People and Security

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

Topics in this section:

Security Modes

The Analyst® software provides three security modes: single-user, integrated, and mixed. Each mode offers slightly different security features. How you use the software should determine your choice of security mode.

Note: Any changes to the security configuration take effect after the software has been restarted.

Topics is this section:

About Security Modes

Situation	Recommended Mode	Method of Access
Only one user of the Analyst® software. or No particular security measures required.	Single User Mode	This mode treats the current user that is logged on to Windows as an Analyst software Administrator with full access to all Analyst software functionality. Anyone who can successfully log on to Windows on the computer will have Analyst software Administrator privileges.
Analyst software users who use an individual username and password to log on to the computer.	Integrated Mode	This mode allows the current user who is logged on to Windows to have access to the Analyst software, providing that the Windows user is also a valid Analyst software user.
Multiple Analyst software users who use the same username and password to log on to Windows.	Mixed Mode	This mode allows the user that is logged on to the Analyst software to be different (or the same) as the current user that is logged on to Windows. The logged on user in the Analyst software can be assigned to a specified role in the same way as in Integrated Mode. This allows you to have a group log on for Windows using a common password, while requiring the Analyst software user to log on to the Analyst software program using his/her own unique user id and password. If you select Mixed Mode, the Screen Lock/Auto Logout feature is enabled for use.

Selecting a Security Mode

Before you select a security mode, consider your security requirements and read about the different security modes that the software offers.

1. **On the Navigation bar, under Configure, double-click Security Configuration.**
2. **In the Security Configuration dialog, click More.**
3. **Click the Security tab.**
4. **In the Security Mode group, click a mode and then click OK.**
5. **Restart the software.**

Selecting an Acquisition Account Mode

1. **On the Navigation bar, under Configure, double-click Security Configuration.**
2. **In the Security Configuration dialog, click More.**
3. **Click the Security tab.**
4. **Select an Acquisition Account option: Client account or Special Acquisition Administration Account.**
5. **If you clicked Special Acquisition Administration Account, the Set Acquisition Account button is enabled.**
6. **To set the Special Acquisition Administration Account, click Set Acquisition Account.**
7. **Type the User name, Password, and if necessary, Domain, and then click OK.**

   If you are using Active Directory in the Native environment, the domain field is not visible and you can type the user name in user principal name (UPN) format.
8. **Click OK.**

Logging in to the Software

Active Directory

If you are using Active Directory in the native environment, the domain field is not visible and you can enter your username in user principal name (UPN) format.

If you are using Active Directory in the mixed environment, you have the option of entering your username in UPN format or normal domain format, depending on which server you are logging on to. If authentication is successful, the Analyst® software will start in the security context of the Analyst software user, not the security context of the currently logged on Windows user.

Analyst Software Security Modes

The Windows Logon dialog controls access to the Analyst software. If the Analyst software is configured to use Integrated Mode, access rights to the Analyst software depend on the user's Windows login and his or her Analyst software security profile.

If you configure the Analyst software to use Mixed Mode security, a user who is not currently logged on to Windows, may log on to the Analyst software without requiring the current Windows user to log out. The user is required to enter a user name, password, and if required, a domain. After three unsuccessful logon attempts, notification is sent to a designated person such as the System Administrator.

If you configure the Analyst software to use Single User Mode security, full administrator access to the Analyst software functionality is granted to anyone who logs on to the workstation.

Logging in to the SQL*LIMS Software

If you are running Analyst® software with the SQL*LIMS software, you must log into the SQL*LIMS application to import or export data to or from SQL*LIMS.

1. In the SQL*LIMS Login dialog, type your SQL*LIMS user name and password.
2. Type your Oracle host string (host name).
3. Select Use OPS$ prefix during logon to automatically append your OPS$ prefix to your SQL*LIMS password.
4. To avoid having to log into the SQL*LIMS application each time the Analyst software needs to query the database, select Remember password for the current session.
5. Click OK. If the current SQL*LIMS user has multiple job types, the Job Type dialog appears.
6. Select the appropriate job type for the current session, and then click OK.

Setting up Software Security

Configure security at the following levels:

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

Topics in this section:

Setting Access Rights to Analyst Software Functionality for User-Defined Roles

Access rights to functionalities in the Analyst® software are set up according to roles. Once a role is defined, a person or people with that role can be granted access to specific components and functionality. Thus, the System Administrator can choose to give a person or people access to functionality and components that are necessary for their particular activities.

1. On the Navigation bar, under Configure, double-click Security Configuration.
2. In the Security Configuration dialog, click More.
3. Click the Roles tab.
4. In the Roles window, click the Role to be configured.
5. In the Access to Analyst window, select the access requirement, and then click the Enable / Disable toggle button.
6. Double-click components in the Access Rights list to enable or disable access as appropriate. To configure access at a functional level, expand the components, and then double-click the functionality to enable or disable it.
7. Click OK.

Setting Access Rights to Projects

Note: When a project is created using the Analyst® software, by default everyone has access to the project, including the project folders and subfolders.

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

   The Projects tab is the default tab.
2. In the left window, click the folder or file.
3. Click View / Edit Access Rights.
4. In the properties dialog, add users or groups and set permissions as required.
5. Click OK to close the Security Configuration dialog.

Adding Access to Remote Instrument Stations

The Analyst® software administrator can select various instrument stations on the network to be accessible by users of the local computer. Users can then view the sample queue and status of the instruments on these remote instrument stations. Even if their role allows them to perform other actions on the local workstation, they cannot perform them on a remote workstation. This procedure describes how to configure access to an instrument through the Remote Viewers tab.

Note: If the workstation is registered with the Administrator Console server, the buttons on the Remote Viewer tab are not available.

1. On the Navigation bar, under Configure, double-click Security Configuration.
2. In the Security Configuration dialog, click the Remote Viewers tab.
3. Click Add.
4. Type the workstation name in the Name field.
5. To select a Domain and Computer, click Browse.
6. Using the Select Computers dialog, select an instrument.
7. If required, type location information in the Location field.
8. If required, type a description in the Description field.
9. Click OK.
10. Click OK to close the Security Configuration dialog.

Removing Access to Remote Instrument Stations

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

6. Click OK to close the Security Configuration dialog.

About Screen Lock and Auto Logout

Screen lock and auto logout are available in Mixed mode. The Administrator can set the screen lock and auto logout time. Once locked, only the currently logged on user, the Administrator, or the Supervisor can either unlock the Analyst® software or log off the Analyst software.

- Screen lock: After a defined period of inactivity, the screen will lock. The Unlock Analyst dialog indicating that the system has been locked, as well as the currently logged on user name and domain, is displayed. The Unlock Analyst dialog also indicates the time left before you are logged out.
- Auto logout: If the screen is not unlocked, after a defined period, the Analyst software client will close and all unsaved data will be lost.

Setting Screen Lock and Auto Logout

1. On the Navigation bar, under Configure, double-click Security Configuration.
2. In the Security Configuration dialog, click More.
3. Click the Security tab.
4. Click Mixed Mode.
5. Select Screen Lock.

   The Auto Logout and Wait fields are enabled.
6. In the Screen Lock Wait field, type the number of minutes to elapse before the screen locks. After a defined period of inactivity, the screen will lock. The Unlock Analyst dialog indicating that the system has been locked, as well as the currently logged on user name and domain, is displayed. The Unlock Analyst dialog also indicates the time left before you are logged out.
7. If required, select Auto Logout, and in the Wait field, type the number of minutes to elapse before the Analyst® software client closes. If the screen is not unlocked, after a defined period, the software client will close and all unsaved data will be lost.

   After the screen lock time has elapsed, the Unlock Analyst screen appears. You have a 10 second grace period to move the mouse or press a key to clear the Unlock Analyst dialog. Only the currently logged on user, Administrator, or Supervisor can either unlock the screen or log out the user.

   Note: If you are automatically logged out, the Analyst software client closes and all unsaved data will be lost.
8. To unlock the screen, type your password, and then click UNLOCK.
9. To log out the user, type your user name if necessary and password and then click LOGOUT.

Setting up Access to the Software

The Analyst® software limits access to people authorized to log on to the workstation and to the Analyst software, using their Windows user name and password for both, except when using Mixed mode. The Analyst software does not allow multiple sessions. Before you can assign a person to a specific role, you must first add the person to the Analyst software. You can assign either a predefined or user-defined role to a person or groups.

Topics in this section:

Adding People to the Software

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

Deleting People from the Software

The system administrator should delete any users who no longer need access to the system.

1. On the Navigation bar, under Configure, double-click Security Configuration.
2. In the Security Configuration dialog, click the People tab.
3. In the left window, highlight the Person/People to be deleted and then click Delete.
4. Click Yes to confirm.
5. Click OK to close the Security Configuration dialog.

Creating a User-Defined Role

You can create new roles and configure system requirements depending on your own specific requirements.

1. On the Navigation bar, under Configure, double-click Security Configuration.
2. In the Security Configuration dialog, click More.
3. Click the Roles tab.
4. Click New Role.
5. Type the Role Name and Description, and then click OK.

   Note: By default, a user-defined role will have full access rights to the Analyst® software. In the Access to Analyst window, a green check mark denotes system access is enabled; a red "X" denotes system access is disabled.
6. To set access rights, double-click components in the Access to Analyst list to enable or disable access as appropriate.

   Tip: To configure access at a functional level, expand the components, and then double-click the functionality to enable or disable it.
7. Click OK to close the Security Configuration dialog.

Assigning People to Roles

You can assign either a predefined or user-defined role to a person or groups.

1. On the Navigation bar, under Configure, double-click Security Configuration.
2. In the Security Configuration dialog, click the People tab.
3. In the left window, select the Person.
4. In the Available Roles window, highlight the required Role, and then click Add.
5. Click OK to close the Security Configuration dialog.

Removing People from Roles

You can remove a person or people from roles if their access to Analyst® software components is no longer required.

1. On the Navigation bar, under Configure, double-click Security Configuration.
2. In the Security Configuration dialog, click the People tab.
3. In the left window, select the Person.
4. In the Role(s) Selected window, highlight the required Role, and then click Remove.
5. Click OK to close the Security Configuration dialog.

Deleting a User-Defined Role

If you no longer require a user-defined role, you can delete it.

Note: If you have one person assigned to a single role, and that role is to be deleted, you will be asked if you want to delete the person as well as the role.

---

1. On the Navigation bar, under Configure, double-click Security Configuration.
2. In the Security Configuration dialog, click More.
3. Click the Roles tab.
4. In the Roles window, highlight the Role to be deleted, and then click Delete.
5. Click Yes to confirm.
6. Click OK.

Auditing

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

Topics in this section:

- Audit Maps
- Audit Trails
- Audit Records

Audit Maps

The active audit map in a project contains the auditing configuration for the Project Audit Trail.

Topics in this section:

- Applying Audit Maps
- Creating Audit Maps
- Modifying Audit Trail Maps
- Copying Audit Trail Maps
- About Using Audit Maps with Projects Created in Previous Versions of Analyst Software

Applying Audit Maps

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

1. Click View > Audit Trail Manager.

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

Creating Audit Maps

The software includes several installed audit maps. View them first to see if modifying one or more of them is easier than creating a completely new one.

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

Note: Some events cannot be audited with a reason. They can only be silently audited or not audited.

---

1. Click View > Audit Trail Manager.

   The Audit Trail Manager window appears.
2. In the left pane, expand the Audit Trail Data folder and then expand the Projects folder.
3. Under Projects, click the project for which you want to create an audit map, or if you are creating an audit map for use with the Instrument Audit Trail, click the Instrument folder.
4. In the Settings tab, click Edit.

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

5. Click **New**.

   The Audit Map Editor dialog displays a new audit map with all events audited.

6. If required, in the Selected Audit Map Description field, type a description of the audit map.

   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**.

7. In the Audit Map table, configure each event as follows:
   - If you want the event to be audited, select the check box in the Audited column.
   - If you want the operators to specify a predefined reason for the change when the event occurs, select the check box in the Reason Prompt column and then in the Predefined Reason columns, specify up to ten reasons.
   - If you want to allow the operators to type a custom reason, make sure that the check box in the Reason Prompt column is selected, and then select the check box in the Custom Reason column.
   - If you want to require electronic signatures for the event, select the check box in the E-Signature column.
   - If you want to make a note about the audit configuration for this event, in the Audit Record Comment column, type your comment.

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

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

   Now that you have created an audit map, you can use it with your project using the procedure, To apply an audit map or you can copy it to another project using the procedure, To copy an audit map to another project.

Modifying Audit Trail Maps

You may want to change the audit configuration of an audit map it you want to apply it to a different audit map, or you might want to modify an installed audit map to better suit your needs. If you copy an audit map to another project or if another audit map with the same name exists in a different project, any changes you make will only apply to the audit map in the project you select. Audit configuration embedded in Results Tables cannot be modified.

CAUTION! If you and someone else are modifying the same audit map at the same time, only the changes made by the person who saved the file last will be used.

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

   The Audit Trail Manager window appears.

2. In the left pane, expand the Audit Trail Data folder and then the Projects folder.
3. Under **Projects**, click the project that contains the audit map you want to modify.
4. In the **Settings** tab, click **Edit**.

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

5. Under **Project**, click the audit map you want to modify.
6. In the Audit Map table, make any changes you want to the configuration.
7. To save the audit map, click **Save**.

Copying Audit Trail Maps

If you have an existing audit map in one project that you want to use for another project, you can copy the audit map from the original project to the other project.

CAUTION! We do not recommend copying .cam files (audit maps) between projects outside of the Analyst® software. Doing so may cause inaccurate audit trails.

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

   The Audit Trail Manager window appears.

2. In the left pane, expand the Audit Trail Data folder, and then expand the Projects folder.
3. Under **Projects**, click the project into which you want to copy the audit map.
4. In the **Settings** tab, click **Edit**.

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

5. Click **New**.
6. The Audit Map Editor dialog displays a new audit map with no events audited. Click **Copy From**.

   The Open dialog appears.

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

   The selected audit map configuration appears.

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

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

When you work with a project that was created in a previous version of the Analyst® software (one that does not use audit maps), the project's audit trail settings will be converted to an audit map and saved in a new audit map file called Default Audit Map. The Project Audit Trail and Quantitation Audit Trail (for new Results Tables) for that project will use the configuration in this new audit map. A project's audit trail settings are converted when an auditable event occurs. A message appears to tell you that the project's audit trail settings have been converted. Note that the settings may also be silently converted to an audit map if you run a script on the project without ever opening the project.

CAUTION! Because audit maps are not supported in previous versions of the Analyst software, We do not recommend opening a project that uses an audit map in a previous version of the Analyst software. Events may not be audited according to the audit map.

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

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

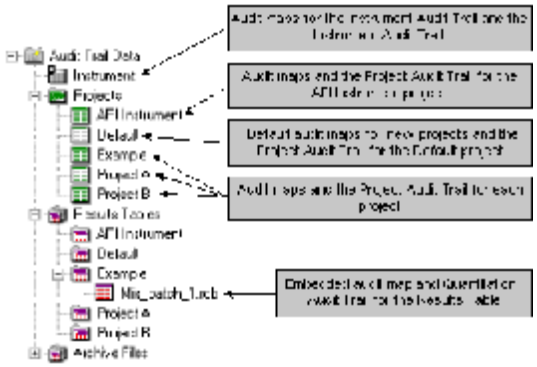
Audit Trails

Descriptions of the three types of audit trails and their relationships to audit maps are summarized in the following table. For more information about the events recorded in audit trails, see **Audit Records**.

Software Audit Trails

Audit Trail	Examples of Events Recorded	Available Audit Maps Stored In	Default Audit Maps
Instrument (one per workstation)	Changes to instrument resolutions, mass calibrations, sample queues, security, and hardware profiles; instrument maintenance log entries	API Instrument project, Project Information folder	N/A
Project (one per project)	Changes to project, data, quantitation, method, batch, tuning, Results Table, and 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 creation and modification of quantitation methods, sample information, and peak integration parameters in Results Tables	Results Table file (.rdb file)	Copied from parent project

The locations of the audit maps and audit trails in the Audit Trail Manager, the component of the software where you configure auditing, are shown in the following figure.



Topics in this section:

- Viewing an Audit Trail
- Viewing an Archived Audit Trail
- Viewing Details for an Audit Record in the Instrument Audit Trail
- Reviewing Peak Integration from a Quantitation Audit Trail
- Printing an Audit Trail
- Viewing the Audit Configuration Embedded in a Results Table
- Creating an Instrument Maintenance Log Entry
- Viewing the Instrument Maintenance Log

Viewing an Audit Trail

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

   The Audit Trail Manager window appears.
2. In the left pane, expand the **Audit Trail Data** folder, and then do one of the following:
   - If you want to view the Instrument Audit Trail, click the **Instrument** folder. To view instrument-specific events, such as Mass Calibration Table(s) Replaced, you must view the Instrument Audit Trail that is recorded on the computer that is directly connected to the instrument.
   - If you want to view a Project Audit Trail, expand the Projects folder, and then click the project that contains the audit trail you want to view.
   - If you want 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 you want to view.

     In the right pane, the History tab appears displaying the audit trail.

Tips:

- You can open a .wiff file from the audit trail if an audited event refers to a .wiff file. 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, you may see different results for the peak than the original results. To see the original results, use the appropriate version of the Analyst® software.

Tip: You can also view the audit trail of a Results Table after opening the Results Table. Click **Tools > Audit Trail > Show.**

Viewing an Archived Audit Trail

Once the Instrument Audit Trail or a Project Audit Trail contains 1000 audit records, the Analyst® software automatically archives the records and begins a new audit trail.

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

   The Audit Trail Manager window appears.
2. In the left pane, expand the **Audit Trail Data** folder, and then expand the **Archive Files** folder.
3. Under **Archive Files**, expand the project that contains the archived audit trail you want to view.
4. Click the audit trail you want to view. The archived audit trail files are named with the type of audit trail and the date and time.

   The archived audit trail appears in the right pane.
5. If the audit trail does not appear, in the right pane, click the **History** tab.

   The audit trail appears.

   You can also open an archived audit trail by right-clicking in the left pane and then clicking **Open Archives**. These files have the extension .ata.

Viewing Details for an Audit Record in the Instrument Audit Trail

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

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

   The Audit Trail Manager window appears.

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

   The audit trail appears.
5. For any record that has additional details, in the History column, click Review.

Reviewing Peak Integration from a Quantitation Audit Trail

Tip: Open Results Tables are indicated in the Audit Trail Manager by an icon highlighted in blue.

1. Open a Results Table.
2. In the History column of the appropriate Quantitation Audit Trail record, click Review. The Review link appears if the area of a peak was changed by modification of the integration parameters or by manual integration.

   The software displays the peak as it appeared before the modification and displays the Quantitation History dialog.

   Note: The Results Table cannot be modified during the review.
3. In the Quantitation History dialog, use the arrow buttons to move to previous and next audit records.

   The display updates to show the relevant data and peak.

Printing an Audit Trail

1. In the Audit Trail Manager, view the audit trail you want to print.
2. In the History tab, right-click, point to Print, and then do one of the following:
   - To print the current page, click Current Page.
   - To print all the pages in the audit trail, click All Pages.

Viewing the Audit Configuration Embedded in a Results Table

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

1. Click View > Audit Trail Manager.

   The Audit Trail Manager window appears.
2. In the left pane, expand the Audit Trail Data folder and then the Results Tables folder.
3. Under Results Tables, expand the project that contains the Results Table and audit map that you want to view.
4. To view the audit map, click the Results Table.

   The audit trail appears in the right pane.
5. In the Settings tab, click Details.

   The Results Table Audit Trail Settings dialog appears displaying the audit trail configuration for the Results Table.

Creating an Instrument Maintenance Log Entry

This section provides steps for adding and viewing Instrument Maintenance Log entries.

1. Click View > Audit Trail Manager.

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

Viewing the Instrument Maintenance Log

1. Click View > Audit Trail Manager.

   The Audit Trail Manager window appears.
2. In the left pane, expand the Audit Trail Data folder.
3. Under Audit Trail Data, click Instrument.
4. If the audit trail does not appear, in the right pane, click the History tab.

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

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

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

Audit Records

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

- record number,
- date and time stamp,
- user name,
- full user name,
- Analyst® software module,
- description of the change,
- reason for the change, if required,
- and electronic signature, if required.

Topics in this section:

Searching for an Audit Record
About Audit Records

Searching for an Audit Record

1. In the Audit Trail Manager, view the audit trail within which you want to find.
2. On the History tab, right-click and then click Search.
   The Audit Trail Search dialog appears.
3. Use the Display all records where list and the Contains field, to select the records you want to view.
4. From the Created between lists, select start and end dates.
5. Click OK.
   Only records that meet your criteria are listed.

About Audit Records

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

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

- record number,
- date and time stamp,
- user name,
- full user name,
- Analyst® software module,
- description of the change,
- reason for the change, if required,
- and electronic signature, if required.

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

Instrument Audit Trail

The Instrument Audit Trail records security events; changes to the instrument resolutions and mass calibrations, sample queues, instrument configuration, and hardware profiles; and entries in the instrument maintenance log. There is one Instrument Audit Trail per installation of the Analyst software.

The Instrument Audit Trail can record the following events:

- Mass Calibration Table(s) replaced
- Mass Calibration Table added
- Resolution Table(s) replaced
- Resolution Table added
- Hardware Profile has been activated*
- Hardware Profile has been deactivated*
- An Instrument Maintenance Log has been entered
- Batch File submitted*
- Sample submitted for acquisition*
- Sample moved from position x to position y of Batch File*
- Move batch*
- Reacquiring sample(s)*
- Mass Calibration Table and Resolution Table changed
- Resolution Table(s) replaced - No Prompt*
- Instrument Settings have been changed
- Instrument Calibration Authorization
- Mass Calibration Table(s) replaced*
- User Logged In*
- User Logged Out*
- User Login Failed*
- Security Sent Notification*
- The Security Configuration has been modified*
- Duo Valve Switch Counter Reset
- User Added*
- User Deleted*
- User Type Added*
- User Type Deleted*
- User Type Changed*
- User Mode Changed*
- User Changed User Type*
- Acquisition Account Changed*
- Screen Lock Changed*
- Auto Logout Changed*
- Instrument Added*
- Instrument Deleted*
- Project Role Added*
- Project Role Changed*

- Project Role Deleted*
- Project Security Changed*
- Tune Parameter Settings Changed*

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

Project Audit Trail

When a project is created, the audit maps are copied from the Default project. Once a project has been created, you can modify the active audit map or apply a new one.

The Project Audit Trail can record the following events:

- Audit map has been created^
- Audit map has been modified^
- Audit map has been deleted^
- Batch File has been created*
- Batch File has been modified*
- Batch Template File has been created*
- Data File has been created*
- Quantitation Method File has been created*
- Quantitation Method File has been modified*
- Quantitation Results Table has been created*
- Quantitation Results Table has been modified*
- Report Template File has been created
- Report Template File has been modified
- Acquisition Method File has been created
- Acquisition Method File has been modified
- Accessed Module*
- Closed Module*
- Sample has been added to Data File*
- Printing document on printer
- Finished printing document on printer*
- Data File has been opened*
- Explore History File has been saved
- Processed Data File has been saved
- Checksum file*
- Project Settings have been changed**
- The processing algorithm has been changed*

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

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

**This event is always audited, but you can specify whether the operator can enter a custom or select a predefined reason.

Quantitation Audit Trail

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

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

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

The Quantitation Audit Trail can record the following events:

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

- Formula column has been added
- Formula name has been changed
- Formula string has been changed
- Formula column has been removed
- 'Custom Title' has changed
- Samples have been added/removed

Administrator Console

The Administrator Console consists of a client and a server. The Administrator Console client is included with the Analyst® software; the Administrator Console server is sold as a separate product. The Administrator Console benefits network administrators in regulated environments where managing large groups of people, projects, and workstations can be costly and time-consuming. However, the Administrator Console can help any administrator manage resources more effectively by providing the option of managing projects centrally or by workstation, or both.

Topics in this section:

Connecting a Workstation to the Administrator Console

To use server-based security, you must register the workstation with the Administrator Console server. Once registered, the workstation will appear in the Workstation Pool.

To set up server-based security, first install the Analyst® software on each workstation and then register the workstation using the Administrator Options. Once the workstation is added to workgroups, you can select one of the workgroups as the workstation's default workgroup.

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

This procedure must be performed on each workstation, using the Analyst software. Generally, this procedure will be performed once during the initial workstation setup.

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

   The Administrator Console Connectivity Settings dialog appears.
2. Select Use Server Based Security.
3. In the Analyst Console Server field, type the name of the server, or click Browse to navigate the server.

   The Analyst software displays a message asking the user to restart the Analyst software in order for the settings to take effect.
4. Restart the Analyst software.

   The Default Workgroup field is used once the workstation is registered to the server. Use the Default Workgroup field to select the default workgroup that appears in the Workgroup field in the Analyst - Logon Information dialog.

(Optional) Setting a Default Workgroup

This procedure must be performed on each workstation where you want to set a default workgroup, using the Analyst® software. Only those workgroups to which the workstation has been added will be available for selection.

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

   The Administrator Console Connectivity Settings dialog appears.
2. In the Default Workgroup field, click the workgroup, and then click OK.
3. Restart the Analyst software.

   The default workgroup will automatically appear in the Workgroup box in the Analyst - Logon Information dialog.