SCIEX
The Power of Precision

Analyst MD Software

Laboratory Director's Guide

IVD-IDV-05-0252-E

April 2022

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

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

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

SCIEX warranties are limited to those express warranties provided at the time of sale or license of its products and are the sole and exclusive representations, warranties, and obligations of SCIEX. SCIEX makes no other warranty of any kind whatsoever, expressed or implied, including without limitation, warranties of merchantability or fitness for a particular purpose, whether arising from a statute or otherwise in law or from a course of dealing or usage of trade, all of which are expressly disclaimed, and assumes no responsibility or contingent liability, including indirect or consequential damages, for any use by the purchaser or for any adverse circumstances arising therefrom.

(GEN-IDV-09-10816-D)

IVD

CE

UK CA

For *In Vitro* Diagnostic Use. Product(s) not available in all countries. For more information contact your local sales representative or refer to sciex.com/diagnostics.

Rx Only.

Trademarks and/or registered trademarks mentioned herein, including associated logos, are the property of AB Sciex Pte. Ltd., or their respective owners, in the United States and/or certain other countries (see sciex.com/trademarks).

AB Sciex™ is being used under license.

© 2022 DH Tech. Dev. Pte. Ltd.

EC REP

Leica Microsystems CMS GmbH
Ernst-Leitz-Strasse 17-37
35578 Wetzlar
Germany

AB Sciex Pte. Ltd.
Blk33, #04-06 Marsiling Industrial Estate Road 3
Woodlands Central Industrial Estate, Singapore 739256

Contents

1 Introduction **7**

2 Security Configuration Overview **8**
Security and Regulatory Compliance 8
Security Requirements 8
Analyst MD Software and Windows Security: Working Together 8
Audit Trails within the Analyst MD Software and Windows 8
Audit Trails in the MultiQuant MD Software 9
21 CFR Part 11 9
System Configuration 10
Windows Security Configuration 10
Users and Groups 10
Active Directory Support 10
Windows File System 11
System Audits 11
File and Folder Permissions 11
Event Logs 12
Windows Alerts 12

3 Electronic Licensing **13**

4 Configure Analyst MD Software Security **14**
Software Security Workflow 14
Analyst MD Software Installation 16
Verify Software Components 17

5 Analyst MD Software Security Configuration **18**
Steps to Configure the Analyst MD Software 18
Location of Security Information 18
About Security Modes and Accounts 18
Select the Security Mode 19
Select an Acquisition Account 21
Set up Screen Lock and Auto LogOut 22
Unlock or Log off from the Analyst MD Software 24
Access to the Analyst MD Software 24

About People and Roles 25
Analyst MD Software Access 28
MultiQuant MD Software Access 40
Add a User or Group to the Analyst MD Software 44
Change a Role 44
Remove People from the Analyst MD Software 44
Create a Custom Role 45
Delete a Custom Role 46
Set Access 46
Windows Firewall Configuration on Acquisition and Client Computers 50
Remote Workstations 52
Print Security Configurations 58

6 System Health Monitoring 59
Auxiliary Traces 59
Enable Auxiliary Traces 59
Show Auxiliary Traces 59
Injection Counter 60
Enable the Injection Counter 60

7 Auditing 62
Audit Trails 62
Audit Maps 63
Setup of Audit Maps 64
Installed Audit Maps 65
Work with Audit Maps 66
Create an Audit Map 66
Change an Audit Map 68
Copy an Audit Map from Another Project 69
Apply an Audit Map 69
View, Print, and Search Audit Trails 70
View an Audit Trail 70
View the Audit Configuration Embedded in a Results Table 70
View Details for an Audit Record in the Instrument Audit Trail 71
View an Archived Audit Trail 71
Print an Audit Trail 72
Search for an Audit Record 72

A Audit Trails 74
Audit Trail Records 74
Audit Trail Archives 75
Instrument Audit Trail Events 75
Project Audit Trail Events 76

Quantitation Audit Trail Events 78
AAC Audit Trail 79

B Additional Security Customization 80
Data File Changes (Explore Processing) 80
Create Explore Processing History Files 81
View an Explore Processing History File 81
Add an Instrument Maintenance Log Entry 81
View an Instrument Maintenance Log Entry 82
Configure E-mail Notification 82
Data File Checksum 83
Verify Data File Checksum 84
Enable or Disable the Data File Checksum Feature 84

C Special Acquisition Account 85

Contact Us 86
Customer Training 86
Online Learning Center 86
SCIEX Support 86
CyberSecurity 86
Documentation 86

Introduction 1

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 MD software and attached instrumentation from a functional perspective.
- The system administrator, who is concerned with system security and system and data integrity.

Security Configuration Overview 2

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

Security and Regulatory Compliance

Security Requirements

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

Analyst MD Software and Windows Security: Working Together

The Analyst MD software and the Windows New Technology File System (NTFS) 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. As a result, only users who are recognized by the Windows Local or Network security settings have access to the system. For more information, refer to the section: Windows Security Configuration.

The Analyst MD 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 the section: About Security Modes and Accounts.

The Analyst MD software also provides completely configurable roles that are separate from the user groups associated with Windows. By using roles, the laboratory director can control access to the software and mass spectrometer on a function-by-function basis. For more information, refer to the section: Access to the Analyst MD Software.

Audit Trails within the Analyst MD Software and Windows

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

The Analyst MD 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 and modification events for projects, tuning, batches, data, acquisition methods, quantitation methods, Results Tables, and report template files, as well as module opening, closing, and printing events. Deletion events recorded in the audit trail are instrument deletion for remote viewer, user deletion in the Analyst MD software, user type deletion, and project role deletion.
- Creation and modification of the quantitation method embedded in the Results Table, modification of sample information in the Results Table, and modification of peak integration parameters.

For a complete list of audit events, refer to the section: Audit Trail Records.

The Analyst MD 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, which capture a range of security-, system-, and application-related events. In most cases, Windows auditing is designed to capture exceptional events, such as a log on failure. The administrator can configure this system to capture a wide range of events, such as access to specific files or Windows administrative activities. For more information, refer to the section: System Audits.

Audit Trails in the MultiQuant MD Software

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

21 CFR Part 11

The Analyst MD software contains the technical controls to support 21 CFR Part 11 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 that use a combination of user ID and password.

- Proper configuration of the Windows operating system.
- Proper procedures and training in the company.

The Analyst MD software is designed to be used as part of a 21 CFR Part 11 compliant system and can be configured to support 21 CFR Part 11 compliance. Whether the use of the Analyst MD software is 21 CFR Part 11 compliant is dependent on the actual usage and configuration of the Analyst MD software in the lab.

Validation services are available through SCIEX Professional Services. For more information, contact complianceservices@sciex.com.

System Configuration

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

Windows Security Configuration

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

For the Analyst MD software to work as intended, users must be part of the Microsoft Windows local user group.

Note: Network acquisition is not supported in the Analyst MD software.

Users and Groups

The Analyst MD 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 about adding and configuring people and roles, refer to the section: Access to the Analyst MD Software.

Active Directory Support

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

Mixed Environment

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

The network includes the following:

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

Native Environment

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

The network includes the following:

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

Windows File System

In the Analyst MD software, files and directories must be stored on a hard-disk partition formatted as the NTFS, which can control and audit access to Analyst MD software files. The File Allocation Table (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 attempt to log on to the system in the event log.

File and Folder Permissions

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

Before selecting the events or actions to be audited, 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 level of access users need to the drive and the folder on each computer. Configure sharing and associated permissions. For more information about file sharing, refer to the Windows documentation.

For information about the Analyst MD software files and folder permissions, refer to the section: Analyst MD Software Security Configuration.

Event Logs

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

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

Customize the event logs as follows:

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

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

Windows Alerts

If a system or user issue occurs, then configure the network to send an automatic message to a designated person, such as the system administrator, on the same computer or another computer.

- On both the sending and receiving computer, start the Messenger in the Windows Services control panel.
- On the sending computer, start the Alert service in the Windows Services control panel.

For more information about creating an alert object, refer to the Windows documentation.

Electronic Licensing 3

Electronic licensing can only be node-locked.

The Activation ID might be required for any future service or support call. To access the Activation ID of the node-locked or server-based license:

- Click **Help** > **About Analyst** in the Analyst MD software window.

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

Configure Analyst MD Software Security 4

This section explains how to configure the software.

Note: The user must have local administrator privileges for the computer on which the software is being installed.

Software Security Workflow

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

Configure security at the following levels:

- Windows authentication: Access to the computer.
- Windows authorization: Access to files and folders.
- Access to the Analyst MD software.
- Selective access to the Analyst MD software functionalities.
- Access to specific projects.
- Access to instrument workstation status.

For the list of tasks for configuring security, refer to the table: Table 4-1. For the options for setting the various security levels, refer to the table: Table 4-2.

Table 4-1 Workflow for Configuring Security

Task	Procedure
Install the Analyst MD software.	Refer to the document: *Analyst MD Software Installation Guide*.
Configure Analyst MD software security.	Refer to the section: Analyst MD Software Security Configuration.
Configure audit trails.	Refer to the section: Auditing.
Configure Windows File Security and NTFS.	Refer to the section: Set Access.

Table 4-1 Workflow for Configuring Security (continued)

Task	Procedure
Maintain system maintenance log for instruments, security, data, and project maintenance.	Refer to the section: Additional Security Customization.

Table 4-2 Security Configuration Options

Option	CFR 21 Part 11
Windows Security	
Format drives to NTFS.	Yes
Configure users and groups.	Yes
Enable Windows auditing, and file and directory auditing.	Yes
Set file permissions.	Yes
Analyst MD Software Installation	
Install the Analyst MD software.	Yes
Install MultiQuant MD software.	Yes
Select audit options.	Yes
Event Viewer (inspect install).	Yes
Analyst MD Software Security	
Select security mode. **Note:** Use of Single User mode is not recommended for the CFR-compliant environment.	Integrated or Mixed
Configure Analyst MD software roles and people.	Yes
Create audit maps, configure instrument, project, and quantitation audit trails.	Yes
Configure email notification.	Yes
Activate Checksum. **Note:** The checksum feature is enabled by default in a fresh installation of the Analyst MD software.	Yes
Common Tasks	

Table 4-2 Security Configuration Options (continued)

Option	CFR 21 Part 11
Add new projects and subprojects.	Yes
Configure project audit trail for new projects and subprojects.	Yes
Transfer existing data.	Yes
Create maintenance log for instrument security, data, project maintenance.	Yes

Analyst MD Software Installation

Before installing the Analyst MD software, read these documents, available on the software installation DVD or web download package: *Software Installation Guide* and *Release Notes*. Be sure to understand the difference between a processing computer and an acquisition computer and then complete the appropriate installation sequence.

Note: We recommend that Windows updates and Internet connectivity for the application computer 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. For the acquisition computer, we highly recommend that only critical Windows updates, such as security changes, be installed. Make sure that adequate virus protection is in place to prevent virus corruption of system functionality.

Windows Requirements

- Only the English version of the Windows 10 operating system is supported. Using a different default language might cause the software to show the file information or the audit trail information incorrectly.
- In the Region and Language settings, make sure that **English (United States)** is set to be the first language.

System Requirements

For minimum installation requirements, refer to the document: *Software Installation Guide*.

Preset Auditing Options

For a description of the installed audit maps, refer to the section: Installed Audit Maps. After installation, the Analyst MD 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 MD software is installed, a Software Component Verification procedure verifies that all of the software components were installed and generates an installation report. This report is an event log item from the Analyst MD 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 the section: Data File Checksum.

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 MD Software Security Configuration 5

This section describes how to configure the Analyst MD software security.

Note: Any changes to the Analyst MD software security configuration take effect after the Analyst MD software is restarted.

Steps to Configure the Analyst MD Software

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

For the general tasks for configuring the Analyst MD software, refer to the table: Table 5-1

Table 5-1 Tasks for Configuring the Analyst MD Software

Task	Refer To
Configure the security mode.	Select the Security Mode.
Configure screen lock and auto log out (Mixed mode only).	Set up Screen Lock and Auto LogOut.
Configure project security.	Set Access.
Configure instrument workstations.	Add Access to a Workstation or Remove Access to a Workstation.

Location of Security Information

If the Analyst MD software is running on a single computer or in a network configuration, then all security information is stored in the `SecurityDB.odb` file in the following folder on the computer:

- `C:\Program Files (x86)\Analyst\Bin`

About Security Modes and Accounts

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

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

Integrated Mode: The user who is currently logged on to Windows has access to the Analyst MD software, providing that the Windows user is also a valid Analyst MD software user.

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

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

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: Use the same account that was used to log on to the Analyst MD software for data acquisition. In Integrated mode, the user who has logged on to Windows is also logged on to the Analyst MD software. In Mixed mode, the Windows user and the Analyst MD software user can be different.

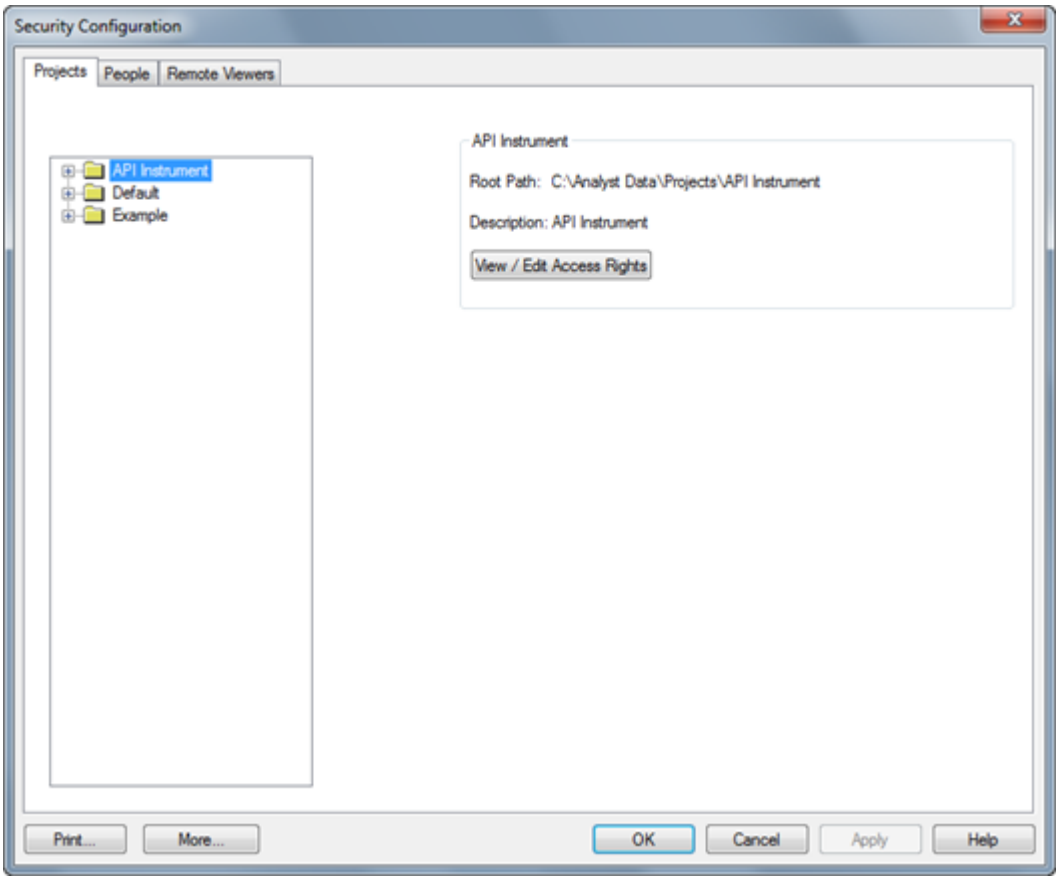
Special Acquisition Administrator Account: We do not recommend network acquisition when using the Analyst MD software. This feature is intended for use in a regulated environment. The operator must provide a user name, domain, and password for this account. After the network administrator sets up this account, it can be used to acquire data regardless of the identity of the current user of the Analyst MD 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. Refer to the section: Special Acquisition Account.

Screen Lock and Auto Logout: For security purposes, the computer screen can be set to lock after a defined period of inactivity. An automatic logout time can also be set, where the Analyst MD 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

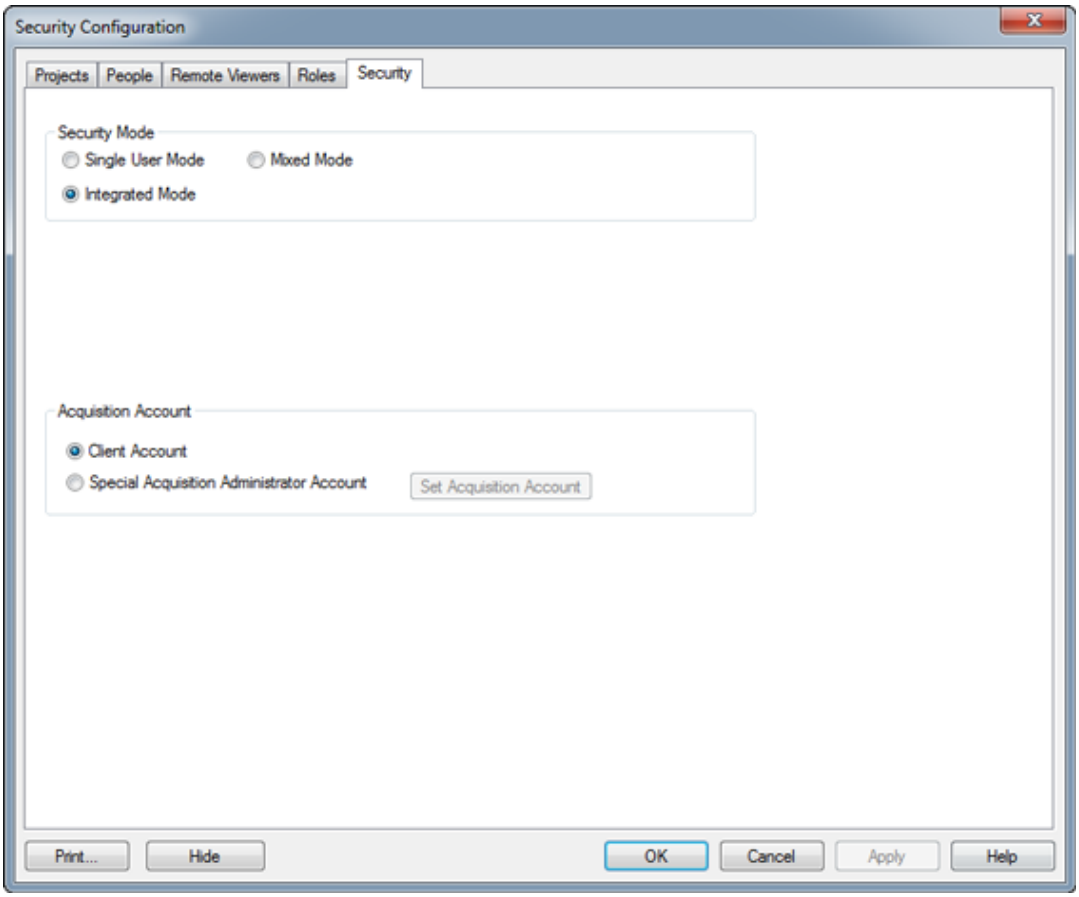
1. On the Navigation bar, under **Configure**, double-click **Security Configuration**.

Figure 5-1 Security Configuration Dialog: Projects Tab



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

Figure 5-2 Security Configuration Dialog: Security Tab



3. In the Security Mode group, click a mode and then click **OK**.
4. Start the Analyst MD software again.

Select an Acquisition Account

1. On the Navigation bar, under **Configure**, double-click **Security Configuration**.
2. Click **More** and then open the Security tab.
3. In the Acquisition Account group, select an acquisition account.
4. If **Special Acquisition Administrator Account** is selected, then do the following:
   a. Click **Set Acquisition Account**.
   b. Type the **User name**, **Password**, and if necessary, **Domain**, and then click **OK**.

   If Active Directory is being used in the native environment, then the domain field is not visible and the user name can be typed in UPN format.

5. Click **OK**.

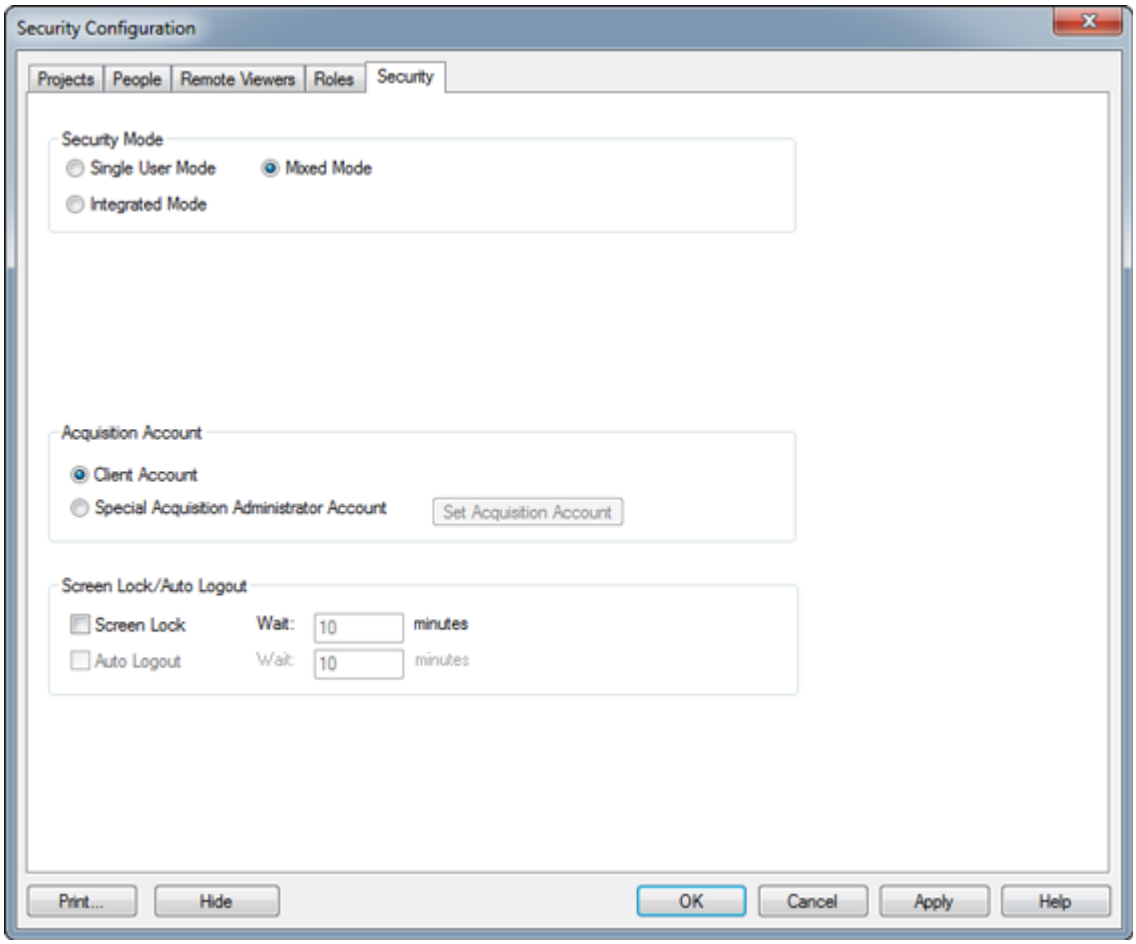
Set up Screen Lock and Auto LogOut

When the screen locks, the Unlock Analyst dialog opens, showing that the system has been locked, as well as the name and domain of the currently logged on user. If the auto logout option is also set, then the time remaining before the Analyst MD 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 MD 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 open the Security tab.
3. Click **Mixed Mode**.

Figure 5-3 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 MD 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.

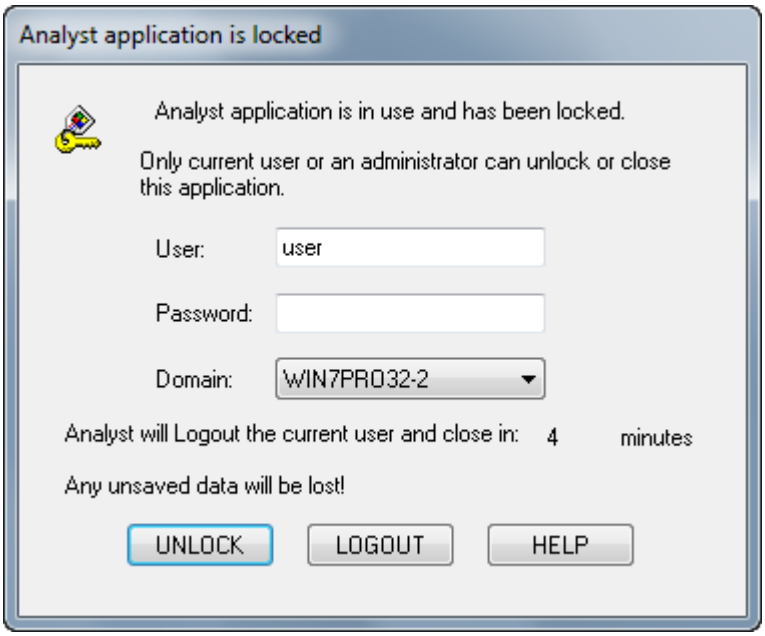
6. If required, select **Auto Logout** and, in the **Wait** field, type the number of minutes to elapse before the Analyst MD software client closes.

   The user has 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 MD software. The Unlock Analyst dialog also indicates the time left before the user is logged out.

Unlock or Log off from the Analyst MD Software

If the Screen Lock is enabled, the Unlock Analyst dialog opens after the Screen Lock time has elapsed.

Figure 5-4 Unlock Analyst Dialog



Do one of the following:

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

Access to the Analyst MD 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.

  Note: Every SCIEX computer is configured with a local Administrator-level account, **abservice**. This account is used by SCIEX service and technical support to install, service, and support the system. Do not remove or deactivate this account. If the account must be removed or deactivated, then prepare an alternate plan for SCIEX access, and communicate it to the local FSE.

- Add user groups containing groups that will have non-administrative tasks.
- Configure system permissions.
- Create suitable procedures and account policies for the users in Group Policy.

Refer to the Windows documentation for more information about 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 computer security. Discuss group policies with the Active Directory administrator as part of a comprehensive Analyst MD software deployment.

About People and Roles

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

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

An Analyst MD software administrator can add Windows users and groups to the Analyst MD 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 MD software roles can access Analyst MD software components.

Table 5-2 Analyst MD Software Roles

Role	Typical Tasks	Preset Access
Administrator	• Manages the system. • Configures security.	• All of the Analyst MD software functionality

Table 5-2 Analyst MD Software Roles (continued)

Role	Typical Tasks	Preset Access
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
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[1]) • Hardware Configuration • Report Template Editor • Sample Queue • Tune • View Status

[1] This feature is not supported in the Analyst MD software.

Table 5-2 Analyst MD 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[1]) • 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
Supervisor	Unlocks software or logs out user.	• Unlock and Logout Application

Analyst MD Software Access

Figure 5-5 Security Configuration Dialog

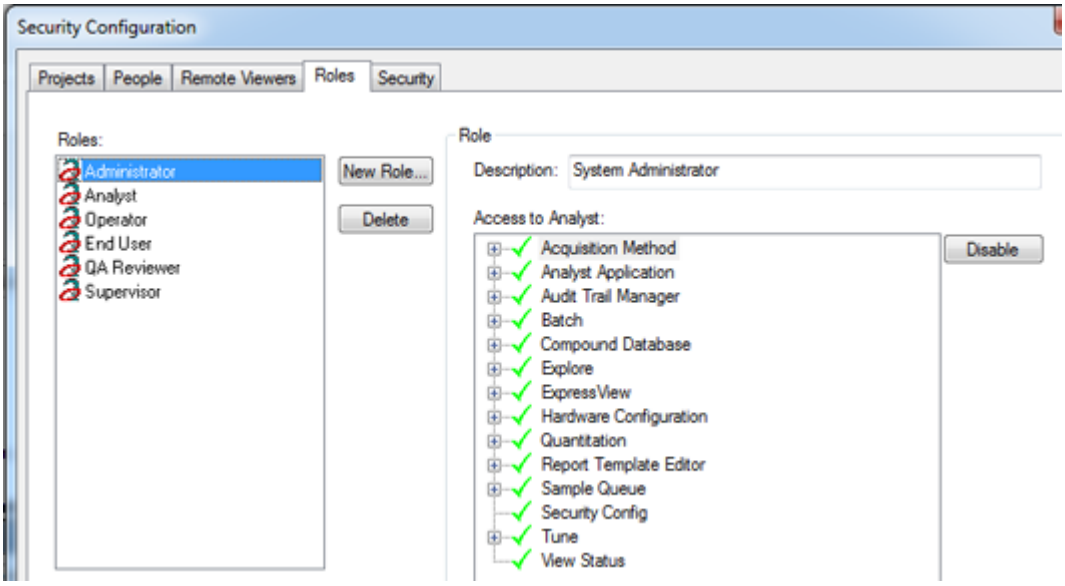


Table 5-3 Analyst MD Software Access to Acquisition Methods

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 5-4 Analyst MD Software Access to Analyst Application

Preset Access	Description
Use Workspace functions[2]	Allows users to use the Workspace functions.

Table 5-4 Analyst MD Software Access to Analyst Application (continued)

Preset Access	Description
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.
Lock/Logout Application	Allows the application to be automatically locked, or the user to be automatically logged out after the specified period of inactivity has elapsed. This functionality is only available in Mixed Mode and when the **Screen Lock** or **Auto Logout** option is selected.

Table 5-5 Analyst MD Software Access to Audit Trail Manager

Preset Access	Description
View Audit Trail Data	Allows users to view audit trail data. Disable access to this permission for all users except Administrators.
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 5-6 Analyst MD Software Access to Batch

Preset Access	Description
Open existing batches	Allows users to open existing batches.
Create new batches	Allows users to create batches.

Table 5-6 Analyst MD Software Access to Batch (continued)

Preset Access	Description
Import	Allows users to import data from existing batches (mdb or other supported 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.
Overwrite batches	Allows users to overwrite existing batches.
Overwrite template batches	Allows users to overwrite existing template batches.

Table 5-7 Analyst MD Software Access to Compound Database

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

Table 5-7 Analyst MD Software Access to Compound Database (continued)

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

Table 5-8 Analyst MD 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**.)

Table 5-8 Analyst MD Software Access to Explore (continued)

Preset Access	Description
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[2]

Table 5-9 Analyst MD Software Access to ExpressView*

Preset Access	Description
Start Express View dialog	Legacy setting[2]
Modify options	Legacy setting[2]

Table 5-10 Analyst MD Software Access to Hardware Configuration

Preset Access	Description
Create	Allows users to create a hardware profile.
Delete	Allows users to delete a hardware profile.

[2] This feature is not supported in the Analyst MD software.

Table 5-10 Analyst MD 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 5-11 Analyst MD 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.

Table 5-11 Analyst MD Software Access to Quantitation (continued)

Preset Access	Description
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.
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 in the Calibration Curve 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**.) Disable access to this permission for all users except Administrators.
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**.)

Table 5-11 Analyst MD Software Access to Quantitation (continued)

Preset Access	Description
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[2]
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**.)
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.

Table 5-11 Analyst MD Software Access to Quantitation (continued)

Preset Access	Description
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**.)
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 the 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.

Table 5-11 Analyst MD Software Access to Quantitation (continued)

Preset Access	Description
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[2]
Modify IS Concentration	Allows users to modify the IS concentrations in a Results Table.
Modify IS Units	Legacy setting[2]
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**.)

Table 5-12 Analyst MD 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.

Table 5-12 Analyst MD Software Access to Report Template Editor (continued)

Preset Access	Description
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 5-13 Analyst MD 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[2]	Allows users to pause the sample, immediately.
Insert Pause Before Selected Sample(s)[2]	Allows users to insert a pause before the next sample.
Continue Sample[2]	Allows users to continue (restart) the current sample.
Next Period[2]	Allows users to acquire the next period, immediately.
Extend Period[2]	Allows users to extend the period that is currently being acquired.
Next Sample[2]	Allows users to acquire the next sample.
Advance Pump Gradient	Legacy setting[2]
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[2]	Allows users to insert a pause in the queue.

Table 5-13 Analyst MD Software Access to Sample Queue (continued)

Preset Access	Description
Delete Sample or Batch	Allows users to delete a sample or a batch in the queue.
Move Batch	Allows users to change the batch order in the queue.

Table 5-14 Analyst MD 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.
Advanced Resolution Table Modification	Allows users to configure resolution using the Advanced button in the Resolution tab.
Auto TOF Mass Calibration	Legacy setting[2]

Table 5-15 Analyst MD 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.

Note: When creating or using formula columns, we recommend that users validate the formulas before use.

MultiQuant MD 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, then 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**.)

Preset Access	Description
Change default quantitation method integration parameters	In the Integration Default dialog, allows users to change the algorithm default parameters. (Click **Edit** > **Project Integration Defaults**.)
Allow Enable Project Modified Peak Warning	Allows users to activate or deactivate the flag that enables the Project Modified Peak Warning option on the Edit menu.
Add samples to Results Table	Allows users to add samples. (Click **Process** > **Add Samples**.)
Remove samples from Results	Table Allows users to remove selected samples. (Click **Process** > **Remove Selected Samples**.)
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.

Preset Access	Description
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
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.

Preset Access	Description
Create, use, or export Metric Plots in Results Tables	Allows users to create and use metric plots in the Results Table (Metric Plot button is enabled) or export metric plots. (Click **File** > **Export**.)
Set Peak Review Title Format	Allows users to modify the Peak Review Title Format in Peak Review. To perform this action, right-click in the Peak Review pane.
Add, Rename, or Modify custom column	Allows users to add, rename, or modify a custom column. Even without this permission, users can run queries that will automatically create custom columns.
Remove custom column	Allows users to delete a custom column in the Results Table.
Modify Results Table column settings	Allows users to modify Results Table column settings within a Results Table.
Save Column Settings as Project Default	Allows users to apply the column settings to the project.
Lock and save Results Table	Allows users to lock and save a Results Table.
Unlock and save Results Table	Allows users to unlock and save a Results Table.
Review and save Results Table	Allows users to review and save the Results Table.
Create or edit queries in Results Tables	Allows users to create or edit queries in a Results Table using one of the following options: • 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 the MultiQuant MD software is uninstalled, then the MultiQuant MD software security items in the Analyst MD software remain. Security items are found on the Roles tab in the Security Configuration dialog.

Add a User or Group to the Analyst MD Software

Note: Any changes to the Analyst MD software security configuration take effect after the Analyst MD software is restarted.

1. On the Navigation bar, under **Configure**, double-click **Security Configuration**.
   The Security Configuration dialog opens.
2. Open the People tab.
3. Click **New Person**.
   The Select Users or Groups dialog opens.
4. Add a user or group.
5. In the Available Roles pane, click a role and then click **Add**.
6. Click **Apply**.
7. Click **OK**.
   The Select Users or Groups dialog closes.
8. Click **OK**.
   The Security Configuration dialog closes.

Change a Role

1. On the Navigation bar, under **Configure**, double-click **Security Configuration**.
   The Security Configuration dialog opens.
2. Open 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**.
   The Security Configuration dialog closes.

Remove People from the Analyst MD Software

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

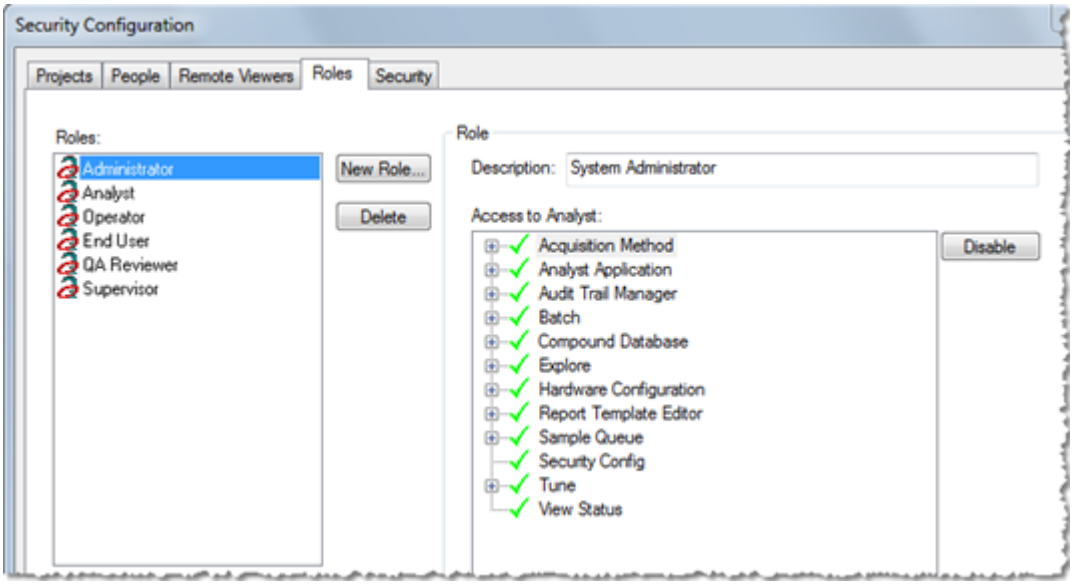
The Security Configuration dialog opens.

2. Open the People tab.
3. In the left pane, click the person to be deleted and then click **Delete**.
4. Click **Apply**.
5. Click **OK**.
   The Security Configuration dialog closes.

Create a Custom Role

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

Figure 5-6 Security Configuration Dialog: Roles Tab



3. Click **New Role**.
   The New Role dialog opens.
4. 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 MD 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**.
   The Security Configuration dialog closes.

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**.
   The Security Configuration dialog opens.
2. Click **More** and then open the Roles tab.
   The Roles pane opens.
3. Select the role and then click **Delete**.
4. Click **Apply**.
5. Click **OK**.
   The Security Configuration dialog closes.

Set Access

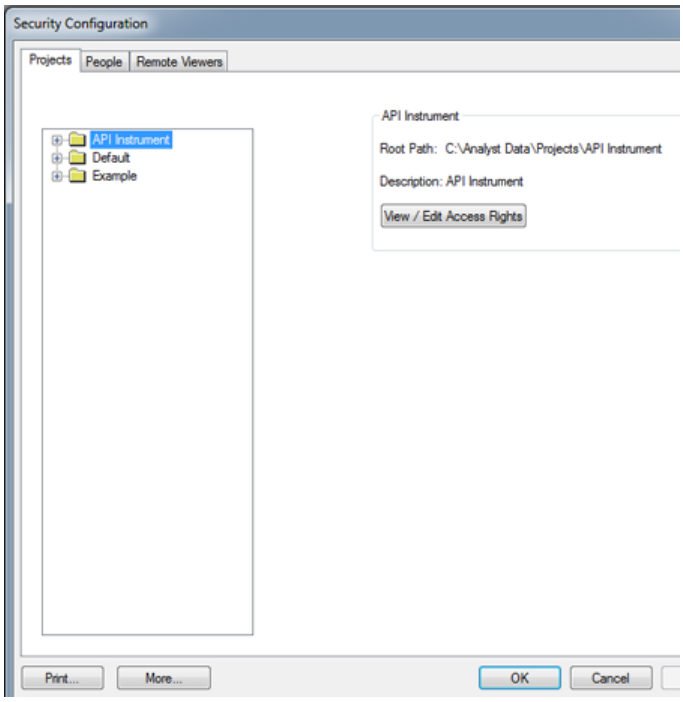
An administrator can configure access to projects and project files by person or group and control access by people or Windows security groups.

To use this feature of the Analyst MD software security, use NTFS for the work route. If the administrator does 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 the section: Windows Security Configuration.

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

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

Figure 5-7 Security Configuration Dialog: Projects Tab



2. In the left pane, click a folder or file.
3. Click **View/Edit Access Rights**.
   The Properties dialog opens.
4. Add or remove users or groups and set permissions as required, and then click **OK**.
5. Click **Apply**.
6. Click **OK**.
   The Select Users or Groups dialog closes.
7. Click **OK**.
   The Security Configuration dialog closes.

Project Folders

Each project contains folders that store different types of files. For information about the contents of the different folders, refer to the table: Table 5-16.

Table 5-16 Project Folders

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

Table 5-16 Project Folders (continued)

Folder	Contents
`\Acquisition Scripts`	Acquisition scripts are not available in the Analyst MD software. This folder is empty. The use of Analyst MD software scripting, which enables the creation of custom scripts (custom analyst operation sequences), should not be used as part of an *in vitro* diagnostic device. Inherent software checks that are conducted when using Analyst MD software are not executed on custom scripts and may lead to hazards.
`\Batch`	Contains all of the acquisition batch files that have been saved. Acquisition batches have the dab extension. This folder also contains a subfolder, `Templates`, that contains acquisition batch templates. Batch templates have the dat extension.
`\Data`	Contains the acquisition data files. These files have the wiff extension.
`\Log`	Contains results of quantitation and compound optimization.
`\Processing Methods`	Contains all qualitative data processing methods used.
`\Processing Scripts`	Contains two data processing scripts. 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

For common Analyst MD software file types, refer to the table: Table 5-17. The `API Instrument` folder contains all of the subdirectories, except `Processing Methods` and `Results`.

Table 5-17 Analyst MD Software Files

Extension	File Type	Folder
ata	Audit trail archives	`Project Information`
atd	• Instrument audit trail data • Instrument audit trail settings • Project audit trail data • Project audit trail settings	Project Information
cam	Audit map	`Project Information`
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`[3]
ins	Instrument data calibration information	`Instrument Data`[3]
log	Log records from automated collection	`Log`
mdb	MS Access database	—
pdf	Portable document data	—
psf	Parameter settings	`Parameter Settings`[3]
qmf	Quantitation method	`Quantitation Methods`
rdb	Results Table. Holds quantitation audit trail data	`Results`

[3] 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.

Table 5-17 Analyst MD Software Files (continued)

Extension	File Type	Folder
rpt	Report template	• `Templates\Batch` • `Templates\Method` • `Templates\ Report` • `Templates\Workspace`
rtf	Rich text format	—
sdb	Quantitation audit trail settings	`Project Information`
tun	Tuning preference file	`Preferences`[3]
txt	Text	—
wiff.scan	Mass spectrometry data file	• `Tuning` Cache[3] • `Data`
xls or xlsx	Excel spreadsheet	`Batch`

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 MD software on a client computer, configure the Windows firewall 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.

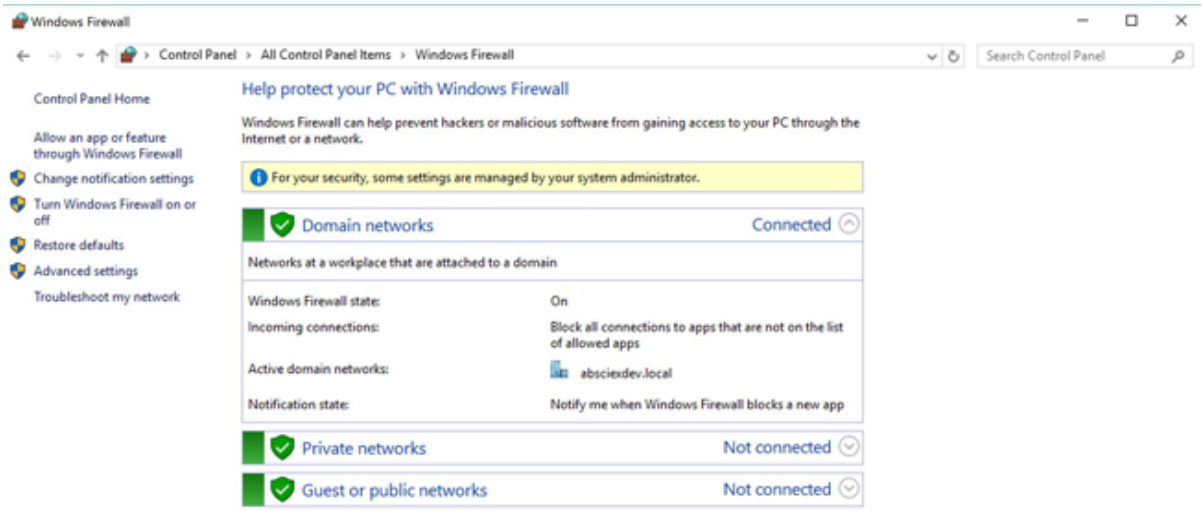
Note: On the acquisition computer, make sure to keep the queue page open after submitting a batch so that the queue can be viewed remotely from the client computer.

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. Open Control Panel and then open Windows Firewall.

Figure 5-8 Control Panel



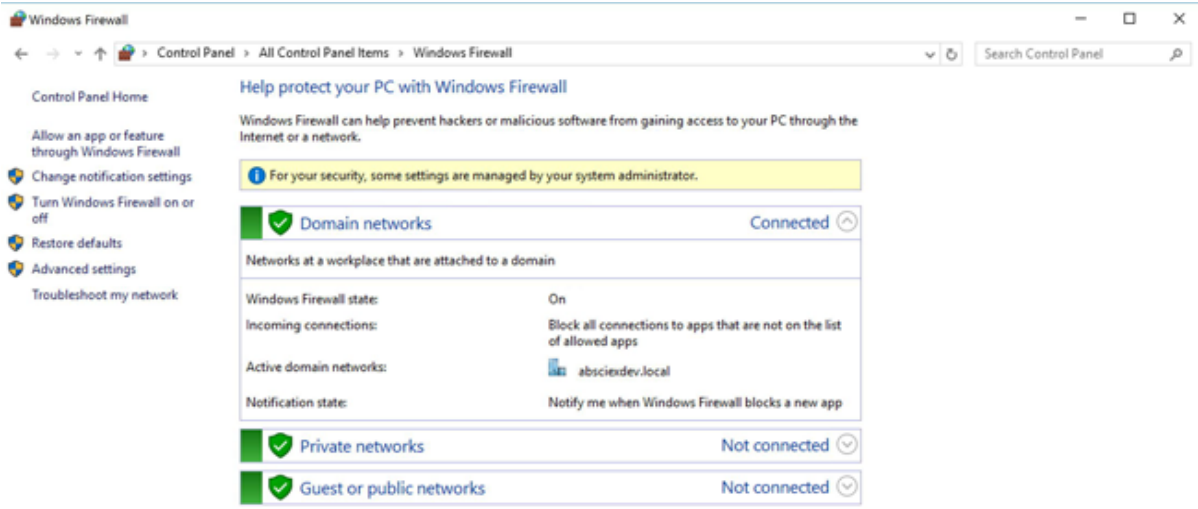
2. Click **Allow an app or feature through Windows Firewall** in the left pane.
3. Click **Change Settings.**
4. Click **Allow another app**.
   The Add an app dialog opens.
5. Click **Browse** and then browse to the `C:\Program Files(x86)\Analyst\bin` folder.
6. Click **AnalystService.exe** and then click **Open**.
7. Click **Add**.
   The AnalystService is added to the **Allowed apps and features** list.
8. If **AB SCIEX Analyst** is not already in the **Allowed apps and features** list, then add **Analyst.exe** by repeating steps 3 to 7. However, instead of selecting AnalystService.exe, select **Analyst.exe** in step 6.
9. Click **OK**.

Configure Windows Firewall on the Client Computer

If Analyst.exe is not in the Allowed apps and features list for the Windows firewall on the client computer, then add it.

1. Open Control Panel and then open Windows Firewall.

Figure 5-9 Control Panel



2. Click **Allow an app or feature through Windows Firewall** in the left pane.
3. Click **Change Settings.**
4. Click **Allow another app**.
   The Add an app dialog opens.
5. Click **Browse** and then browse to the `C:\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 apps and features** list.
8. Click **OK**.

Remote Workstations

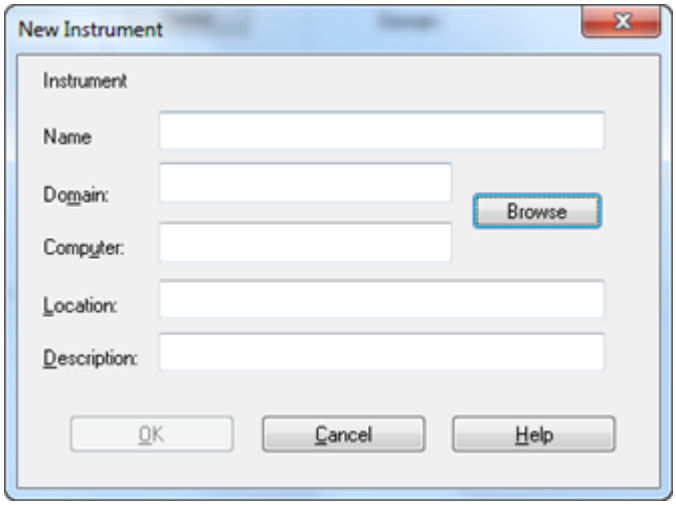
A list of mass spectrometers can be set up on a local computer and then the sample queues of those mass spectrometers can be remotely monitored. Users can only view the sample queue and the status of the mass spectrometers on these remote workstations. Even if they can perform other actions on the local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

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

Add Access to a Workstation

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

Figure 5-10 New Instrument Dialog



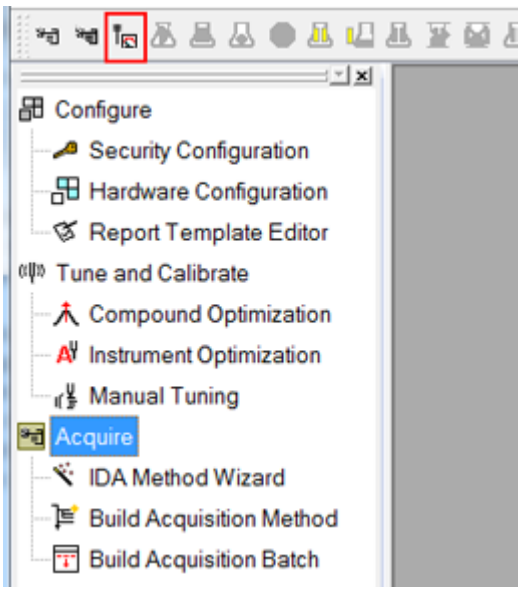
4. Type the workstation name in the **Name** field.
   If Active Directory is being used in the native environment, then the domain field is not visible and a user name can be typed in UPN format.
5. If required, type location information in the **Location** field.
6. Click **Browse** to browse to a **Domain** and **Computer**.
   The Select Computers dialog opens.
7. Select a mass spectrometer by clicking **Object Types**.
   The Windows Security dialog opens.
8. Type the domain credentials and then click **OK**.
   The Select Computers dialog is shown.
9. Click **Locations**.
   The Locations dialog opens.
10. Click the network where the remote acquisition computer is located and then click **OK**.
    The Select Computers dialog is shown.
11. Type the name of the acquisition computer in the **Enter the object names to select** box.
12. Click **Check Names**.

13. Click **OK**.
14. If required, type a description in the **Description** field in the New Instrument dialog.
15. Click **OK**.
    The acquisition computer name and the domain name are shown in the Remote Viewers tab.
16. Click **Apply**.
17. Click **OK**.
    The Security Configuration dialog closes.
18. Start the Analyst MD software again.

View Remote Instrument Status and Sample Acquisition Queue

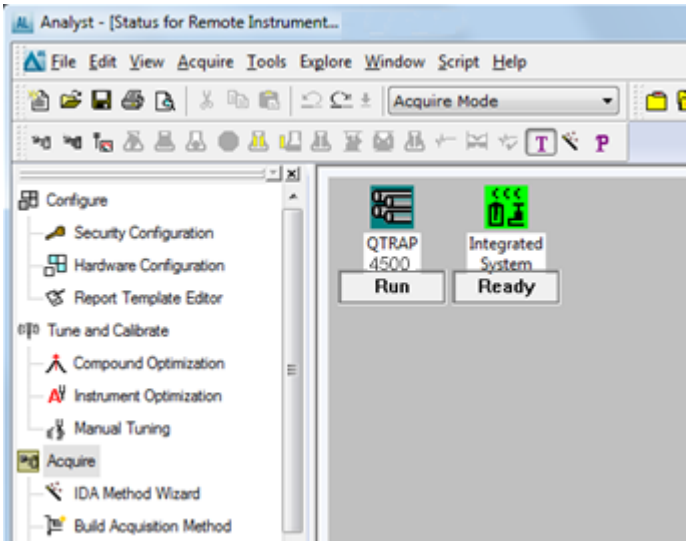
To remotely view the instrument and connected devices status and sample acquisition queue on the acquisition computer, use the **Status for Remote Instrument** icon in the Analyst MD software on the client computer.

Figure 5-11 Status for Remote Instrument Icon in the Analyst MD Software



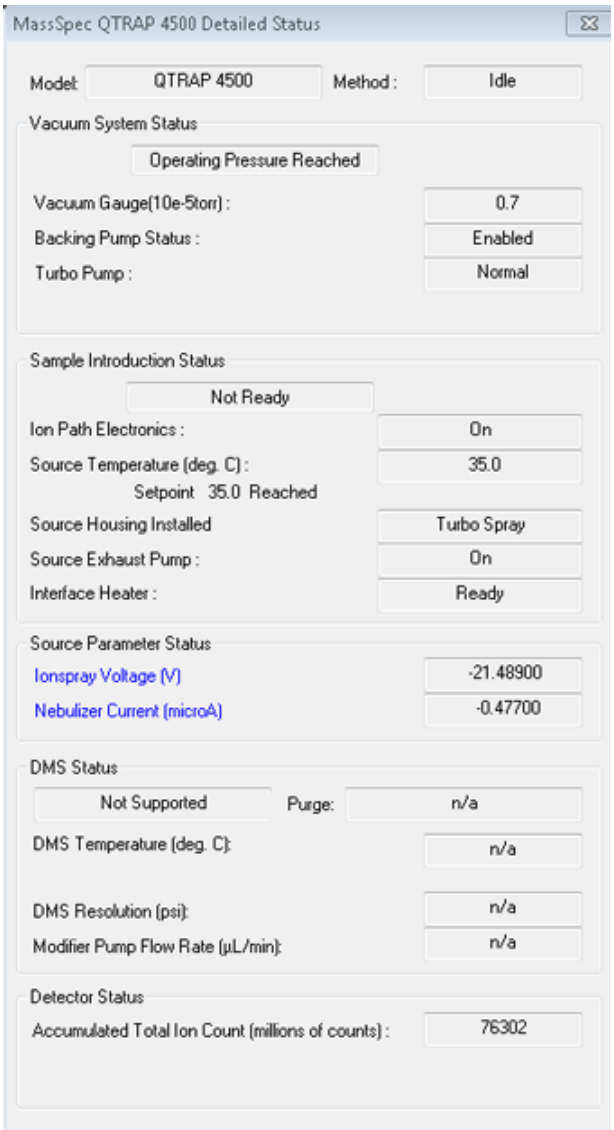
1. Log on to the Analyst MD software as the same domain-based user that was used to add the remote instrument in the Security Configuration dialog in Add Access to a Workstation.
2. In the Analyst MD software on the client computer, with **Acquire** mode selected, click the **Status for Remote Instrument**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

Figure 5-12 Remote Instrument Station and Integrated Device Shown in the Analyst MD Software



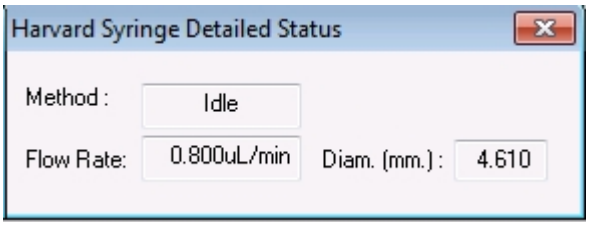
4. Double-click the remote instrument icon to view the detailed status.

Figure 5-13 Detailed Status of the Remote Instrument



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

Figure 5-14 Detailed Status for the Integrated Syringe

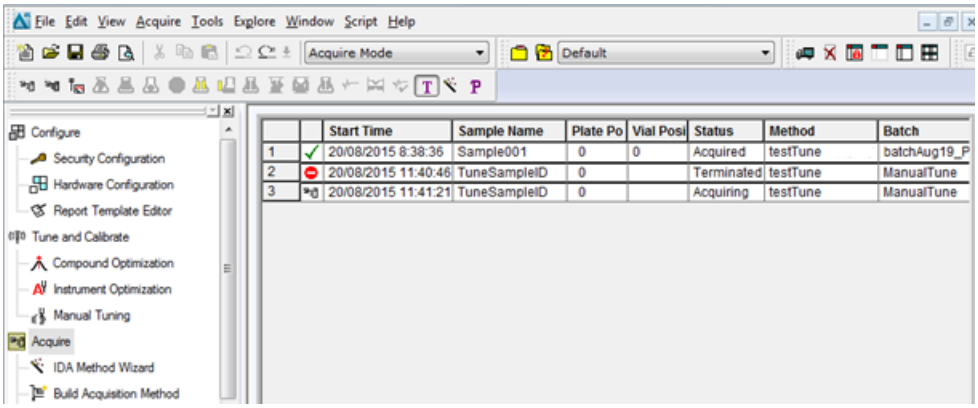


6. To view the sample acquisition queue on the acquisition computer, in **Acquire** mode, click the **Instrument Queue** icon on the toolbar in the Analyst MD software.

Note: The queue page must be open on the acquisition computer 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 MD software.

Figure 5-15 Sample Acquisition Queue on the Acquisition Computer



Remove Access to a Workstation

1. On the Navigation bar, under **Configure**, double-click **Security Configuration**.
2. In the Security Configuration dialog, open the Remote Viewers tab.
3. In the left pane, select a computer.
4. Click **Delete**.
5. Click **Yes** to confirm.
6. Click **OK** to close the Security Configuration dialog.

7. Start the Analyst MD software again.

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**.
   The Security Configuration dialog opens.
2. Click **Print**.
3. Click **Apply**.
4. Click **OK**.
   The Security Configuration dialog closes.

System Health Monitoring 6

Auxiliary Traces

The auxiliary traces for an LC system, such as the pump pressure trace and the column oven temperature trace, can be stored in the data file for each sample. These traces can be used to monitor the health of an LC system. The traces, especially the pump pressure trace, can also help to troubleshoot LC-related issues.

The axiliary traces feature is supported in Analyst MD software, version 1.7.3 and later.

Enable Auxiliary Traces

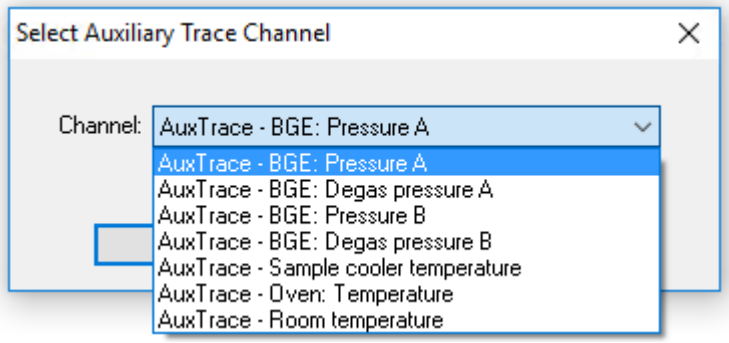
To enable the auxiliary traces feature, follow these steps when configuring the LC device in the hardware profile.

1. In the Create New Hardware Profile or Edit Hardware Profile dialog, select the LC system and then click **Setup Device**.
2. Select the **Enable Aux Trace Monitoring** check box.
3. Make sure that the LC system configuration is complete, and then click **OK**.
4. Activate the hardware profile.
5. Acquire data.

Show Auxiliary Traces

1. Make sure that the correct project folder is selected.
2. On the Navigation bar, under **Explore**, double-click **Open Data File**.
   The Select Sample dialog opens.
3. In the **Data Files** field, click the data file that was acquired after the auxiliary trace monitoring was enabled.
4. In the **Samples** list, select a sample, and then click **OK**.
5. Click **Explore** > **Show** > **Show Auxiliary Traces**.

Figure 6-1 Select Auxiliary Trace Channel dialog



6. In the **Channel** list, select a channel, and then click **OK**.
   The selected auxiliary trace is shown in a new pane below the active pane.

Injection Counter

With the injection counter, the user can monitor the number of sample injections on a given analytical column on a single LC-MS/MS system. This feature helps the user know when to switch column to prevent a batch re-run.

Enable the Injection Counter

1. Make sure that the system is in Standby state.
2. In **Configure** mode, click **Tools** > **Settings** > **Injection Counter Options**.
3. Select the **Enable Injection Counter** check box.
4. Complete a row for each analytical column on which injections will be counted.
   Each row contains the fields in the following table.

Table 6-1 Injection Counter Dialog Fields

Field	Description
Active	Select to enable injection counting for this analytical column. When this option is selected, the number of the injections on this analytical column is incremented by one for each injection. If column switching is used, then multiple analytical columns can be active at the same time.
Column Description	Type information to identify the column in reports and displays. Include information such as brand, type, particle size, column diameter, and column length.
Column S/N	Type the serial number of the analytical column.

Table 6-1 Injection Counter Dialog Fields (continued)

Field	Description
Number of injections	When configuring the injection counter settings, type the number of injections that have already been made on the analytical column. If the injection counter feature is enabled, then the software automatically increments this field during the operation of an LC system that has an autosampler.
Threshold	Type the number of injections that will trigger a warning. When the user submits a batch that will cause the number of injections to exceed this threshold, then a warning is shown. The user can then choose to continue or cancel the batch and use a different analytical column. Different active analytical columns can have different thresholds. **Note:** Make sure to update the injection counter settings after installing a different column.

5. To add additions analytical columns, click **+** and then repeat step 4.

Note: To remove an analytical column from the list, click the minus sign (**-**) to the right of the column.

6. Click **OK**.

Auditing 7

This section explains how to use the auditing functionality. For information about Windows auditing functions, refer to the section: System Audits.

Audit Trails

The Analyst MD 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 MD Software Audit Trails 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
			• On a new installation, Default Audit Map

Table 7-1 Analyst MD Software Audit Trails Audit Trails (continued)

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

Project (one per project)	• Changes to:
	  • Project
	  • Method
	  • Quantitation
	  • Batch
	  • Data
	  • Results Table
	  • Tuning
	  • 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 MD software automatically archives the records and begins a new audit trail. For more information, refer to the section: Audit Trail Records.

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.

Many audit maps can be created for the mass spectrometer and projects, but only one audit map can be used at a time for each acquisition computer 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, specify whether it is audited, if an electronic signature is required, and up to ten predefined reasons for the event.

When the user creates a new 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 the user creates 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 the active audit map (applied to the project) is changed, then the original audit configuration remains embedded in the Results Table file. The embedded configuration can be distinguished from the changed audit map by the last modified date and time shown on the Settings tab.

Setup of Audit Maps

Before working with projects that require auditing, configure audit maps that are appropriate to standard operating procedures. Several default audit maps are present when the Analyst MD software is installed, but one or more of them can be customized. At a minimum, make sure that one appropriate audit map is available for the Instrument Audit Trail and one appropriate audit map is available for each project.

Table 7-2 Checklist for Configuring Auditing

Task	Refer To
Create an audit map for the Instrument Audit Trail.	• Create an Audit Map. • Change an Audit Map.
Apply the audit map to the Instrument Audit Trail.	• Apply an Audit Map.
Create a default active audit map for new projects.	• Create an Audit Map. • Change an Audit Map.
Specify the default active audit map for new projects.	• Apply an Audit Map.

Table 7-2 Checklist for Configuring Auditing (continued)

Task	Refer To
Configure the audit map to be used for each existing project.	• Create an Audit Map. • Change an Audit Map. • Copy an Audit Map from Another Project.
Apply an audit map to each existing project.	• Apply an Audit Map.

Installed Audit Maps

The software includes several audit maps. To view or modify an installed audit map, refer to the section: Change an Audit Map.

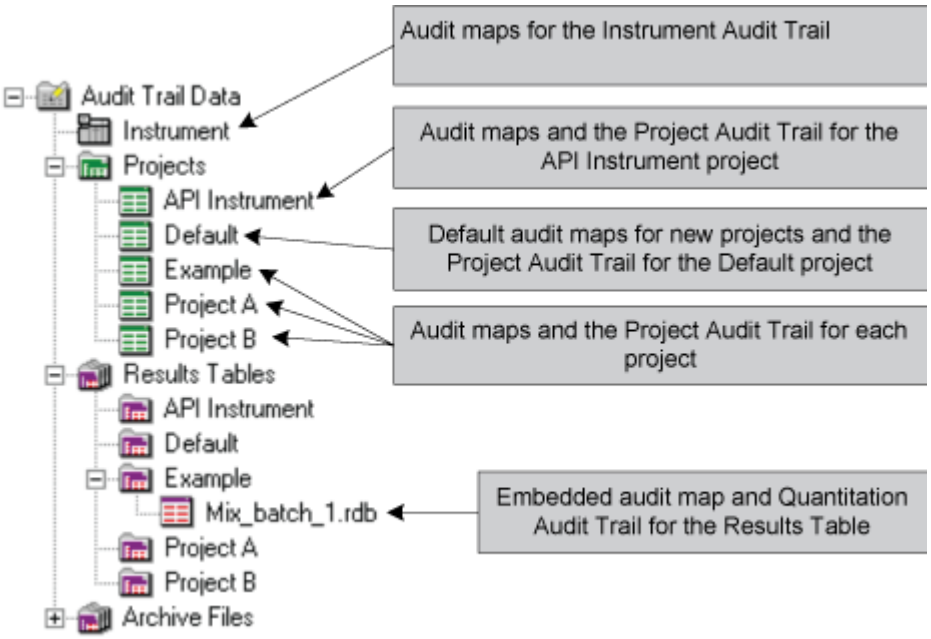
Table 7-3 Installed Audit Maps

Audit Map	Description
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 MD software. If the audit trail settings of a project created in a previous version of the Analyst MD software have been converted, then the default audit map contains that audit configuration.
Full Audit Map	All of the events are audited. Electronic signatures and reasons are required for all of the events.
No Audit Map	No events are audited.
Quant Only Audit Map	Only quantitation events are audited. These events require an electronic signature and a reason.
Silent Audit Map	All of the events are audited. Electronic signatures and reasons are not required for any events.

For descriptions of the types of audit trails and their relationships to audit maps, refer to the table: Table 7-1. For information about the events recorded in audit trails, refer to the section: Audit Trail Records.

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

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



For information about the auditing process, refer to the table: Table 7-2.

Work with Audit Maps

The Analyst MD 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 the section: Installed Audit Maps. For a checklist of suggested steps for setting up auditing, refer to the section: Setup of Audit Maps.

If an active audit map is deleted in the Analyst MD software or in File Explorer, then the project that uses that audit map uses the default audit map (`Default Audit Map.cam`). The default audit map cannot be deleted.

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.

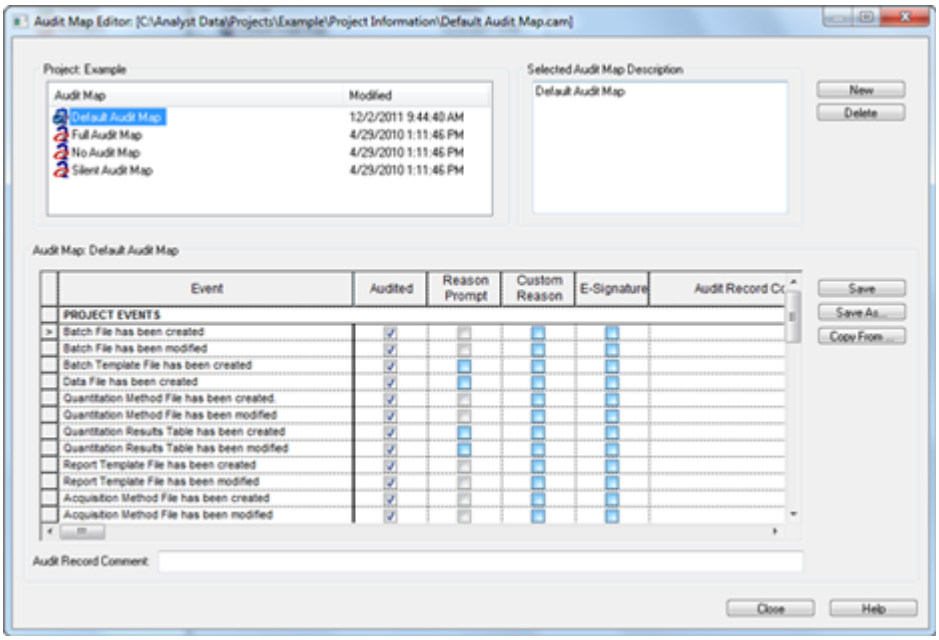
1. Click **View** > **Audit Trail Manager**.
   The Audit Trail Manager window opens.
2. In the left pane, expand the **Audit Trail Data** folder.
3. Expand the **Projects** folder.

4. In the Projects section, click the project for which an audit map is being created. To create an audit map for use with the Instrument Audit Trail, click the `API Instrument` folder.

   Tip! To create an audit map for use with the Instrument Audit Trail, click **Instrument** above the `Projects` folder.

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:

   - To audit the event, 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**.

- To require users 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.
- To require users 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.
- To require electronic signatures for the event, select the check box in the **E-Signature** column.
- To add a note about the audit configuration for this event, type a 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 it will be used.

   The audit map can now be used with the project or copied to another project. Refer to the sections: Apply an Audit Map) or Copy an Audit Map from Another Project).

Change an Audit Map

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

CAUTION: Potential Data Loss. Do not modify an audit map that is being modified by another user. Only the changes made by the last person to save the audit map 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 to be modified.
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 be modified.
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 MD 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 the audit map will be pasted.
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:
   - To apply an audit map to the **Instrument Audit Trail**, then click **Instrument**.
   - To apply an audit map to a project, expand the **Projects** folder and then click the project to which the audit map will be applied.

- To specify 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 to be applied.
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.

Tip!

- If an audited event refers to a wiff file, then open the wiff file from the **Audit Trail**. In the **Change Description** column, click the link to the file.
- To view the sample peak data using the quantitation method and sample index stored in an audit record, open the corresponding **Results Table** and then in the audit trail **History** column, click **Review**. If the quantitation method has been changed from the one used when the audit record was created, then different results might show for the peak than the original results. To see the original results, use the appropriate version of the software.

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

The user 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 1,000 audit records, the Analyst MD 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 to be viewed.
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! Alternatively, 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.

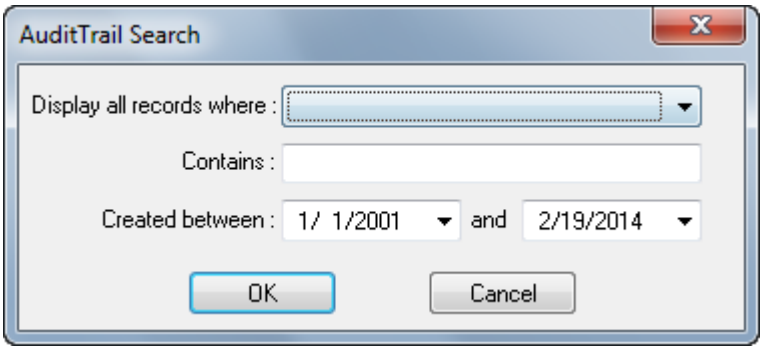
Print an Audit Trail

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 to be found.
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.

Audit Trails A

This section provides 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 MD software module
- Description of the change
- Reason for the change, if required
- Electronic signature, if required

Audit Trail Records

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

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 MD software module
- Description of the change
- Reason for the change, if required
- Electronic signature, if required

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 Events

Each computer has one Instrument Audit Trail. It records events such as additions or replacements to the mass calibration resolution tables, system configuration changes, security events, and entries in the Instrument Maintenance Log. For computers not directly connected to 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.[4]
- Hardware profile has been deactivated.[4]
- An Instrument Maintenance Log has been entered.
- Batch file submitted.[4]
- Sample submitted for acquisition.[4]
- Sample moved from position x to position y of Batch File.[4]
- Move batch.[4]
- Reacquiring sample(s).[4]
- Mass calibration table and resolution table changed.
- Resolution table(s) replaced - No Prompt.[4]
- Instrument settings have been changed.

[4] This event cannot be audited with a reason. It can be silently audited or not audited.

- Instrument calibration authorization.
- Mass calibration table(s) replaced.[4]
- User logged in.[4]
- User logged out.[4]
- User login failed.[4]
- Security sent notification.[4]
- The security configuration has been modified.[4]
- Duo valve switch counter reset.
- User added.[4]
- User deleted.[4]
- User type added.[4]
- User type deleted.[4]
- User type changed.[4]
- User mode changed.[4]
- User changed user type.[4]
- Acquisition account changed.[4]
- Screen lock changed.[4]
- Auto logout changed.[4]
- Instrument added.[4]
- Instrument deleted.[4]
- Project role added.[4]
- Project role changed.[4]
- Project role deleted.[4]
- Project security changed.[4]
- Tune parameter settings changed.[4]

Project Audit Trail Events

Each project has a Project Audit Trail. It records events such as the creation, modification, and deletion of projects, 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.[5]
- Audit map has been modified.[5]
- Audit map has been deleted.[5]
- Batch file has been created.[6]
- Batch file has been modified.[6]
- Batch template file has been created.[6]
- Data file has been created.[6]
- Quantitation method file has been created.[6]
- Quantitation method file has been modified.[6]
- Quantitation Results Table has been created.[6]
- Quantitation Results Table has been modified.[6]
- 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.[6]
- Closed module.[6]
- Sample has been added to data file.[6]
- Printing document on printer.
- Finished printing document on printer.[6]
- Data file has been opened.[6]
- Explore history file has been saved.
- Processed data file has been saved.
- Checksum file.[6]
- Project settings have been changed.[7]
- The processing algorithm has been changed.[6]

[5] This event is always silently audited and does not appear in the Audit Map Editor dialog.
[6] This event cannot be audited with a reason. It can be silently audited or not audited.
[7] This event is always audited.

Quantitation Audit Trail Events

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 changed 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.

AAC Audit Trail

Each Analyst Administrator Console (AAC) server has a corresponding audit trail. This feature is not supported in the Analyst MD software.

Additional Security Customization B

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

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 an Explore Processing History file is created, it cannot be modified or deleted within the Analyst MD software.

After saving the history of the changes to a data file, use this history to view the data file at any point during the changes. Users 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 MD 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 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, open 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 open the History tab in the right pane.
   The audit trail opens.
5. For the record for the Instrument Maintenance Log entry to be viewed, 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

The Analyst MD software can be configured 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 software is in Integrated or Mixed Mode. For information about security modes, refer to the section: Analyst MD Software and Windows Security: Working Together.

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 MD 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 the message is to be sent. For example: username@domain.com.

7. In the **From** field, type the name to be shown in the **From** field of the message. For example, type the name of the computer to keep a record of 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**.

Note: If the email notification is not received in the **Inbox**, then check the **Junk E-mail** folder.

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 MD software. If users upgrade to the current version of the Analyst MD software, then their checksum setting before the upgrade is maintained.

The checksum feature must be used if the mass spectrometer is used as an in vitro diagnostics device.

If the Data File Checksum feature is enabled, then whenever the user creates a data (wiff) file, the software generates a checksum value using an algorithm based on the MD5 public encryption algorithm and saves the value in the file. When the checksum is verified, the 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 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 the file was saved when the Data File Checksum feature was disabled.

Verify Data File Checksum

Whenever a data file is opened, the user 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 large data files. During acquisition, the checksum of the file that is being created cannot be verified.

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

   The ExplorDir message dialog opens showing the result of the checksum comparison as Valid, Invalid, or Not found.

Enable or Disable the Data File Checksum Feature

The Analyst MD 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 the Data File Checksum feature is enabled, then a check mark is shown next to the command. If the Data File Checksum feature is disabled, then the check mark disappears.

Special Acquisition Account C

Note: SCIEX does not support the use of the network acquisition feature with the Analyst MD software.

In a regulated environment where data is being acquired to a network folder, most users usually do not have delete rights for the destination folder. This can cause issues because the Analyst MD software requires delete access to successfully acquire data to a network folder.

The special acquisition account (SAA) functionality supports network acquisition in a closed network environment by giving delete rights only to the AnalystService. To enable this functionality, the laboratory administrator creates an account with Full control permission for the appropriate folders, and then specifies that account in the Special Acquisition Administrator Account group in the Security Configuration dialog in the Analyst MD software. The Analyst MD software can then acquire data successfully, even though most users do not have delete rights. For information about selecting an acquisition account, refer to the section: Select an Acquisition Account.

The SAA must have:

- Full Control (recommended) or Modify (minimum) permission for the server data folder.
- Full Control (recommended) or Modify (minimum) permission for the `WIFF_CACHE_BACKUP` folder.

The SAA does not need to:

- Belong to the Administrator group on the computer.
- Belong to the Analyst Administrator Console (AAC) User Pool, the Console Administrators workgroup, or any other workgroup.
- Be in the Analyst MD software security database.

Contact Us

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 Now Learning Hub

SCIEX 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 SCIEX website at sciex.com or contact us in one of the following ways:

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

CyberSecurity

For the latest guidance on cybersecurity for SCIEX products, visit sciex.com/productsecurity.

Documentation

This version of the document supercedes all previous versions of this document.

To view this document electronically, Adobe Acrobat Reader is required. To download the latest version, go to https://get.adobe.com/reader.

To find software product documentation, refer to the release notes or software installation guide that comes with the software.

To find hardware product documentation, refer to the *Customer Reference* DVD that comes with the system or component.

Note: To request a free, printed version of this document, contact sciex.com/contact-us.