpressView. (In Configure mode, click Tools > Configure ExpressView.)

Table 2-12 Analyst Software Access to Hardware Configuration

Preset access	Description
Create	Allows users to create a hardware profile.
Delete	Allows users to delete a hardware profile.
Edit	Allows users to edit a hardware profile.
Activate/Deactivate	Allows users to activate or deactivate a hardware profile.

Table 2-13 Analyst Software Access to Quantitation

Preset access	Description
Create quantitation method	Allows users to create new quantitation methods.
Change default method options	Allows users to change the default method options.
Use full method editor	Allows users to use the Quantitation Method Editor.
Create "automatic" methods	Allows users to create an quantitation method within the Quantitation Wizard.
Modify existing methods	Allows users to modify (overwrite) existing quantitation methods.
Change peak names (in wizard)	Allows users to change peak names in the Quantitation Wizard.
Change default number of smooths (in wizard)	Legacy setting, now disabled.
Change "advanced" parameters (in wizard)	Allows users to change the Advanced parameters in the Quantitation Wizard. If users do not have this option, the Advanced button is hidden.
Change concentration units (in wizard)	Allows users to change the concentration units in the Advanced parameters in the Quantitation Wizard.
Create new results tables	Allows users to create a new Results Table using the Quantitation Wizard or by selecting New from the File menu. The Save As button will not be disabled by this option.
Open existing results tables	Allows users to open existing Results Tables.
When saving, replace existing results tables	Allows users to overwrite existing Results Tables.

Table 2-13 Analyst Software Access to Quantitation (Continued)

Preset access	Description
Edit results tables' method	Allows users to modify the quantitation method file. In Quantitate mode, click Tools > Results Table > Modify Method. This modifies the actual file and not the embedded method within a Results Table.
Create new "standard" queries (from wizard)	Allows users to create a new standard query using the Quantitation Wizard.
Exclude standards from calibration	Allows users to exclude standards from calibration from Calibration pane, Results Table, and Statistics pane.
Add and Remove samples from results table	Allows users to add or remove samples. (In Quantitate mode, click Tools > Results Table > Add/Remove samples.)
Display metric plots	Allows users to display metric plots from a Results Table. (In a Results Table right-click and then click Metric Plot.)
Create or modify formula columns	Allows users to create or modify formula columns in a Results Table.
Modify sample name	Allows users to modify sample names.
Export results table as text file	Allows users to export a Results Table as a text file. (In Quantitate mode, with a Results Table open, click Tools > Results Table > Export as Text.)
Export settings from results table	Allows users to export table settings to new Results Table settings. (Right-click in a Results Table and then click Table Settings > Export To New Table Settings.)
Modify custom column title	Allows users to modify the title of a custom column. A formula column is not a custom column.
Modify results table settings	Allows users to modify table settings from a Results Table (right-click and then click Table Settings > Edit) or global table settings (in Quantitate mode, click Tools > Settings > New Quantitation Results Table Settings.) This security is not required to change between existing table settings.
Modify global (default) settings	Allows users to modify global table settings. (In Quantitate mode, click Tools > Settings > New Quantitation Results Table Settings.)
Modify audit trail settings	Legacy setting, now disabled.
Disable, enable and clear audit trail	Allows users to clear the quantitation audit trail from a Results Table. This option does not control the audit trail settings available from View > Audit Trail Manager.
Change results table column visibility	Allows users to select the columns to display in a Results Table. (To access the Table Settings dialog, in the Results Table, right-click and then click Table Settings > Edit.)
Change results table column precision	Allows users to modify the Significant Figures, Scientific Notation, or Precision columns in a Results Table. (To access the Table Settings dialog, in the Results Table, right-click and then click Table Settings > Edit. Click Columns and then click Edit.)
Run temporary queries	Legacy setting, now disabled.

Table 2-13 Analyst Software Access to Quantitation (Continued)

Preset access	Description
Modify or save queries	<p>Allows users to modify existing or save new queries. (To modify queries, Ctrl+right-click in the Results Table, click Query and then select an existing query.)</p> <p>Allows users to modify queries in a Results Table. (In a Results Table, right-click and then click Table Settings > Edit > Queries. Select an existing query and then click Edit.)</p>
Run temporary sorts	Legacy setting, now disabled.
Modify or save sorts	Legacy setting, now disabled.
Use metric plot settings dialog	Legacy setting, now disabled.
Modify or create metric plot settings	<p>Allows users to create new metric plots from the Results Table. (In the Results Table, right-click and then click Metric Plot > New.)</p> <p>Allows users to modify metric plot from a Results Table. (In a Results Table, right-click and then click Table Settings > Edit > Metric Plot. Select an existing metric plot and then click Edit.)</p> <p>This security item does not prevent users from modifying existing metric plots by running a metric plot, right-clicking in the plot, and then selecting Edit Settings.</p>
Create Analyte Groups	Allows users to create analyte groups from a Results Table. (In a Results Table, right-click and then click Analyte Group > New.)
Modify Analyte Groups	Allows users to modify Analyte Groups. (In a Results Table right-click and then click Table Settings > Edit > Analyte Groups. Click an existing group and then click Edit.)
Change default peak review options	Allows users to change the default peak settings. (In Quantitate mode, click Tools > Settings > Quantitation Peak Review Settings.)
Change "simple" parameters in peak review	Allows users to change simple parameters in peak review. When a peak review pane is open, simple parameters are the ones visible when the Show or Hide Parameters button is clicked once.
Change "advanced" parameters in peak review	Allows users to change the Advanced parameters in peak review. When the peak review pane is open, advanced parameters are the ones visible when the Show or Hide Parameters button is clicked twice.
Manually integrate	Allows users to manually integrate peaks by using the Manual Integration Mode from the peak review pane.
"Update" method in peak review	Allows users to update and revert a method after the quantitation method has been changed for a specific peak in peak review pane.

Table 2-13 Analyst Software Access to Quantitation (Continued)

Preset access	Description
Add or modify annotation	Allows users to add or modify sample annotations in the peak review pane or window using the Sample Annotation option from the right-click menu or by adding a Sample Annotation column to the Results Table.
Change regression parameters	Allows users to change the regression settings in a calibration curve pane.
Modify Sample ID	Allows users to add or modify the sample ID in a Results Table.
Modify Sample Type	Allows users to change the sample type in a Results Table.
Modify Sample Comment	Allows users to add or modify the sample comment in a Results Table.
Modify Weight to Volume ratio	Allows users to modify the weight-to-volume ratio in a Results Table.
Modify Dilution Factor	Allows users to modify the dilution factor in a Results Table.
Modify Analyte Concentration	Allows users to modify the analyte concentrations in a Results Table.
Modify Analyte Units	Legacy setting, now disabled.
Modify IS Concentration	Allows users to modify the IS concentrations in a Results Table.
Modify IS Units	Legacy setting, now disabled.
Modify Processing Algorithms	Allows users to change the quantitation algorithm. (In Quantitate mode, click Tools > Settings > Quantitation Integration Algorithm.)
Enable or Disable percent rule in Manual Integration	Allows users to change the manual integration (Percent Rule). (In Quantitate mode, click Tools > Settings > Quantitation Peak Review Settings.)

Table 2-14 Analyst Software Access to Report Template Editor

Preset access	Description
Create/modify report templates	Allows users to create new report templates and modify the existing ones.
Open report templates as read-only	Allows users to open .rpt files in read-only format. (Click File > Open.)
Print	Allows users to print in any mode.
Select report templates	Allows users to select existing report templates in the Print dialog.

Table 2-15 Analyst Software Access to Sample Queue

Preset access	Description
Start Sample	Allows users to start a sample in the queue.
Abort Sample	Allows users to abort a sample in the queue.

Table 2-15 Analyst Software Access to Sample Queue (Continued)

Preset access	Description
Stop Sample	Allows users to stop a sample in the queue.
Stop Queue	Allows users to stop the queue.
Pause Sample Now	Allows users to pause the sample immediately.
Insert Pause Before Selected Sample(s)	Allows users to insert a pause before the next sample.
Continue Sample	Allows users to continue (restart) the sample.
Next Period	Allows users to acquire the next period immediately.
Extend Period	Allows users to extend the period that is currently being acquired.
Next Sample	Allows users to acquire next sample.
Advance Pump Gradient	Legacy setting, now disabled.
Equilibrate	Allows users to equilibrate the system.
Stand By	Allows users to put the instrument into standby mode.
Ready	Allows users to put the instrument into ready mode.
Reacquire	Allows users to reacquire samples.
Insert Pause	Allows users to insert a pause in the queue.
Delete Sample or Batch	Allows users to delete a sample or a batch in the queue.
Move Batch	Allows users to change the batch order in the queue.

Table 2-16 Analyst Software Access to Tune

Preset access	Description
Edit parameter settings	Allows users to edit parameter settings. (In Tune and Calibrate mode, click Tools > Settings > Parameter Settings.)
Edit tuning options	Allows users to edit the tuning options.
Edit instrument data	Allows users to edit instrument data.
Manual tune	Allows users to use the Manual Tuning feature in Tune and Calibrate mode.
Calibrate from current spectrum	Allows users to calibrate using a spectrum.
Instrument optimization	Allows users to run the Instrument Optimization feature in Tune and Calibrate mode.
Compound optimization	Allows users to run the Compound Optimization feature. The Compound Optimization feature is not available in the Analyst TF software.
Tuning Instrument	Allows users to use the features the Tune and Calibrate mode features.
Advanced Resolution Table Modification	Allows user to configure resolution using the Advanced button in the Resolution tab.

Table 2-16 Analyst Software Access to Tune (Continued)

Preset access	Description
Auto TOF Mass Calibration	Allows users to perform mass calibration (for TOF instruments only.)

Table 2-17 Analyst Software Access Rights

Preset access	Description
Security Config	Allows users to configure security-related settings.
View Status	Allows users to view the status of remote instruments.

MultiQuant Software Access

Table 2-18 MultiQuant Software Access

Preset access	Description
Create session file	Allows users to create a Results Table.
Create quantitation method	Allows users to create quantitation methods.
Modify quantitation method files	Allows users to modify the quantitation methods located in the Quantitation Methods folder in the Analyst Data folder.
Allow Export and Create Report of unlocked Results Table	Allows users to export or create reports of unlocked Results Tables.
Create automatic method	Allows users to select the Automatic Method option when they are creating Results Tables.
Replace existing Results Table when saved	Allows users to update existing Results Tables but does not allow them to create a new Results Table using an existing Results Table name. For example, if a Results Table called RT1 is created, users can update it but they cannot create a new Results Table using the name RT1. Users cannot name an untitled Results Table using an existing Results Table name.
Change default quantitation method integration algorithm	In the Integration Default dialog, allows users to change the algorithm. (Click Edit > Project Integration Defaults.)
Change default quantitation method integration parameters	In the Integration Default dialog, allows users to change the algorithm default parameters. (Click Edit > Project Integration Defaults.)
Allow Enable Project Modified Peak Warning	Allows users to activate or deactivate the flag that enables the Project Modified Peak Warning option on the Edit menu.
Add samples to Results Table	Allows users to add samples. (Click Process > Add Samples.)
Remove samples from Results Table	Allows users to remove selected samples. (Click Process > Remove Selected Samples.)

Table 2-18 MultiQuant Software Access (Continued)

Preset access	Description
Export, import, or remove External Calibration	Allows users to export, import, or remove an external calibration using one of the following options: <ul style="list-style-type: none"> • Click Process > Export Calibration. • Click Process > Import External Calibration. • Click Process > Remove External Calibration.
Use, edit, or clear Isotopic Correction	Allows users to use, edit, or clear an isotopic correction using one of the following options: <ul style="list-style-type: none"> • Click Process > Use Default Isotope Correction. • Click Process > Edit Current Isotope Correction. • Click Process > Clear Previous Isotope Correction.
Change Audit Map settings	Allows users to modify the project audit map and modify the audit map definition. (Click Audit Trail > Audit Map Manager.)
Modify Sample Name	Allows users to modify the sample name in the Results Table.
Modify Sample Type	Allows users to modify the sample type (standard, QC, unknown) in the Results Table.
Modify Sample ID	Allows users to modify the sample ID in the Results Table.
Modify Actual Concentration	Allows users to modify the actual concentration of the standard and QC in the Results Table.
Modify Dilution Factor	Allows users to modify the dilution factor in the Results Table.
Modify Comment Fields	Allows users to modify comment fields: <ul style="list-style-type: none"> • Component Comment • IS Comment • IS Peak Comment • Peak Comment • Sample Comments
Allow manual integration	Allows users to enable manual integration mode in Peak Review.
Allow set to Peak Not Found	Allows users to use the Set peak to not found functionality in Peak Review. To perform this action, right-click in the Peak Review pane.
Include or exclude a peak from the Results Table	Allows users to include or exclude peaks from Results Tables, Statistics tables, and calibration curves.
Modify regression settings for fit and weight	Allows user to modify the regression settings in the calibration curve pane when using the Modify Results Table Method functionality and when using the New Quantitation Method wizard.

Table 2-18 MultiQuant Software Access (Continued)

Preset access	Description
Modify Results Table integration parameters for a single chromatogram	Allows user to modify a single chromatogram.
Modify quantitation method for the Results Table component	Allows user to apply the modifications from the single chromatograms to the component. Users must have this permission and the Modify Results Table integration parameters for a single chromatogram permission enabled if they want to update and then apply single modifications to components.
Create, use, or export Metric Plots in Results Tables	Allows users to create and use metric plots in the Results Table (Metric Plot button is enabled) or export metric plots. (Click File > Export.)
Set Peak Review Title Format	Allows users to modify the Peak Review Title Format in Peak Review. To perform this action, right-click in the Peak Review pane.
Add, Rename, or Modify custom column	Allows users to add, rename, or modify a custom column. Even without this permission, users can run queries that will automatically create custom columns.
Remove custom column	Allows users to delete a custom column in the Results Table.
Modify Results Table column settings	Allows users to modify Results Table column settings within a Results Table.
Save Column Settings as Project Default	Allows users to apply the column settings to the project.
Lock and save Results Table	Allows users to lock and save a Results Table.
Unlock and save Results Table	Allows users to unlock and save a Results Table.
Review and save Results Table	Allows users to review and save the Results Table.
Create or edit queries in Results Tables	Allows users to create or edit queries in a Results Table using one of the following options: <ul style="list-style-type: none"> • Click Process > Create Simple Query. • Click Process > Edit Simple Query.
Use Results Table queries	Allows users to run queries. (Click Process > Query.)
Use unencrypted MultiQuant queries	Allows users to run .xls queries from within the MQ settings folder.



Note: If you uninstall the MultiQuant software, the MultiQuant software security items in the Analyst software remain. (Security items are found on the Roles tab in the Security Configuration dialog.)

Adding a User or Group to the Analyst Software

1. On the **Navigation** bar, under **Configure**, double-click **Security Configuration**.
2. In the **Security Configuration** dialog, click the **People** tab.
3. Click **New Person**.
4. Using the **Select Users or Groups** dialog, add a user or group.
5. In the **Available Roles** pane, click a role and then click **Add**.
6. Click **OK** to close the **Security Configuration** dialog.

Changing a Role

1. On the **Navigation** bar, under **Configure**, double-click **Security Configuration**.
2. In the **Security Configuration** dialog, click the **People** tab.
3. In the left pane, click the person and then do one of the following:
 - In the **Available Roles** pane, click the required role and then click **Add** to add a role.
 - In the **Role(s) Selected** pane, click the required role and then click **Remove** to remove a role.

Removing People from the Analyst Software

1. On the **Navigation** bar, under **Configure**, double-click **Security Configuration**.
2. In the **Security Configuration** dialog, click the **People** tab.
3. In the left pane, select the person to be deleted and then click **Delete**.

Creating a Custom Role

1. On the **Navigation** bar, under **Configure**, double-click **Security Configuration**.
2. Click **More** and then click the **Roles** tab.

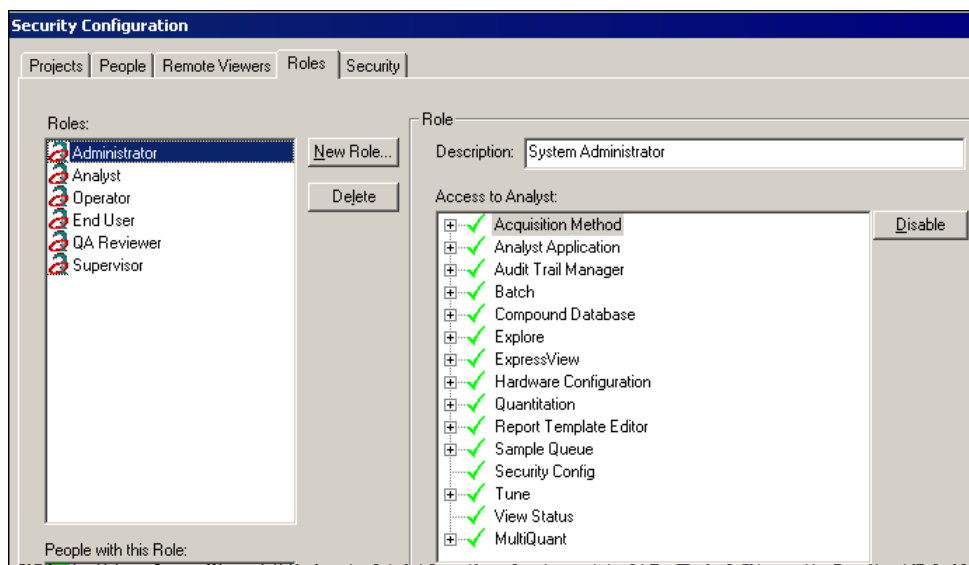


Figure 2-5 Roles tabs

3. Click **New Role**.
The New Role dialog appears.
4. Type the **Role Name** and **Description** in the appropriate fields and then click **OK**.



Note: All new user-defined roles have full access to the Analyst software. In the Access to Analyst pane, a green check mark indicates that system access is enabled; a red X means that system access is denied.

5. Double-click components in the **Access to Analyst** list to enable or disable access.
6. To configure access at a functional level, expand the components, and then double-click the functionality to enable or disable it.

Deleting a Custom Role



Note: If you have one person assigned to a single role, and that role is to be deleted, you are prompted to delete the person as well as the role.

1. On the **Navigation** bar, under **Configure**, double-click **Security Configuration**.
2. In the **Security Configuration** dialog, click **More** and then click the **Roles** tab.
3. In the **Roles** pane, select the role and then click **Delete**.

Setting Access to Projects and Project Files

You can configure access to projects and project files by person or group and control access by people or Windows security groups.

To use this feature of Analyst software security, use NTFS for your work route. If you do not set up project security, operator access to the project files depends on the data setup for each Windows user in NTFS. For more information, see [Windows Security Configuration on page 11](#).



Note: When a project is created using the Analyst software, all users have access to the project folders and subfolders.

1. On the **Navigation** bar, under **Configure**, double-click **Security Configuration**.

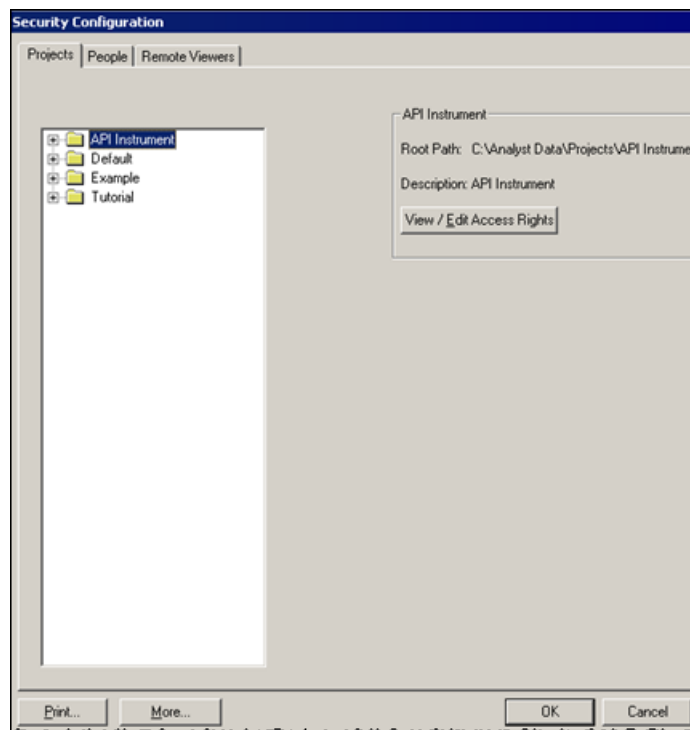


Figure 2-6 Projects tab

2. In the left pane of the **Security Configuration** dialog, click, click a folder or file.
3. Click **View/Edit Access Rights**.
The Properties dialog appears.
4. Add or remove user or groups and set permissions as required, and then click **OK**.

Common Analyst software and MultiQuant software file types and are listed in [Table 2-19](#). The API Instrument folder has all the subdirectories, except Processing Methods and Results.

Table 2-19 Analyst Software and MultiQuant Software Files

Extension	File type	Subfolder name
.aasf	<ul style="list-style-type: none"> Acquisition script Acquisition script (supplied example) 	<ul style="list-style-type: none"> Acquisition Scripts Example Scripts
.ata	Audit trail archives	Project Information
.atd	<ul style="list-style-type: none"> Instrument audit trail data Instrument audit trail settings Project audit trail data Project audit trail settings 	Project Information
.cam	Audit map	Project Information
.cset	MultiQuant software Results Table Column settings	Results
.dab	Acquisition batch	Batch
.dam	Acquisition method	Acquisition Methods
.dat	Acquisition batch template	Batch\Templates
.dll	Dynamic link library	Processing Scripts
.eph	Explore processing history data	Processing Methods
.hwprof	Hardware profile	Configuration*
.ins	Instrument data calibration information	Instrument Data*
.mdb	MS Access database	
.pdf	Portable document data	
.psf	Parameter settings	Parameter Settings*
.qmap	MultiQuant audit map	Project Information
.qmethod	MultiQuant quantitation method	Quantitation Methods
.qmf	Quantitation method	Quantitation Methods
.qsession	MultiQuant Results Table; holds quantitation audit trail data	Results
.rdb	Results Table; holds quantitation audit trail data	Results
.rpt	Report template	Templates\Templates\MethodTemplates\ReportTemplates\Workspace
.rtf	Rich text format	
.rtf	Log records from automated collection	Log
.sdb	Quantitation audit trail settings	Project Information
.tun	Tuning preference file	Preferences*

* Exists only in the API Instrument folder. All other subfolders exist within each project folder. They may be in the project level folder or within each subproject.

Table 2-19 Analyst Software and MultiQuant Software Files (Continued)

Extension	File type	Subfolder name
.txt	Text	
.wiff	Mass spectrometry data	<ul style="list-style-type: none"> • Tuning Cache* • Data
.xls	Excel spreadsheet	Batch

*** Exists only in the API Instrument folder. All other subfolders exist within each project folder. They may be in the project level folder or within each subproject.**

In the Example Project, the following formats are supported for importing batch information:

- .mdb
- .txt
- .xls
- .dbf: d base 5 and Fox Pro.

Adding Access to a Workstation

You can set up a list of instruments on a local computer and then remotely monitor the sample queues of those instruments. Users can only view the sample queue and the status of the instruments on these remote instrument stations. Even if they can perform other actions on the local workstation, they cannot perform them on a remote workstation.



Note: If the workstation is registered with the Administrator Console server, the buttons on the Remote Viewer tab are unavailable.

1. On the **Navigation** bar, under **Configure**, double-click **Security Configuration**.
2. In the **Security Configuration** dialog, click the **Remote Viewers** tab and then click **Add**.

Figure 2-7 New Instrument dialog

3. Type the workstation name in the **Name** field.

If you are using Active Directory in the native environment, the domain field is not visible and you can type a user name in UPN format.

4. Click **Browse** to navigate to a Domain and Computer.
5. Using the **Select Computers** dialog, select an instrument.
6. If required, type location information in the **Location** field.
7. If required, type a description in the **Description** field.
8. Click **OK**.

The information is displayed in the Remote Viewers tab.

Removing a Workstation

1. On the **Navigation** bar, under **Configure**, double-click **Security Configuration**.
2. In the **Security Configuration** dialog, click the **Remote Viewers** tab.
3. In the left pane, select an instrument.
4. Click **Delete** and then click **Yes**.

Printing Security Configurations

You can print a copy of the security configurations to keep on file.

1. On the **Navigation** bar, under **Configure**, double-click **Security Configuration**.
2. In the **Security Configuration** dialog, click **Print**.

This section describes the Analyst[®] Administrator Console (AAC) and explains how to configure and use it to centrally manage people, projects, and workstations.



Note: To use the Administrator Console and register workstations with the server, you must have Analyst software version 1.4.1 or later installed on each workstation.

The Administrator Console consists of a client and a server. The Administrator Console client is included with the Analyst software; the Administrator Console server is sold as a separate product. If you want to purchase the Administrator Console server and use the Administrator Console, contact your sales representative.

Topics in this section:

- [About the Administrator Console on page 41](#)
- [Setup of Workgroups on page 43](#)
- [Administrator Console Ongoing Tasks on page 56](#)

About the Administrator Console

This section describes the benefits of using the Administrator Console to manage workgroups, and it also provides an overview of its components and the console administrator role. For information on setting up workgroups, see [Setup of Workgroups on page 43](#).



Note: The console administrator must have network permission to set up network folders and set project permissions.

Benefits of Using the Administrator Console

The Administrator Console benefits network administrators in regulated environments where managing large groups of people, projects, and workstations can be costly and time-consuming. However, the Administrator Console can help any administrator manage resources more effectively by providing the option of managing projects centrally or by workstation, or both.

You can also use network acquisition in conjunction with the Administrator Console when managing projects centrally. For information on configuring network acquisition, see [Network Acquisition on page 63](#).

The Administrator Console consists of the following components:

- Administrator Console server.
- Administrator Console client.

Administrator Console Server

The Administrator Console server is installed on a computer from the Administrator Console installation CD. The Administrator Console client is also automatically installed during server installation.



Note: The Administrator Console server cannot be installed on the same workstation as the Analyst software.

If you have a firewall on the computer running the Administrator Console server, the 633(tcp), 1634(tcp), and 6001(tcp) ports must be opened on both the client and server computers.

All security information is stored in the database on the server. During installation, the security database is automatically populated with the preset Analyst software roles and users. Additionally, each time the Analyst software is started, the backup copy of the database on each registered workstation is updated to reflect the master copy on the Administrator Console server.

Administrator Console Client

The Administrator Console client is a Microsoft Management Console plug-in. It is installed on a workstation as part of the Analyst software installation, or it can be installed alone on a separate machine. When the Administrator Console client is installed on a workstation, the console administrators can use it to access the server remotely.

The Administrator Console client shows a tree view in the left pane containing Workgroups, Roles, User Pool, Project Root Pool, and Workstation Pool nodes. The right pane shows the contents of each node. A pool consists of all the potential users, project roots, and workstations that can be added to a workgroup.

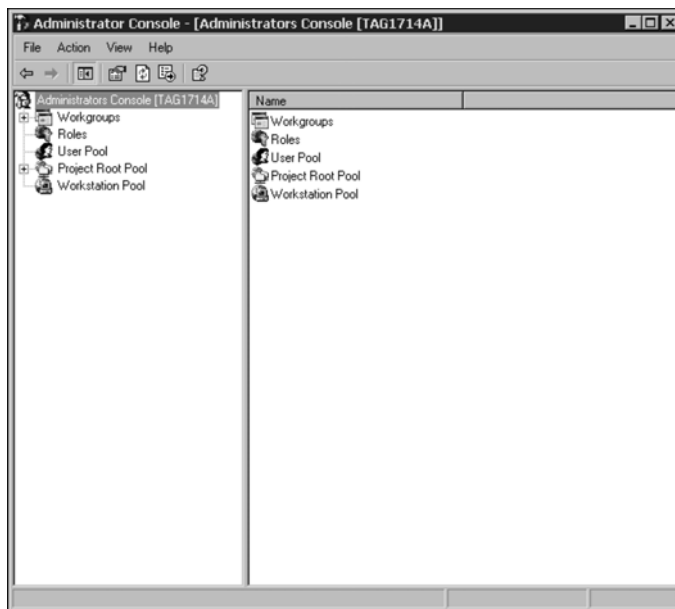


Figure 3-1 Administrator Console client

Console Administrators

The console administrators, who might also be the network or laboratory administrators, can use the Administrator Console to access projects and workstations, and assign roles from a central location. Instead of adding users to projects from each separate workstation, the console administrators can group all the users who are working on the same projects and who require access to the same workstations from a central location. Workstations can access this information on the Administrator Console server.

The person who installs the Administrator Console software on the server is automatically added to the users group in the console administrators workgroup, and is given the administrator role. The administrator account on the server is also added to the users group. For more information on the console administrators workgroup, see [Console Administrators Workgroup on page 45](#).



Note: To make sure that a workstation can always be accessed by one of the console administrators, add at least one console administrator to each workgroup.

Access to the Administrator Console client is strictly controlled. At startup, the Administrator Console checks whether the user is a member of the Console Administrators workgroup and has local administrator privileges. The authenticity checking done by the Administrator Console combines security checks by Windows and the Analyst software.

Setup of Workgroups

This section explains the concept of workgroups and how to set them up using the Administrator Console. After setting up the workgroups, you can modify them as required. For more information on modifying existing workgroups, see [Administrator Console Ongoing Tasks on page 56](#).



Note: Changes made to the database take effect when the Analyst software is restarted.

Overview of Tasks

For the tasks required to initially set up the Administrator Console to create workgroups, see [Table 3-1](#). Some tasks are optional.



Note: After you register a workstation with the Administrator Console server, add users and roles using the Administrator Console client. In the Analyst software, in the Security Configuration dialog, the People and Roles tabs as well as the Security mode option on the Security tab are read-only. If you log on to the Local workgroup, these tabs are enabled.

Table 3-1 Tasks for Setting Up the Administrator Console

	Task	Procedure
<input type="checkbox"/>	Connecting the Administrator Console client to the server.	See To connect the Administrator Console client to the server (standalone application) on page 46 or see To connect the Administrator Console client to the server (workstation) on page 46 .
<input type="checkbox"/>	Using the Administrator Console client, create or configure roles (optional).	See Creating Roles on page 47 .
<input type="checkbox"/>	Using the Administrator Console client, add users to the User Pool.	See Adding Users or Groups to the User Pool on page 48 .
<input type="checkbox"/>	Using the Administrator Console client, set the Default Project location (optional).	See Selecting a Template Project on page 49 .
<input type="checkbox"/>	Using the Administrator Console client, create or add projects and root directories (optional).	See Creating a Root Folder on page 49 .
<input type="checkbox"/>	Using the Administrator Console client, create workgroups.	See Creating a Workgroup on page 51 .
<input type="checkbox"/>	At each workstation, run the Analyst software and register the workstation.	See To register a workstation on page 53 .
<input type="checkbox"/>	At each workstation, run the Administrator Console client and add the workstation to a workgroup.*	See Adding Workstations to a Workgroup on page 54 .
<input type="checkbox"/>	Setting a default workgroup for each workstation (optional).	See Setting a Default Workgroup for the Analyst Logon Information dialog on page 55 .
*You can immediately add a workstation to a workgroup while you are at the workstation, or you can register the workstation and add it to a workgroup when required.		

About Workgroups

Workgroups consist of users, workstations, and projects. The Workstation Pool is automatically updated each time a workstation is registered with the Administrator Console server. To use server-based security, register the workstation with the Administrator Console server.



Note: Alternatively, if you manage Windows file security through the IT department, you can create workgroups containing users and workstations only.

Create a workgroup by adding resources from their respective pools. Before creating any workgroups, make sure you add all potential users to the User Pool and projects to the Project Root Pool.

If required, create additional roles or modify the default roles. You can also select the security mode for each workgroup. For more information on security modes, see [Analyst Software and Windows Security: Working Together on page 9](#).

For an example of workstations registered with the server, see [Figure 3-2](#). If server-based security is no longer required for a particular workstation, manage security for the workstation locally through the Analyst software.

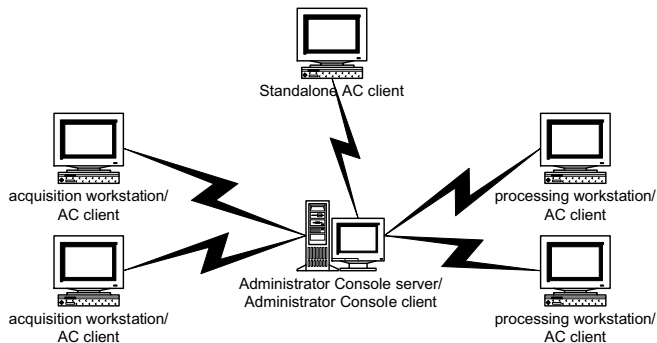


Figure 3-2 Example of Administrator Console server and Administrator Console client and workstations

Console Administrators Workgroup

The console administrators workgroup, which is created during server installation and cannot be deleted, appears in the Administrator Console client. The workgroup contains users only—projects and workstations cannot be added.

The security mode for the workgroup is preset to Integrated mode, and the users in the workgroup include the local administrator and the user who installed the Administrator Console on the server. If required, change the security mode. For more information, see [To change the security mode of a workgroup on page 60](#).

Set File Permissions

Each time users and projects in the workgroup are changed, run the Set File Permissions function to update the Windows file permissions for the projects in that workgroup. This function sets read, write, and delete permissions for all users in the workgroup to all projects in the workgroup. It appends new permissions to existing projects in the workgroup and assigns Console Administrators full control to the project.

To use the Set File Permissions function, console administrators needs the Change Permissions rights on the folders that they are trying to change.



Note: Use Windows security to limit access by the user to the projects within their workgroup.

If you delete a user from the workgroup or add new projects, these changes are not reflected at the project level until Set File Permissions is run. Members of the Console Administrators workgroup are also updated in every project.

Connecting the Administrator Console Client to the Server

Install the Administrator Console client either as a standalone application or as part of the Analyst software installation. If the Administrator Console client is installed on a workstation as part of the Analyst software installation, connect the Administrator Console to the same Administrator

Console server as the workstation or another Administrator Console server. This enables you to connect the Administrator Console client to different Administrator Console servers without affecting the security settings for the workgroup.



Note: If the workstation loses its connection to the server, users can still log on to the workstation using the local database on the workstation or the backup copy of the master database.

To connect the Administrator Console client to the server (standalone application)

After installing the Administrator Console, establish the connection between the client and server. Use this procedure to browse to the server location.

1. If you are using Windows 7, right-click the AAC Icon and then click Run as. In the Run As dialog, click The following user: and then select Administrator. In the Command Line, type “Administrator Console.msc” and then click Enter. If you do not run the application as an administrator, then the database will not be displayed properly.
2. If you are using Windows XP, run the Administrator Console client.
The Browse for Computer dialog appears.
3. Browse to the server and then click **OK**.

To connect the Administrator Console client to the server (workstation)

After installing the Administrator Console, establish the connection between the client and server. Use this procedure to browse to the server location.

1. If you are using Windows 7, right-click the AAC Icon and then click Run as. In the Run As dialog, click The following user: and then select Administrator. In the Command Line, type “Administrator Console.msc” and then click Enter. If you do not run the application as an administrator, then the database will not be displayed properly.
2. If you are using Windows XP, run the Administrator Console client.
3. Right-click **Administrators Console** and then click **Properties**.
The Administrator Console Properties dialog appears.

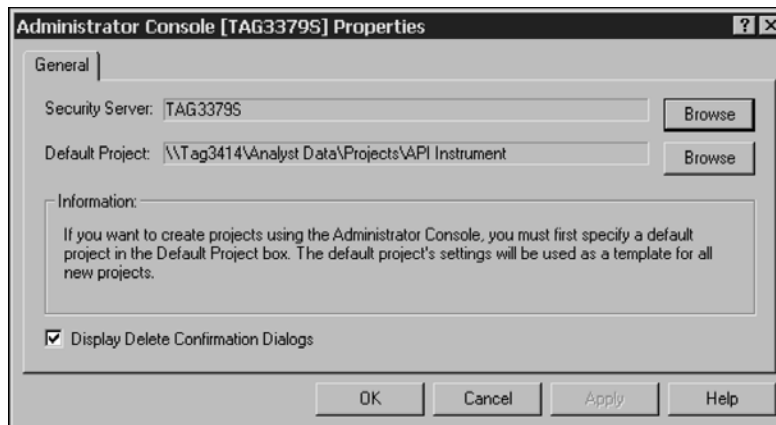


Figure 3-3 Administrator Console Properties dialog

- Next to the **Security Server** field, click **Browse** to navigate to the server and then click **OK**.

Creating Roles

The Analyst software has six predefined roles. If you require additional ones, either create a new role or copy an existing role and assign access rights. For more information on roles, see [Access to the Analyst Software on page 21](#).



Note: When using the Administrator Console to create new roles, the new role has all access rights disabled. Copied roles have the same access rights as the original role.

- Right-click **Roles** and then click **New Role**.
The Create Role dialog appears.
- In the **Name** field, type a name.
- In the **Description** field, type a description, and then click **OK**.
- Right-click the new role and then click **Properties**.

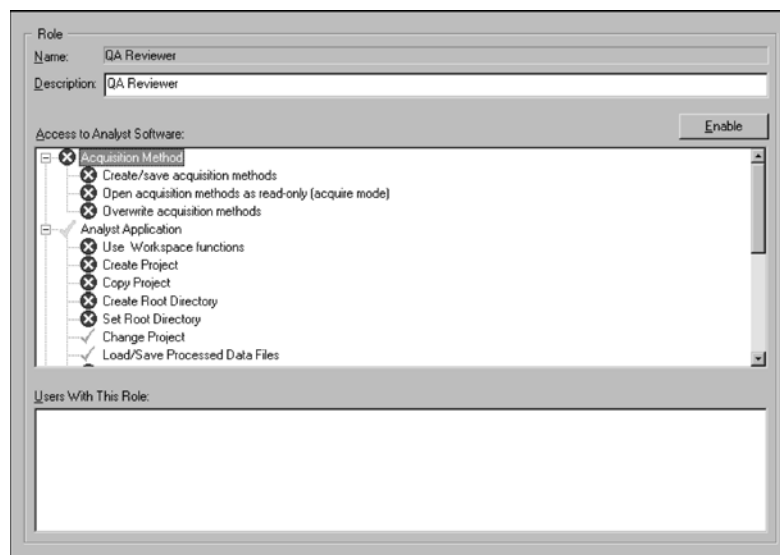


Figure 3-4 Properties dialog

- To provide access as required, double-click components in the **Access to Analyst Software** list and then click **OK**.



Tip! To configure access at a functional level, expand the components and then double-click the functionality to enable or disable it.

Copying a Role

- Click **Roles**.
- In the right pane, right-click and then click **Copy**.

The Copy Role dialog appears.

3. In the **Name** field, type a name.
4. In the **Description** field, type a description and then click **OK**.
5. Right-click the new role and then click **Properties**.

The properties dialog appears.

6. To provide access as required, double-click components in the **Access to Analyst Software** list and then click **OK**.



Tip! To configure access at a functional level, expand the components and then double-click the functionality to enable or disable it.

Adding Users or Groups to the User Pool

Only users authorized to log on to the workstation and to the Analyst[®] software can access the Analyst software. Before adding users to workgroups, they must be added to the User Pool. For more information on users, roles, and accessing the Analyst software, see [Access to the Analyst Software on page 21](#).

1. Right-click **User Pool** and then click **Add Users or Groups**.
The Select Users or Groups dialog appears.
2. Add users, groups, or Windows groups as required, and then click **OK**.



Tip! To add users or groups directly to both the workgroup and the User Pool, click the required workgroup, right-click **Users** and then click **Add Users or Groups**. To add users or groups from the network, click **Add Windows User**.

About Projects and Root Directories



Note: When setting up a root directory for the Administrator Console, make sure that the path name does not include the word “Projects”.

To create projects using the Administrator Console, specify a template project. The default project must be a shared folder, and its settings are copied and used as a template for all new projects.

A root directory is the specified folder in which the Analyst software looks for data. To be certain that project information is stored safely, create the root directory using the Analyst software. Do not create projects by copying them in Windows Explorer. Add projects to the Project Root Pool before adding them to a workgroup.

If you create projects outside the Administrator Console client, refresh the project root. When you refresh, you synchronize the contents of the Project Root Pool with the contents of the project roots on the network but the NTFS permissions remain unchanged.

Selecting a Template Project

Use this procedure to select a template project to use as a template for all new projects.



Note: The template project must be on a shared drive so that it can be accessed by workstations on the network.

1. Run the Administrator Console client.
2. Right-click **Administrators Console** and then click **Properties**.

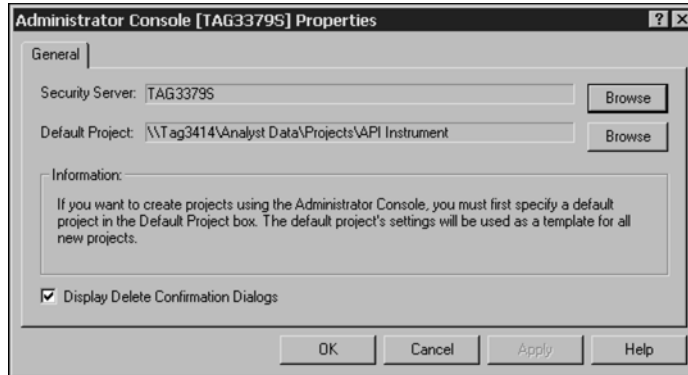


Figure 3-5 The Administrator Console Properties dialog

3. Next to the **Default Project** field, click **Browse** to navigate to the default project and then click **OK**.

Creating a Root Folder

Use this procedure to create a root folder and have the folder appear in the Project Root Pool.



Tip! Local drives are not accessible on the network. You can create a root folder only if the drives are shared.

1. Right-click **Project Root Pool** and then click **Create Project Root**.
The Create Root Folder dialog appears.
2. In the **Root Folder Location** field, type the folder location or click **Browse** to navigate to the root folder location.
3. In the **Root Folder Name** field, type the root folder name and then click **OK**.
The database is updated and the new root folder appears in the Project Root Pool.

Adding an Existing Root Directory

Use this procedure to add an existing root directory to the Project Root Pool. Any projects under the root project are automatically added.

1. Right-click **Project Root Pool** and then click **Add Existing Project Root**.
The Browse for Folder dialog appears.

2. Browse to the root directory location and then click **OK**.
The root directory appears in the Project Root Pool.

Refresh a Project Root

Use this procedure to synchronize the contents of the Project Root Pool with the contents of the project roots on the network. Refresh each project root individually.

- Expand **Project Root Pool**, right-click the project root, and then click **Refresh**.

Create a Project

1. Expand **Project Root Pool**, right-click the root, and then click **Create Project**.

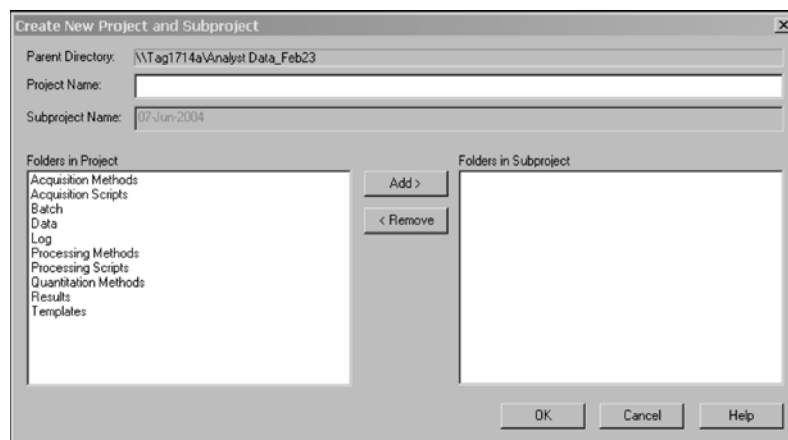


Figure 3-6 Create New Project and Subproject dialog

2. In the **Project Name** field, type the project name.



If you do not create a subproject at the same time that you create the project, you will not be able to do so later.

3. If you are using subprojects, in the **Folders in Project** list, select the folders to store in the subprojects, and then click **Add** to move them to the **Folders in Subproject** list.
4. The preset **Subproject Name** is the current date as provided by the system. If required, in the **Subproject Name** field, type a new name.
5. Click **OK**.

Adding an Existing Project

Use this procedure to add an existing project to a project root.

1. Expand **Project Root Pool**, right-click the project, and then click **Add Existing Project**.

The Browse for Folder dialog appears.

2. Browse to the project location and then click **OK**.

The project appears in the right pane.

About Workgroups

This section explains how to set up workgroups using the Administrator Console. Create the workgroup first and then add users, projects, and workstations to it. After creating the workgroup, select a security mode, and enable screen lock and auto logout, if required. For more information on screen lock and auto logout, see [Setting up Screen Lock and Auto Log Out on page 20](#).



Note: You can type a maximum of 1024 characters in the Change Description box of the Administrator Console Audit Trail. When you add or delete large numbers of users and projects, the event is audited; however, user and project names are not recorded in the Description field after the maximum is reached.

The security mode setting for the workgroup takes precedence over the security mode setting for the workstation if the workstation is registered with the Administrator Console server and is a member of the workgroup.

If you manage Windows file security through the IT department, you can create workgroups containing users and workstations only. If you choose to manage projects using the Administrator Console, all users in the workgroup are assigned read, write, and delete permissions and console administrators are assigned full control of the project.

Do not add local users to workgroups. The Administrator Console is a network application and only network users should be added to a workgroup. For information on creating projects, see [Create a Project on page 50](#).



Note: In each workgroup, there should be one user assigned the administrator role. Only an administrator or supervisor can unlock the Analyst software screen if the currently logged on user is unavailable.

Creating a Workgroup

1. Select a default workgroup for each workstation. For more information, see [Setting a Default Workgroup for the Analyst Logon Information dialog on page 55](#).
2. Right-click **Workgroup** and then click **New Workgroup**.
The Create Workgroup dialog appears.
3. In the **Workgroup Name** field, type a name.
4. In the **Description** field, type a description, and then click **OK**.

The workgroup is created and added into the Workgroup sub-tree, and the administrator console creates the appropriate workgroup name on the server.



Note: The Integrated mode is preset. If no default workgroup is selected, the security settings from the Console Administrators workgroup are used. For more information on security modes, see [Workgroup Security Modes and Logging on to the Analyst Software on page 55](#).

5. If required, change the security mode and set screen lock and auto log out.

- i. Right-click the new workgroup and then click **Properties**.

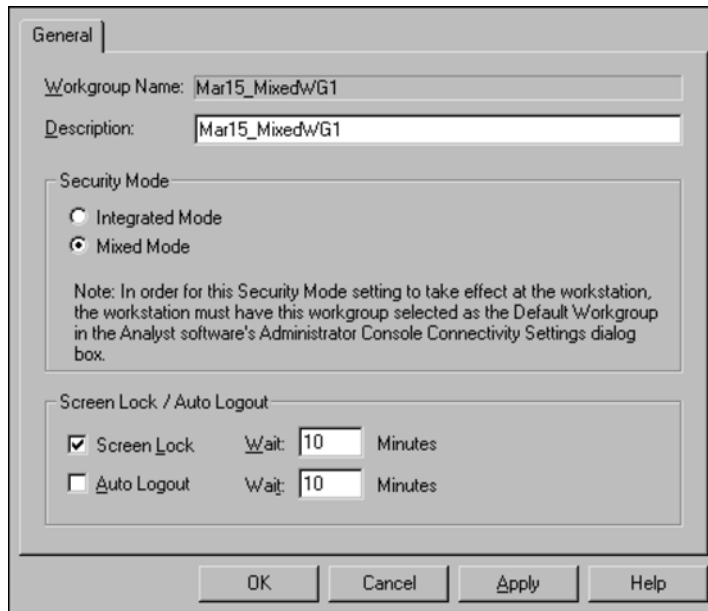


Figure 3-7 Properties dialog

- ii. Click a mode to change the security mode.
 - iii. Select **Screen Lock** to enable screen lock and, if required, change the preset Wait time.
 - iv. Select **Auto Logout** to enable auto logout and, if required, change the preset Wait time.
 - v. Click **OK**.
6. Add users, projects, and workstations to the new workgroup.
 7. For the changes to take effect, after all changes to the workgroup have been made, right-click the workgroup, and then click **Set File Permissions**. For more information, see [Set File Permissions on page 45](#).
 8. Restart the Analyst software on each workstation for the changes to take effect.

Adding Users or Groups to a Workgroup



Note: All users added to the workgroup are automatically assigned the Operator role.

1. Expand **Workgroups** and then expand the workgroup.
2. Right-click **User** and then click **Add Users or Groups**.
The Add Users or Groups to Workgroup dialog appears.
3. In the **Available Users from User Pool** list, click the user or group, and then click **Add**.



Tip! Add or select multiple users by pressing Shift and then selecting the required users.

4. If the required user is not in the list, you can add the name. Click **Add Windows User**, select the user or groups, and then click **OK**.
5. For the project permissions to take effect, after all changes to the workgroup have been made, right-click the workgroup, and then click **Set File Permissions**. For more information, see [Set File Permissions on page 45](#).

Adding or Removing a Role

For information on creating user-defined roles, see [Creating Roles on page 47](#).

1. Expand **Workgroups**, expand the workgroup, and then click **User**.
2. In the pane on the right, right-click the user and then click **Properties**.
The Properties dialog appears.
3. In the **Available Roles** list, click the role, click **Add** or **Remove**, as required, and then click **OK**.

Adding Projects to a Workgroup



Note: If a project is added to more than one workgroup, user access to the project is appended, not overwritten. For example, Workgroup 1 has User A, User B, and Project_01; Workgroup 2 has User B and User C. If Project_01 is also added to Workgroup 2, then Users A, B, and C will all have access to Project_01.

1. Expand **Workgroups** and then expand the workgroup.
2. Right-click **Project** and then click **Add Project**.
The Add Project to Workgroup dialog appears.
3. In the **Available Projects** list, click the project, click **Add**, and then click **OK**.
Each user is assigned read and write permissions to all projects in the workgroup.
4. For the project permissions to take effect, after all changes to the workgroup have been made, right-click the workgroup and then click **Set File Permissions**. For more information, see [Set File Permissions on page 45](#).

To register a workstation

Using the Analyst software, perform this procedure on each workstation during the initial workstation setup.



Tip! After registering the workstation, you can add it to a workgroup or workgroups, and then select a default workgroup for the users of that workstation.

1. In **Configure** mode, click **Tools > Settings > Administrator Options**.

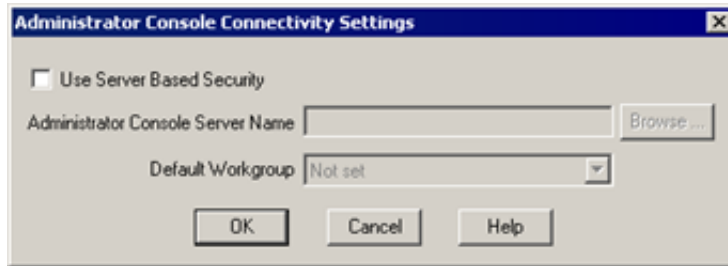


Figure 3-8 Administrator Console Connectivity Settings dialog

2. Select the **Use Server Based Security** check box.
3. In the **Administrator Console Server Name** field, type the name of the server or click **Browse** to navigate to the server.
4. Restart the Analyst software.

The workstation appears in the Workstation Pool in the Administrator Console software.

The Default Workgroup field is enabled after the workstation is registered with the server. Use the Default Workgroup field to select the default workgroup that appears in the Workgroup field in the Analyst - Logon Information dialog. For more information, see [Setting a Default Workgroup for the Analyst Logon Information dialog on page 55](#).

Adding Workstations to a Workgroup



Note: A workstation appears in the Workstation Pool only if it has been registered with the Administrator Console server.

1. Expand **Workgroups** and then expand the workgroup.
2. Right-click **Workstation** and then click **Add Workstation**.
The Add Workstation to Workgroup dialog appears.
3. In the **Available Workstations in Workstation Pool** list, click the workstation, click **Add**, and then click **OK**.
4. For the changes to take effect, after all changes to the workgroup have been made, right-click the workgroup and then click **Set File Permissions**. For more information, see [Set File Permissions on page 45](#).

Setting a Default Workgroup for the Analyst Logon Information dialog

Using the Analyst software, perform this procedure on each workstation. Only those workgroups to which the workstation has been added are available for selection. If you set a default workgroup, the security settings from the Console Administrators workgroup are used.

1. In **Configure** mode, click **Tools > Settings > Administrator Options**.

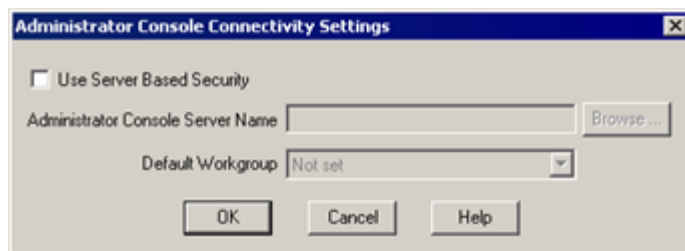


Figure 3-9 Administrator Console Connectivity Settings dialog



Note: The Workgroup field contains only the workgroups to which the workstation belongs. If the user is not a member of any of those workgroups, the user will not be able to log on to the workstation.

2. In the **Default Workgroup** field, select the workgroup and then click **OK**.
3. Restart the Analyst software.

The default workgroup appears in the Workgroup field in the Analyst - Logon Information dialog.

Changing the Default Workgroup when in Integrated Mode

When working in Integrated mode on a workstation that has a default workgroup set, you are automatically logged on to that workgroup when the Analyst software starts. To work in a workgroup other than the default workgroup, use the following procedure.

1. Press Shift and then run the Analyst software.

The Analyst - Logon Information dialog appears.

2. Click the workgroup and then click **OK**.

Users can log on using the server-based security from the chosen workgroup if they are members of the selected workgroup.

Workgroup Security Modes and Logging on to the Analyst Software

Log on to a workstation following the normal Windows and Analyst software procedure. If the workstation is registered with the server, then the Analyst - Logon Information dialog contains an additional Workgroup field, and users must select a workgroup.



Note: If a workgroup is not specified in the Administrator Console Connectivity Settings dialog, then the security mode from the Console Administrators workgroup is used.

Selecting a preset workgroup in the Administrator Console Connectivity Settings dialog determines how the user can log on to the Analyst software. If a preset workgroup is selected in the Administrator Console Connectivity Settings dialog, the Analyst - Logon Information dialog behaves as follows:

- In **Mixed Mode**, the default workgroup appears in the **Workgroup** field, and users can log on only if they are members of this workgroup.
- In **Integrated Mode**, the Analyst software automatically logs the user in using the server-based security information from the default workgroup. If required, the user can change the default workgroup and work in another workgroup. For more information, see [Changing the Default Workgroup when in Integrated Mode on page 55](#).

Audit Trails

Audit trail functionality is available in the Administrator Console. The audit map for the Administrator Console is stored in the database on the server.

You can read the audit trail from any workstation registered with the Administrator Console. Every Administrator Console event is silently audited according to the Administrator Console audit map. You cannot edit the Administrator Console audit map. For more information on audit trails, see [Auditing on page 69](#).

Administrator Console Ongoing Tasks

Perform various maintenance tasks as required. For example, delete resources from workgroups or from pools, or change the attributes of the Administrator Console and workgroups. For more information on creating workgroups, see [Creating a Workgroup on page 51](#).

- [Synchronizing the Administrator Console Client and Server on page 57](#)
- [Changing the Attributes of the Administrator Console Client on page 57](#)
- [Deleting Roles on page 57](#)
- [Changing the Properties of a Role on page 58](#)
- [Deleting Users or Groups on page 58](#)
- [Deleting Projects on page 58](#)
- [Deleting Workstations on page 59](#)
- [Deleting Workgroups on page 59](#)
- [Changing the Attributes of a Workgroup on page 59](#)
- [Deleting Users, Projects, or Workstations from a Workgroup on page 60](#)
- [Changing a Role on page 61](#)
- [Reviewing Project Permissions on page 61](#)

Synchronizing the Administrator Console Client and Server

If multiple Administrator Console clients access the server at the same time, refresh the Administrator Console client before you begin making any changes and periodically while modifying workgroups, roles, users, and workstations. Refreshing synchronizes the client with the server, which makes sure that any changes made using other Administrator Console clients are reflected in the current Administrator Console client. Refresh projects as well; however, projects are refreshed from the project root. For more information, see [Refresh a Project Root on page 50](#).

To refresh the Administrator Console client

- Right-click **Administrator Console** and then click **Refresh**.

Changing the Attributes of the Administrator Console Client

If the Administrator Console server name or location changes, update the information in the Administrator Console client so that security modifications continue to be downloaded to each workstation.

You can also prevent deletion confirmation dialogs from appearing each time a resource is deleted.

To change the server location

1. Right-click **Administrator Console** and then click **Properties**.
The Administrator Console Properties dialog appears.
2. Click **Change**, browse to the new server location, and then click **OK**.

To prevent the deletion confirmation dialog from appearing

Caution: After the option is turned off, deletions will happen automatically and you will not be given the option of cancelling the deletion.

1. Right-click **Administrator Console** and then click **Properties**.
The Administrator Console Properties dialog appears.
2. Clear the **Display Delete Confirmation Dialogs** check box and then click **OK**.

Deleting Roles

If you no longer require a user-defined role, delete it from the database.



Note: If you delete a user-defined role, the role is removed from all the users and groups in each workgroup to which it was assigned. If a user is assigned a single role and that role is deleted, the user will no longer have access to the Analyst software.

1. Click **Roles**.
2. In the right pane, right-click the role and then click **Delete**.

Changing the Properties of a Role

You can change the properties or description of a role.

1. Click **Roles**.
2. In the right pane, right-click the role and then click **Properties**.
The Properties dialog appears.
3. If required, in the **Description** field, type a description.
4. To change access rights, click the functionality from the **Access to Analyst Software** list and then click **Enable/Disable** to enable or disable access as required.

Deleting Users or Groups

You can delete users or groups from the User Pool.

1. Click **User Pool**.
2. In the right pane, right-click the users or groups and then click **Delete**.

Deleting Projects

You can delete an individual project from the project root, or, if you want to delete all the projects in the project root, you can delete the project root from the Project Root Pool. When a project root is deleted, the underlying projects are also deleted from the Project Root Pool.



Note: Deleting projects using the Administrator Console only removes the projects from the Project Root Pool in the Administrator Console. That is, the same projects on the network are not deleted; only the references to those projects are removed. No data is lost and the NTFS permissions are unchanged.

If you delete projects outside the Administrator Console client, refresh the project root. Refreshing synchronizes the contents of the Project Root Pool with the contents of the project roots on the network.

To delete a project from the project root

1. Expand **Project Root Pool** and then click the project root.
2. In the right pane, right-click the project and then click **Delete**.

To delete a project root from the Project Root Pool

- Expand **Project Root Pool**, right-click the project root and then click **Delete**.

To refresh a project root

Use this procedure to synchronize the contents of the Project Root Pool with the contents of the project roots on the network. Refresh each project root individually.

- Expand **Project Root Pool**, right-click the project root and then click **Refresh**.

Deleting Workstations

If a workstation is no longer in use or no longer required to be part of a workgroup, then delete it from the Workstation Pool. Deleting a workstation from the Workstation Pool removes it from any workgroups to which it was assigned. No data is lost on the workstation when it is removed from the pool. Delete workstations using either the Administrator Console client or the Analyst software.

To delete a workstation using the Administrator Console client

1. Click **Workstation Pool**.
2. In the right pane, right-click the workstation and then click **Delete**.

To delete a workstation using the Analyst software

1. In **Configure** mode, click **Tools > Settings > Administrator Options**.
The Administrator Console Connectivity Settings dialog appears.

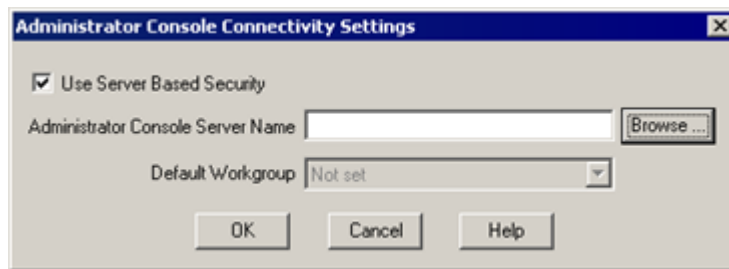


Figure 3-10 Administrator Console Connectivity Settings dialog

2. Clear the **Use Server Based Security** check box.
3. Restart the Analyst software.

Deleting Workgroups

If a workgroup is no longer required, delete it from the Workgroup tree. Deleting a workgroup only removes the workgroup from the Administrator Console. No data is lost from the workstation.

- Expand **Workgroups**, right-click the workgroup and then click **Delete**.

Changing the Attributes of a Workgroup

If required, change the description of a workgroup, change the security mode, or rename a workgroup.

To change the description of a workgroup

1. Expand **Workgroups**, right-click the workgroup and then click **Properties**.
The Properties dialog appears.
2. In the **Description** field, type a new workgroup description and then click **OK**.

To change the security mode of a workgroup

1. Expand **Workgroups**, right-click the workgroup and then click **Properties**.
The Properties dialog appears.
2. In the **Security Mode** section, click a security mode option and then click **OK**.

To enable or disable screen lock and auto logout

1. Expand **Workgroups**, right-click the workgroup and then click **Properties**.
The properties dialog appears.
2. In the **Screen Lock/Auto Logout** section, select or clear the **Screen Lock and Auto Logout** check boxes as required.
3. If required, in the **Wait** field, type a new wait time.

To rename a workgroup

1. Expand **Workgroups**, right-click the workgroup and then click **Rename**.
The name is highlighted.
2. Type the new workgroup name.

After you rename the workgroup, all workstations with the old workgroup name set as the default have to select a new workgroup for logging on to the Analyst software. The Default Workgroup field in the Administrator Console Connectivity Settings dialog is not updated with the new workgroup name.

Deleting Users, Projects, or Workstations from a Workgroup

Delete users, projects, and workstations from workgroups, as required. Deleting removes them from the workgroup, but they are still present in their respective pools.

To delete a user from a workgroup

1. Expand **Workgroups**, expand the workgroup, and then click **Users**.
2. In the right pane, right-click the user or groups and then click **Delete**.
3. For the changes to take effect, after all changes to the workgroup have been made, right-click the workgroup and then click **Set File Permissions**.

Read, write, and delete permissions for that user are removed from all the projects in the workgroup if the same user-project combination is not in any other workgroup, and the database is updated.

To delete a project from a workgroup

1. Expand **Workgroups**, expand the workgroup, and then click **Projects**.
2. In the right pane, right-click the project and then click **Delete**.
3. For the changes to take effect, after all changes to the workgroup have been made, right-click the workgroup and then click **Set File Permissions**.

Read, write, and delete permissions for that project are removed from all the users in the workgroup if the same user-project combination is not in any other workgroup, and the database is updated.

To delete a workstation from a workgroup

1. Expand **Workgroups**, expand the workgroup, and then click **Workstations**.
2. In the right pane, right-click the workstation and then click **Delete**.

Changing a Role

You can change the role assigned to a user.

Use this procedure to add, remove, or change a role. For information on creating user-defined roles, see [Creating Roles on page 47](#).

1. Expand **Workgroups**, expand the workgroup, and then click **User**.
2. In the right pane, right-click the user to change and then click **Properties**.
The Properties dialog appears.
3. In the **Available Roles** list, click the role.
4. Click **Add** and then click **OK**.

Reviewing Project Permissions

You can review the permissions of a project and change individual permissions. We recommend that you review permissions only and not change them because the individual changes will be reset each time the Set File Permissions feature is run on the workgroup.

1. Expand **Workgroups**, expand the workgroup, and then click **Projects**.
2. In the right pane, right-click the project and then click **Permissions**.
The properties dialog appears.
3. Click the **Security** tab to review the permissions.



This section describes how network acquisition works in the Analyst[®] software and the benefits and limitations of network-based projects. It also contains procedures on how to configure network acquisition.

Topics in this section:

- [About Network Acquisition on page 63](#)
- [Benefits of Using Network Acquisition on page 63](#)
- [File Security, File Formats, and Data Backup on page 64](#)
- [Configuring Network Acquisition on page 66](#)

About Network Acquisition

You can use network acquisition to acquire data from one or more instruments into network-based project folders that can be processed on remote workstations. This process is network-failure tolerant and makes sure that no data is lost if the network connection fails during acquisition.



Note: Network acquisition is supported in Integrated and Mixed Mode security only.

When using network-based projects, system performance can be slower than when using a local project. Since the audit trails also reside in the network folders, any activity that generates an audit record is also slower. When viewing network files, it may take some time for files to open, depending on the network performance. Network performance is not only related to the physical network hardware, but also to network traffic and design.



Note: If you use network acquisition in a regulated environment, synchronize the local computer time with the server time for accurate timestamps. The server time is used for the file creation time. The Audit Trail Manager records the file creation time using the local computer time.

Caution: Acquire data to a data file only from one instrument at a time. Acquiring data to the same data file from more than one instrument could result in data loss.

Benefits of Using Network Acquisition

Network data acquisition provides a secure method of working with project folders that reside entirely on network servers. This reduces the complexity involved in collecting data locally and then moving the data to a network location for storage. Also, since network drives are typically backed up automatically, the need to back up local drives is reduced or eliminated.



Note: The API Instrument folder is located on the local drive and is not automatically backed up.

If you append data to an existing file, the Analyst software copies the file from the network to the cache folder and acquires to the file locally.

File Security, File Formats, and Data Backup

Every Analyst software user who is acquiring data over the network must have read and write permission to the network project. If large files are generated, or if high-throughput analyses are used, use the flat file format to prevent data corruption and allow data to be transferred over the network more efficiently. The flat file option is preset in the Analyst software. During acquisition, the backup process runs in the background, transferring data from the local workstation to the network project folder.

Network Project Security

Users can log on to the Analyst software only in a root directory to which they have access.



Note: To have access to the project, all users require a minimum of read permission to the project folders, and a minimum of read and write permission to the Project Information folder.

When using a network root directory, default and user-created projects reside on the network. API Instrument and Example projects reside on the local drive and are not visible to a remote workstation.

The acquisition account setting determines the rights under which the backup process runs, and all account information is encrypted and stored in the registry. An Analyst software administrator can use the special acquisition account setting to select one of the following options:

- Client Account: Uses the privileges of the user logged on to the Analyst software.
- SAA (special acquisition administrator) Account: Uses the privileges of an independent user entered by an administrator in the Security tab.

Special Acquisition Account

Typically, the SAA user has full security rights to the Network Project folder. In contrast, the Analyst user who is logged on cannot delete data from the \Analyst Data\Projects\Data subfolder. In all cases where the client has access to the project, acquisition is unimpaired and data is saved to the cache. Whether the data is transferred to the network depends on how the SAA user has been set up.

Only valid SAA users can log on to or be added to the Analyst software. If an SAA user is invalid, the Analyst software generates a warning when the account information is entered.

If an SAA user is valid but has inappropriate folder access rights, no other rights are used, and backup to the network will not occur until the SAA user rights have been modified appropriately, or another acquisition account is selected. For information on selecting an acquisition account, see [Selecting an Acquisition Account on page 19](#).

Options for Data File Formats

The flat file format allows improved Analyst software performance in reading and writing large data files and is recommended when:

- Acquiring a file larger than 10 MB to the network.
- Performing high-throughput analyses.

The flat file format option splits the data file into two files: a .scan file, which contains scan information, and a .wiff file, which contains general information about the file such as acquisition, method, batch, device, and real-time data.

This differs from the compound file format where all information is located in one large .wiff file. Flat means these files are ordinary files where data is stored byte after byte and not organized in special structures as in compound documents. Flat files are more stable, less likely to become corrupted, and smaller than compound files. The uncomplicated structure makes reading and writing data more efficient, which simplifies the transfer of large amounts of data over the network. Data in compound documents is more difficult to transmit over the network because of structural limitations. Both file formats are available for local and network acquisition.

Data Backup Process

Whenever acquiring data to a network location, a cache is created to store the data locally until a backup to the network is completed and verified. The backup process runs at the end of each sample as a low priority process in the background. This process transfers the cached data to the network at a rate that reduces effects on the Analyst software performance, and it accommodates a wide range of network performance. When acquisition is complete, the backup process confirms that the network data file is identical to the cached file, optimizes the network data file size, and then deletes the cached file.

While the cached file is present, it appears on the acquisition station. A remote workstation can see the network copy, which is updated after the sample is totally acquired.

After acquisition and file transfer are completed, performance returns to normal. If at any point the backup process is interrupted, as in the instance of a network failure, acquisition to the cache continues uninterrupted. The cached files remain and are viewable from the acquisition workstation. The backup process is reinitialized whenever the Analyst software is actively acquiring, or when the Analyst software is restarted. The process requires reinitialization if:

- There has been an acquisition or network error.
- The process failed to verify that the network and cached copies were identical. This can happen if the file is locked by another process, such as being open in the Analyst software on either the acquisition or a remote workstation.

Every time the Analyst software is restarted, the backup process checks the cache and attempts to back up any files remaining. Restarting the Analyst software is the best way to successfully complete an interrupted backup.

During network acquisition, critical activities are logged in the audit trails for history tracking purposes. The Project Audit Trail resides on the network, recording audited activity in the project through acquisition and remote workstations, and it can be viewed from all workstations with appropriate access permissions.

Deleting the Contents of the Cache Folder

You can delete, or clean up, the contents of the cache folder. Clean the cache folder when a batch is stopped and is not restarted. This synchronizes the cache folder and the network folder.

1. In **Acquire** mode, click **Acquire > Stop Sample**.
2. Click **Acquire > Standby**.

The contents of the cache folder are deleted.

Configuring Network Acquisition

After selecting the acquisition account type, enable the flat file format, if required, and then set up the root directories for the network projects.

A network administrator must set up network-based project folders before you can acquire data. On the server, create and set the root directory containing the projects to which you want to acquire data. For more information on setting up projects and subprojects, see [About Projects and Root Directories on page 48](#).

Creating a Root Directory



Note: Use the Analyst software to create the root directory to be sure that the project information is stored safely. Do not create projects by copying them in Windows Explorer.

1. Click **Tools > Project > Create Root Directory**.
2. Browse to the location where you want to create the root directory.
3. In the **New text** field, name the directory and then click **OK**.

Setting the root directory



Note: Map the root directory using a universal naming convention path (`\\SERVERNAME\ROOTDIRECTORY`) and not to a network drive letter. The network drive letter may not be the same on every workstation.

1. Click **Tools > Project > Set Root Directory**.
2. In the **Browse for Folder** dialog, click **Browse** to navigate to the existing root directory, and then click **OK**.

After the root directory has been set, you can set up projects.

Changing the File Format

1. In **Configure** mode, click **Tools > Settings > Queue Options**.

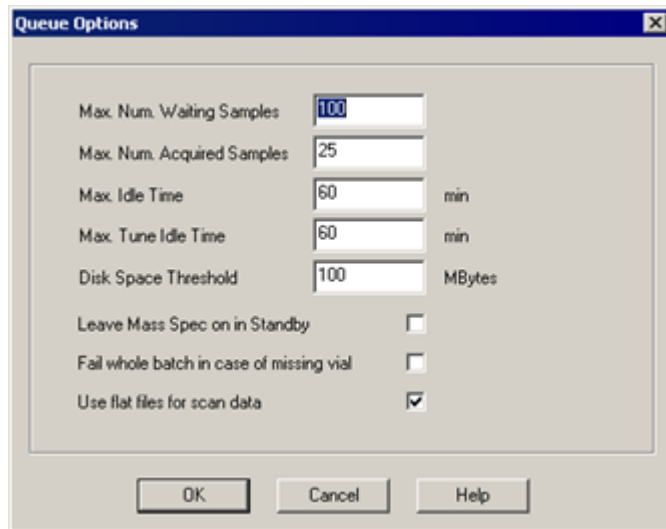


Figure 4-1 Queue Options dialog

2. The flat file option is preset. If you do not want to use the flat file format during acquisition, clear the **Use flat files for scan data** check box, and then click **OK**.

Selecting an Acquisition Account

1. On the **Navigation** bar, under **Configure**, double-click **Security Configuration**.
2. In the **Security Configuration** dialog, click **More** and then click the **Security** tab.
3. Click an acquisition account.
4. If you click **Special Acquisition Administrator Account**:
 - Click **Set Acquisition Account**.
 - Type the **User name**, **Password**, and if necessary, **Domain**, and then click **OK**.
 - If you are using Active Directory in the native environment, the domain field is not visible and you can type the user name in UPN format.
5. Click **OK**.



This section explains how to use the auditing functionality in the Analyst[®] software. For information about Windows auditing functions, see [System Audits on page 12](#).

Topics in this section:

- [About Audit Trails on page 69](#)
- [About Audit Maps on page 70](#)
- [Setup of Audit Maps on page 70](#)
- [Working with Audit Maps on page 72](#)
- [Viewing, Printing, and Searching Audit Trails on page 75](#)

About Audit Trails

The Analyst software groups audited events by instrument, by project, and by quantitation into audit trails, which are files that store records of the audited events. Audit trails, combined with files such as .wiff files and Results Table files, constitute valid electronic records that can be used for compliance purposes.

Table 5-1 Analyst Software Audit Trails

Audit trail	Examples of events recorded	Available audit maps stored in	Default audit maps
Instrument (one per workstation)	<ul style="list-style-type: none"> • Changes to: <ul style="list-style-type: none"> • Instrument resolutions • Mass calibrations • Sample queues • Security • Hardware profiles • Instrument maintenance log entries 	<ul style="list-style-type: none"> • API Instrument project • Project Information folder 	N/A
Project (one per project)	<ul style="list-style-type: none"> • Changes to: <ul style="list-style-type: none"> • Project • Data • Quantitation • Method • Batch • Tuning • Results Table • Report template files • Opening and closing of modules • Printing 	<ul style="list-style-type: none"> • Each project • Project Information folder 	Copied from the default project

Table 5-1 Analyst Software Audit Trails (Continued)

Audit trail	Examples of events recorded	Available audit maps stored in	Default audit maps
Quantitation (one per Results Table)	Changes to: <ul style="list-style-type: none"> • Quantitation methods • Sample information • Peak integration parameters 	Results Table file (.rdb file)	Copied from parent project

After the Instrument Audit Trail or a Project Audit Trail contains 1000 audit records, the Analyst software automatically archives the records and begins a new audit trail. For more information, see [Audit Trail Records on page 79](#).

About Audit Maps

Audit maps are files that specify:

- Events that are audited.
- Audited events that require the operator to specify reasons for the change.
- Audited events that require electronic signatures.

You can create many audit maps for the instrument and projects, but only use one audit map at a time for each instrument and project. The audit map used is called the active audit map for that instrument or project.

Each audit map contains a list of all the events that can be audited. Depending on where the map is used, the events apply to the Instrument Audit Trail or the Project and Quantitation Audit Trails. For each event, you can specify if it is audited, the type of audit, if an electronic signature is required, and up to ten predefined reasons for the event.

When creating a new Analyst software project, the audit maps for the project are copied from the Default project. The active audit map in the Default project becomes the active map in the new project.

When creating a new Results Table, the Quantitation Audit Trail configuration is defined by the quantitation events in the active audit map for the project. When saving a Results Table, the audit configuration from the active audit map is permanently stored with the Results Table. If you change the active audit map (applied to the project), the original audit configuration remains embedded in the Results Table file. You can distinguish the embedded configuration from the changed audit map by the last modified date and time displayed on the Settings tab.

Setup of Audit Maps

Before you begin working with projects that require auditing, set up audit maps appropriate to your standard operating procedures. Several default audit maps are present when the Analyst software is installed, but you may want to modify one or more of them for your own use. At a minimum, make sure you have one appropriate audit map for the Instrument Audit Trail and one appropriate audit map for each project.

Installed Audit Maps

The Analyst software includes several audit maps. To view or modify an audit map, see [Changing an Audit Map on page 74](#).

Default Audit Map: At installation, the default audit map is the active audit map for new projects. By default, all events are silently audited in the Analyst software. If you have converted the audit trail settings of a project created in a previous version of Analyst software, the default audit map contains that audit configuration.

No Audit Map: No events are audited.

Silent Audit Map: All events are audited. Electronic signatures and reasons are not required for any events.

Full Audit Map: All events are audited. Electronic signatures and reasons are required for all events.

Quant Only Audit Map: Only quantitation events are audited. These events require an electronic signature and a reason.

For descriptions of the three types of audit trails and their relationships to audit maps, see [Table 5-1](#). For more information about the events recorded in audit trails, see [Audit Trail Records on page 79](#).

For the locations of the audit maps and audit trails in the Audit Trail Manager, see [Figure 5-1](#).

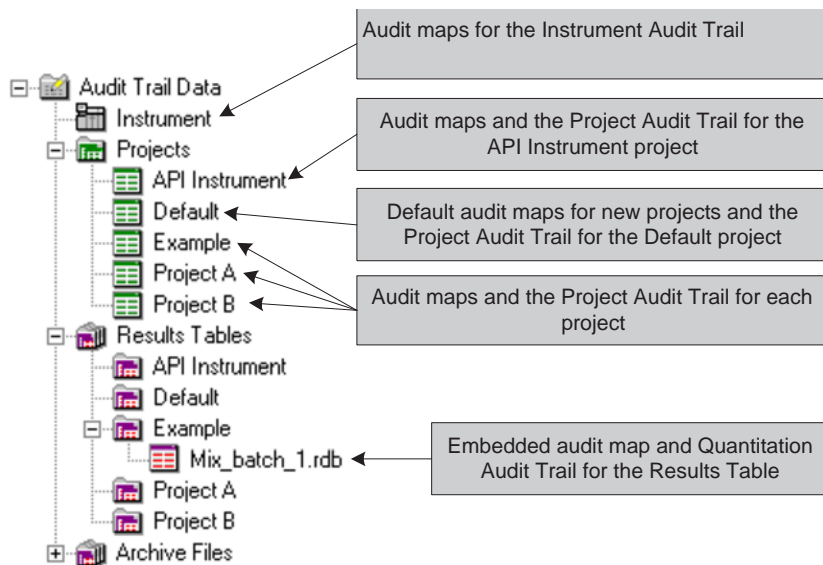


Figure 5-1 Location of audit maps

For information about the auditing process, see [Table 5-2](#). If you have upgraded from a previous version of the Analyst software, see [About using Audit Maps with Projects Created in Previous Versions of the Analyst Software on page 78](#).

Table 5-2 Checklist for Setting Up Auditing

	Task	Procedure
<input type="checkbox"/>	Create an audit map for the Instrument Audit Trail.	<ul style="list-style-type: none"> • See Creating an Audit Map on page 72. • See Changing an Audit Map on page 74.
<input type="checkbox"/>	Apply the audit map to the Instrument Audit Trail.	<ul style="list-style-type: none"> • See Applying an Audit Map on page 75.
<input type="checkbox"/>	Create a default active audit map for new projects.	<ul style="list-style-type: none"> • See Creating an Audit Map on page 72. • See Changing an Audit Map on page 74.
<input type="checkbox"/>	Specify the default active audit map for new projects.	<ul style="list-style-type: none"> • See Applying an Audit Map on page 75.
<input type="checkbox"/>	Configure the audit map you want to use for each existing project.	<ul style="list-style-type: none"> • See Creating an Audit Map on page 72. • See Changing an Audit Map on page 74. • See Copying an Audit Map from Another Project on page 74.
<input type="checkbox"/>	Apply the configured audit map to each existing project.	<ul style="list-style-type: none"> • See Applying an Audit Map on page 75.

Working with Audit Maps

The Analyst software includes several installed audit maps. View them to decide whether modifying one or more of them would be easier than creating a completely new one. For descriptions of the audit maps, see [Installed Audit Maps on page 71](#). To view or modify an installed audit map, see [Changing an Audit Map on page 74](#). If you know that a suitable audit map exists in a different project, copy the audit map. For a checklist of suggested steps for setting up auditing, see [Table 5-2](#).

If you delete an active audit map (in the Analyst software or in Windows Explorer), the project that uses that audit map uses the default audit map (Default Audit Map.cam). You cannot delete the default audit map.

Creating an Audit Map

The active audit map for the project determines which events are recorded in the Project Audit Trail and in the Quantitation Audit Trails for any Results Tables that are created.

1. Click **View > Audit Trail Manager**.
The Audit Trail Manager window appears.
2. In the left pane, expand the **Audit Trail Data** folder and then expand the **Projects** folder.
3. In the **Projects** section, click the project for which you want to create an audit map. If you are creating an audit map for use with the Instrument Audit Trail, click the **API Instrument** folder.

- On the **Settings** tab, click **Edit**.

The Audit Map Editor dialog appears with the active audit map displayed.

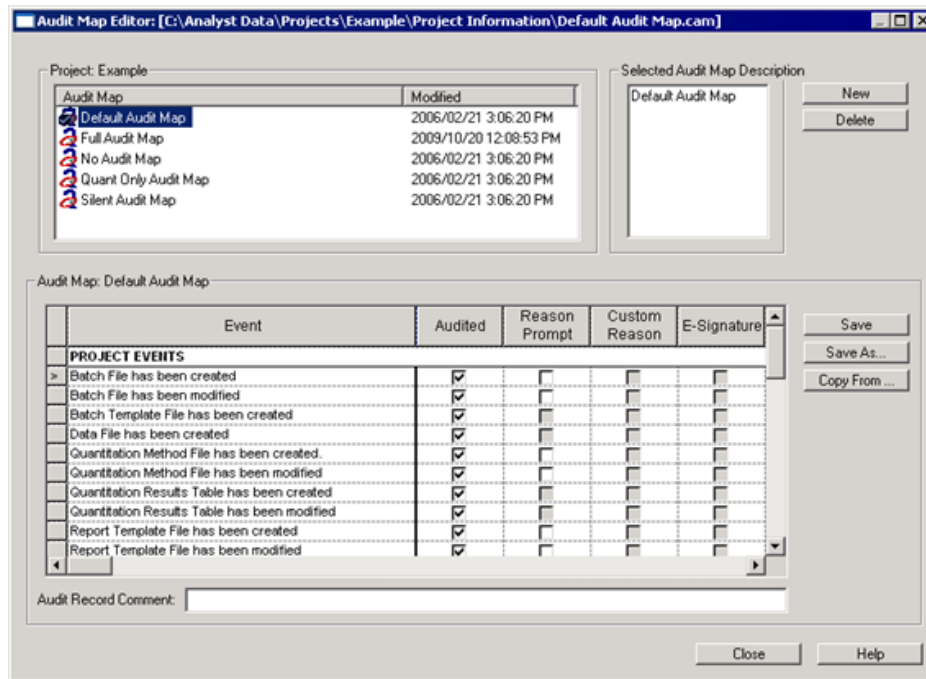


Figure 5-2 Audit Map Editor dialog

- Click **New**.

The Audit Map Editor dialog displays a new audit map no events audited.

- If required, in the **Selected Audit Map Description** field, type a description of the audit map.
- In the Audit Map table, configure each event as follows:
 - If you want the event to be audited, select the check box in the **Audited** column.



Tip! To fill consecutive cells in a column with the same text or check box value, type the text in the first row and then select the rows in the column starting with the first row. On the selected rows, right-click and then click **Fill Down**.

- If you want the operators to specify a predefined reason for the change when the event occurs, select the check box in the **Reason Prompt** column and then in the **Predefined Reason** columns, specify up to ten reasons.
- If you want the operators to type a custom reason, select the check box in the **Reason Prompt** column, and then select the check box in the **Custom Reason** column.
- If you want to require electronic signatures for the event, select the check box in the **E-Signature** column.
- If you want to make a note about the audit configuration for this event, in the **Audit Record Comment** column, type your comment.



Note: Save the audit map (with a .cam extension) in the Project Information subfolder of the project folder in which you want to use it.

8. To save the audit map configuration, click **Save**.

Now that you have created an audit map, use it with your project (see [Applying an Audit Map on page 75](#)) or copy it to another project (see [Copying an Audit Map from Another Project on page 74](#)).

Changing an Audit Map

Any changes you make apply only to the audit map in the project you select. Audit configurations embedded in Results Tables cannot be modified.

Caution: If you and another user are modifying the same audit map at the same time, only the changes made by the person who saved the file last are used.

1. Click **View > Audit Trail Manager**.
The Audit Trail Manager window appears.
2. In the left pane, expand the **Audit Trail Data** folder and then the **Projects** folder.
3. In the **Projects** section, click the project that contains the audit map you want to modify.
4. On the **Settings** tab, click **Edit**.
The Audit Map Editor dialog appears with the active audit map displayed.
5. In the **Projects** section, click the audit map to modify.
6. In the Audit Map table, make any changes to the configuration. For more information about the table, click **Help**.
7. To save the audit map, click **Save**.

Copying an Audit Map from Another Project

Audit maps can be copied from one project to another.

Caution: Do not copy .cam files (audit maps) between projects outside of the Analyst software as this may cause inaccurate audit trails.

1. Click **View > Audit Trail Manager**.
The Audit Trail Manager window appears.
2. In the left pane, expand the **Audit Trail Data** folder and then expand the **Projects** folder.
3. In the **Projects** section, click the project into which you want to paste the audit map.
4. On the **Settings** tab, click **Edit**.
The Audit Map Editor dialog appears with the active audit map displayed.
5. Click **New**.

The Audit Map Editor dialog displays a new audit map with no events audited.

6. Click **Copy From**.

The Open dialog appears.

7. Browse to and select the audit map file to copy and then click **Open**. Audit map files have the extension .cam and are stored in the Project Information folder of each project.

The selected audit map configuration appears.

8. To save the copied audit map to the current project, click **Save**.

Applying an Audit Map

When applying an audit map to the Instrument Audit Trail or a Project Audit Trail, it becomes the active audit map. The audit configuration in the active audit map determines which events are recorded in the audit trails.

The active audit map in a project contains the auditing configuration for the Project Audit Trail and the auditing configuration for the Quantitation Audit Trail of any Results Tables that are created.

1. Click **View > Audit Trail Manager**.

The Audit Trail Manager window appears.

2. In the left pane, expand the **Audit Trail Data** folder and then do one of the following:
 - If you are applying an audit map to the **Instrument Audit Trail**, click the **Instrument** folder.
 - If you are applying an audit map to a project, expand the **Projects** folder and then click the project for which you want to apply the audit map.
 - If you are specifying the default active audit map for new projects, expand the **Projects** folder and then click **Default**.
3. In the right pane, click the **Settings** tab.
4. In the **Available Audit Trail Maps** field, click the audit map you want to apply.
5. Click **Apply**.

Viewing, Printing, and Searching Audit Trails

This section gives instructions for viewing audit trails, archived audit trails, and instrument maintenance log entries. It also provides steps for searching and sorting audit records within audit trails.

Viewing an Audit Trail

1. Click **View > Audit Trail Manager**.

The Audit Trail Manager window appears.

2. In the left pane, expand the **Audit Trail Data** folder, and then do one of the following:

- To view the Instrument Audit Trail, click the **Instrument** folder. To view instrument-specific events, such as Mass Calibration Table(s) Replaced, view the Instrument Audit Trail recorded on the computer directly connected to the instrument.
- To view a Project Audit Trail, expand the **Projects** folder and then click the project that contains the audit trail.
- To view a Quantitation Audit Trail, expand the **Results Tables** folder, expand the appropriate project folder, and then click the **Results Table** file for the audit trail.

Viewing the Audit Configuration Embedded in a Results Table

The audit configuration used for a Results Table is embedded in the Results Table file when the Results Table is created. The Results Table audit configuration cannot be changed. The timestamp displayed next to the audit map name indicates when the audit map used to embed the configuration was last saved.

1. Click **View > Audit Trail Manager**.
The Audit Trail Manager window appears.
2. In the left pane, expand the **Audit Trail Data** folder and then the **Results Tables** folder.
3. In the **Results Tables** section, expand the project that contains the Results Table for which you want to view the audit map.
4. Click the **Results Table** file for which you want to view the audit map.
The audit trail appears in the right pane.
5. On the **Settings** tab, click **Details**.
The Results Table Audit Trail Settings dialog appears displaying the audit trail configuration for the Results Table.

Viewing Details for an Audit Record in the Instrument Audit Trail

You can view details for the following audited events: changes to the mass calibration table, changes to the resolution table, or entries in the Instrument Maintenance Log.

1. Click **View > Audit Trail Manager**.
The Audit Trail Manager window appears.
2. In the left pane, expand the **Audit Trail Data** folder.
3. In the **Audit Trail Data** section, click **Instrument**. If the audit trail does not appear, in the right pane, click the **History** tab.
The audit trail appears.
4. For any record that has additional details, in the **History** column, click **Review**.

Viewing an Archived Audit Trail

After the Instrument Audit Trail or a Project Audit Trail contains 1000 audit records, the Analyst software automatically archives the records and begins a new audit trail. The archived audit trail files are named with the type of audit trail and the date and time, for example, PAT-Archive-200209300820.ata.

1. Click **View > Audit Trail Manager**.
The Audit Trail Manager window appears.
2. In the left pane, expand the **Audit Trail Data** folder and then expand the **Archive Files** folder.
3. In the **Archive Files** section, expand the project that contains the archived audit trail you want to view.
4. Click the audit trail you want to view.
The archived audit trail appears in the right pane.
5. If the audit trail does not appear, in the right pane, click the **History** tab.
The audit trail appears.



Tip! You can also open an archived audit trail by right-clicking in the left pane and then clicking **Open Archives**. The Open dialog appears. Browse to the appropriate project folder and then, from the Project Information folder, select the archived audit trail file. These files have the extension .ata.

Printing an Audit Trail

1. Click **View > Audit Trail Manager** and then select the audit trail.
2. In the **Audit Trail Manager**, select the audit trail.
3. On the **History** tab, right-click, click **Print**, and then do one of the following:
 - To print the current page, click **Current Page**.
 - To print all the pages in the audit trail, click **All Pages**.

Searching for an Audit Record

1. Click **View > Audit Trail Manager** and then select the audit trail.
2. In the **Audit Trail Manager**, view the audit trail that you want to search.
3. On the **History** tab, right-click and then click **Search**.

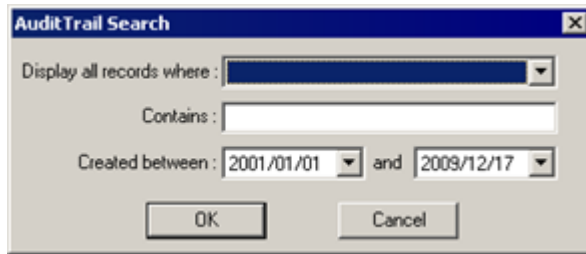


Figure 5-3 Audit Trail Search dialog

4. Use the **Display all records where** list and the **Contains** field to choose the records you want to find.
5. If required, select start and end dates from the **Created between** lists.
6. Click **OK**.

Only records that meet the criteria are listed.



Tip! To list all records, click **All**. To sort the records numerically, alphabetically, or by date, click the appropriate column heading.

About using Audit Maps with Projects Created in Previous Versions of the Analyst Software

When working with a project that was created in a previous version of the Analyst software (one that does not use audit maps), the audit trail settings for the project are converted to and saved as a new audit map file called Default Audit Map. The Project Audit Trail and Quantitation Audit Trail (for new Results Tables) for that project use the configuration in this new audit map. Any audit trail settings for the project are converted when an auditable event occurs. A message appears informing you that the audit trail settings for the project have been converted.



Note: The settings may also be silently converted to an audit map if you run a script on the project without ever opening the project.

Caution: Because audit maps are not supported in previous versions of the Analyst software, do not use a previous version of the Analyst software to open a project that uses an audit map. Events may not be audited according to the audit map.

When the Analyst software converts audit trail settings to an audit map, all events in the new audit map are configured in the same way as the original settings. Any predefined reasons in the original settings then apply to all the events in the audit map.

Results Tables that were created with a previous version of the Analyst software are converted to use the audit map functionality only when they are opened in the later version. You cannot open a Results Table whose audit trail settings have been converted to an audit map in a previous version of the Analyst software.

This section provides more information about audit trails and audit maps, including lists of all audited events that are stored in the Instrument, Project, and Quantitation Audit Trails.

For each audited change to a file or audited event, the following information is stored:

- Record number.
- Date and timestamp.
- User name.
- Full user name.
- Analyst[®] software module.
- Description of the change.
- Reason for the change, if required.
- Electronic signature, if required.

Audit Trail Records

The Instrument, Project, and Quantitation Audit Trails are encrypted files. All audit trail files are stored in the project directories under the root directory.

Audit Trail Archives

Audit records accumulate in the Project Audit Trail and Instrument Audit Trail and can create large files that are difficult to navigate and manage. Quantitation Audit Trails typically have a smaller, more manageable number of records.

When the Instrument Audit Trail or a Project Audit Trail reaches 1000 records, a final record stating that the file has been archived is added. The audit trail is automatically saved in the Project Information folder with a name indicating the type of audit trail and the date and time, for example, "PAT-Archive-200209300820.ata". A new Instrument Audit Trail or Project Audit Trail is created, and the first record of the archived audit trail gives the path.

Instrument Audit Trail

Each workstation has one Instrument Audit Trail. It records events such as additions or replacements to the mass calibration resolution tables, system configuration changes, security events, and entries in the Instrument Maintenance Log. For computers not directly connected to an instrument, the Instrument Audit Trail records only security events.

The Instrument Audit Trail records the following events:

- Mass calibration tables replaced.
- Mass calibration table added.
- Resolution tables replaced.
- Resolution table added.
- Hardware profile has been activated.*
- Hardware profile has been deactivated.*
- An Instrument Maintenance Log has been entered.
- Batch file submitted.*
- Sample submitted for acquisition.*
- Sample moved from position x to position y of Batch File.*
- Move batch.*
- Reacquiring sample(s).*
- Mass calibration table and resolution table changed.
- Resolution table(s) replaced - No Prompt.*
- Instrument settings have been changed.
- Instrument calibration authorization.
- Mass calibration table(s) replaced.*
- User logged in.*
- User logged out.*
- User login failed.*
- Security sent notification.*
- The security configuration has been modified.*
- Duo valve switch counter reset.
- User added.*
- User deleted.*
- User type added.*
- User type deleted.*
- User type changed.*
- User mode changed.*
- User changed user type.*
- Acquisition account changed.*
- Screen lock changed.*
- Auto logout changed.*
- Instrument added.*
- Instrument deleted.*

- Project role added.*
- Project role changed.*
- Project role deleted.*
- Project security changed.*
- Tune parameter settings changed.*

* This event cannot be audited with a reason. It can be silently audited or not audited.

Project Audit Trail

Each project has a Project Audit Trail. It records events such as creation, modification, and deletion events for project, data, quantitation, method, batch, tuning, Results Table, and report template files, as well as module opening, closing, and printing events.

The Project Audit Trail can record the following events:

- Audit map has been created.‡
- Audit map has been modified.‡
- Audit map has been deleted.‡
- Batch file has been created.*
- Batch file has been modified.*
- Batch template file has been created.*
- Data file has been created.*
- Quantitation method file has been created.*
- Quantitation method file has been modified.*
- Quantitation results table has been created.*
- Quantitation results table has been modified.*
- Report template file has been created.
- Report template file has been modified.
- Acquisition method file has been created.
- Acquisition method file has been modified.
- Accessed module.*
- Closed module.*
- Sample has been added to data file.*
- Printing document on printer.
- Finished printing document on printer.*
- Data file has been opened.*
- Explore history file has been saved.
- Processed data file has been saved.
- Checksum file.*

- Project settings have been changed.**
- The processing algorithm has been changed.*

‡ This event is always silently audited and does not appear in the Audit Map Editor dialog.

* This event cannot be audited with a reason. It can be silently audited or not audited.

** This event is always audited.

Quantitation Audit Trail

One Quantitation Audit Trail is stored in every Results Table file. When a Results Table is created, the active audit map in the project is saved in the Results Table file for use with the Quantitation Audit Trail. This embedded audit map cannot be modified after the creation of the Results Table. Any changes to the Results Table are audited based on the embedded audit map. Changes to the active audit map (within the project) are not updated in existing Results Tables, but any new Results Tables will use the changed active audit map.

A Quantitation Audit Trail event description includes the operation performed on the data, such as the points removed from a calibration, automatic and manual baseline fitting, and curve fitting changes.

In a Quantitation Audit Trail, audit records related to the integration of sample peaks have additional details. These records include the latest quantitation processing parameters associated with each sample in the Results Table. For example, the audit trail for a Results Table could include the parameters used for all manual corrections to the automatic peak integrations.

The Quantitation Audit Trail can record the following events:

- Quantitation method has been updated.
- Quantitation peak has been reverted back to original.
- Quantitation peak has been integrated.
- Results Table has been created.
- Quantitation method has been changed
- Files have been added to Results Table.
- Files have been removed from Results Table.
- Results Table accessed by QA Reviewer.
- Results Table has been saved.
- Results Table audit trail entries have been removed.
- "Use IT" has been changed.
- "Sample Name" has been changed.
- "Sample ID" has been changed.
- "Sample Type" has been changed.
- "Sample Comment" has been changed.
- "Sample Annotation" has been changed.
- "Weight to Volume Ratio" has been changed.
- "Dilution Factor" has been changed.

- “Concentration” has been changed.
- “Analyte Annotation” has changed.
- Formula column has been added.
- Formula name has been changed.
- Formula string has been changed.
- Formula column has been removed.
- “Custom Title” has changed.
- Samples have been added/removed.

Administrator Console Audit Trail

Each Administrator Console server has a corresponding audit trail. If the Analyst software is connected to a server, this audit trail becomes visible. It records security setting changes such as adding or removing users. All events are silently audited and you cannot edit this audit map. For more information about the Administrator Console, see [Analyst Administrator Console on page 41](#).



This section explains how to use the auditing functionality in the MultiQuant™ software.

Topics in this section:

- [About the Audit Trail Manager on page 85](#)
- [About Audit Maps on page 86](#)
- [Setting up Audit Maps on page 86](#)
- [Audit Configurations on page 88](#)
- [Viewing, Searching, and Printing Audit Trails on page 89](#)
- [About the Audit Trail Viewer on page 91](#)

About the Audit Trail Manager

The MultiQuant software groups quantitation audited events into audit trails. Audit trails are files that store records of the audited events. Audit Trails, combined with files such as .wiff files, quantitation methods, and Results Table files, constitute valid electronic records that can be used for compliance purposes. See also [Auditing on page 69](#) for information about auditing in the Analyst® software.

The Audit Trail Manager in the MultiQuant software maintains all the events as defined in the audit map. The Audit Trail Manager captures the electronic signatures and reasons, including the user, date, and details of the changes. It also records additional information, such as comments, according to the MultiQuant audit map.



Tip! A session file contains the Results Table, a copy of the quantitation method, a copy of the Audit Map at time of creation, as well as the entire audit trail for the entire session.

When the MultiQuant software creates or modifies a .qsession or .qmethod file, the event is captured in the Project Audit Trail on the History tab in the Analyst software. The following events are captured:

- Quantitation method file has been created.
- Quantitation method file has been modified.
- Quantitation Results Table has been created.
- Quantitation Results Table has been modified.

If the E-signature or Reason Prompt is selected for creating or modifying the Quantitation method file, then the Audit Trail dialog generated by the Analyst software appears in the MultiQuant software.

Table B-1 MultiQuant Audit Trails

Audit trail	Examples of events recorded
Quantitation (one per Results Table)	Changes to: <ul style="list-style-type: none"> • Creation and modification of session files. • Sample information. • Peak integration parameters.

About Audit Maps

The MultiQuant software maintains all change history to the processing settings information associated with the quantitation results. The software audits all events according to the active project audit map, and it captures all electronic signatures and link, to respective records.

Setting up Audit Maps

Before you begin to work with projects that require auditing, set up audit maps appropriate to your standard operating procedures. Several audit maps are available when the MultiQuant software is installed, but you may want to modify one or more of them for your own use.

Each audit map has its own pool of predefined reasons that must be created. Unlike in the Analyst software, in the MultiQuant software, all the audit maps are stored in one .qmap file. The .qmap files are stored in the <drive>:\Analyst Data\Projects\<project name>\Project Information folder.



Tip! If you want to audit the printing or exporting of session events, or if you are exporting calibration data, then you must enable the Session file saved event in the Audit Map. We recommend that you also add a predefined reason that is specific to those events.

Creating or Changing an Audit Map

The MultiQuant software installs several audit maps. View them to decide whether modifying one or more of them would be easier than creating a completely new one.

Caution: If you and another user are modifying the same audit map at the same time, only the changes made by the person who saved the file last are used.

The active audit map for the project determines which events are recorded in the in the audit trail for any Results Tables that are created.



Note: After you save a Results Table, the active audit map is saved with the Results Table and the audit map cannot be modified.

1. Click **Audit Trail > Audit Map Manager**.

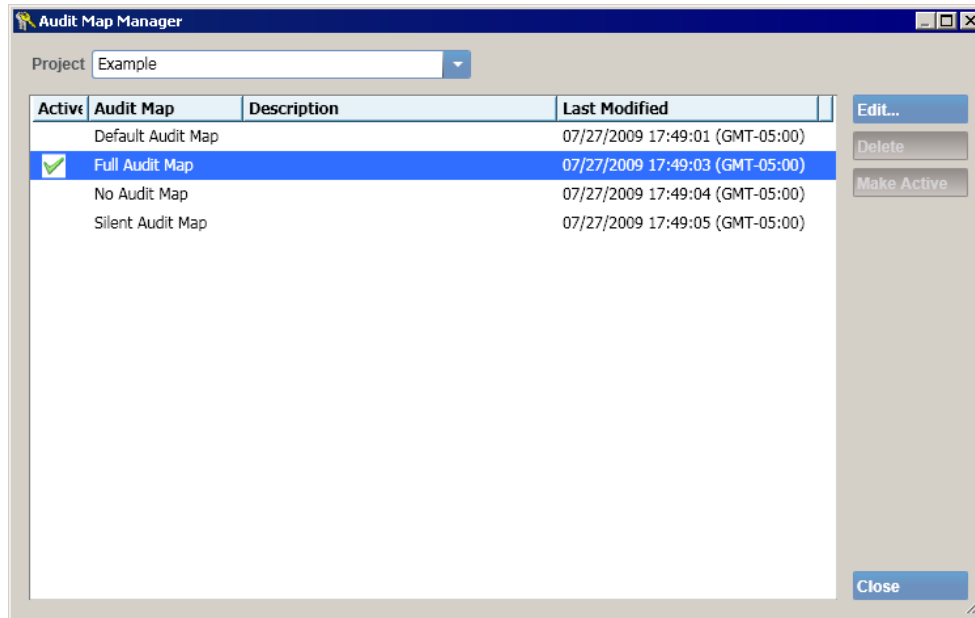


Figure B-1 Audit Map Manager

2. In the **Project** list, click the project for which you want to create or modify the audit map.
3. Select an audit map and then click **Edit**.

The Audit Map Manager dialog appears with the active audit map displayed.

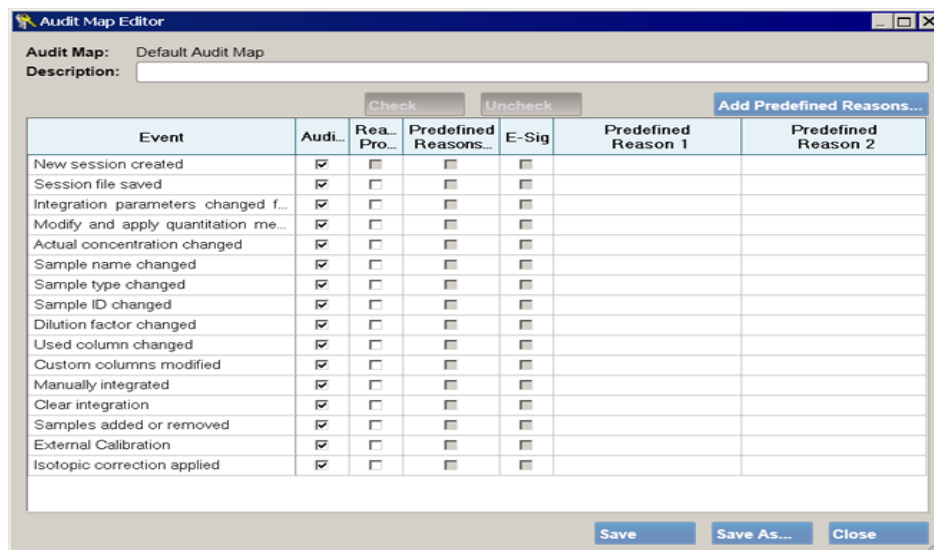


Figure B-2 Audit Map Editor

4. If required, in the **Description** field, type a description of the audit map.

5. In the Audit Map table, configure each event as follows:

- If you want the event to be audited, select the check box in the **Audited** column.



Tip! To fill consecutive cells in a column with the check box value, press Ctrl or Shift, click the cells, and then click the **Check** button.

- If you want the operators to type a custom reason or choose a predefined reason, then select the check box in the **Reason Prompt** column.
- If you want the operators to only select a predefined reason for the change when the event occurs, select the check boxes in the **Reason Prompt** and the **Predefined Reasons Only** columns. In the **Predefined Reason _** columns, select up to ten reasons.



Tip! To add a predefined reason, click **Add Predefined Reasons**.

- If you want to require electronic signatures for the event, select the check box in the **E-Sig** column.

6. Do one of the following:

- To create an audit map, click **Save As**, type a name for the audit map and then click **Close**.
- To edit the audit map, click **Save**.

7. Click **Make Active**.

When you apply an audit map, it becomes the active audit map. The audit configuration in the active audit map determines which events are recorded in the audit trails from this point on.



Note: Creating or modifying audit maps are audited in the Analyst software project audit trail.

Audit Configurations

The audit configuration used for a Results Table is embedded in the Results Table file when the Results Table is created. This configuration cannot be changed. The timestamp displayed next to the audit map name indicates when the audit map used to embed the configuration was last saved.



Note: If you want to move your data then you must move the whole project, maintaining the file structure. If you do not maintain the file and folder structure you may not be able to view your Results Table or chromatograms.

Viewing Audit Configurations Embedded in the Results Table

1. Open a Results Table.
2. Click **Audit Trail > View Session Audit Map**.

Viewing, Searching, and Printing Audit Trails

You can view the audit trail records for each session file. You can also filter the audited events in the MultiQuant software audit trail based on a set of specified criteria or you can perform a keyword search, which highlights every occurrence of the text.

The MultiQuant software also provides you with the ability to export the audit trail records to a read-only file format.

Viewing the Audit Trail Results in the Audit Trail Viewer

1. Open a Results Table.
2. Click **Audit Trail > View Session Audit Map**.
3. To change projects, click the **Projects** list and then select another project.
4. To view other sessions, click the **Sessions** list and then select another session. You can also select to view all the sessions in the project at the same time.

Performing a Keyword Search

1. Open a Results Table.
2. Click **Audit Trail > Audit Trail Viewer**.
3. In the **Find** field, type the word that you want to find in Audit Trail results and then click **Go**.

If matches are found, the Find field turns green, the number of matches is shown, and the words are highlighted in yellow. If matches are not found, the Find field turns pink.
4. Use the **Next** and **Prev** buttons to move between the matches.

Filtering Audited Events

1. Open a Results Table.
2. Click **Audit Trail > Audit Trail Viewer**.
3. Click **Filter**.

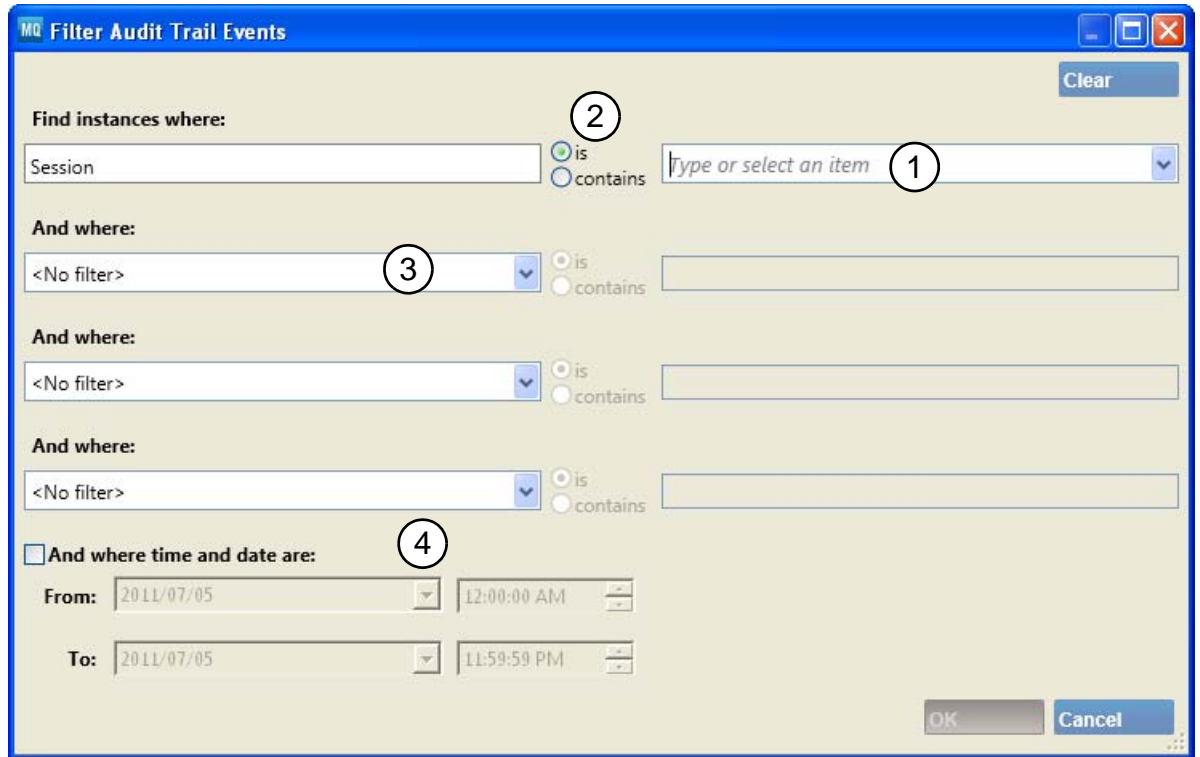


Figure B-3 Filter Audit Trail Events dialog

Item	Description
1	Name of the session file. You can filter one session file or all the session files for the active project.
2	The <i>is</i> and <i>contains</i> options filter on exact or partial matches respectively.
3	Description: Type the partial or full Event Type. Sample Name: Type the partial or full sample name. Full User Name: Type the partial or full name of the user. E-Signature: Select Yes or No. Reason: Type the partial or full reason.
4	Date: You can filter on events that occurred during a specific date and time.

- In the Filter Audit Trail Events dialog, use the lists to select filter criteria.



Note: You cannot edit the Session field.

- To reset all the search parameters to No filter, click **Clear**.
- Click **OK** to filter the events.



Tip! To remove the filter, in the Audit Trail Viewer, click **Remove Filter**.

Printing the Audit Trail Viewer

- Click **Print** and then select a printer.
You can print a secure PDF using pdfFactory.



Note: Only the saved events portion of the Audit Trail Viewer is printed.

Exporting the Audit Trail Viewer

- Click **Export** and then type a file name.
The file is exported as a tab-delimited text file.



Note: Only the saved events portion of the Audit Trail Viewer is exported.

About the Audit Trail Viewer

The Audit Trail Viewer displays the whole history of a particular sample in the session file. Session files are saved in the <drive>:\Analyst Data\Projects\<project name>\Results folder.

The Audit Trail Viewer hierarchy is as follows. For reference, see [Figure B-4 Audit Trail Viewer dialog on page 92](#).

- Audit trail hierarchy:
 - Save event (2): When a session file is saved, a save event is created, which captures any changes since the previous save event as well as every value in the Results Table.
 - Change event (4): The action performed to modify the Results Table.
 - Change description (5): Details of the change event.
- Session file (6): Use this field to select a session file or all session files.
- Find (1): A keyword search without filtering. Highlights every occurrence of the text.
- Filter (7): Displays only the events that match the selected criteria.
- Dark blue highlight (3): Selected save event.
- Previous version (8): Displays the previous version of the selected session file.

Audit Trail Results

Project: Example Session: SQT1

Find: [] [Next] [Prev]

View updated on: 09/18/2009 10:56:55 (GMT-05:00)

Date	Description	Session	Reason	Full User Name	E-Signature
09/18/2009 10:56:35	The session file 'C:\Analyst Data\Projects\Example\Results\SQT1.qsession' has been locked.	SQT1		Scott, Judith	No
09/18/2009 10:56:18	The session file 'C:\Analyst Data\Projects\Example\Results\SQT1.qsession' has been saved.	SQT1		Scott, Judith	No

Change Event Details

Date	Description
09/18/2009 10:56:35	New session created
09/18/2009 10:56:36	A new session has been created with the integration algorithm 'SignalFinder'.

Results Table Comparison

SQT1: Results Table of the selected Save Event [09/18/2009 10:56:35]

Index	Sample Name	Sample ID	Sample Type	IS	Component Nam	IS Name	Component Group Name	Actual Concentratio
1	STD 1		Standard	<input checked="" type="checkbox"/>	minoxidol	rescinnamine		2.00 4.1
2	STD 1		Standard	<input type="checkbox"/>	tolbutamide	rescinnamine		2.00 2.8
3	STD 1		Standard	<input type="checkbox"/>	reserpine	rescinnamine		2.00 4.2
4	STD 1		Standard	<input checked="" type="checkbox"/>	rescinnamine	N/A		1.00 5.9

SQT1: Previous version of the Results Table of the selected Save Event [09/18/2009 10:56:18]

Index	Sample Name	Sample ID	Sample Type	IS	Component Nam	IS Name	Component Group Name	Actual Concentratio
1	STD 1		Standard	<input checked="" type="checkbox"/>	minoxidol	rescinnamine		2.00 4.1
2	STD 1		Standard	<input type="checkbox"/>	tolbutamide	rescinnamine		2.00 2.8
3	STD 1		Standard	<input type="checkbox"/>	reserpine	rescinnamine		2.00 4.2
4	STD 1		Standard	<input checked="" type="checkbox"/>	rescinnamine	N/A		1.00 5.9

Peak Cal. Curve

STD 1 - minoxidol (Standard) 210.2 / 164.2 - Mix_batch...
 Area: 4.104e4, Height: 5.929e3, RT: 1.17 min

RT: 1.03
 RTW: 30.0
 URT: No
 RLP: Yes
 MPH: 0.00
 S/N: 2.0
 Cfd: 50.0

STD 1 - minoxidol (Standard) 210.2 / 164.2 - Mix_batch...
 Area: 4.104e4, Height: 5.929e3, RT: 1.17 min

RT: 1.03
 RTW: 30.0
 URT: No
 RLP: Yes
 MPH: 0.00
 S/N: 2.0
 Cfd: 50.0

Figure B-4 Audit Trail Viewer dialog

This section contains instructions for using the additional features the Analyst[®] software provides for securing your data.

Topics in this section:

- [Data File Changes \(Explore Processing\) on page 93](#)
- [Data File Checksum on page 96](#)

Data File Changes (Explore Processing)

The Explore Processing History is a file containing a record of changes to the processing parameters used with a data file. These records must be created manually to keep track of the changes made. Only the current changes are saved. After you create an Explore Processing History file, you cannot modify or delete it within the Analyst software.

After you have saved the history of the changes to a data file, use this history to view the data file at any point during the changes. You cannot modify the history or save a previous version of the data file from the history.

Explore Processing History files record the following processing parameters:

- Smooth/Previous Point Weight.
- Smooth/Current Point Weight.
- Smooth/Next Point Weight.
- Gaussian Smooth/Filter Width.
- Gaussian Smooth/Distance.
- Centroid Options/Merge Distance.
- Centroid Options/Minimum Width.
- Centroid Options/Use Peak Maximum for X Value.
- Baseline Subtract/Windows Width.
- Threshold.
- Noise Filter/Minimum Peak Width.
- Base Peak Chromatogram/Mass Tolerance.
- Add.
- Subtract.

Creating Explore Processing History Files

An Explore Processing History file (.eph) cannot be modified or deleted within the Analyst software.

- In **Explore** mode, in a data file pane, right-click and then click **Save Explore History**. Explore Processing History files are stored in the Processing Methods subfolder of the project folder.



Tip! To keep track of your Explore Processing History files, save the history file with a name similar to that of the data file.

Viewing an Explore Processing History file

1. Click **File > Open**.
The Open dialog appears.
2. In the **Files of type** list, click **Explore History Files** (.eph).
3. In the **Files** field, click the file and then click **OK**.
The .wiff file appears with the Explore Processing History file in a pane below it.
4. To show the .wiff file using the processing parameters on the History tab, under the History column, click **Review**.
5. To print the **Explore Processing History** window, on the **History** tab, right-click, click **Print**, and then click either **Current Page** or **All Pages**.
6. To display the current data processing history of a data file in the active pane, in **Explore** mode, click **Explore > Show > Show History**. The history that appears is not automatically saved and cannot be used to review processing.

Adding an Instrument Maintenance Log entry

When the instrument receives service such as system maintenance, cleaning, and reference checks, record the maintenance information in the Instrument Audit Trail using the Instrument Maintenance Log.

1. Click **View > Audit Trail Manager**.
The Audit Trail Manager window appears.
2. In the left pane, expand the **Audit Trail Data** folder.
3. In the **Audit Trail Data** section, click **Instrument**.
4. In the right pane, click the **Maintenance Log** tab.
5. Type the maintenance information in the appropriate fields.
6. To save the log entry, click **Submit**.

Viewing an Instrument Maintenance Log entry

1. Click **View > Audit Trail Manager**.
The Audit Trail Manager window appears.

2. In the left pane, expand the **Audit Trail Data** folder.
3. In the **Audit Trail Data** section, click **Instrument**. If the audit trail does not appear, in the right pane, click the **History** tab.

The audit trail appears.

4. For the record for the Instrument Maintenance Log entry you want to view, in the **History** column, click **Review**.

The Audit Trail History dialog appears showing the details of the log entry.



Tip! To find all log entries in the Instrument Audit Trail, click Search. In the Audit Trail Search dialog, use the options to display all records where Change Description contains Instrument Maintenance.

Configuring Email Notification

You can configure the Analyst software to send an email message if there are three log on errors within one day. This email notification is available only if the workstation is in Integrated Mode or Mixed Mode. For information about security modes, see [Analyst Software and Windows Security: Working Together on page 9](#)

The recipient of the email must have access to a valid account on an SMTP-compliant mail server, and the computer with the Analyst software must have access to an SMTP server.

1. Click **View > Audit Trail Manager**.

The Audit Trail Manager window appears.

2. In the left pane of the Audit Trail Manager window, right-click, click **Options**, and then click **E-Mail Notification Settings**.

The Audit Trail Options dialog appears displaying the Security Mail Settings tab.

3. Select the **Send e-mail message(s) after 3 logon failures within 24hr.** check box.
4. In the **SMTP Server** field, type the name of the SMTP server.



Note: The SMTP account sends mail to the email server. Use your email application to determine the SMTP server.

5. In the **Port Number** field, type the port number.
The Default button inserts the default port number, 25.
6. In the **To** field, type the email address to which you want the message sent; for example: username@domain.com.
7. In the **From** field, type the name you want to appear in the **From** field of the message. For example, type the name of the computer so that you will know which computer had the log on failures. The value in the **From** field cannot include spaces.
8. In the **Subject** field, type the subject of the message.
9. In the **Message** field, type the body of the message.
10. To check the configuration, click **Send Test Mail**.
11. To save the configuration, click **OK**.



Tip! To disable the electronic mail notification, clear the **Send email message(s) after 3 logon failures within 24hr.** check box.

Data File Checksum

If you have enabled the Data File Checksum feature, whenever you create a .wiff file (data file), the Analyst software generates a checksum value using an algorithm based on the MD5 public encryption algorithm and saves the value into the file. When you verify the checksum, the Analyst software calculates the checksum and compares the calculated checksum to the checksum stored in the file.

The checksum comparison can have three outcomes:

- If the values match, the checksum is valid.
- If the values do not match, the checksum is invalid. An invalid checksum indicates that either the file has been modified outside of the Analyst software or the file was saved when checksum calculation was enabled and the checksum is different from the original checksum.
- If the file has no stored checksum value, the checksum is not found. A file has no stored checksum value because either the file is from a previous version of the Analyst software or the file was saved when the Data File Checksum feature was disabled.

Verifying Data File Checksum

Whenever you open a data file, you can verify the checksum. This section provides steps for verifying a checksum and for enabling and disabling the Data File Checksum feature.

The checksum calculation can take over a minute for a one-gigabyte data file. During acquisition, you cannot verify the checksum of the file that is being created.

1. Click **File > Open Data File**.
The Select Sample dialog appears.
2. In the **Data Files** field, select a .wiff file (data file).
3. Click **Verify Checksum**.

The ExplorDir message box appears displaying the result of the checksum comparison.

- If the values do not match, the checksum is invalid. An invalid checksum indicates that either the file has been modified outside of the Analyst software or the file was saved when checksum calculation was enabled and the checksum is different from the original checksum.
- If the file has no stored checksum value, the checksum is not found. A file has no stored checksum value because either the file is from a previous version of the Analyst software or the file was saved when the Data File Checksum feature was disabled.

Enabling or Disabling the Data File Checksum Feature

The Analyst software indicates if the Data File Checksum feature is enabled by a check mark next to the command in the shortcut menu of the Audit Trail Manager.

1. Click **View > Audit Trail Manager**.
2. In the left pane of the Audit Trail Manager window, right-click, click **Options**, and then click **Data File Checksum**.

If you are enabling the Data File Checksum feature, a check mark appears next to the command. If you are disabling the Data File Checksum feature, the check mark disappears.



This section explains how to migrate data from the Macintosh MassChrom software to the Analyst[®] software. If you are using data files developed with the MassChrom software in the Analyst software system, you must convert these files to the Analyst file format (.wiff). The conversion must be done on a Macintosh computer.

Previous versions of the Analyst software and MassChrom software included Macintosh translator utilities. For a list of items on the installation disk, see [Table D-1](#).

Table D-1 Installation Disk Contents

Name	Description
InstFileGenerator	Instrument file conversion program.
ExptFile Converter	Experiment file conversion program.
Examples	Example Mac files used in the file converters.
Read Me First	Release Notes.

MassChrom Data Files Translation

Macintosh formatted API data files can be translated to single or multiple Analyst software format files (.wiff). Single or multiple Macintosh formatted data files can be selected before performing any file translation. Translated files do not have a checksum because they were collected by earlier versions of the Analyst software that did not have the Checksum feature.

The software requires a Power Macintosh or a G3 with a minimum of 32 MB of RAM, 230 MB of internal hard disk storage, and a CD drive.

The API File Converters are fully compatible with Systems 8.0, 8.1, and 8.5.x (including HFS+).

Translating API Files to .wiff Files

The program window shows the translation process, and a progress bar shows the progress of the conversion. After the conversion is complete, you can transfer the files to a workstation and read them using the Analyst software.

1. Run the **File Translator** program.
2. Click the **Translate** menu.
A list showing the different file translation options appears.
3. To convert multiple Macintosh files to Analyst software files, from the list choose **API to Multiple WIFF**.
Multiple Macintosh files translate to the same number of .wiff files. The .wiff file names are the same as the Macintosh file names with .wiff appended to the end.
4. To convert multiple Macintosh files to a single .wiff file, from the list choose **API to Single WIFF**.
5. Click **Select Destination Folder** to choose a location for the .wiff files.
6. Use the **File** dialog to browse to the destination folder.

7. Click **Select Files for Translation** to select files.
8. Use the directory dialog to browse to the appropriate folder that contains the files to be translated.
9. Click **Translate**.

If you selected the single .wiff file option, you are prompted for a destination folder and .wiff file name.

Generating Instrument Files

The Instrument File Generator (InstFileGenerator) combines the necessary parts of Macintosh state and calibration files to generate an Analyst software instrument file (.ins file).

1. Run the Instrument File Generator program.
The Instrument File Generator window appears.
2. Choose an instrument type or model from the **Instrument Model** menu.
3. To open a state or calibration file, click the corresponding **Load file** button.
A dialog appears prompting you for a file name.
4. Type the file name.
5. To begin generating the INS files for the chosen instrument model, click **Generate**.

The log window records all actions taken by the user from the start of the program. Any errors found are also recorded in this window. To print the contents of the window, click the Print command on the File menu.

Converting Experiment Files

The Experiment File Converter (ExptFileConverter) combines the necessary parts of a Macintosh state file and a Macintosh experiment file to generate a data acquisition method file (.dam).

1. Run the Experiment File Converter program.
The Experiment File Converter window appears.
2. Choose an instrument type or model from the **Instrument Model** menu.
3. Click either **Load State File** or **Load Expt File** to open a state or experiment file, as required.

A dialog appears prompting you for a file name.

4. Type the file name.
5. Click **Convert** to begin generating the DAM files for the chosen instrument model.

The log window records all actions taken by the user from the start of the program. Any errors found are also recorded in this window.

6. To print the contents of the window, select **File > Print**.

Symbols

.aasf files 38
.ata files 38
.atd files 38
.cam files 38
.cset files 38
.dab files 38
.dam files 38
.dat files 38
.dll files 38
.eph files 38
.hwpf files 38
.ins files 38, 100
.mdb files 38
.pdf files 38
.psf files 38
.qmap 38
.qmf 38
.qmf files 38
.qsession 38
.rdb files 38
.rpt files 38
.rtf files 38
.sdb files 38
.tun files 38
.txt files 39
.wiff files
 data file formats 65
 overview 39
 translating from API files 99
 verify checksum of a data file 96
.xls files 39

A

access modes
 overview 18
 screen lock and auto logout 20
 selecting 19
 See also security modes
access. *See* permissions
accounts
 acquisition 18
 client 18
 SAA 18

acquisition accounts
 overview 18
 selecting 19
 selecting for network acquisition 67
 user principal name format 19, 67
Active Directory
 mixed environment 12
 native environment 12
 security and 22
adding
 entry to Instrument Maintenance log 94
 existing projects 50
 existing root directories 49
 projects to a workgroup 53
 projects to more than one workgroup 53
 projects to Project Root Pool 49
 roles using the Administrator Console 47
 users to a workgroup 52
 users to the User Pool 48
 workstations to workgroups 54
 See also creating
Administrator Console
 Analyst software requirements 41
 audit trails 56, 83
 benefits 41
 client, overview 42
 Console administrators 43
 deleting roles 57
 illustration 45
 logging on to the Analyst software 55
 overview 41
 Remote Viewer tab 39
 security database 42
 server, overview 42
 shared drives 49
 synchronizing 57
 task workflow 43
 workgroups, setting up 43
 See also people, roles
Administrator Console client
 changing the attributes 57
 connecting to the server 46
 deleting workstations 59
 installing 42
 overview 42

- synchronizing 57
 - Administrator Console server
 - changing location of 57
 - firewalls 42
 - installing 42
 - overview 42
 - synchronizing 57
 - administrator role
 - Administrator Console 51
 - Console Administrators 43
 - overview 22
 - workgroups and 51
 - alerts
 - configuring 95
 - overview 13
 - Analyst software
 - 21 CFR Part 11 11
 - Application Event log 10
 - audit maps created in previous software versions 78
 - audit trails, overview 10
 - configuring security 17
 - converting MassChrom software to 99
 - deleting workstation 59
 - installing 17
 - permissions 21
 - roles, overview 22
 - unlocking 21
 - verifying installation of 17
 - Windows security and 9
 - API files 99
 - archived audit trails
 - overview 79
 - viewing 70, 77
 - attributes
 - Administrator Console client 57
 - workgroups, changing 59
 - audit maps
 - applying 75
 - creating 72, 86
 - default 71
 - full 71
 - installed audit maps 70, 86
 - location in the Audit Trail Manager 71
 - MultiQuant software 86
 - MultiQuant software, creating or modifying 86
 - MultiQuant software, setting up 86
 - overview 70
 - quant only 71
 - saving 74
 - silent audit map 71
 - audit records
 - searching 77
 - viewing 76
 - Audit Trail Manager, MultiQuant software 85
 - Audit Trail Viewer, MultiQuant software 91
 - audit trails
 - Administrator Console 56, 83
 - archived 70, 77
 - archives 79
 - illustration 71
 - instrument 69, 79
 - location in the Audit Trail Manager 71
 - MultiQuant software 10
 - MultiQuant software, viewing, searching, printing 89
 - overview 10, 69
 - project 69, 81
 - quantitation 70, 86
 - Results Tables 76, 88
 - searching 77
 - viewing 75
 - audit trails, archived 76
 - auditing
 - FAT file system 12
 - MultiQuant software 85
 - system audits 12
 - auto logout
 - disabling 21
 - enabling 20
 - overview 18
 - Results Tables 21
 - setting up 20
-
- ## **B**
- backup process
 - cache folder 65
 - network acquisition 64
-
- ## **C**
- cache folder
 - data backup process 65
 - deleting contents 66
 - synchronizing 66
 - CFR compliance 11
 - changing
 - attributes of the Administrator Console client 57
-

- default workgroup 55
- role properties 58
- roles 35
- Set File Permissions 45
- workgroup descriptions 59
- client account
 - described 18
 - network acquisition 64
- client. *See* Administrator Console client
- Code of Federal Regulations. *See* CFR compliance
- compliance. *See* security
- compound files
 - overview 65
 - selecting format for 67
- configuring
 - network acquisition 66
 - project security 37
 - remote queues 39
 - security 17
- connecting, Administrator Console client to the server 45
- Console administrators
 - overview 43
 - workgroup 45
- converting
 - experiment files 100
 - instrument files 100
- creating
 - audit maps 72, 86
 - projects 48
 - roles 35
 - roles using the Administrator Console 47
 - root directories for network acquisition 66
 - See also* adding

D

- data backup
 - cache folder 65
 - overview 64
 - process 65
- Data File Checksum
 - disabling 97
 - enabling 97
 - overview 96
 - verifying 96
- Default Audit Map 71
- default projects, selecting 49
- default workgroups, changing 55

- deleting
 - cache folder contents 66
 - deletion confirmation dialog, suppressing 57
 - project roots 58
 - projects from workgroups 60
 - roles from the Administrator Console 57
 - user-defined roles 36
 - users from the User Pool 58
 - users from workgroups 60
 - workgroups from the Workgroup tree 59
 - workstations from the Workstation Pool 59
 - workstations from workgroups 61
 - workstations using the Analyst software 59
 - See also* removing
- deletion confirmation dialog, suppressing 57
- disabling Data File Checksum 97

E

- editing. *See* changing
- enabling Data File Checksum 97
- End User role 23
- event logs 10
- Event Viewer 13
- Explore Processing History
 - overview 93
 - viewing 94
- exporting
 - Audit Trail Viewer 91

F

- FAT, file systems 12
- FDA compliance 9
- file formats
 - changing 67
 - overview 64
- files
 - configuring security 37
 - converting experiment files 100
 - converting instrument files 100
 - Data File Checksum 96
 - Explore Processing History 93
 - FAT 12
 - file translations 99
 - flat file option 64
 - MultiQuant file types 38
 - NTFS 12
 - permissions 13
 - permissions for network acquisition 64

- Set File Permissions 45
 - types of 37
- filtering, audited events in the MultiQuant software 89
- flat files
 - configuring network acquisition 66
 - high-throughput analysis, use in 64
 - options 65
 - overview 65
- folders
 - configuring security 37
 - permissions 13
- Food and Drug Administration. *See* FDA compliance
- Full Audit Map, described 71

G

- generating instrument files 100
- GLP compliance 9
- Good Laboratory Practices. *See* GLP

I

- installing
 - Administrator Console client 42
 - Administrator Console server 42
- Instrument Audit Trail
 - applying audit maps 75
 - audit map and audit trail location 69
 - logged events 79
 - viewing archived records 70, 77
 - viewing audit records 76
- Integrated mode
 - changing the default workgroup 55

L

- local users and the Administrator Console 51
- locking screen. *See* screen lock
- logging out. *See* auto logout

M

- mapping root directories 66
- MassChrom software
 - generating instrument files from 100
 - overview 99
 - translating API files to .wiff files 99
- mixed environment, Active Directory support 12
- Mixed mode
 - default workgroups 56

- monitoring, remote queues 39
- MultiQuant software
 - audit maps 86
 - audit maps, creating or modifying 86
 - audit maps, setting up 86
 - Audit Trail Manager 85
 - audit trails 10
 - audit trails, viewing, searching, printing 89
 - auditing 85
 - exporting, Audit Trail Viewer 91
 - file types 38
 - screen lock 20
 - software access 32

N

- native environment, Active Directory support 12
- network acquisition
 - acquisition accounts 64
 - benefits 63
 - configuring 66
 - data backup process 65
 - data file formats 65
 - deleting contents of the cache folder 66
 - network administrators 66
 - overview 63
 - potential data loss 63
 - project security 64
 - SAA and 64
 - use in regulated environments 63
- network projects. *See* projects
- New Technology File System. *See* NTFS
- NTFS, file systems 9, 12

O

- Operator role 23

P

- people
 - changing roles 35
 - overview 22
 - removing from the Analyst software 35
 - See also* users, Administrator Console
- permissions
 - files 13
 - folders 13
 - MultiQuant software 32
 - project folder 11
 - projects 61

Set File Permissions 45

printing

- audit trails 77
- MultiQuant audit trails 89
- security configurations 40

Project Audit Trail

- applying audit maps 75
- location of audit maps and audit trails 69
- logged events 81
- viewing archived records 70, 77

project folder permissions 13

Project Root Pool, adding projects 48

project root, refreshing 58

projects

- adding existing projects 50
- adding to more than one workgroup 53
- adding to the Project Root Pool 48
- audit maps 70
- audit maps created in previous software versions 78
- creating 48
- deleting from project root 58
- deleting from workgroups 60
- network project security 64
- network-based projects 63
- refreshing the project root 50
- reviewing project permissions 61
- security 37
- Set File Permissions 45

properties. *see* attributes

Q

QA Reviewer role 23

Quant Only Audit Map 71

Quantitation Audit Trail

- location of audit maps and audit trails 70, 86
- logged events 82

queue, configuring remote queues 39

R

refreshing

- Administrator Console client and server 57
- file permissions 45
- project roots 50, 58

registering workstations 53

regulatory compliance. *See* security

remote sample queue monitoring 39

removing

- people from the Analyst software 35
- projects from workgroups 60
- roles 36
- users from workgroups 60
- workgroups from the Workgroup tree 59
- workstation using the Analyst software 59
- workstations from the Workstation Pool 59
- workstations from workgroups 61
- See also* deleting

renaming workgroups 60

Results Tables

- audit maps 70
- logged events 82
- previous versions of Analyst software and 78
- quantitation audit trails 82
- screen lock and auto logout 21
- viewing audit trails 76, 88

roles

- Administrator 22
- Analyst 22
- changing 35
- changing properties 58
- copied roles and access rights 47
- creating using the Administrator Console 47
- deleting from the Administrator Console 57
- End User 23
- Operator 23
- QA Reviewer 23
- Supervisor 23

root directories

- adding existing root directories 49
- creating for network acquisition 66
- network acquisition 64
- selecting for network acquisition 66

S

SAA

- network acquisition and 64
- overview 18
- selecting 67

screen lock

- administrator role 51
- disabling 60
- enabling 60
- MultiQuant software 20
- overview 18
- setting up 20

- unlocking 21
- searching
 - audit records 77
 - MultiQuant software audit trails 89
- security
 - 21 CFR Part 11 11
 - Analyst software and Windows security 9
 - FAT file system 12
 - levels 15
 - network acquisition 64
 - overview 9
 - printing configurations for 40
 - project 37
 - reviewing project permissions 61
 - task 15
 - Windows 11
 - workgroup 55
 - workgroups 60
- security database, Administrator Console 42
- security modes
 - for workgroups 51
 - logging on to the Analyst software 55
 - overview 18
 - screen lock and auto logout 19, 20
 - workgroups, changing 60
- selecting
 - acquisition accounts for network acquisition 67
 - root directories 66
- server. *See* Administrator Console server
- Set File Permissions 45
- shared drives and network access 49
- silent audit map 71
- Single User mode 18
- software, configuring Analyst software security 17
- Special Acquisition Administrator Account.
See SAA
- subfolders
 - names of 38
 - saving audit maps 74
 - user access 37
- Supervisor role 23
- synchronizing
 - Administrator Console client and server 57
 - cache folder 66
 - project roots 50, 58
- synchronizing. *See* refreshing
- system audits. *See* audit trails

T

- translating API files to .wiff files 99
- 21 CFR Part 11 compliance 11

U

- UNC. *See* universal naming convention
- universal naming convention, root directories 66
- unlocking screen 21
- UPN format. *See* user principal name format
- user groups
 - adding to User Pool 48
 - adding to workgroups 52
- User Pool
 - adding users 48
 - deleting users 58
 - described 42
- user principal name format
 - acquisition accounts 19, 67
 - Active Directory support 12
- user-defined roles
 - creating 35
 - deleting 36
- users
 - adding to the User Pool 48
 - adding to workgroups 52
 - deleting from the User Pool 58
 - deleting from workgroups 60
 - overview 22
 - Set File Permissions 45
 - See also* people, Administrator Console

V

- viewing
 - archived records 70, 77
 - audit trails 75
 - audit trails, MultiQuant software 89
 - Explore Processing History files 94
 - Instrument Audit Trail records 76

W

- Windows
 - audit trails 10
 - event logs 10
 - file system 12
 - network acquisition 11
 - NTFS 9
 - security 11

- workgroups
 - adding projects to 53
 - adding users to 52
 - adding workstations to 54
 - changing description of 59
 - changing security modes 60
 - changing the default workgroup 55
 - creating 51
 - default 55
 - deleting from the Workgroup tree 59
 - deleting projects from 60
 - deleting users from 60
 - deleting workstations from 61
 - local users 51
 - Mixed mode 56
 - overview 44
 - permissions 51
 - renaming 60
 - security modes 51
 - security settings 51
 - Set File Permissions 45
 - setting a default workgroup 55
- workstations
 - adding to the remote queue 39
 - adding to workgroups 54
 - audit trails and 56
 - connecting the Administrator Console client to the server 46
 - deleting from workgroups 61
 - deleting using the Analyst software 59
 - registering 53
 - removing from the remote queue 40

