Analyst® 1.7 Software

Laboratory Director's Guide

RUO-IDV-05-0268-C

October 2017

AB Sciex Pte. Ltd.
Blk 33, #04-06
Marsiling Ind Estate Road 3
Woodlands Central Indus. Estate.
SINGAPORE 739256

Contents

Foreword

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 Analyst® software are installed automatically with the software and are available from the Start menu. A complete list of the available documentation can be found in the Help. To view the Help, press **F1**.

- To access the documentation on computers configured with the Windows 7 operating system, click **Start > All Programs > SCIEX > Analyst**.
- To access the documentation on computers configured with the Windows 10 operating system, click **Start > SCIEX Analyst > Analyst Documentation**.

Documentation for the mass spectrometer can be found on the *Customer Reference* DVD for the mass spectrometer.

Documentation for the ion source can be found on the *Customer Reference* DVD for the ion source.

For the latest versions of the documentation, visit the SCIEX website at sciex.com.

Contact Us

SCIEX Support

- sciex.com/contact-us
- sciex.com/request-support

Customer Training

- In North America: NA.CustomerTraining@sciex.com
- In Europe: Europe.CustomerTraining@sciex.com

- Outside the EU and North America, visit sciex.com/education for contact information.

Online Learning Center

- SCIEX**University**

CyberSecurity

For the latest guidance on cybersecurity for SCIEX products, visit sciex.com/Documents/brochures/win7-SecurityGuidance.pdf.

Technical Support

SCIEX and its representatives maintain a staff of fully-trained service and technical specialists located throughout the world. They can answer questions about the system or any technical issues that might arise. For more information, visit the website at sciex.com.

Security Configuration Overview 1

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, then refer to *Analyst Administrator Console on page 61*.

Topics in this section:

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 support 21 CFR Part 11 compliance for the use of electronic record keeping.
- Flexible and effective management of access to critical mass spectrometer 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.

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 using 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, refer to Windows Security Configuration on page 11.

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

- Single User mode
- Mixed mode
- Integrated mode (default setting)

For more information about security modes and security settings, refer to About Security Modes and Accounts on page 23.

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 mass spectrometer on a function-by-function basis. For more information, refer to Access to the Analyst® Software on page 29.

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, 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 mass spectrometer, device, and software interactions are recorded in detail here.

Windows maintains event logs that 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, refer to 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 compliance 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 configuration of Windows operating system.
- Proper procedures and training in your company.

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 of the subfolders to use the software to manage security. If the root directory is on a local computer, then the 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 as intended, users should be part of the Windows local user group. If certain users need to be able to stop the AnalystService, then this specific access can be set up without giving the user all of the local administrator privileges and thereby compromising local security.

If you plan to use network acquisition, then 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, refer to Access to the Analyst® Software on page 29.

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, specify user accounts in UPN (user principal name) format.

Mixed or Native Environment

The network includes the following:

- Windows 2008 R2 and 2012 servers.
- Windows 7, 32-bit and 64-bit clients.
- Windows 10, 64-bit clients.

If the Analyst® software starts in the mixed environment, then the log on window contains the user name, password, and domain fields.

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

The auditing feature of the Windows system can be enabled to detect security breaches or system intrusions. Auditing can be set to record different types of system-related events. For example, the auditing feature can be enabled to record any failed or successful login attempt to access the system in the event log. Logs can be viewed using the Event Viewer.

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, refer to 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 of 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, refer to the Microsoft Windows documentation.

For information about the Analyst® software files and folder permissions, refer to Analyst® Software Security Configuration on page 22.

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 issue occurs, then 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 the Control Panel, the Messenger must be started on the sending and receiving computers and the Alert service must be started on the sending computer. For more information about creating an alert object, refer to the Microsoft Windows documentation.

Electronic Licensing 2

Electronic licensing can be node-locked or server-based.

- To access the Activation ID of the node-locked or server-based license, click **Help > About Analyst** in the Analyst® software window. The activation ID might be needed for any future service or support call.

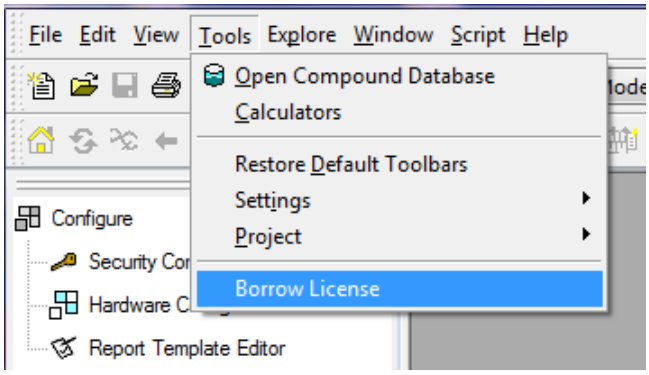
Note: Make sure to renew the license before it expires.

Borrow or Return Server-based Electronic License

A license is required to use the Analyst® software. Users who want to reserve a license to work offline, when using server-based licensing, can borrow a license for up to 7 days using the following procedure. During the borrowing period, the borrowed electronic license is guaranteed to the computer.

1. In the Analyst® software window, click **Tools > Borrow License**.

Figure 2-1 Borrow License

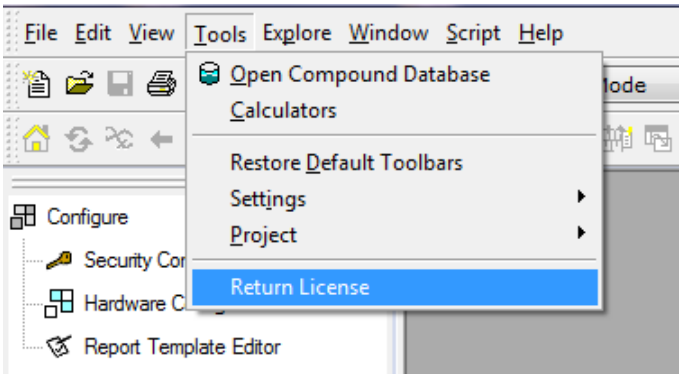


Note: This feature is not available for node-locked licenses.

After an electronic license is borrowed, the menu option changes to Return License, and the number of available licenses is reduced by one on the licensing server.

2. To return the borrowed electronic license, connect to the network, and then click **Tools > Return License** in the Analyst® software window.

Figure 2-2 Return License



Configure Analyst® Software Security 3

This section explains how to configure the software. If you are using the Administrator Console to centrally manage security, refer to Analyst Administrator Console on page 61.

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

Topic in this section:

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 functionalities.
- Access to specific projects.
- Access to instrument workstation status.

Table 3-1 contains the list of tasks for configuring security and Table 3-2 shows the options for setting the various security levels.

Table 3-1 Workflow Process for Configuring Security

Task	Procedure
Install the Analyst® software.	Refer to the Analyst® software installation guide.
Install MultiQuant™ software (if required.)	Refer to the MultiQuant™ software installation guide.
Configure Analyst® software security.	Refer to Analyst® Software Security Configuration on page 22.
Configure audit trails.	Refer to Auditing on page 93.

Table 3-1 Workflow Process for Configuring Security (continued)

Task	Procedure
Configure Windows File Security and NTFS.	Refer to Set Access to Projects and Project Files on page 47.
Maintain system maintenance log for instruments, security, data, and project maintenance.	Refer to Additional Security Customization on page 120.
Transfer or translate existing data.	Refer to Data System Conversion on page 125.

Table 3-2 Security Configuration Options

Option	CFR	Mid-Range	Non GLP
Windows Security			
Format drives to NTFS.	Yes	Yes	Optional
Configure users and groups.	Yes	Yes	Optional
Enable Windows auditing, and file and directory auditing.	Yes	Optional	Optional
Set file permissions.	Yes	Optional	Optional
Analyst® Software Installation			
Install Analyst® software.	Yes	Yes	Yes
Install MultiQuant™ software.	Yes	Yes	Yes
Select audit options.	Yes	Optional	No
Event Viewer (inspect install).	Yes	Yes	Yes
Analyst® Software Security			
Select security mode.	Integrated or Mixed	Any	Single user
Configure Analyst® software roles and people.	Yes	Yes	No
Create audit maps, configure instrument, project, and quantitation audit trails.	Yes	Optional	No
Configure email notification.	Yes	Optional	No
Activate Checksum.	Yes	Optional	No
Create audit maps in the MultiQuant™ software.	Yes	Optional	No
Common Tasks			

Table 3-2 Security Configuration Options (continued)

Option	CFR	Mid-Range	Non GLP
Add new projects and subprojects.	Yes	Yes	Yes
Configure project audit trail for new projects and subprojects.	Yes	Optional	No
Transfer existing data.	Yes	Yes	Yes
Create maintenance log for instrument security, data, project maintenance.	Yes	Yes	Yes

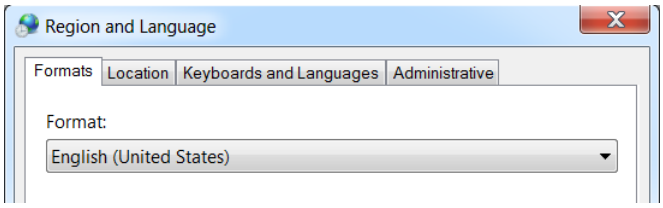
Analyst® Software Installation

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.

- Only the English version of the Windows 7 or 10 operating system is supported.

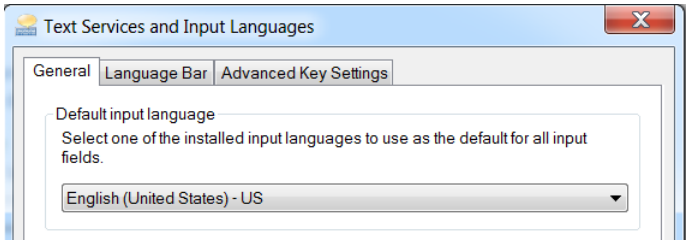
- The following settings must be completed in the Control Panel.
  - (**On Windows 7 operating system**) In the Region and Language dialog, on the Formats tab, set the **Format** field to **English (United States)**.

    Figure 3-1 Region and Language Dialog - Windows 7

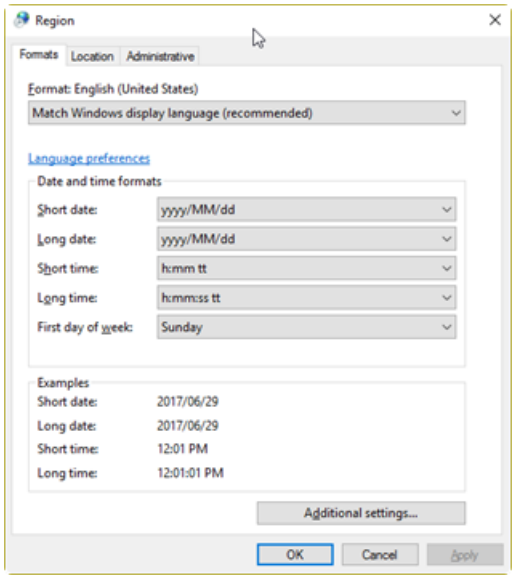
  - Click the Keyboards and Languages tab and then click **Change Keyboards**.
  - In the Text Services and Input Languages dialog, on the General tab, select **English (United States) - US** as the default input language.

    Figure 3-2 Text Services and Input Languages Dialog - Windows 7

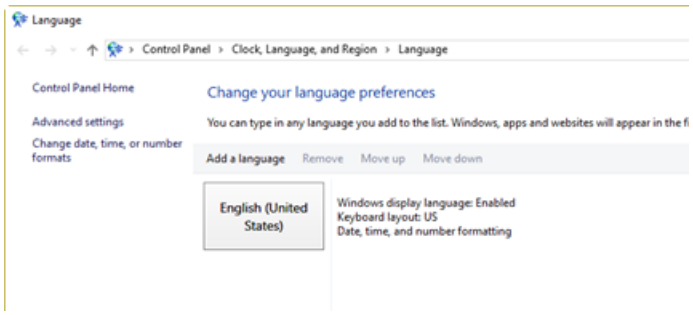
  - (**On Windows 10 operating system**) In the Control Panel, click **Clock, Language, and Region > Region** and then in Region dialog, select **English (United States)** in the **Format** field.

    Figure 3-3 Region Dialog - Windows 10



- Click **Apply**.
- Click **OK**.
- In the Control Panel, click **Clock, Language, and Region > Language** and then select **English (United States)** as the default input language.

Figure 3-4 Language Dialog - Windows 10



Setting the Format field and the default input language field to a different value might cause the software to show the file information or the audit trail information incorrectly.

Note: Microsoft Windows updates and Internet connectivity for the application computer should be disabled to prevent modification to the Windows components. If updates and Internet connectivity are not disabled, then the system must be validated after updates to Windows or the .NET framework. Make sure that adequate virus protection in place to prevent virus corruption of system functionality.

System Requirements

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

Preset Auditing Options

Depending on the software version, the preset auditing options might 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.

Verify Software Components

After the Analyst® software is installed, a Software Component Verification procedure checks that all of 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, refer to Data File Checksum on page 123.

1. Click **Start > 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.
5. In the Event Detail message, in the **Description** field, go to **Total files verified**. Errors should read zero.

Analyst® Software Security Configuration 4

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.

Topics in this section:

Steps to Configure the Analyst® Software

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

Table 4-1 contains the general tasks for configuring the Analyst® software.

Table 4-1 Tasks for Configuring the Analyst® Software

Task	Procedure
Configure the security mode.	Refer to Select the Security Mode on page 24.
Configure screen lock and auto log out (Mixed mode only).	Refer to Set up Screen Lock and Auto Log Out on page 27.

Table 4-1 Tasks for Configuring the Analyst® Software (continued)

Task	Procedure
Configure project security.	Refer to Set Access to Projects and Project Files on page 47.
Configure instrument workstations.	Refer to Add Access to a Workstation on page 55 or Remove a Workstation on page 59.

Location of Security Information

When the Analyst® software is running on a single workstation or in a network configuration (without the use of the Administrator Console), all security information is stored in the \Program Files\Analyst\Bin folder on the Windows 7 (32-bit) operating system or in the \Program Files (x86)\Analyst\Bin folder on the Windows 7 (64-bit) or Windows 10 (64-bit) operating system on that workstation, in a file called SecurityDB.odb.

When the software is running in a networked environment, the Windows security information is stored on the server and workstation. The security information is stored separately on each workstation in the Bin folder.

If you are using the Administrator Console, a copy of the mass spectrometer security database is saved in both a local folder and a network folder. The local copy is the working copy. The network copy is used to replace the local copy when there are changes to the database.

Note: Projects and other files can be stored on any workstation that is part of a network.

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 of the 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, refer to Workgroup Security Modes and Logging on to the Analyst® Software on page 79.

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 can 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, refer to Workgroup Security Modes and Logging on to the Analyst® Software on page 79.

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 can be different.

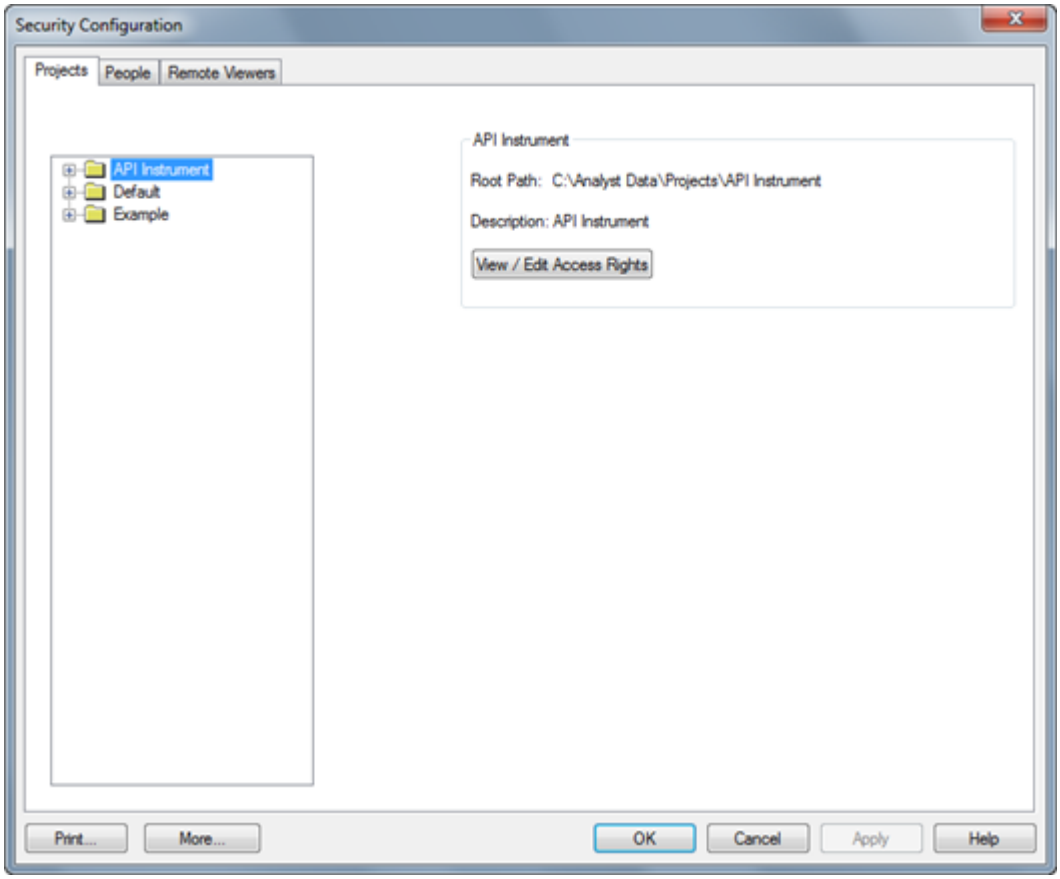
Special Acquisition Administrator Account: This feature is intended for use in a regulated environment. The operator must provide a user name, domain, and password for this account. After the network administrator sets up this account, it can be used to acquire data regardless of the identity of the current user of the Analyst® software. Although the current user might 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.

Select the Security Mode

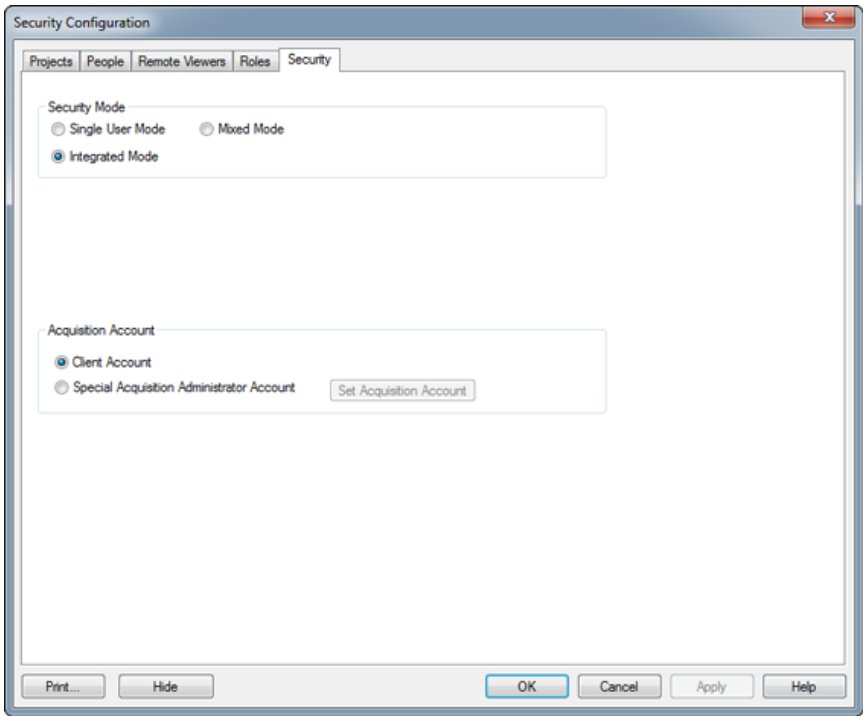
1. On the Navigation bar, under **Configure**, double-click **Security Configuration**.

Figure 4-1 Security Configuration Dialog: Projects Tab



2. Click **More** and then click the **Security** tab.

Figure 4-2 Security Configuration Dialog: Security Tab



3. In the **Security Mode** section, click a mode and then click **OK**.
4. Restart the Analyst® software.

Select 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**, then do the following:

   a. Click **Set Acquisition Account**.

   b. Type the **User name**, **Password**, and if necessary, **Domain**, and then click **OK**.

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

Set up Screen Lock and Auto Log Out

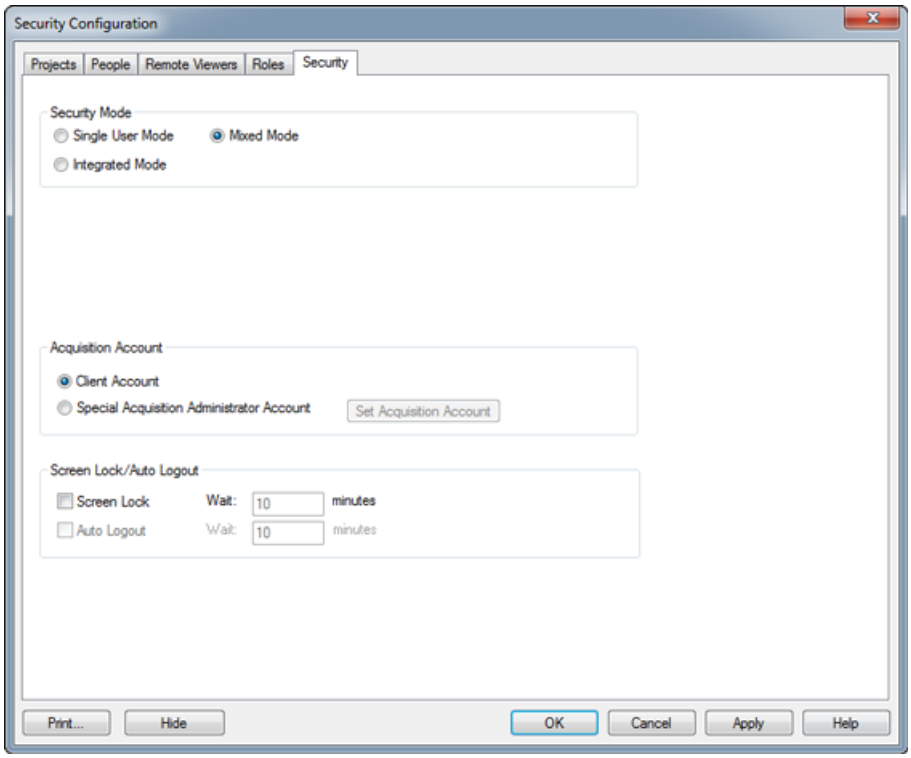
When the screen locks, the Unlock Analyst dialog opens indicating that the system has been locked, as well as the currently logged on user name and domain. If the auto logout option is also set, then the time remaining before the Analyst® software closes is also shown. Only the currently logged on user, 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**.
2. Click **More** and then click the **Security** tab.
3. Click **Mixed Mode**.

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

Figure 4-3 Security Configuration Dialog: 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, then after a defined period, the Analyst® software client closes. If acquisition is taking place, then it continues. However, if a Results Table, the Method Editor, or anything else is open and not saved, then any changes and unsaved data are lost.

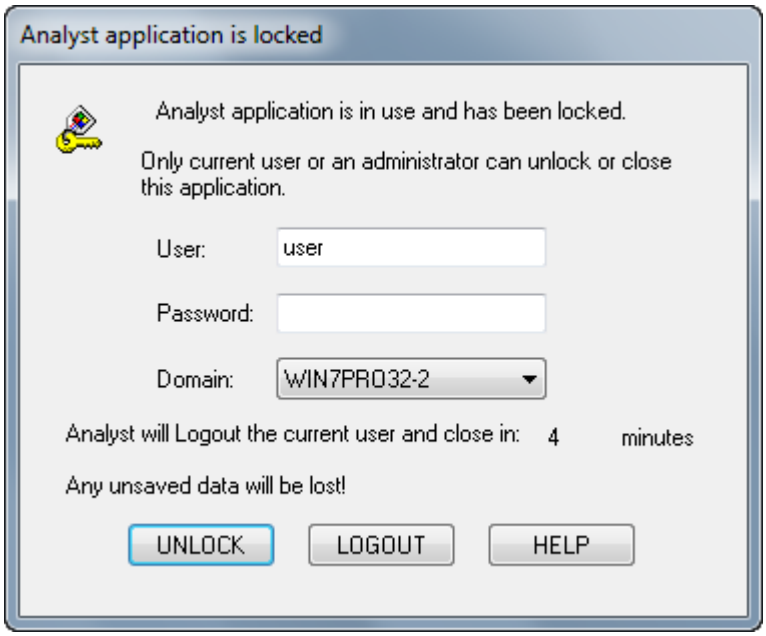
6. If required, select **Auto Logout** and, in the **Wait** field, type the number of minutes to elapse before the Analyst® software client closes.

   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.

Unlock or Log off from the Analyst® Software

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

Figure 4-4 Unlock Analyst Dialog



- Do one of the following:
  - To unlock the screen, type your user name, if necessary, and password, and then click **UNLOCK**.

- To log out, type your user name, if necessary, and password, and then click **LOGOUT**.

Access to the Analyst® Software

Before configuring security, do the following:

- Remove all of the 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 have non-administrative tasks and configure system permissions.
- Create suitable procedures and account policies for users in group policy.

Refer to the Microsoft 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 created, 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, refer to Analyst Administrator Console on page 61.

Table 4-2 Analyst® Software Roles

Role	Typical Tasks	Preset Access
Administrator	• Manages the system. • Configures security.	• All of the Analyst® software and MultiQuant™ software functionality
Analyst	• Oversees mass spectrometer operation. • Analyzes data for use by the end-user.	• Acquisition Method • Analyst Application • Audit Trail Manager • Compound Database • Explore • Hardware Configuration • Quantitation • Report Template Editor • Sample Queue • Tune • View Status • MultiQuant
Operator	Oversees daily use of the system, including maintenance, sample organization, data gathering, and processing.	• Acquisition Method • Analyst Application • Audit Trail Manager • Batch • Compound Database • Explore • ExpressView (legacy setting*) • Hardware Configuration • Report Template Editor • Sample Queue • Tune • View Status

Table 4-2 Analyst® Software Roles (continued)

Role	Typical Tasks	Preset Access
End User	• Provides samples. • Receives processed results. • Integrates results with input and output from other applications.	• Acquisition Method • Analyst Application • Audit Trail Manager • Compound Database • Explore • ExpressView (legacy setting*) • Report Template Editor • View Status
QA Reviewer	• Reviews data. • Reviews audit trails. • Reviews quantitation results.	• Analyst Application • Audit Trail Manager • Quantitation • Report Template Editor • View Status • MultiQuant
Supervisor	Unlocks software or logs out user.	• Unlock and Logout Application and MultiQuant™ software
*This feature is not supported in the Analyst® software.		

Analyst® Software Access

Figure 4-5 Security Configuration Dialog

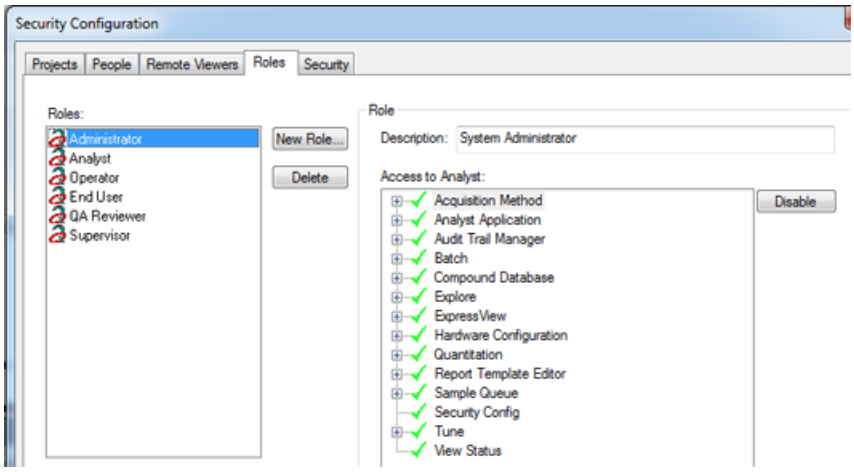


Table 4-3 Analyst® Software Access to Acquisition Methods

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 4-4 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.
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.

Table 4-4 Analyst® Software Access to Analyst Application (continued)

Preset Access	Description
Unlock/Logout Application	Allows the application to be automatically locked after the specified wait time of inactivity has elapsed. This functionality is only available in Mixed Mode and when the Screen Lock option is selected.
*This feature is not supported in the Analyst® software.	

Table 4-5 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 4-6 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 file formats).
Save batches	Allows users to save batches.
Use template batches	Allows users 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 users 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 is enabled.

Table 4-6 Analyst® Software Access to Batch (continued)

Preset Access	Description
Overwrite batches	Allows users to overwrite existing batches.
Overwrite template batches	Allows users to overwrite existing template batches.

Table 4-7 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.
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 4-8 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	Allows users to set up or select the library database location.
Setup library user options	Allows users to set up security information such as user name and password for the library.
Add library record	Allows users 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.
Delete MS spectrum	Allows user to delete a selected MS spectrum.
Delete UV spectrum	Allows users to delete a UV spectrum.
Delete structure	Allows users to delete a structure.
View library	Allows users to use 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. (Right-click a spectrum, or in **Explore** mode, click **Explore > Library Search.)**
Select processing algorithm to retrieve peak list	Legacy setting*
*This feature is not supported in the Analyst® software.	

Table 4-9 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.

Table 4-9 Analyst® Software Access to Hardware Configuration (continued)

Preset Access	Description
Edit	Allows users to edit a hardware profile.
Activate/Deactivate	Allows users to activate or deactivate a hardware profile.

Table 4-10 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 a 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)	Allows users to specify default number of smooths in the Quantitation Wizard.
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.
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.

Table 4-10 Analyst® Software Access to Quantitation (continued)

Preset Access	Description
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 show 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	Allows users to edit audit trail settings.
Disable, enable and clear audit trail	Legacy setting*
Change results table column visibility	Allows users to select the columns to include in a Results Table. (To access the Table Settings dialog, right-click in the Results Table and then click **Table Settings > Edit.)**

Table 4-10 Analyst® Software Access to Quantitation (continued)

Preset Access	Description
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, right-click in the Results Table, and then click **Table Settings > Edit.** Click **Columns** and then click **Edit**.)
Run temporary queries	Allows users to run queries.
Modify or save queries	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.) 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**.)
Run temporary sorts	Allows users to sort queries.
Modify or save sorts	Allows users to edit or save sorts.
Use metric plot settings dialog	Allows users to use the metric plot settings dialog.
Modify or create metric plot settings	Allows users to create new metric plots from the Results Table. (In the Results Table, right-click and then click **Metric Plot > New.)** 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**.) 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.
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.)**

Table 4-10 Analyst® Software Access to Quantitation (continued)

Preset Access	Description
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.
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*
Modify IS Concentration	Allows users to modify the IS concentrations in a Results Table.
Modify IS Units	Legacy setting*

Table 4-10 Analyst® Software Access to Quantitation (continued)

Preset Access	Description
Modify Processing Algorithm	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.)**
*This feature is not supported in the Analyst® software.	

Table 4-11 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 4-12 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.
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 current sample.
Next Period	Allows users to acquire the next period, immediately.

Table 4-12 Analyst® Software Access to Sample Queue (continued)

Preset Access	Description
Extend Period	Allows users to extend the period that is currently being acquired.
Next Sample	Allows users to acquire the next sample.
Advance Pump Gradient	Legacy setting*
Equilibrate	Allows users to equilibrate the system.
Stand By	Allows users to put the mass spectrometer into Standby mode.
Ready	Allows users to put the mass spectrometer 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.
*This feature is not supported in the Analyst® software.	

Table 4-13 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 create, delete, and update reference tables for calibration standards, and edit the offset drops from Unit resolution for Low and Open resolution.
Edit instrument data	Allows users to edit mass spectrometer calibration and resolution tables.
Manual tune	Allows users to use the Manual Tuning feature in Tune and Calibrate mode.
Calibrate from current spectrum	Allows users to calibrate using the current 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.
Tuning Instrument	Allows users to tune and calibrate the mass spectrometer.

Table 4-13 Analyst® Software Access to Tune (continued)

Preset Access	Description
Advanced Resolution Table Modification	Allows users to configure resolution using the Advanced button in the Resolution tab.
Auto TOF Mass Calibration*	Legacy setting*
*This feature is not supported in the Analyst® software.	

Table 4-14 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 mass spectrometers.

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.)**

Preset access	Description
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.)**
Export, import, or remove External Calibration	Allows users to export, import, or remove an external calibration using one of the following options: • 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: • 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: • Component Comment • IS Comment • IS Peak Comment • Peak Comment • Sample Comments

Preset access	Description
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.
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.

Preset access	Description
Create or edit queries in Results Tables	Allows users to create or edit queries in a Results Table using one of the following options: • 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.)

Add a User or Group to the Analyst® Software

Note: Any changes to the Analyst® software security configuration take effect after restarting 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 **Apply**.
7. Click **OK**.
8. Click **OK** to close the Security Configuration dialog.

Change 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.

4. Click **Apply**.
5. Click **OK**.
6. Click **OK** to close the Security Configuration dialog.

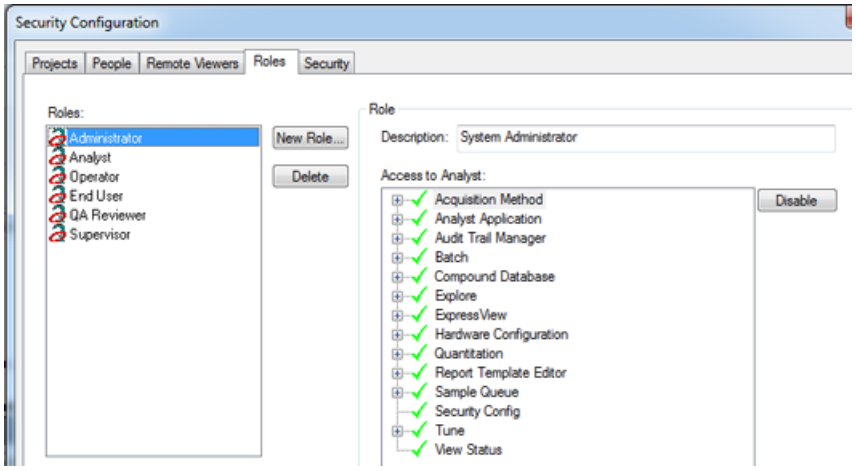
Remove People from the Analyst® Software

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, click the person to be deleted and then click **Delete**.
4. Click **Apply**.
5. Click **OK**.
6. Click **OK** to close the Security Configuration dialog.

Create a Custom 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.

Figure 4-6 Roles tab



3. Click **New Role**.
4. In the New Role dialog, type the **Role Name** and **Description** in the appropriate fields.
5. Click **OK**.

Note: All of the 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 indicates that system access is denied.

6. Double-click components in the **Access to Analyst** list to enable or disable access.
7. To configure access at a functional level, expand the components and then double-click the functionality to enable or disable it.
8. Click **Apply**.
9. Click **OK**.
10. Click **OK** to close the Security Configuration dialog

Delete a Custom Role

Note: If you have one person assigned to a single role, and that role is to be deleted, then 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**.
4. Click **Apply**.
5. Click **OK**.
6. Click **OK** to close the Security Configuration dialog.

Set 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.

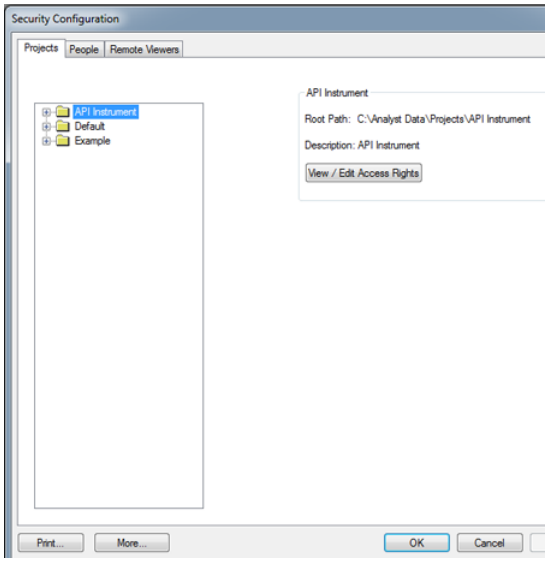
To use this feature of the Analyst® software security, use NTFS for your work route. If you do not set up project security, then operator access to the project files depends on the data setup for each Windows user in NTFS. For more information, refer to Windows Security Configuration on page 11.

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

Set Access

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

Figure 4-7 Security Configuration Dialog: Projects Tab



2. In the left pane of the Security Configuration dialog, click a folder or file.
3. Click **View/Edit Access Rights**.
4. In the Properties dialog, add or remove users or groups and set permissions as required, and then click **OK**.
5. Click **Apply**.
6. Click **OK**.
7. Click **OK** to close the Security Configuration dialog.

Project Folders

Within each project there are folders that can contain different types of files. For example, the Data folder contains acquisition data files. Table 4-15 describes the contents of the different folders.

Table 4-15 Project Folders

Folder	Contents
\Acquisition Methods	Contains all acquisition methods used. Acquisition methods have the dam extension.

Table 4-15 Project Folders (continued)

\Acquisition Scripts	Contains all the acquisition batch scripts available.
\Batch	Contains all the acquisition batch files used. Acquisition batches have the dab extension. It also contains a subfolder, Templates, that contains acquisition batch templates. Batch templates have the dat extension.
\Data	Contains the acquisition data files (wiff extension).
\Log	Contains results of quantitation and compound optimization.
\Processing Methods	Contains all qualitative data processing methods used. Contains all Explore History files that were saved to capture the processing history of a data file.
\Processing Scripts	Contains all data processing scripts available. Processing scripts stored in the API Instrument project are available from the Scripts menu.
\Project Information	Contains all project information and settings for the project. This folder cannot be stored in a subproject.
\Quantitation Methods	Contains all quantitation methods used. Quantitation methods have the qmf extension.
\Results	Contains all quantitation Results Table files (rdb extension).
\Templates	Contains report templates (rpt extension).

Software File Types

Common Analyst® software and MultiQuant™ software file types are listed in Table 4-16. The API Instrument folder contains all of the subdirectories, except Processing Methods and Results.

Table 4-16 Analyst® Software and MultiQuant™ Software Files

Extension	File Type	Subfolder Name
aasf	• Acquisition script • Acquisition script (supplied example)	• Acquisition Scripts • Example Scripts
ata	Audit trail archives	Project Information

Table 4-16 Analyst® Software and MultiQuant™ Software Files (continued)

Extension	File Type	Subfolder Name
atd	• 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
hwpf	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

Table 4-16 Analyst® Software and MultiQuant™ Software Files (continued)

Extension	File Type	Subfolder Name
rpt	Report template	• Templates\Batch • Templates\Method • Templates\ Report • Templates\Workspace
rtf	Rich text format	—
rtf	Log records from automated collection	Log
sdb	Quantitation audit trail settings	Project Information
tun	Tuning preference file	Preferences*
txt	Text	—
wiff	Mass spectrometry data file	• Tuning Cache* • Data
wiff scan	Mass spectrometry data file	• Tuning Cache* • Data
xls or xlsx	Excel spreadsheet	Batch
* Exists only in the API Instrument folder. All of the other subfolders exist within each project folder. They can 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 or xlsx

Windows Firewall Configuration on Acquisition and Client Computers

To remotely manage a mass spectrometer using the Analyst® software on a client computer, the Windows firewall must be configured on both the acquisition and client computers. The Windows firewall on the acquisition computer must be configured to allow both Analyst.exe and AnalystService.exe to run. On the client computer, the Windows firewall must be configured to allow Analyst.exe to run.

Note: Both the acquisition computer, to be remotely accessed, and the client computer, from where the acquisition computer will be accessed, should be on the same network domain.

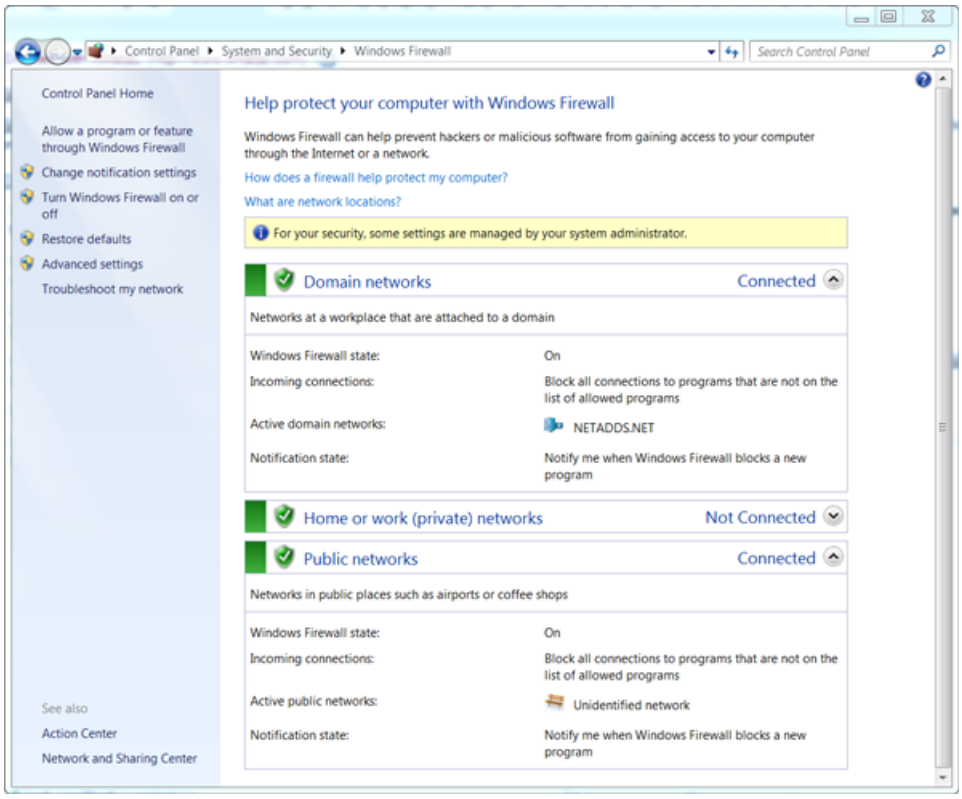
Note: On the acquisition computer, make sure to keep the queue page open after submitting a batch so that the queue can be viewed remotely from the client computer.

Configure Windows Firewall on the Acquisition Computer

The acquisition computer must be configured to allow Analyst.exe and AnalystService.exe through its Windows firewall.

1. Click **Start > Control panel > System and Security > Windows Firewall.**

Figure 4-8 Control Panel



2. Click **Allow a program or feature through Windows Firewall** in the left pane.
3. Click **Change Settings.**
4. Click **Allow another program**.

5. In the Add a Program dialog, click **Browse** and then do one of the following:

   - On computers configured with the Windows 7 (32-bit) operating system, navigate to the <drive>:\Program Files\Analyst\bin folder.
   - On computers configured with the Windows 7 (64-bit) or Windows 10 (64-bit) operating systems, navigate to the <drive>:\Program Files(x86)\Analyst\bin folder.

6. Click **AnalystService.exe** and then click **Open**.
7. Click **Add**.

   The AnalystService is added to the Allowed programs and features list.

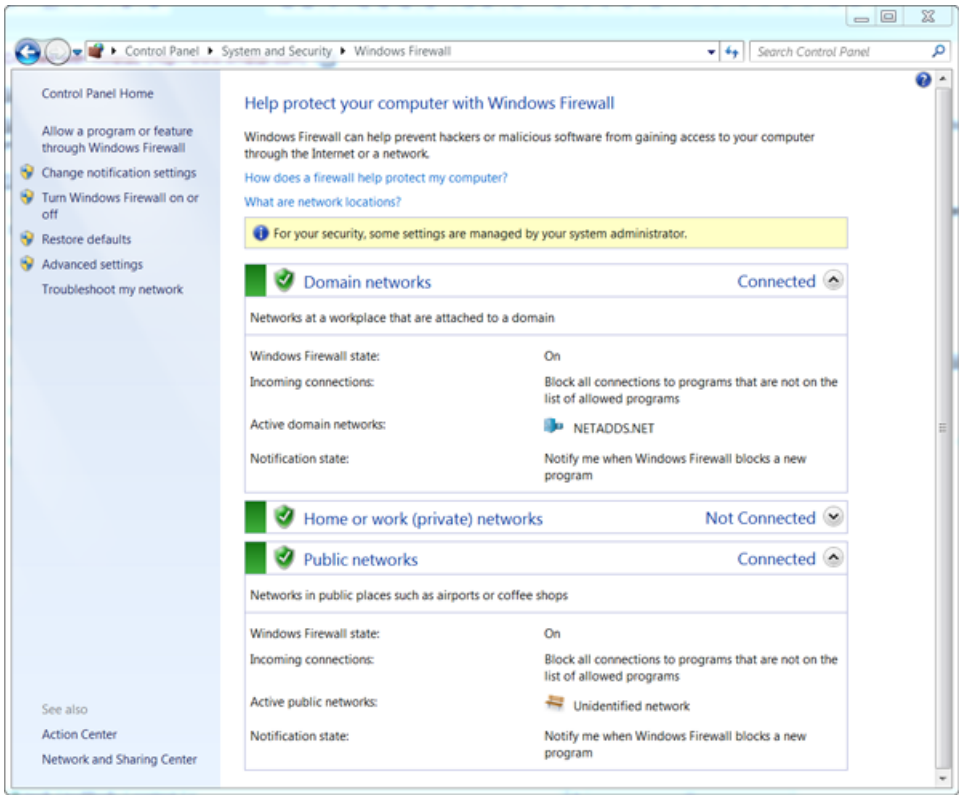
8. If **AB SCIEX Analyst** is not already listed in the **Allowed programs and features list**, then add **Analyst.exe** by repeating steps 4 to 7. However, instead of selecting AnalystService.exe, select **Analyst.exe** in step 6.
9. Click **OK**.

Configure Windows Firewall on the Client Computer

On the client computer, the Windows firewall must be configured to allow Analyst.exe if it is not already listed in the Allowed programs and features list.

1. Click **Start > Control panel > System and Security > Windows Firewall.**

Figure 4-9 Control Panel



2. Click **Allow a program or feature through Windows Firewall** in the left pane.
3. Click **Change Settings.**
4. Click **Allow another program**.
5. In the Add a Program dialog, click **Browse** and then do one of the following:

   - On computers configured with the Windows 7 (32-bit) operating system, navigate to the <drive>:\Program Files\Analyst\bin folder.
   - On computers configured with the Windows 7 (64-bit) or Windows 10 (64-bit) operating systems, navigate to the <drive>:\Program Files(x86)\Analyst\bin folder.

6. Click **Analyst.exe** and then click **Open**.
7. Click **Add**.

   AB SCIEX Analyst is added to the Allowed programs and features list.

8. Click **OK**.

Add Access to a Workstation

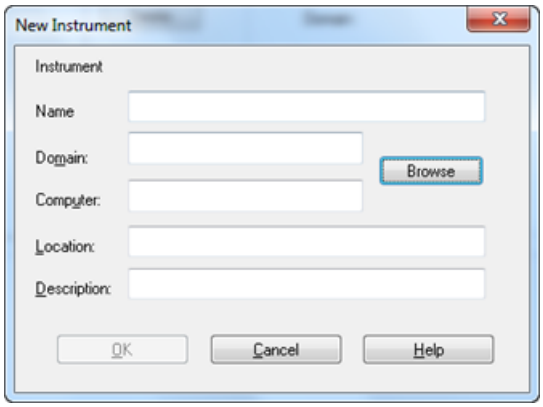
A list of mass spectrometers can be set up on a local computer and then the sample queues of those mass spectrometers can be remotely monitored. Users can only view the sample queue and the status of the mass spectrometers on these remote workstations. Even if they can perform other actions on the local workstation, they cannot perform them on a remote workstation.

Note: Both the acquisition computer, to be remotely accessed, and the local computer, from where the acquisition computer will be accessed, should be on the same network domain.

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

1. Log in to the Analyst® software as a domain-based (user@domain) user.
2. On the Navigation bar, under **Configure**, double-click **Security Configuration**.
3. In the Security Configuration dialog, click the **Remote Viewers** tab and then click **Add**.

Figure 4-10 New Instrument Dialog



4. In the New Instrument dialog, type the workstation name in the **Name** field.

   If you are using Active Directory in the native environment, then the domain field is not visible and you can type a user name in UPN format.
5. Click **Browse** to navigate to a **Domain** and **Computer**.
6. In the Select Computers dialog, select a mass spectrometer.
7. If required, type location information in the **Location** field.
8. In the Windows Security dialog, enter the domain credentials.
9. In the Locations dialog, click the network where the remote acquisition computer is located and then click **OK**.

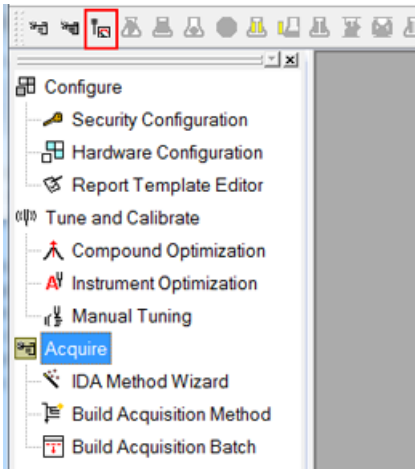
10. In the Select Computers dialog, type the name of the acquisition computer in the **Enter the object names to select** box.
11. Click **Check Names**.
12. Click **OK**.
13. If required, type a description in the **Description** field in the New Instrument dialog .
14. Click **OK**.

    The acquisition computer name and the domain name are shown in the **Remote Viewers** tab.
15. Click **Apply**.
16. Click **OK**.
17. Click **OK** to close the Security Configuration dialog.
18. Restart the Analyst® software.

View Remote Instrument Status and Sample Acquisition Queue

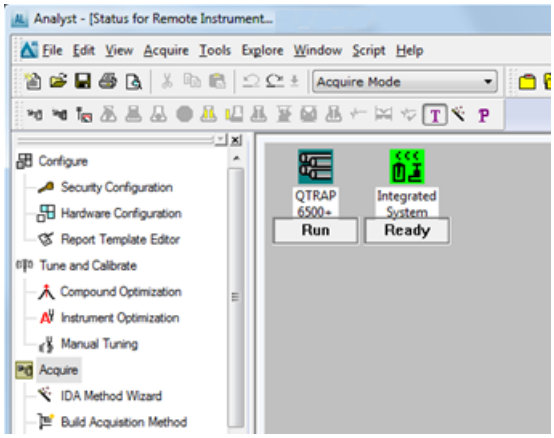
To remotely view the instrument and connected devices status and sample acquisition queue on the acquisition computer, use the Status for Remote Instrument icon in the Analyst® software on the client computer.

Figure 4-11 Status for Remote Instrument Icon in the Analyst® Software



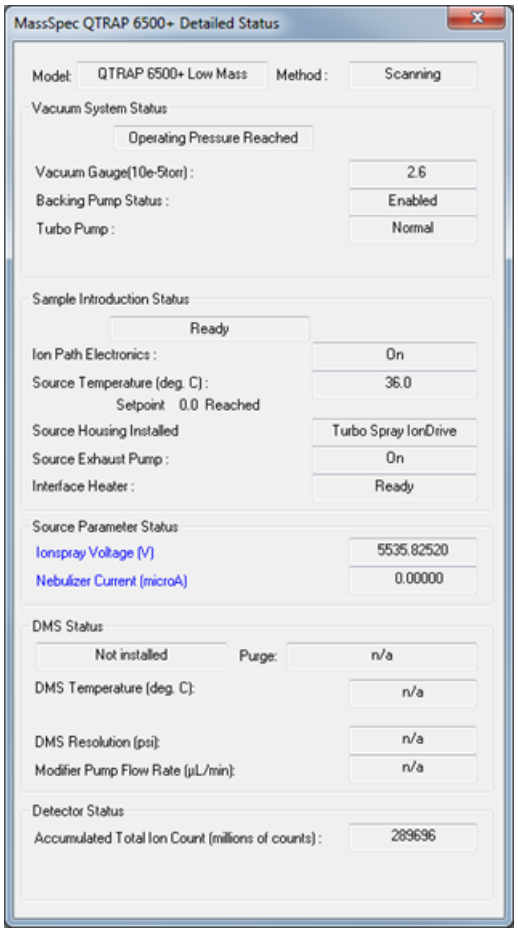
1. Log in to the Analyst® software as the same domain-based user that was used to add the remote instrument in the Security Configuration dialog in Add Access to a Workstation on page 55.
2. In the Analyst® software on the client computer, with **Acquire** mode selected, click the **Status for Remote Instrument** icon.
3. In the Remote Instrument Station dialog, select the instrument in the **Select the Instrument Station** box and then click **Connect**.

Figure 4-12 Remote Instrument Station and Integrated Device Shown in the Analyst® Software



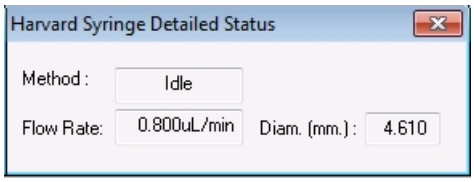
4. Double-click on the remote instrument icon to view the detailed status.

Figure 4-13 Detailed Status of the Remote Instrument



5. Double-click on the integrated syringe icon to view the detailed status.

Figure 4-14 Detailed Status for the Integrated Syringe



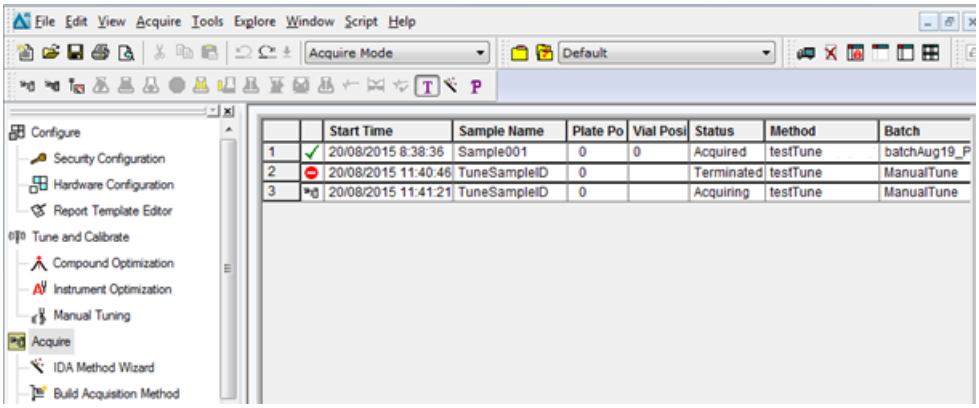
6. To view the sample acquisition queue on the acquisition computer, in **Acquire** mode, click the **Instrument Queue** icon on the toolbar in the Analyst® software.

Note: The queue page must be open on the acquisition computer in order for the queue to be remotely viewed from the client computer.

7. In the Remote Instrument Station dialog, select the instrument in the **Select the Instrument Station** box and then click **Connect**.

   The sample acquisition queue on the acquisition computer is shown in the Analyst® software.

Figure 4-15 Sample Acquisition Queue on the Acquisition Computer



Remove 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 a mass spectrometer.
4. Click **Delete**.
5. Click **Yes**.
6. Click **Apply**.
7. Click **OK**.
8. Click **OK** to close the Security Configuration dialog.
9. Restart the Analyst® software.

Print Security Configurations

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**.
3. Click **Apply**.
4. Click **OK**.
5. Click **OK** to close the Security Configuration dialog.

Analyst Administrator Console 5

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 the 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

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, refer to Setup of Workgroups on page 64.

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, refer to Network Acquisition on page 67 on page 88.

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.

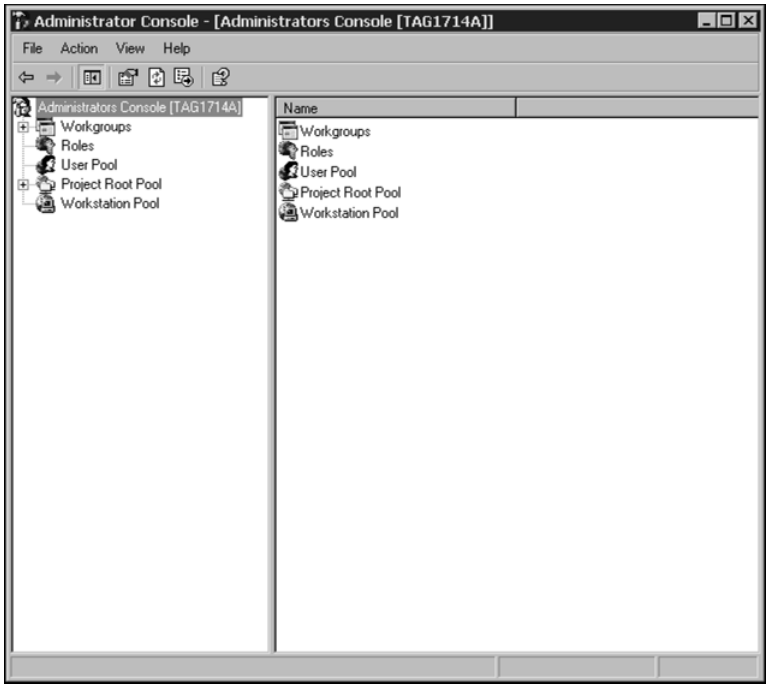
All security information is stored in the database on the server. During installation, the security database is automatically populated with the preset Analyst® software roles and users. Additionally, each time the Analyst® software is started, the backup copy of the database on each registered workstation 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 5-1 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, refer to Console Administrators Workgroup on page 66.

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, refer to Administrator Console Ongoing Tasks on page 80.

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, refer to Table 5-1. 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 5-1 Tasks to Set Up the Administrator Console

Task	Procedure
Connect the Administrator Console client to the server.	Refer to Connect the Administrator Console Client to the Server (Standalone Application) on page 67 or refer to Connect the Administrator Console Client to the Server (Workstation) on page 67.
Create or configure roles using the Administrator Console client (optional).	Refer to Create Roles on page 68.
Add users to the User Pool using the Administrator Console client.	Refer to Add Users or Groups to the User Pool on page 70.
Set the Default Project location using the Administrator Console client (optional).	Refer to Select a Template Project on page 71.
Create or add projects and root directories using the Administrator Console client (optional).	Refer to Create a Root Folder on page 71.
Create workgroups using the Administrator Console client.	Refer to Create a Workgroup on page 74.
At each workstation, run the Analyst® software and register the workstation.	Refer to Register a Workstation on page 77.

Table 5-1 Tasks to Set Up the Administrator Console (continued)

Task	Procedure
At each workstation, run the Administrator Console client and add the workstation to a workgroup.*	Refer to Add Workstations to a Workgroup on page 78.
Set a default workgroup for each workstation (optional).	Refer to *Set a Default Workgroup for the Analyst Logon Information Dialog on page 78*.
*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.

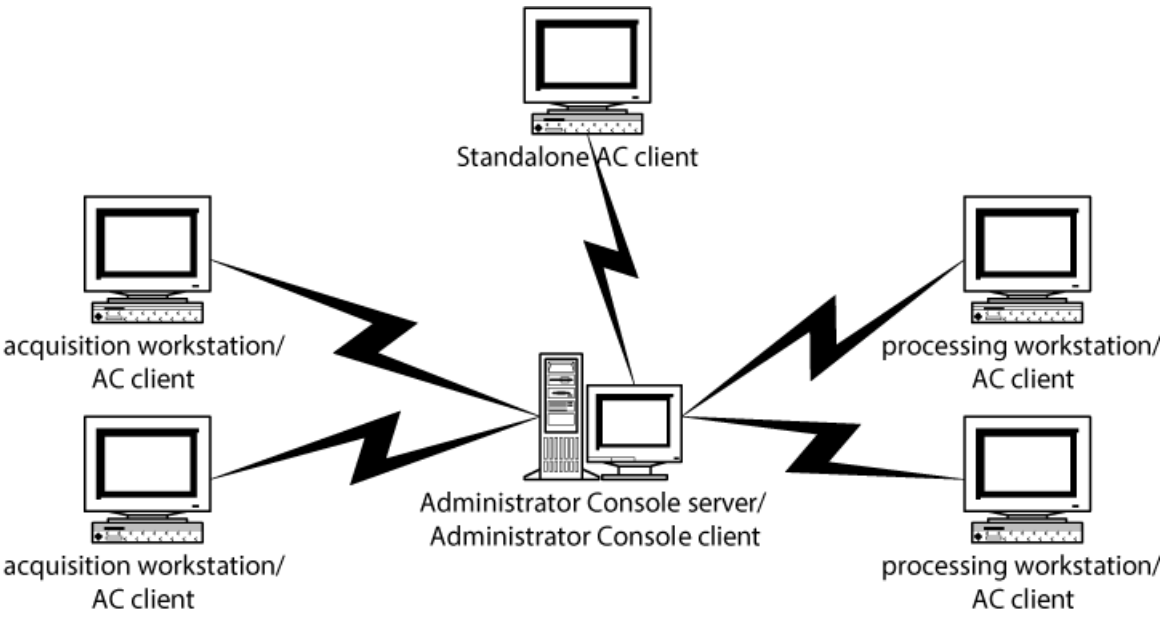
Note: Alternatively, if you manage Windows file security through the IT department, you can create workgroups containing users and workstations only.

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, refer to Analyst® Software and Windows Security: Working Together on page 9.

For an example of workstations registered with the server, refer to Figure 5-2. If server-based security is no longer required for a particular workstation, manage security for the workstation locally through the Analyst® software.

Figure 5-2 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, is visible 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, refer to Change the Security Mode of a Workgroup on page 84.

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 require 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.

Connect 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.

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. Right-click the **AAC** icon and then click **Run as**.

   a. In the Run As dialog, click **The following user**.

   b. Click **Administrator**.

   c. 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 shown properly.

   The Browse for Computer dialog opens.

2. Browse to the server and then click **OK**.

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. Right-click the **AAC** icon and then click **Run as**.

   a. In the Run As dialog, click **The following user**.

   b. Click **Administrator**.

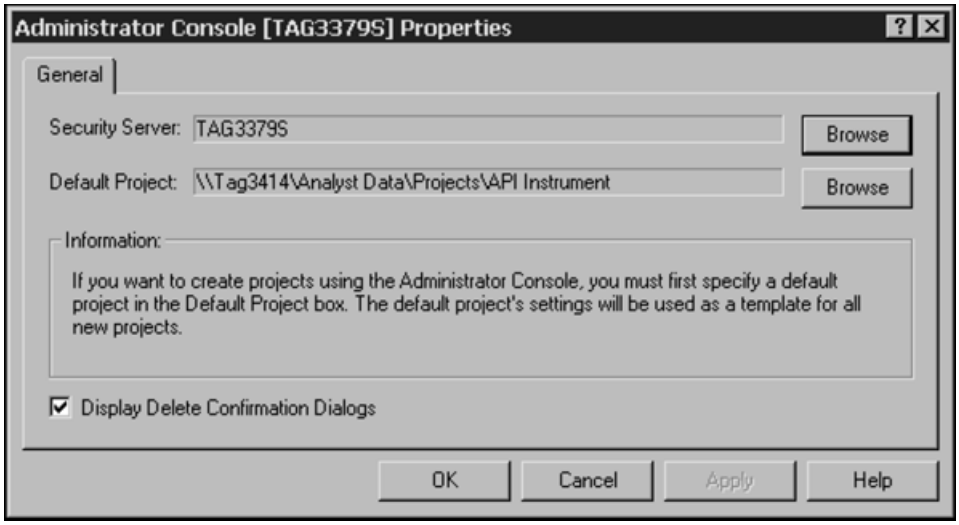
   c. In the Command Line, type **Administrator Console.msc** and then click **Enter**. If you do not run the application as an administrator, then the database will not be shown properly.

   The Browse for Computer dialog opens.

2. Right-click **Administrators Console** and then click **Properties**.

   The Administrator Console Properties dialog opens.

Figure 5-3 Administrator Console Properties Dialog



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

Create Roles

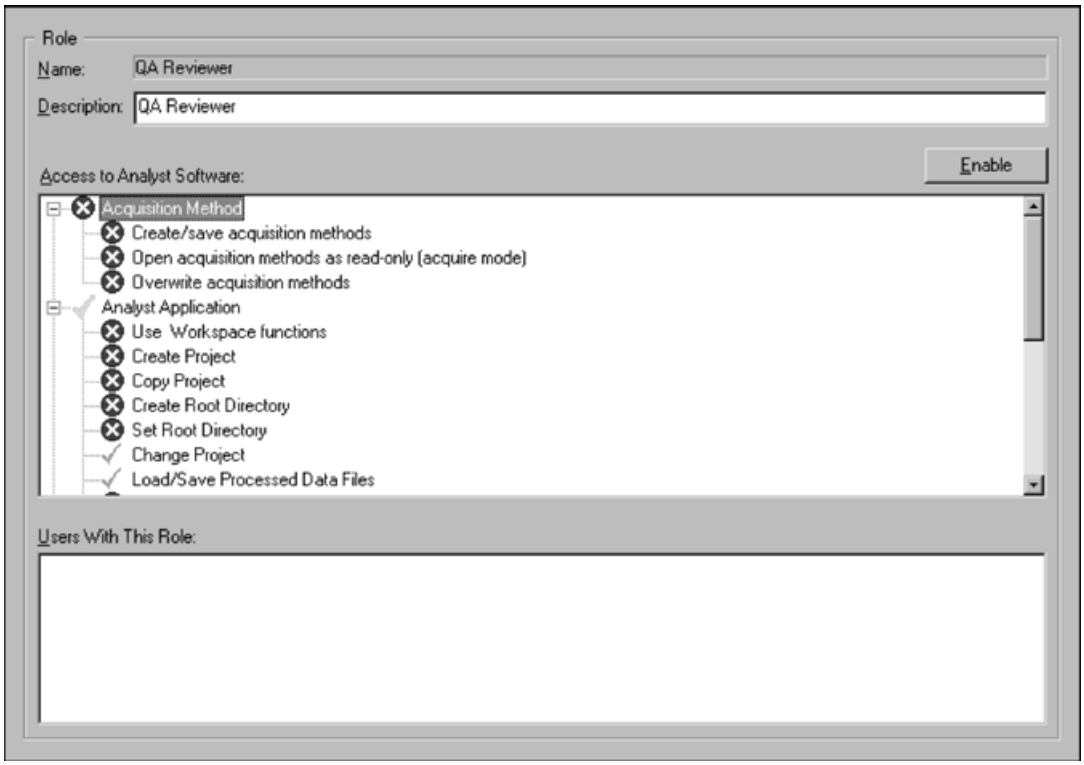
The Analyst® software has six predefined roles. If you require additional ones, either create a new role or copy an existing role and assign access rights. For more information on roles, refer to Access to the Analyst® Software on page 29.

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.

1. Run the Administrator Console client.
2. Right-click **Roles** and then click **New Role**.

   The Create Role dialog opens.
3. In the **Name** field, type a name.
4. In the **Description** field, type a description.
5. Click **OK**.
6. Right-click the new role and then click **Properties**.

Figure 5-4 Properties Dialog



7. 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.

Copy a Role

1. Run the Administrator Console client.
2. Click **Roles**.
3. In the right pane, right-click and then click **Copy**.

   The Copy Role dialog opens.
4. In the **Name** field, type a name.
5. In the **Description** field, type a description and then click **OK**.

6. Right-click the new role and then click **Properties**.

   The properties dialog opens.

7. 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.

Add 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, refer to Access to the Analyst® Software on page 29.

1. Run the Administrator Console client.
2. Right-click **User Pool** and then click **Add Users or Groups**.

   The Select Users or Groups dialog opens.

3. 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 of 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.

Select a Template Project

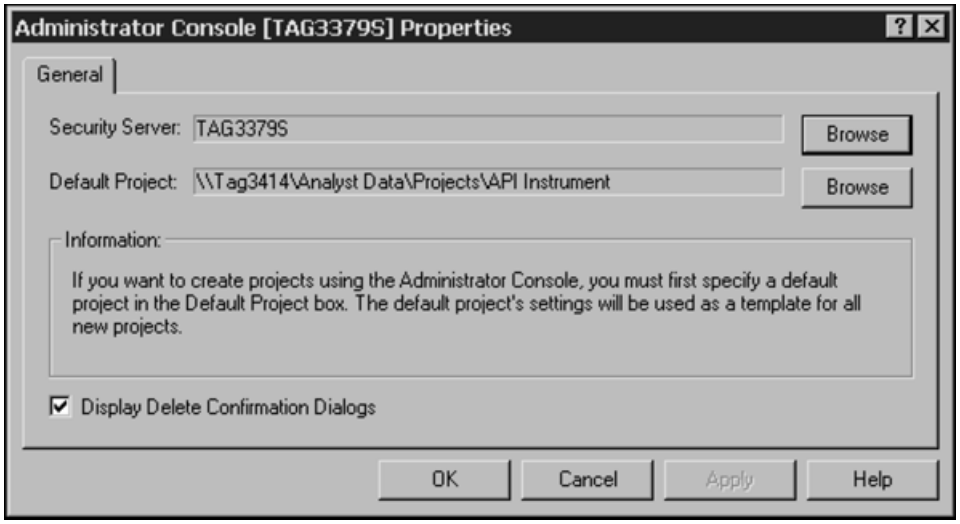
Use this procedure to select a template project to use as a template for all new projects.

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**.

   The Administrator Console Properties dialog opens.

   Figure 5-5 Administrator Console Properties Dialog



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

Create 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. Run the Administrator Console client.
2. Right-click **Project Root Pool**.
3. Click **Create Project Root**.

   The Create Root Folder dialog opens.

4. In the **Root Folder Location** field, type the folder location or click **Browse** and then navigate to the root folder location.
5. In the **Root Folder Name** field, type the root folder name and then click **OK**.

   The database is updated and the new root folder opens in the Project Root Pool.

Add 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. Run the Administrator Console client.
2. Right-click **Project Root Pool** and then click **Add Existing Project Root**.

   The Browse for Folder dialog opens.
3. Browse to the root directory location.
4. Click **OK**.

   The root directory is shown in the Project Root Pool.

Refresh a Project Root

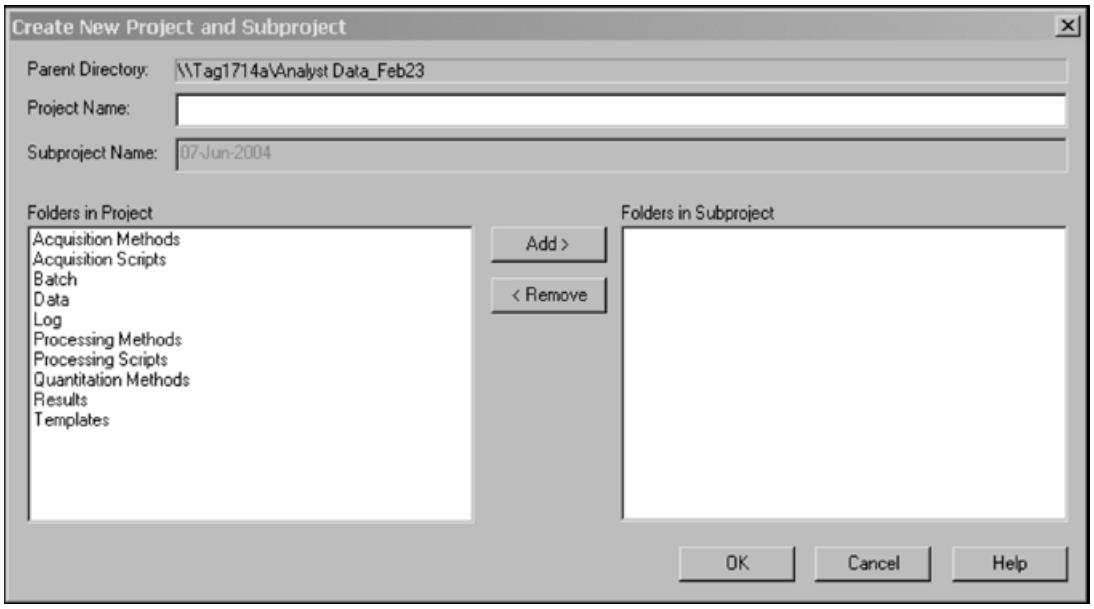
Use this procedure to synchronize the contents of the Project Root Pool with the contents of the project roots on the network. Refresh each project root individually.

1. Run the Administrator Console client.
2. Expand **Project Root Pool**, right-click the project root, and then click **Refresh**.

Create a Project

1. Run the Administrator Console client.
2. Expand **Project Root Pool**, right-click the root, and then click **Create Project**.

Figure 5-6 Create New Project and Subproject Dialog



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

Note: 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.

4. 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.
5. The preset **Subproject Name** is the current date as provided by the system. If required, in the **Subproject Name** field, type a new name.
6. Click **OK**.

Add an Existing Project

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

1. Run the Administrator Console client.
2. Expand **Project Root Pool**, right-click the project, and then click **Add Existing Project**.

   The Browse for Folder dialog opens.
3. Browse to the project location and then click **OK**.

   The project opens in the right pane.

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, refer to Set up Screen Lock and Auto Log Out on page 27.

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, refer to Create a Project on page 72.

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.

Create a Workgroup

1. Run the Administrator Console client.
2. Select a default workgroup for each workstation. For more information, refer to Set a Default Workgroup for the Analyst Logon Information Dialog on page 78.
3. Right-click **Workgroup** and then click **New Workgroup**.

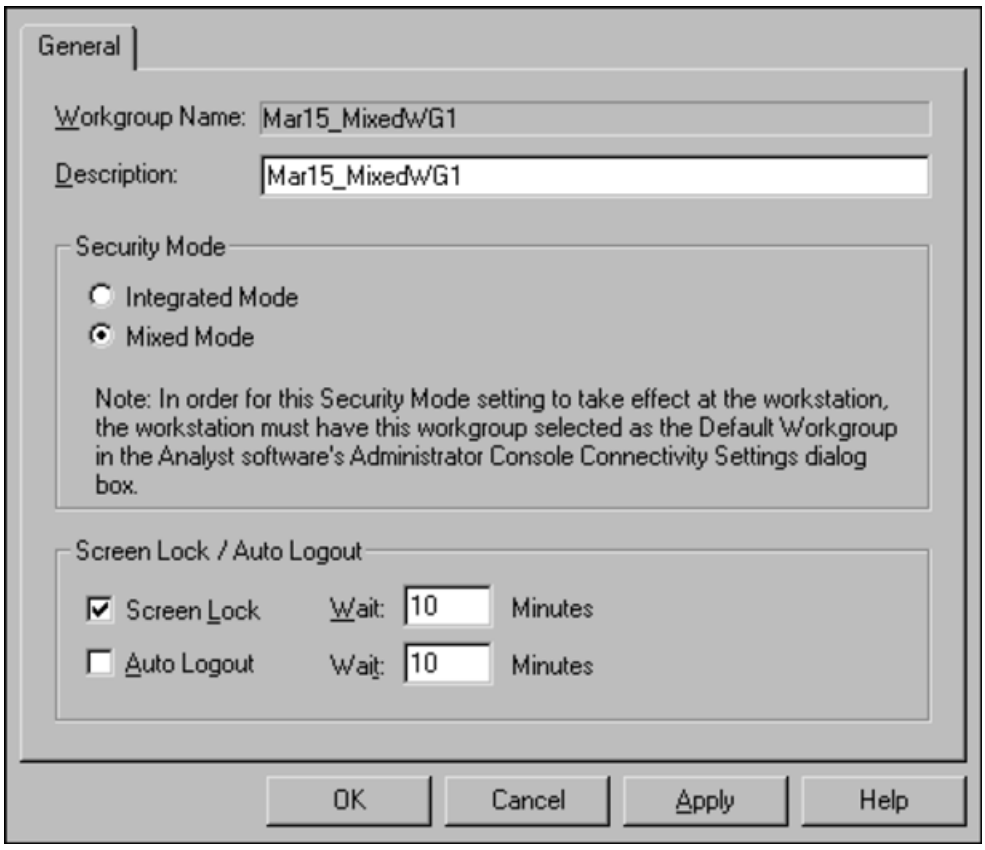
   The Create Workgroup dialog opens.
4. In the **Workgroup Name** field, type a name.
5. In the **Description** field, type a description, and then click **OK**.

   The workgroup is created and added into the Workgroup sub-tree. 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, refer to Workgroup Security Modes and Logging on to the Analyst® Software on page 79.
6. If required, change the security mode and set screen lock and auto log out.

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

Figure 5-7 Properties Dialog



b. Click a mode to change the security mode.

c. Select the **Screen Lock** check box to enable screen lock and, if required, change the preset Wait time.

d. Select the **Auto Logout** check box to enable auto logout and, if required, change the preset Wait time.

e. Click **OK**.

7. Add users, projects, and workstations to the new workgroup.
8. 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, refer to Set File Permissions on page 66.
9. Restart the Analyst® software on each workstation for the changes to take effect.

Add Users or Groups to a Workgroup

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

1. Run the Administrator Console client.
2. Expand **Workgroups** and then expand the workgroup.
3. Right-click **User** and then click **Add Users or Groups**.

   The Add Users or Groups to Workgroup dialog opens.
4. 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.

5. If the required user is not in the list, click **Add Windows User**, select the user or groups, and then click **OK**.
6. 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, refer to Set File Permissions on page 66.

Add or Remove a Role

For information on creating user-defined roles, refer to Create Roles on page 68.

1. Run the Administrator Console client.
2. Expand **Workgroups**, expand the workgroup, and then click **User**.
3. In the pane on the right, right-click the user and then click **Properties**.

   The **Properties** dialog opens.
4. In the **Available Roles** list, click the role, click **Add** or **Remove**, as required, and then click **OK**.

Add 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 added to Workgroup 2, then Users A, B, and C will all have access to Project_01.

1. Run the Administrator Console client.
2. Expand **Workgroups** and then expand the workgroup.
3. Right-click **Project** and then click **Add Project**.

   The Add Project to Workgroup dialog opens.
4. 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.

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, refer to Set File Permissions on page 66.

Register a Workstation

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

Note: 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.**
2. Select the **Use Server Based Security** check box.

Figure 5-8 Administrator Console Connectivity Settings Dialog

3. Select the **Use Workgroup Based Project Security** check box if required.

   By default (Use Workgroup Based Project Security check box not selected), users are able to see all projects in their root directory, whether or not they are granted access through their workgroup. Users also retain their logged-on security privileges when switching to those projects. If the Use Workgroup Based Project Security check box is selected, users only see projects for which their workgroup has access. Also, users are forced to re-authenticate their credentials if they change root directories. This option is useful for environments where strict project control is required.

4. In the **Administrator Console Server Name** field, type the name of the server or click **Browse** to navigate to the server.
5. Restart the Analyst® software.

   The workstation opens 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 is shown in the Workgroup field in the Analyst - Logon Information dialog. For more information, refer to Set a Default Workgroup for the Analyst Logon Information Dialog on page 78.

Add Workstations to a Workgroup

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

1. Run the Administrator Console client.
2. Expand **Workgroups** and then expand the workgroup.
3. Right-click **Workstation** and then click **Add Workstation**.

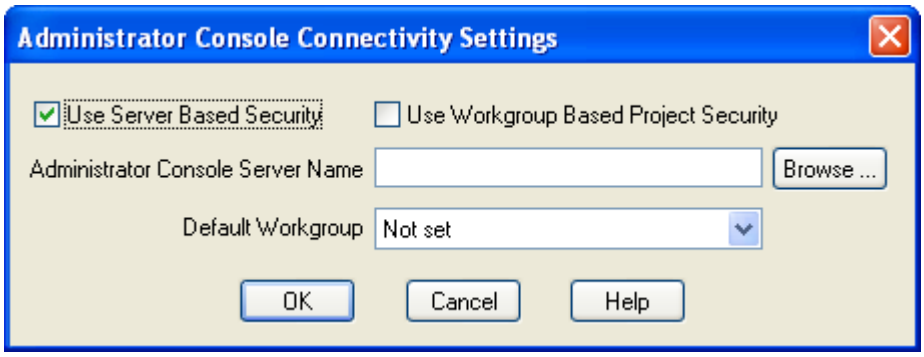
   The Add Workstation to Workgroup dialog opens.
4. In the **Available Workstations in Workstation Pool** list, click the workstation, click **Add**, and then click **OK**.
5. For the changes to take effect, after all changes to the workgroup have been made, right-click the workgroup and then click **Set File Permissions**. For more information, refer to Set File Permissions on page 66.

Set 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 5-9 Administrator Console Connectivity Settings Dialog



Note: The Default 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 is shown in the Workgroup field in the Analyst - Logon Information dialog.

Change the Default Workgroup 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 opens.
2. Click the workgroup.
3. 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 is shown 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, refer to Change the Default Workgroup in Integrated Mode on page 79.

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, refer to Auditing on page 93.

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, refer to Create a Workgroup on page 74.

- Synchronize the Administrator Console Client and Server on page 80
- Change the Attributes of the Administrator Console Client on page 81
- Delete Roles on page 81
- Change the Properties of a Role on page 82
- Delete Users or Groups on page 82
- Delete Projects on page 82
- Delete Workstations on page 62 on page 83
- Delete Workgroups on page 84
- Change the Attributes of a Workgroup on page 84
- Delete Users, Projects, or Workstations from a Workgroup on page 85
- Change a Role on page 64 on page 86
- Review Project Permissions on page 65 on page 86

Synchronize 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, refer to Refresh a Project Root on page 83.

Refresh the Administrator Console Client

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

Change 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 opening each time a resource is deleted.

Change the Server Location

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

   The Administrator Console Properties dialog opens.
3. Click **Change**, browse to the new server location, and then click **OK**.

Deactivate the Deletion Confirmation Dialog

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

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

   The Administrator Console Properties dialog opens.
3. Clear the **Display Delete Confirmation Dialogs** check box and then click **OK**.

Delete 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. Run the Administrator Console client.
2. Click **Roles**.

3. In the right pane, right-click the role and then click **Delete**.

Change the Properties of a Role

You can change the properties or description of a role.

1. Run the Administrator Console client.
2. Click **Roles**.
3. In the right pane, right-click the role and then click **Properties**.

   The **Properties** dialog opens.
4. If required, in the **Description** field, type a description.
5. 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.

Delete Users or Groups

You can delete users or groups from the User Pool.

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

Delete 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.

Delete a Project from the Project Root

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

Delete a Project Root from the Project Root Pool

1. Run the Administrator Console client.
2. Expand **Project Root Pool**, right-click the project root and then click **Delete**.

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.

1. Run the Administrator Console client.
2. Expand **Project Root Pool**, right-click the project root and then click **Refresh**.

Delete 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. Delete workstations using either the Administrator Console client or the Analyst® software.

Delete a Workstation using the Administrator Console Client

1. Run the Administrator Console client.
2. Click **Workstation Pool**.
3. In the right pane, right-click the workstation and then click **Delete**.

Delete a Workstation using the Analyst® Software

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

   The Administrator Console Connectivity Settings dialog opens.

Figure 5-10 Administrator Console Connectivity Settings Dialog

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

Delete 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.

1. Run the Administrator Console client.
2. Expand **Workgroups**, right-click the workgroup and then click **Delete**.

Change the Attributes of a Workgroup

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

Change the Description of a Workgroup

1. Run the Administrator Console client.
2. Expand **Workgroups**, right-click the workgroup and then click **Properties**.

   The Properties dialog opens.
3. In the **Description** field, type a new workgroup description and then click **OK**.

Change the Security Mode of a Workgroup

1. Run the Administrator Console client.
2. Expand **Workgroups**, right-click the workgroup and then click **Properties**.

The Properties dialog opens.

3. In the **Security Mode** section, click a security mode option and then click **OK**.

Enable or Disable Screen Lock and Auto Logout

1. Run the Administrator Console client.
2. Expand **Workgroups**, right-click the workgroup and then click **Properties**.

   The Properties dialog opens.

3. In the **Screen Lock/Auto Logout** section, select or clear the **Screen Lock and Auto Logout** check boxes as required.
4. Type a new wait time in the **Wait** field if required.

Rename a Workgroup

1. Run the Administrator Console client.
2. Expand **Workgroups**, right-click the workgroup and then click **Rename**.

   The name is selected.

3. Type the new workgroup name.

   After you rename the workgroup, all workstations with the previous 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.

Delete 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.

Delete a User from a Workgroup

1. Run the Administrator Console client.
2. Expand **Workgroups**, expand the workgroup, and then click **Users**.
3. In the right pane, right-click the user or groups and then click **Delete**.
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**.

   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.

Delete a Project from a Workgroup

1. Run the Administrator Console client.
2. Expand **Workgroups**, expand the workgroup, and then click **Projects**.
3. In the right pane, right-click the project and then click **Delete**.
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**.

   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.

Delete a Workstation from a Workgroup

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

Change 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, refer to Create Roles on page 68.

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 opens.
3. In the **Available Roles** list, click the role.
4. Click **Add** and then click **OK**.

Review 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 opens.

3. Click the **Security** tab to review the permissions.

Network Acquisition 6

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.

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: Potential Data Loss. 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, refer to Select an Acquisition Account on page 26.

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 opens 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.

Delete 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.

Configure 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, refer to *About Projects and Root Directories on page 70*.

Create 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**.

Set 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.

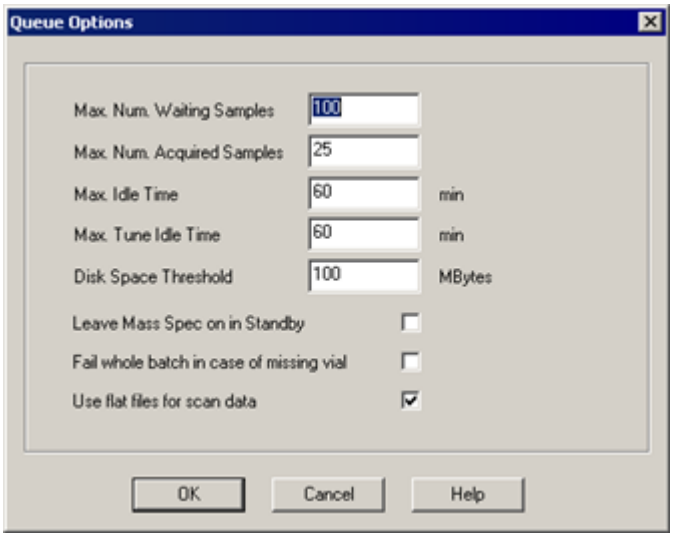
1. Click **Tools > Project > Set Root Directory.**
2. In the Browse for Folder dialog, click **Browse** to navigate to the existing root directory.
3. Click **OK**.

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

Change the File Format

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

Figure 6-1 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.
3. Click **OK**.

Select an Acquisition Account

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

Auditing 7

This section explains how to use the auditing functionality in the Analyst® software. For information about Windows auditing functions, refer to System Audits on page 12.

Topics in this section:

About Audit Trails

The Analyst® software groups audited events by mass spectrometer, project, and 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 7-1 Analyst® Software Audit Trails

Audit Trail	Examples of Events Recorded	Available Audit Maps Stored In	Default Audit Maps

Instrument (one per workstation)	• Changes to:
	  • Instrument resolutions
	  • Mass calibrations
	  • Sample queues
	  • Security
	  • Hardware profiles
	• Instrument maintenance log entries
		• API Instrument project
		• Project Information folder
			N/A

Project (one per project)	• Changes to:
	  • Project
	  • Data
	  • Quantitation
	  • Method
	  • Batch
	  • Tuning
	  • Results Table
	  • Report template files
	• Opening and closing of modules
	• Printing
		• Each project
		• Project Information folder
			Copied from the default project

Quantitation (one per Results Table)	Changes to: • 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, refer to Audit Trail Records on page 105.

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 mass spectrometer and projects, but only use one audit map at a time for each acquisition station and each project. The audit map used is called the active audit map for that mass spectrometer or project.

Each audit map contains a list of all of 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 audit 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 shown 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 might want to modify one or more of them for your own use. At a minimum, make sure that 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, refer to Change an Audit Map on page 99.

Default Audit Map: At installation, the default audit map is the active audit map for new projects. By default, all of the 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 the Analyst® software, then the default audit map contains that audit configuration.

No Audit Map: No events are audited.

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

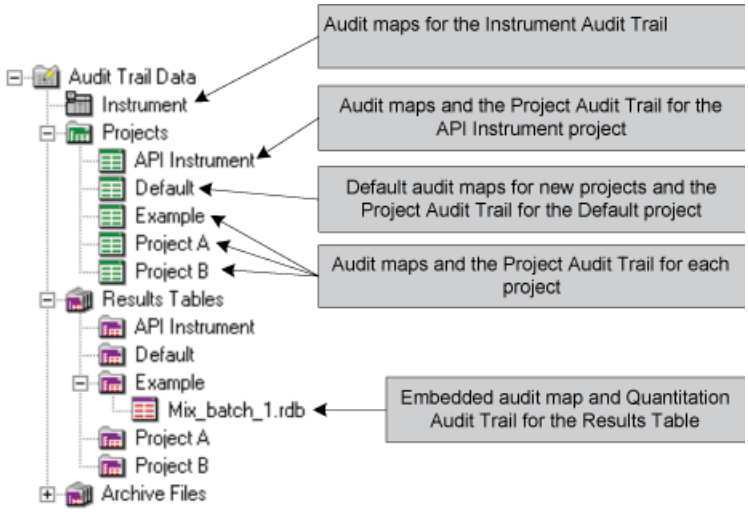
Full Audit Map: All of the events are audited. Electronic signatures and reasons are required for all of the events.

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, refer to Table 7-1. For more information about the events recorded in audit trails, refer to Audit Trail Records on page 105.

For the locations of the audit maps and audit trails in the Audit Trail Manager, refer to Figure 7-1.

Figure 7-1 Audit Trail Manager: Location of Audit Maps and Audit Trails



For information about the auditing process, refer to Table 7-2. If you have upgraded from a previous version of the Analyst® software, then refer to About using Audit Maps with Projects Created in Previous Versions of the Analyst Software on page 104.

Table 7-2 Checklist for Setting Up Auditing

Task	Procedure
Create an audit map for the Instrument Audit Trail.	• Refer to Create an Audit Map on page 97. • Refer to Change an Audit Map on page 99.
Apply the audit map to the Instrument Audit Trail.	• Refer to Apply an Audit Map on page 100.
Create a default active audit map for new projects.	• Refer to Create an Audit Map on page 97. • Refer to Change an Audit Map on page 99.
Specify the default active audit map for new projects.	• Refer to Apply an Audit Map on page 100.
Configure the audit map you want to use for each existing project.	• Refer to Create an Audit Map on page 97. • Refer to Change an Audit Map on page 99. • Refer to Copy an Audit Map from Another Project on page 100.
Apply the configured audit map to each existing project.	• Refer to Apply an Audit Map on page 100.

Work 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 new one. For descriptions of the audit maps, refer to Installed Audit Maps on page 95. To view or modify an installed audit map, refer to Change an Audit Map on page 99. If you know that a suitable audit map exists in a different project, then copy the audit map. For a checklist of suggested steps for setting up auditing, refer to Table 7-2 on page 97.

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

Create 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 opens.

2. In the left pane, expand the **Audit Trail Data** folder.

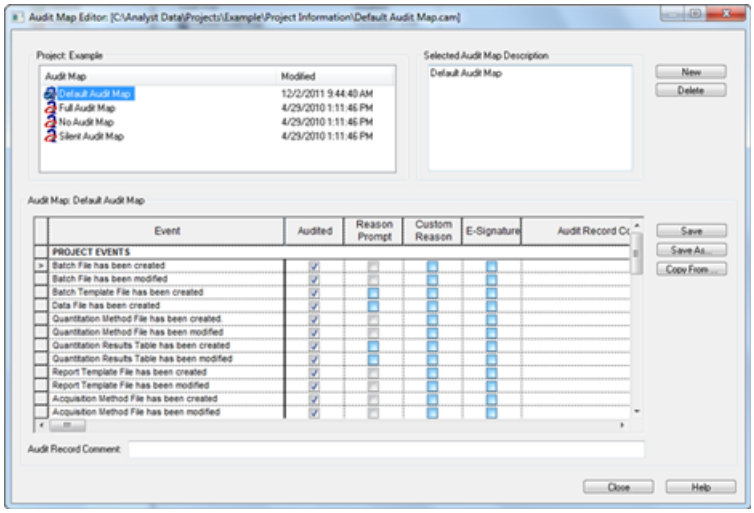
3. Expand the **Projects** folder.
4. In the Projects section, click the project for which you want to create an audit map. If you are creating an audit map for use with the Instrument Audit Trail, then click the **API Instrument** folder.

> **Tip!** You can also click **Instrument** above the **Projects** folder to create an audit map for use with the Instrument Audit Trail.

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

   The Audit Map Editor dialog opens with the active audit map shown.

Figure 7-2 Audit Map Editor Dialog



6. Click **New**.

   A new audit map, with no events audited, is shown.
7. If required, in the **Selected Audit Map Description** field, type a description of the audit map.
8. In the **Audit Map** table, configure each event as follows:

   - If you want the event to be audited, then 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** column, 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 electronic signatures for the event, then select the check box in the **E-Signature** column.
- If you want to make a note about the audit configuration for this event, then type your comment in the **Audit Record Comment** column.

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

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.

Now that you have created an audit map, use it with your project (refer to Apply an Audit Map on page 100) or copy it to another project (refer to Copy an Audit Map from Another Project on page 100).

Change 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: Potential Data Loss. If you and another user are modifying the same audit map at the same time, then only the changes made by the person who saved the file last are retained.

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

   The Audit Trail Manager window opens.
2. In the left pane, expand the **Audit Trail Data** folder.
3. Expand the **Projects** folder.
4. In the **Projects** section, click the project that contains the audit map you want to modify.
5. On the **Settings** tab, click **Edit**.

   The Audit Map Editor dialog opens with the active audit map shown.
6. In the **Projects** section, click the audit map to modify.
7. In the Audit Map table, make any changes to the configuration. For more information about the table, click **Help**.
8. To save the audit map, click **Save**.

Copy an Audit Map from Another Project

Audit maps can be copied from one project to another.

CAUTION: Potential Wrong Result. Do not copy cam files (audit maps) between projects outside of the Analyst® software as this can cause inaccurate audit trails.

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

   The Audit Trail Manager window opens.
2. In the left pane, expand the **Audit Trail Data** folder.
3. Expand the **Projects** folder.
4. In the **Projects** section, click the project into which you want to paste the audit map.
5. On the **Settings** tab, click **Edit**.

   The Audit Map Editor dialog opens with the active audit map shown.
6. Click **New**.

   The **Audit Map Editor** dialog shows a new audit map, with no events audited.
7. Click **Copy From**.

   The Open dialog opens.
8. 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 opens.
9. To save the copied audit map to the current project, click **Save**.

Apply an Audit Map

When an audit map is applied 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 opens.
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**, then click **Instrument**.
- 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**.

View, Print, and Search Audit Trails

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

View an Audit Trail

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

   The Audit Trail Manager window opens.
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 **Instrument**. 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 mass spectrometer.
   - 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.

View 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 shown 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 opens.
2. In the left pane, expand the **Audit Trail Data** folder.

3. Expand the **Results Tables** folder.
4. In the **Results Tables** section, expand the project that contains the Results Table for which you want to view the audit map.
5. Click the **Results Table** file for which you want to view the audit map.

   The audit trail opens in the right pane.
6. On the **Settings** tab, click **Details**.

   The Results Table Audit Trail Settings dialog opens showing the audit trail configuration for the Results Table.

View 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 opens.
2. In the left pane, expand the **Audit Trail Data** folder.
3. In the **Audit Trail Data** section, click **Instrument**. If the audit trail is not shown, then click the **History** tab in the right pane.

   The audit trail opens.
4. For any record that has additional details, click **Review** in the **History** column.

View 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-201609300820.ata.

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

   The Audit Trail Manager window opens.
2. In the left pane, expand the **Audit Trail Data** folder.
3. Expand the **Archive Files** folder.
4. In the **Archive Files** section, expand the project that contains the archived audit trail that you want to view.
5. Click the audit trail you want to view.

   The archived audit trail opens in the right pane.
6. If the audit trail does not open, then click the **History** tab in the right pane.

The audit trail opens.

Tip! You can also open an archived audit trail by right-clicking in the left pane and then clicking **Open Archives**. The Open dialog opens. 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.

Print an Audit Trail

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

   The Audit Trail Manager window opens.
2. Select the audit trail.
3. Right-click in the **History** tab, click **Print**, and then do one of the following:

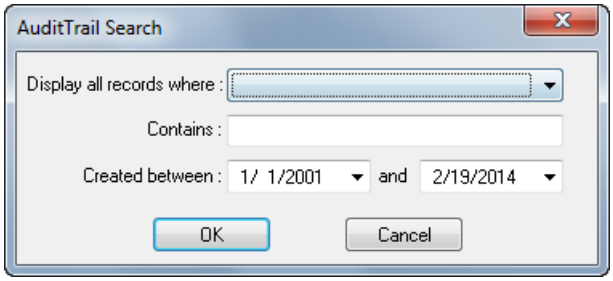
   - To print the current page, click **Current Page**.
   - To print all of the pages in the audit trail, click **All Pages**.

Search for an Audit Record

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

   The Audit Trail Manager window opens.
2. Select the audit trail.
3. View the audit trail that you want to search.
4. Right-click in the **History** tab and then click **Search**.

Figure 7-3 Audit Trail Search Dialog



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

7. Click **OK**.

   Only records that meet the criteria are listed.

   Tip! To list all of the 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 is shown 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: Potential Wrong Result. 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.

Audit Trail Records A

This section provides more information about audit trails and audit maps, including lists of all of the 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.

Topic in this section:

Audit Trail Records

The Instrument, Project, and Quantitation Audit Trails are encrypted files. All of the 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-201609300820.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 Trial. 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 a mass spectrometer, 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 the creation, modification, and deletion of a 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, refer to Analyst Administrator Console on page 61.

Auditing Using the MultiQuant Software B

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

Topics in this section:

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. Refer to Auditing on page 93 for information about auditing in the Analyst® software.

The Audit Trail Manager in the MultiQuant™ software maintains all of 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™ software 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 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 opens in the MultiQuant™ software.

Table B-1 MultiQuant Audit Trails

Audit Trail	Examples of Events Recorded
Quantitation (one per Results Table)	Changes to: • Creation and modification of session files. • Sample information. • Peak integration parameters.

About Audit Maps

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

Set 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 might 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 of 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.

Create or Change 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 one.

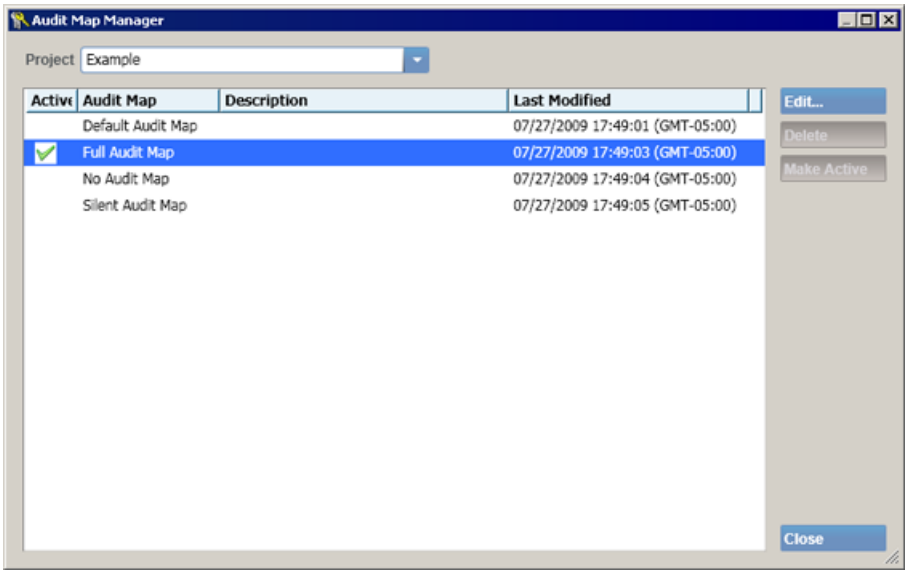
CAUTION: Potential Data Loss. If two users are modifying the same audit map at the same time, then only the changes made by the person who saved the file last are retained.

The active audit map for the project determines which events are recorded 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.**

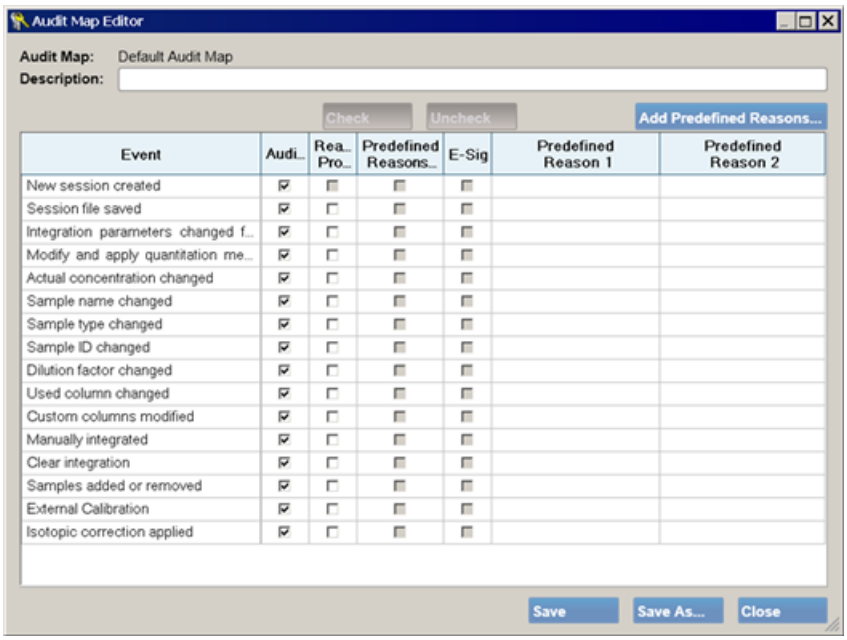
Figure B-1 Audit Map Manager



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 opens with the active audit map shown.

Figure B-2 Audit Map Editor



4. Type a description of the audit map in the **Description** field, if required.
5. In the Audit Map table, configure each event as follows:

   - If you want the event to be audited, then 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 **Check**.

   - 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, then 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, then 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 an audit map is applied, 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 shown 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, then you might not be able to view your Results Table or chromatograms.

View Audit Configurations Embedded in the Results Table

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

View, Search, and Print 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.

View 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 of the sessions in the project at the same time.

Perform a Keyword Search

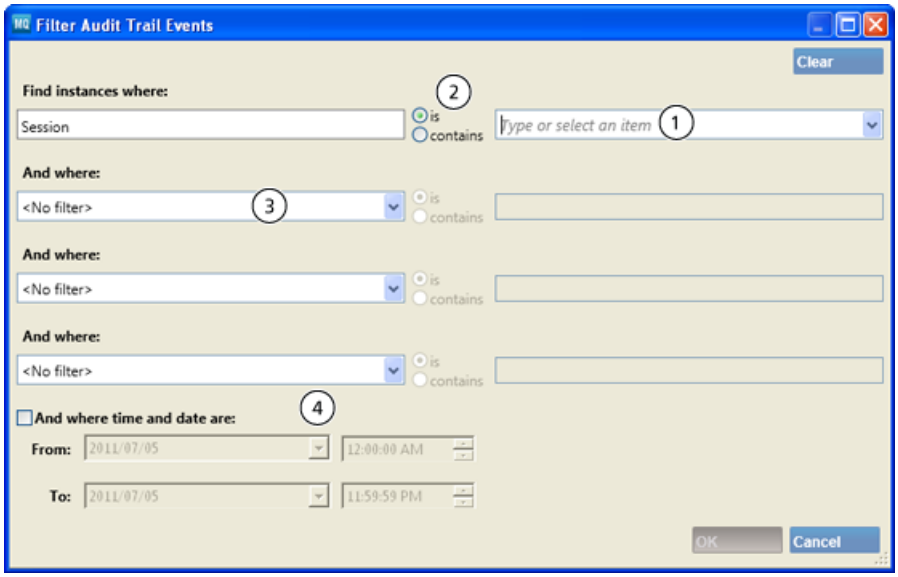
1. Open a Results Table.
2. Click **Audit Trail > Audit Trail Viewer.**
3. In the **Find** field, type the word that you want to find in the Audit Trail results and then click **Go**.

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

Filter 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 of the session files for the active project.
2	The *is* and *contains* 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 timeframe.

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

Note: You cannot edit the **Session** field.

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

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

Print the Audit Trail Viewer

1. Open a Results Table.
2. Click **Print** and then select a printer.

   Users can print a secure PDF using pdfFactory.

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

Export the Audit Trail Viewer

1. Open a Results Table.
2. 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.

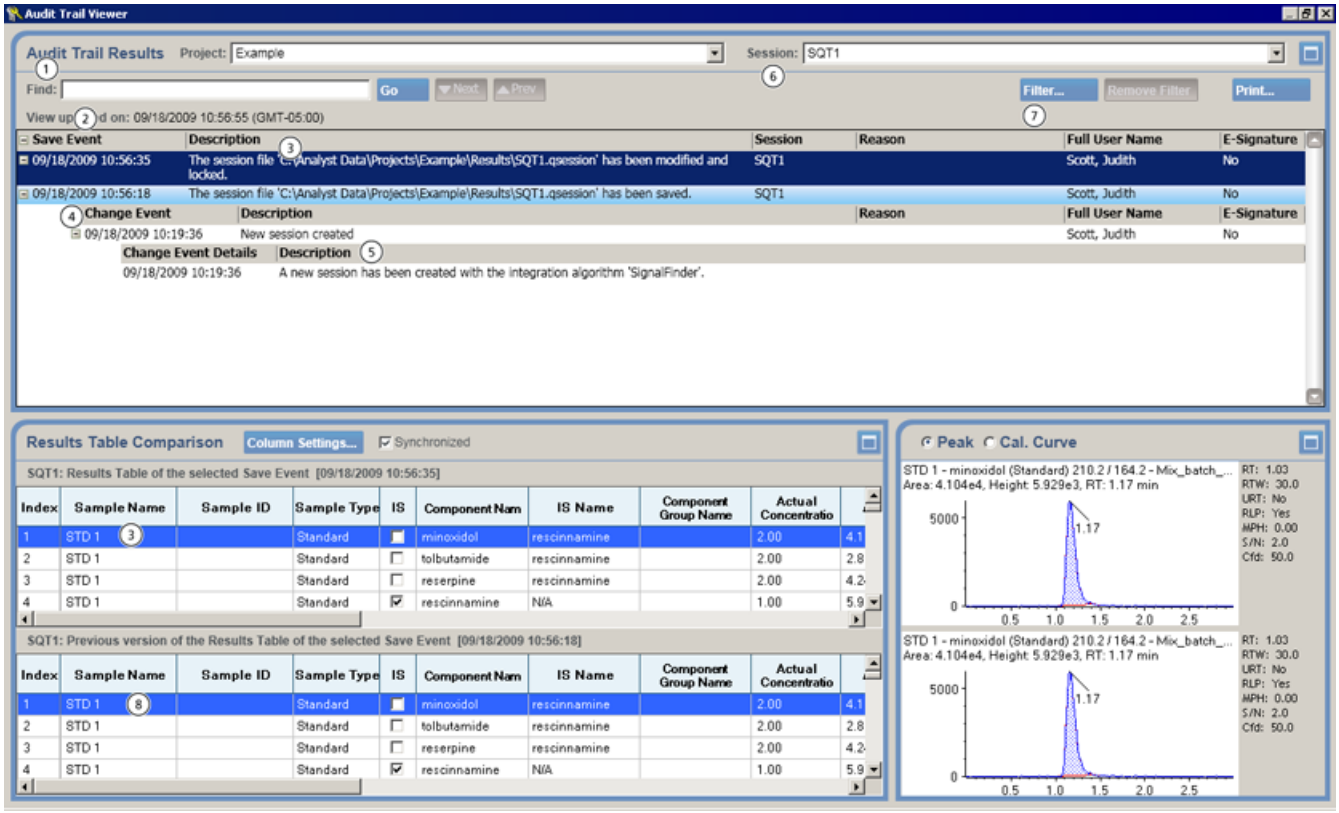
About the Audit Trail Viewer

The Audit Trail Viewer shows the entire 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, refer to Figure B-4.

- 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 of the session files.
- Find (1): A keyword search without filtering. Highlights every occurrence of the text.
- Filter (7): Shows only the events that match the selected criteria.
- Dark blue highlight (3): Selected save event.
- Previous version (8): Shows the previous version of the selected session file.

Figure B-4 Audit Trail Viewer Dialog



Additional Security Customization C

This section contains information about the additional features that the Analyst® software provides to secure data.

Topics in this section:

Data File Changes (Explore Processing)

The Explore Processing History is a file containing a record of the changes made 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

Create Explore Processing History Files

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

- In **Explore** mode, right-click in a data file pane, 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.

View an Explore Processing History File

1. Click **File > Open.**

   The Open dialog opens.
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 opens 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, click **Review** under the History column.
5. To print the Explore Processing History window, right-click in the **History** tab, click **Print**, and then click either **Current Page** or **All Pages**.
6. To show the current data processing history of a data file in the active pane, in **Explore** mode, click **Explore > Show > Show History.** The history that is shown is not automatically saved and cannot be used to review processing.

Add an Instrument Maintenance Log Entry

When the mass spectrometer 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 opens.
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**.

View an Instrument Maintenance Log Entry

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

   The Audit Trail Manager window opens.

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

   The audit trail opens.

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

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

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

Configure E-mail Notification

You can configure the Analyst® software to send an e-mail message if there are three log on errors within one day. This e-mail notification is available only if the workstation is in Integrated or Mixed Mode. For information about security modes, refer to Analyst® Software and Windows Security: Working Together on page 9.

The recipient of the e-mail 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 opens.

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

   The Audit Trail Options dialog opens showing 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 e-mail server. Use your e-mail 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 e-mail address to which you want the message sent. For example: username@domain.com.
7. In the **From** field, type the name you want to be shown 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

We recommend that users use datafile checksums. The checksum feature is a cyclic redundancy check to verify data file integrity. The checksum feature is enabled by default for fresh installation of the Analyst® software. In case users upgrade to the current version of the Analyst® software, users checksum setting before the upgrade is maintained.

If you have enabled the Data File Checksum feature, then 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 in 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, then the checksum is valid.
- If the values do not match, then 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, then 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.

Verify 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 opens.

2. In the **Data Files** field, select a wiff file (data file).
3. Click **Verify Checksum**.

   The ExplorDir message dialog opens showing the result of the checksum comparison.

   - If the values do not match, then 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, then 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.

Enable or Disable 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.**

   The Audit Trail Manager window opens.

2. Right-click in the left pane of the Audit Trail Manager window and then click **Options.**
3. Click **Data File Checksum**.

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

Data System Conversion D

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, refer to *Table D-1 on page 125*.

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+).

Translate 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 opens.

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.

Generate 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 opens.
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 opens 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.

Convert 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 opens.

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 opens 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.**

Revision History

Revision	Description	Date
A	First release of document.	April 2013
B	Updated the copyright page. Changed AB SCIEX to SCIEX where required. Updated the Active Directory Support section. Removed information about ExpressView. Changed Alerter to Alert in the Alerts section. Removed information about the Windows XP operating system. Added the storage location for security information on a Windows 7 (64-bit) OS. Updated the caution in the section "About using Audit Maps with Projects created in Previous Versions of the Analyst Software". Added a new note and a few new steps in the "Add Access to a Workstation" section. Added a new step in the "Remove a Workstation" section.	September 2015

Revision	Description	Date
	Added the following four new topics: Windows Firewall Configuration on Acquisition and Client Computers Configure Windows Firewall on the Acquisition Computer Configure Windows Firewall on the Client Computer View Remote Instrument Status and Sample Acquisition Queue	
C	Added Contact Us. Added Windows 10 (64-bit) where required. Updated screenshots in View Remote Instrument Status and Sample Acquisition Queue section The Configure Analyst Software Security Chapter is now divided into two chapters. Removed period from the file extensions that are listed without a filename. Updated the following sections: Related Documentation, Analyst® Software and Windows Security: Working Together, Mixed or Native Environment content in the Active Directory Support, System Audits section, Updated Analyst® Software Installation section with Windows 10 screen shots and information, Location of Security Information, Analyst® Software Access, About People and Roles, Software File Types, Audit Trails within the Analyst® Software and Windows, Add a User or Group to the Analyst® Software, and Data File Checksum Added a tip and a note in Create an Audit Map section. Added information about borrowing or returning server-based electronic license.	October 2017