TapeStation Software Revision 5.1

Security Module Quick Start Guide

For Research Use Only. Not for use in diagnostic procedures.

What Is The Agilent TapeStation Security Module Software?

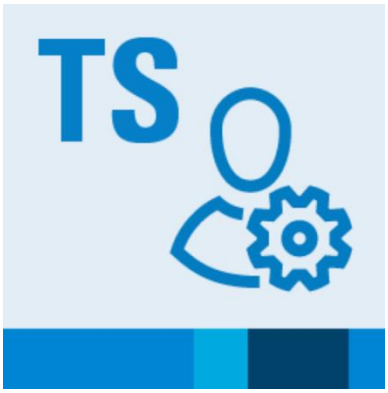


Figure 1 Desktop icon of the TapeStation Administration software

The Agilent TapeStation software revision 5.1 Security Module (further referred to as Security Module) supports using the TapeStation systems in regulated laboratory environments by providing a feature set including workflow management, access control, electronic signatures, *Report Templates* and *Audit Trails*. This software edition comes with a separate installer.

After installing the Security Module, a TapeStation Administration software is installed and visible (Figure 1) in addition to the standard software elements. See Table 1 for a general overview of the TapeStation software parts and functions.
The Security Module *User* authentication is enforced and supported by a database stored locally on the system. A user must be logged in to be able to use the software. *Projects* represent containers of related work which allow assigning roles with specific permissions associated. Roles which are assigned to individual users connect them with specific *Projects*. There are also system roles and permissions for those actions that are not related to a *Project*. Measurement data is stored in data files.

All major steps when using the Security Module in the proposed order are illustrated in Figure 2. Some steps are done only occasionally:

- Setting up P*rojects*
- Setting up *Users* and assigning *Roles*
- Instrument verification

Other tasks are reoccurring

- Sample analysis
- Data analysis
- Workflow finalization, reporting

Table 1 Overview on the Agilent TapeStation software functions

Icon	Name	Functions
	Administration software	- User management - Setting up and editing of projects - Creation of customized roles - Assigning of roles to users - Defining of data paths for projects - Creation of reports on projects, roles, users, system wide activities - General security settings for the software
	Controller software	- Control the instrument during runs - Sample selection and description - Capture of notes and lot information - Run of analytical assays based on barcodes - Hardware diagnostics and functional verification context - Maintenance counter - Needle and electrode cartridge change
	Analysis software	- Data analysis and reporting - Review as electropherogram and gel image - Integration, peak and region annotation - Size, quantity, molarity, purity determination - Calculation of RIN^e, DIN, %cfDNA or ribosomal ratios - Report templates - Sample comparison across multiple files
	Agilent Information Center	- Repository for all TapeStation user information - Instrument operation, explained using animated workflows - Access to the PDF Assay Quick Guides - Good measurement practices - Troubleshooting information - Instructions translated into multiple languages

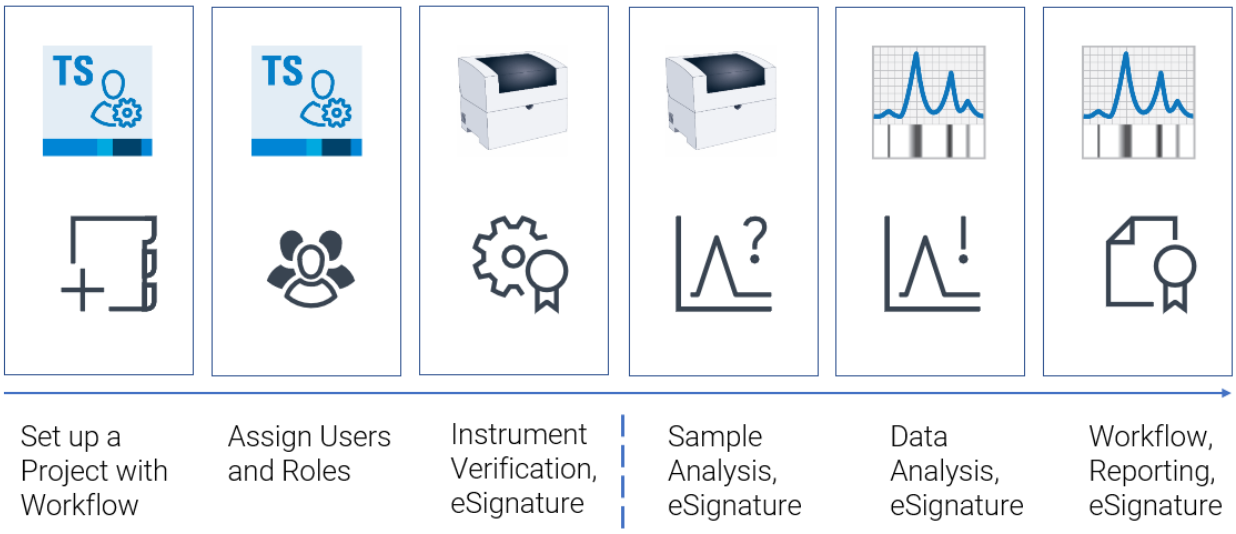


Figure 2 Major tasks when using the Security Module. On the left side are occasional preparative tasks. On the right side are reoccurring tasks.

Installation Of The TapeStation Security Module Software

The 4200 TapeStation models G2991A, G2991B and G2992A are typically distributed as bundle with laptops which are tested and fully supported by Agilent. These laptops come with preinstalled standard software which is removed prior to installation of the Security Module software.

In case a 3rd party laptop is used, see installation instructions in the readme file on the installation medium, or within the downloaded files. The readme file provides installation advice and last-minute information. It also provides useful information on:

- PC Hardware (minimum requirements)
- Operating System Requirements
- System Suitability
- Known Problems or Limitations

When the TapeStation Administration software is opened for the first time, a *User* with *System Administrator Role* is created automatically. Setting up further *Users* and administration of their *Roles* is described later (see page 12). The selection between the two authentication mode options (Windows local accounts or network Active Directory) is determined with the selection of the source of the first *User* (Figure 3). The selection should be done carefully as it is complicated to revert, see page 41. This selection is exclusive, a mixture of the two modes for authentication is not possible.

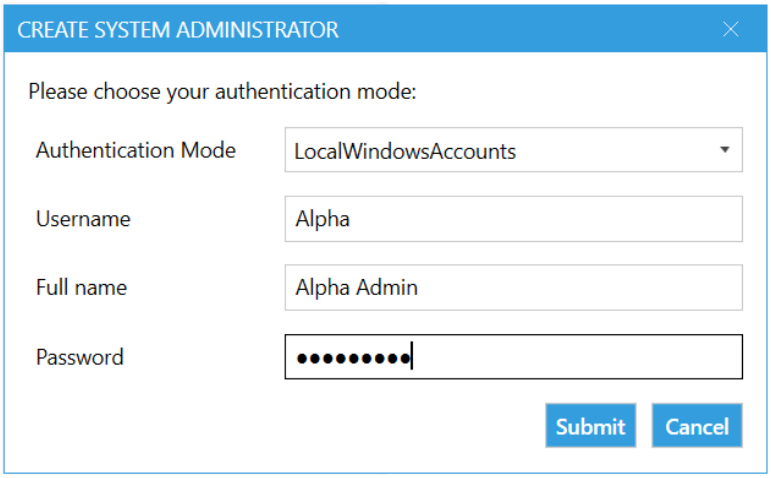


Figure 3 Initial opening of the TapeStation Administration software creates a *System Administrator*. The first and all subsequent *Users* are local Windows accounts in this example.

Differences between the TapeStation Security Module software edition and the standard edition are:

- The first *User* launching the TapeStation Administration software (Figure 3) will be made *System Administrator* of the Security Module software by default. This *Role* can be transferred on to other *Users* later. At least one *System Administrator* must be kept active.
- When the Security Module is installed, several features in the TapeStation Controller software and the Analysis software become restricted. Those features will need permissions, which are assigned to *User Roles*.
- A direct upgrade of TapeStation software from the standard edition to the Security Module edition is not possible. It requires a complete uninstallation, PC restart and new installation of the Security Module software.
- When the TapeStation Security Module software is uninstalled, databases with existing *Users*, *Roles* and *Projects* are not deleted. A transfer of this data from or to other Security Module installations is not possible. A reinstallation on the same laptop reestablishes the previous situation. An update path will be provided for future revisions of the Security Module software. This will allow *Users*, *Roles*, *Projects*, and result data folders to be imported.
- The TapeStation Analysis software of the Security Module cannot be installed standalone without the TapeStation Controller software.
- Data review is done exclusively on the system laptop. Review on other computers can only happen outside the Security Module software, after exporting data. This is since *Projects*, *Roles* and *Audit Trails* are maintained on the laptop used for the run itself.

CAUTION

Loss of data

In case all *System Administrators* are removed from the laptop or from the Windows Active Directory, the entire Security Module software will become unusable and cannot be recovered.

✓ Do not remove all *System Administrators* from the laptop or from the Windows Active Directory.

Initial Tasks When Working With The Security Module Software

Setting Up A Project

Any analytical run must happen within a *Project*.

A *Project* is a container for requirements (for example number of steps within a workflow, *Roles*/permissions required), conditions (*Report Templates*) and information (project descriptions, data directory) related to a planned type of work.

Administrators can add, edit or archive *Projects*. The *Projects* tab (Figure 4) gives an overview on existing *Projects* and their parameters. This *Project* is selected in the Controller software from the list of active *Projects* prior to sample analysis (see page 23).

In a later section Table 2 shows predefined *System* and *Project Roles*. This overview helps understanding the assignments within the *Project* setup. Refer to the Glossary for brief explanations on dedicated terms.

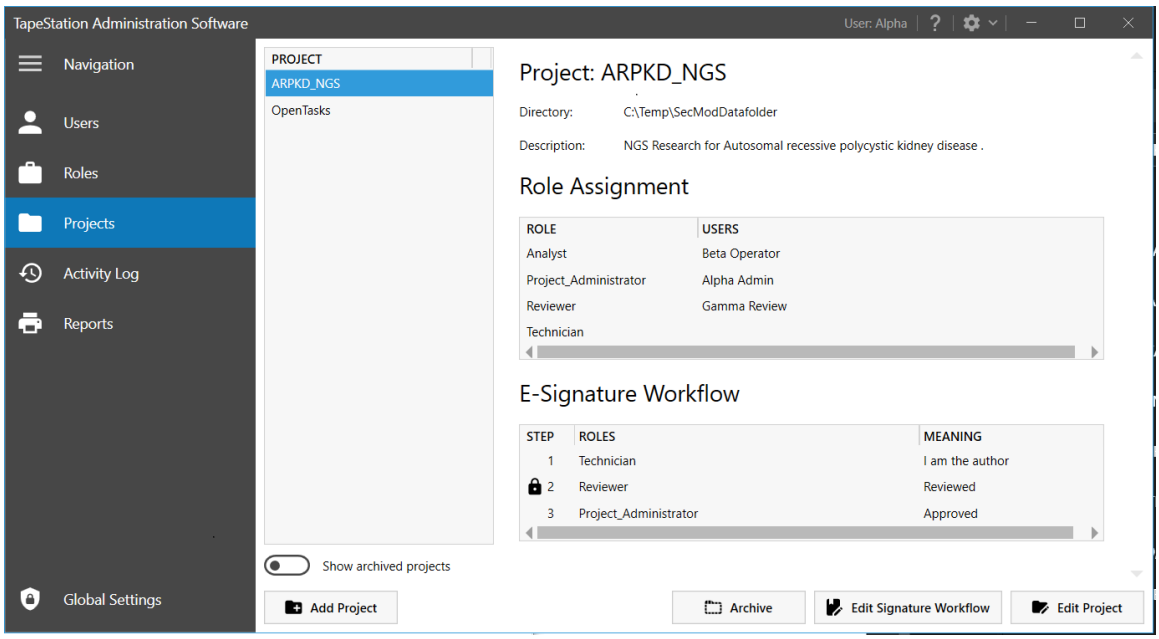


Figure 4 *Projects* tab in Administration software, overview on an existing *project*

Addition of a new *Project* can be done by a *Project Creator* or *System Administrator* by their default permissions given from the system wide roles. For new *Projects* they automatically become the first *Project Administrator*. Further *Project Administrator*s can be set up and get a *Project* related *Role* to manage their *Projects*. Granted permissions, per *Role*, can be customized and so they may deviate from the default, see Setting up *Users* and Roles (on page 12) and customization of roles (page 18).

Select Add Project to create a new one. In the *Project* setup dialog (Figure 6) for new *Projects* mandatory fields are marked with an asterisk:

- Name
- Output Directory

The *Project Name* is the identifier which is selectable in the TapeStation Controller software and will appear as identifier in the TapeStation Analysis software as well. Short identifiers are recommended while the description field allows addition of details. The Output Directory should be a carefully selected and dedicated local data folder accessible by the Security Module software. Such folder might be protected by a third-party software to control access permissions. It completes the system to have a secured backend outside the TapeStation Security Module software (see Secure Data Storage, page 35).

CAUTION

Data Integrity

The TapeStation software does not provide a content management system.

Unauthorized modifications could lead to loss of data.

✓ It is the user's organizations responsibility to set up and control a compliant data management system.

All *Users* registered within the Security Module (see Figure 10) are listed and can be assigned to a *Role* in a *Project* (Figure 6). Similarly, all existing *Project Roles* (default and customized ones) are offered in tabs with the *Role* name and number of assigned *Users* on it. The number of available *Users* (vertical, with tick boxes) and *Roles* (horizontal, tabs) depends on the individual setup the administrator provided.

Please note that a *Role* assignment of a *User* to a *Project* can also be changed from the *Users* dialog of the Administration software. This might happen when adding a new *User* or editing a *User* (Figure 11). Both pathways will result in the same.

Let any other *User* log off while setting up or modifying a *Project*.

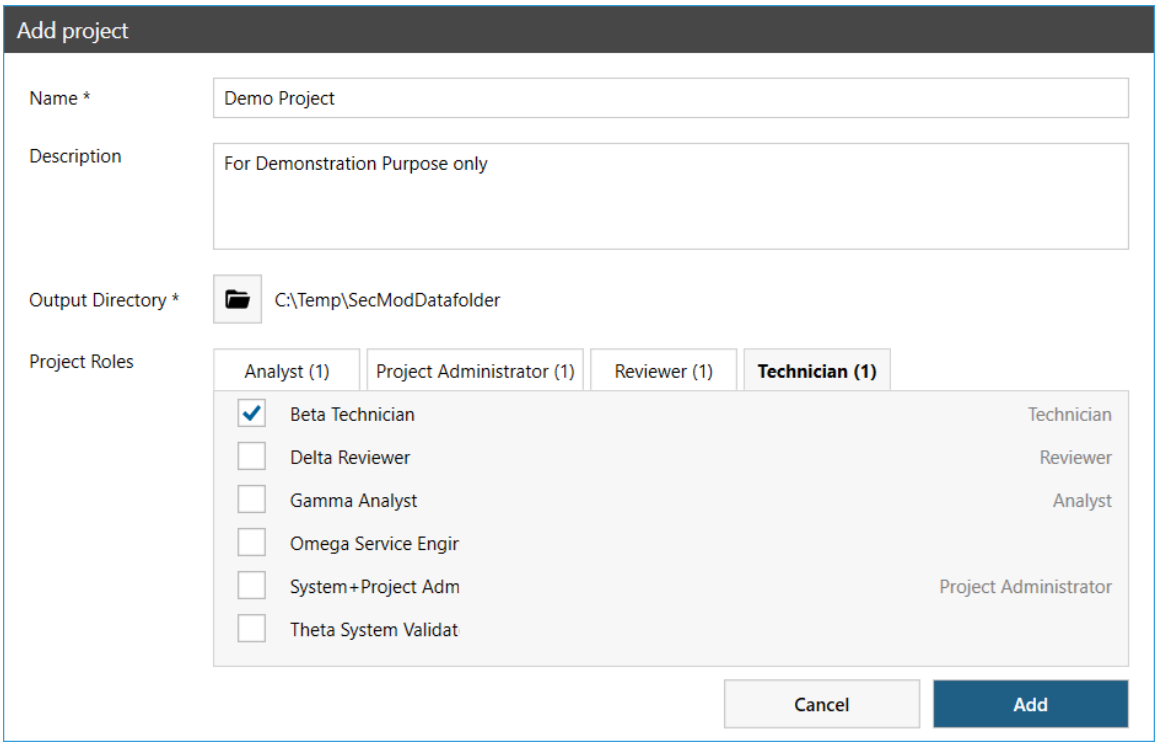


Figure 6 Addition of a new *Project* by a *System Administrator* or *Project Creator*

Workflow Within Projects

In Figure 7 a simple example workflow with three *Users* is shown. In the *Project* design phase, the *Project Administrator* assigns respective roles to *Users*. The *Users* were set up in the system, previously, by a *System Administrator*.

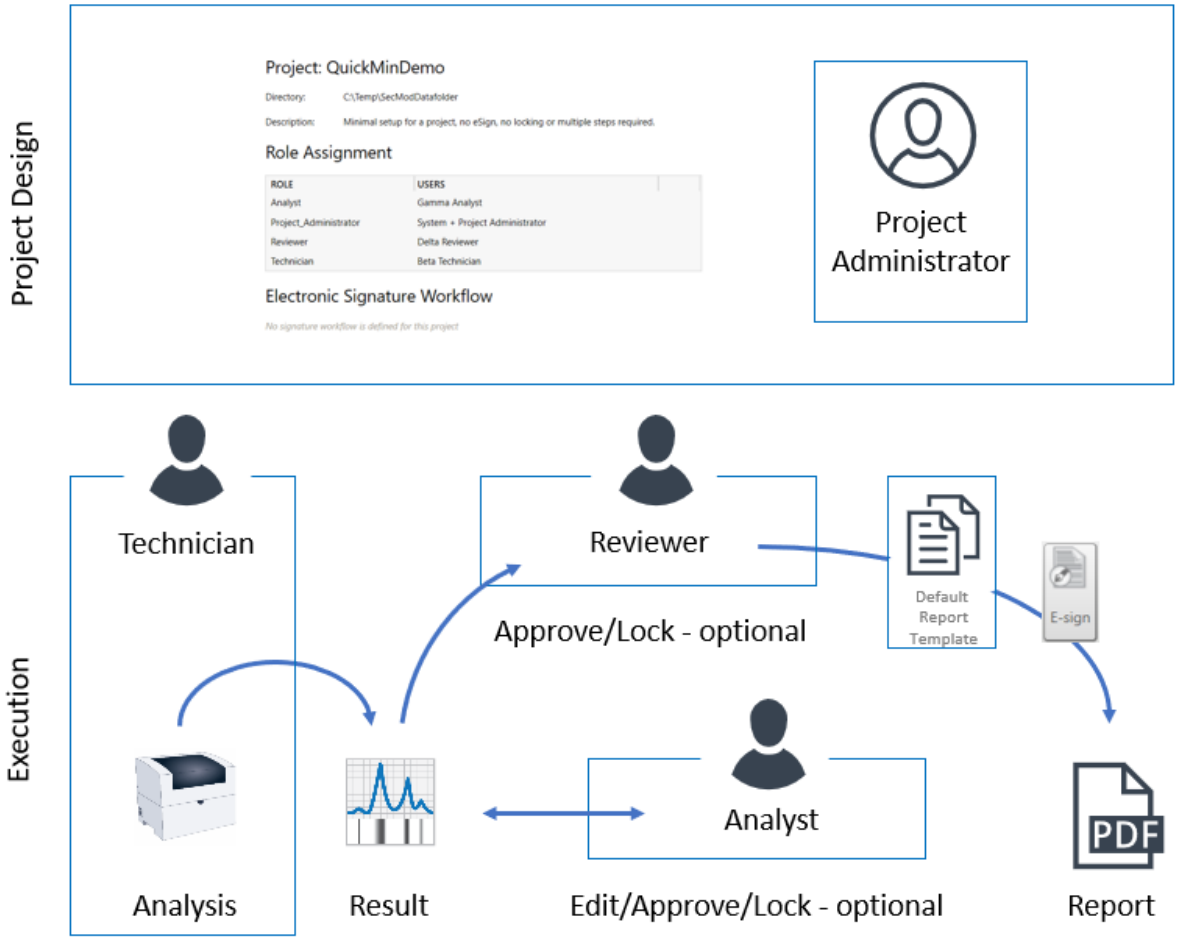


Figure 7 Simple example workflow

The *Technician* runs the analysis with the TapeStation Controller software. Results will be created and automatically shown in the TapeStation Analysis software.

The *Analyst* has the option to edit the data. This may include integration adjustments to boundaries or peaks, approval status changes, locking of the data file, and to ultimately save the data. These steps are finalized by an electronic signature with a reason for change (not shown).

The *Reviewer* has the option to review and approve the data as well as to print it by using the *Reporting Template* (see Figure 25). These steps are finalized by an electronic signature with a reason for change.

Electronic Signature Workflow

An *Electronic Signature Workflow* forces to follow a given number of steps in a sequential order.
Defining a *Signature Workflow* is optional for a *Project*. An example workflow with three *Users* will be demonstrated in Figure 9. The implementation starts from the *Projects* tab (Figure 4) with the Edit Signature Workflow button (Figure 8). In case a *Signature Workflow* is used, it can have multiple steps assigned to various roles. The roles execute their respective tasks in the Controller software, such as the *Technician* executing an analytical run and saving the data in the TapeStation Analysis software. In the Analysis software, the data is edited, analyzed, and reviewed by an *Analyst* prior to a final approval by a *Reviewer*.

The Meaning which is recorded to the *Audit Trail* when the respective *User* executes the required step in the Analysis software can be set to a certain predefined text or to 'Any'. The setting 'Any' allows selection of a predefined list of *Meanings*. To customize texts under the 'Any' list, see *Global Settings*, page 30. In addition, the *User* is given the option to also add free text comments to the *Meaning* at the moment the electronic signature is applied when finalizing the step of the workflow.

A data file can be locked automatically at one defined step (lock symbol) from further editing. See information on locking on page 32.
For good laboratory practice, it is recommended to keep a *Project* workflow as it is once the first analysis was done. If not, then two files might be created under different policies, which is correctly documented from the activities log file of the system and *Audit Trails*.

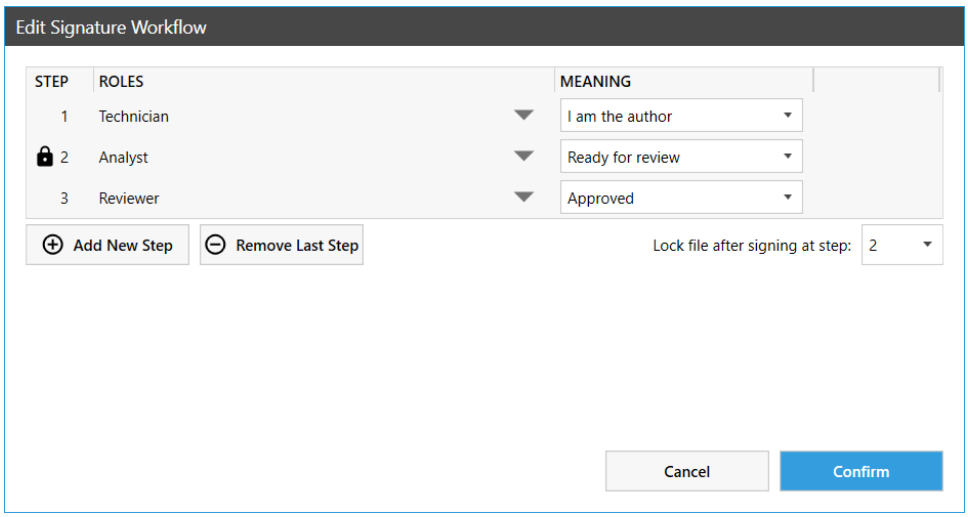


Figure 8 Editing the *Signature Workflow* with predefined *Meanings*

Example Project With Signature Workflow

The following paragraph showcases in Figure 8 an Example *Signature Workflow* with three different *Users*.

In the *Project* design phase, the *Project Administrator* creates three steps and assigns a different *Role* to each step. The *Users* with the respective roles were set up in the system previously, which is not shown in the figure. *Meanings* have been defined with which the *User* can transition the data to the next step. The transition is accompanied by giving their electronic signature.

The *Project Administrator* defined: In step 2 the file should be locked from further modification (see lock symbol). Furthermore, a *Report Template* (see Figure 25) was set up to be used within the *Project* (not shown).

The *Technician* runs the analysis with the TapeStation Controller software in step 1 and results will automatically be shown in the TapeStation Analysis software. The *Technician* will apply the electronic signature and save data for the next steps. In step 2 the *Analyst* edits the data, adjusts integration boundaries or peaks, and finalizes the step with an electronic signature. This locks the file automatically as defined by the project. Subsequently, the process continues with step 3. In the last step the *Reviewer* has the option to review and approve the data as well as to print them by using the *Reporting Template* (see page 27).

Be aware that audit events like integration changes, peak additions, or peak assignments are not reviewed and not explicitly signed by the *Reviewer* in this example *Project* as the locking event in step 2, done by the *Analyst*, blocks this. A review would lead to another change to the data file, which is disallowed here. A different workflow that allows a review of audit events (see page 32) requires an additional step in between by a *Reviewer*. Locking can be set up to occur after that step.

All three roles have the option to revoke their signature in case it was the last electronic signature applied. This might be desired to send the process back to the previous step for corrections. A *Reviewer* can view the *Audit Trail* at any time.

Figure 9 Example *Signature Workflow* with three *Users* and three steps

Setting Up Users And Roles

A *User* is an individual with a valid account from the repository of *Users* (depending on the authentication mode). A *Role* defines the functions a *User* can have based on the permissions that were granted. The TapeStation Security Module software has predefined *System* and *Project Roles* (Table 2). For description of available permissions see page 16 and for customization of roles see page 18.

Let any other user log off while setting up or modifying *Users* and roles.

Table 2 Predefined System and Project Roles

Roles	Role Description
System Roles	
Agilent Service Role	Required by Agilent Service engineer
Project Creator	Create and manage their own projects
System Administrator	Manages users, roles and projects
System Validator	Runs instrument maintenance, tests and test reports, including system verification
Project Roles	
Analyst	Works primarily with Analysis software
Project Administrator	Manages projects and project-wide settings
Reviewer	Reviews, approves, and reports data
Technician	Works primarily at the instrument with the Controller software

The *User* dialog from the TapeStation Administration software gives an overview on existing *Users* (Figure 10). The username, full name, the assigned *System and Project Roles* are listed. The *User* ID number is unique. A report on the *Users* can be generated in the *Reports* dialog (see Figure 27).

The *User* dialog allows an administrator to Add User, Deactivate and Edit *Users*. *Users* can be added either from the Active Directory or from local users of this laptop. The choice between the two authentication modes is done with the choice from which source the first *User* (Figure 3) was selected.
Predefined and customized roles per *Project* can be assigned to existing *Users* from the *User* dialog. The *User* dialog gives an overview to which *Project* the respective *User* was assigned an active *Role*.

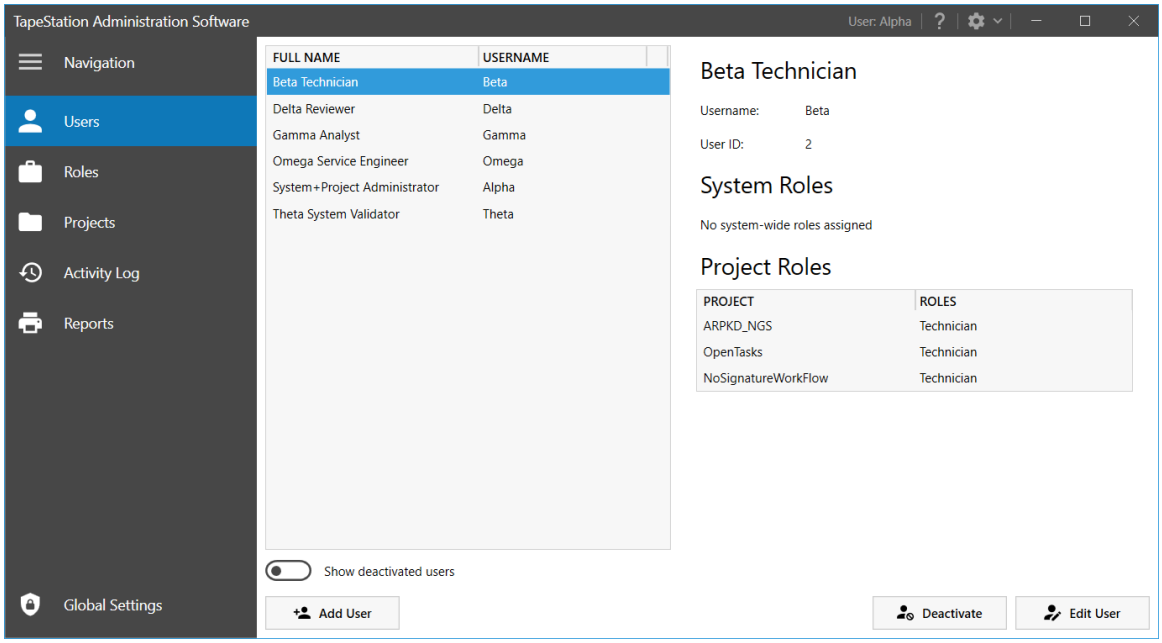


Figure 10 *Users* dialog for the TapeStation Administration software

Users can be added by clicking the button **Add User**. Only Administrators can add *Users* by searching either the *Full Name* or *Username* in the *User* repository, see Figure 11. *Users* shall be set up with their Full Name because this information is shown in *Audit Trails* and Electronic Signatures (E-sign) together with the *Username*. *Users* can be assigned any available *Role* for *Projects* that have already been set up depending on the desired workflow. This assignment can be changed or updated at any point by the administrator.

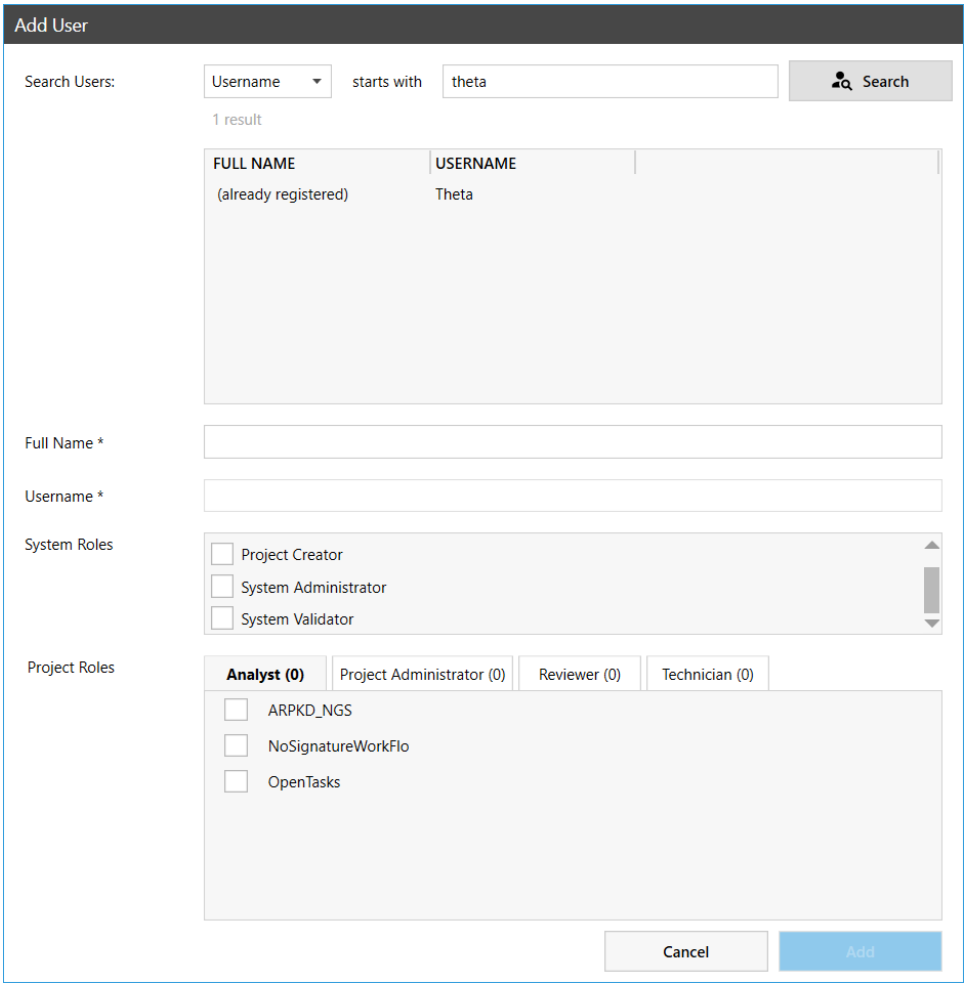


Figure 11 Add *User* dialog for managing *Users* and their roles

A leading exclamation mark with a *User* (see Figure 12) will appear when

- A *User* is locked out for too many failed logon attempts.
- The *User* is not yet assigned to a *Project*.

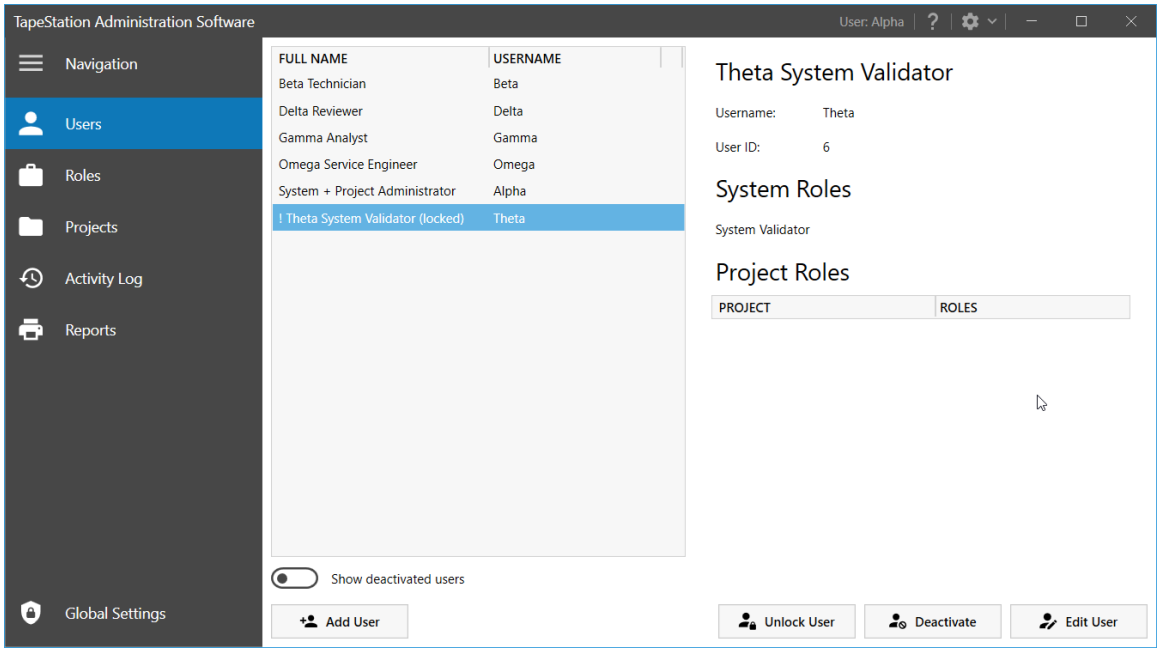


Figure 12 Exclamation mark indicates locked out *Users* or those with no *Project* assigned

Unlock Users or Deactivate *Users* can be done by administrators from within the Administration software. There is no need to remove the windows account to remove a *User*. The Show deactivated users function allows to review deactivated *Users*. A dialog (Figure 13) allows to Reactivate these *Users* again.

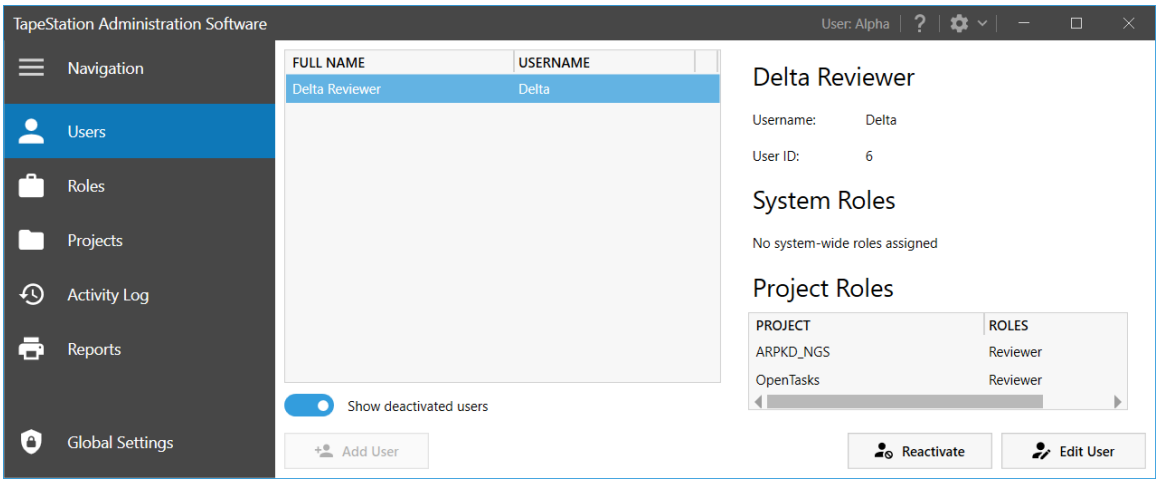


Figure 13 Deactivated *Users* can be visualized and optionally reactivated

Permission Per Role

Below is the table that lists all default roles and their permissions for a TapeStation Security Module software installation.

System Roles (Table 3) are not related to an individual *Project* and are valid system wide. They typically have an administrative character or are related to instrument maintenance or verification.
Project Roles (Table 4) are focused on *Projects* with actual analytical runs, executing the defined workflows, reporting or tasks related to auditing.

Table 3 System Role Permissions

	System Administrator	Project Creator	System Validator	Agilent Service Role
System Administration				
Create administrative reports	x			
Create project	x	x		
Edit EPG view settings	x			
Edit instrument name	x			
Manage projects	x			
Manage roles	x			
Manage global settings	x			
Manage users	x			
Read all users	x	x		
Instrument Maintenance				
Maintenance functionality			x	x
Review maintenance and test reports	x		x	x
Run system verification tests	x		x	x

Table 4 Project Role Permissions

	Technician	Analyst	Project Administrator	Reviewer
Instrument				
Start a run	x			
Abort or stop a run	x			
Edit reagent lot	x			
Edit sample descriptions	x			
Edit run notes	x			
Edit project specific controller settings	x		x	
Edit filename prefix	x			
Edit file output settings	x			
Edit allowing expired ScreenTape device			x	
Edit ScreenTape lot	x			
Project Administration				
Edit project			x	
View project	x		x	x
Data Access				
Unlock file			x	
Lock file		x		x
Review audit trail			x	x
General Analysis				
Revoke E-sign	x	x		x
Edit sample name in analysis software	x			
Import file			x	
Load file	x	x	x	x
Modify ladder		x		
Edit marker alignment		x		
Revert all file changes		x		
Edit study and comments in analysis software		x		
Edit RIN^e options		x		
Edit DIN options		x		
Edit %cfDNA options		x		
Create, update, and delete peaks		x		
Select wells for analysis		x		x
Change display and gel settings		x		x
Change sample approval status		x		x
Change RNA type		x		
Add, delete, edit region		x		
Save file	x	x	x	x

Table 4 Project Role Permissions

Reporting Exporting	Technician	Analyst	Project Administrator	Reviewer
Create, edit, save and delete report templates			x	
Snapshot EPG				x
Snapshot gel				x
Create report				x
Export data			x	

To see the permissions of a *User* who is currently logged on, one can navigate to the drop-down menu in the TapeStation Controller software interface (Figure 36) and TapeStation Analysis software interface (Figure 37).

Customization Of Roles

There are default assignments of permissions to a *Role* as shown in Table 3 and Table 4. Two types of customizations of these roles can be done by an administrator.

- Changing the permissions for an existing predefined *System* or *Project Role* to have different permissions as initially designed in (see Edit Role, Figure 14).
- Creation of new roles with a new descriptive name and with a customized set of permissions (Add Project Role, Add System Role).

All roles can be deleted except the *System Administrator* and *Agilent Service roles*. These two roles are mandatory and required by the Security Module software. All dialogs for the below listed tasks have a similar interface (as in Figure 15) and allow changing the Names, Descriptions and Permissions:

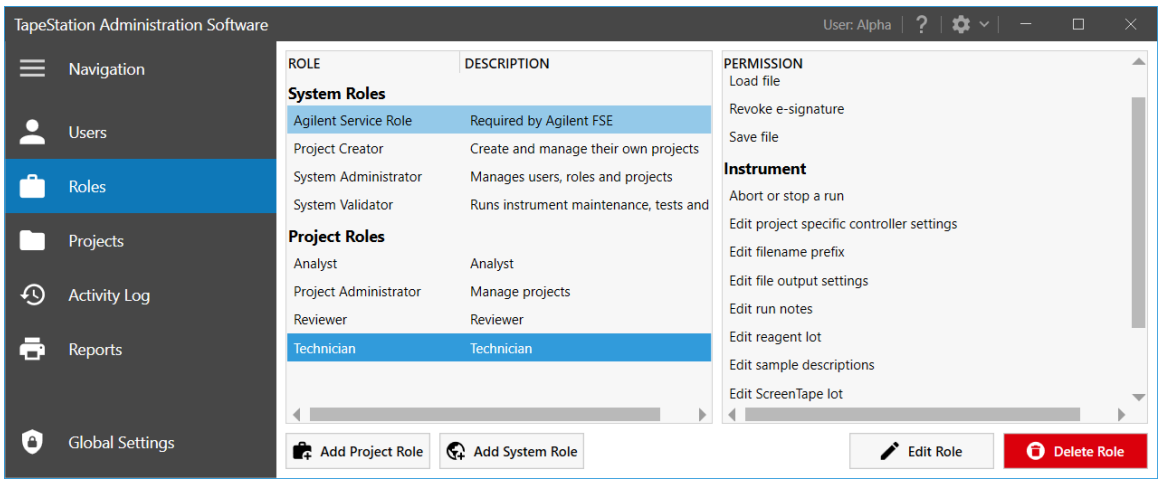


Figure 14 Review Role Permissions, editing and creation of new *Project* or *System Roles*

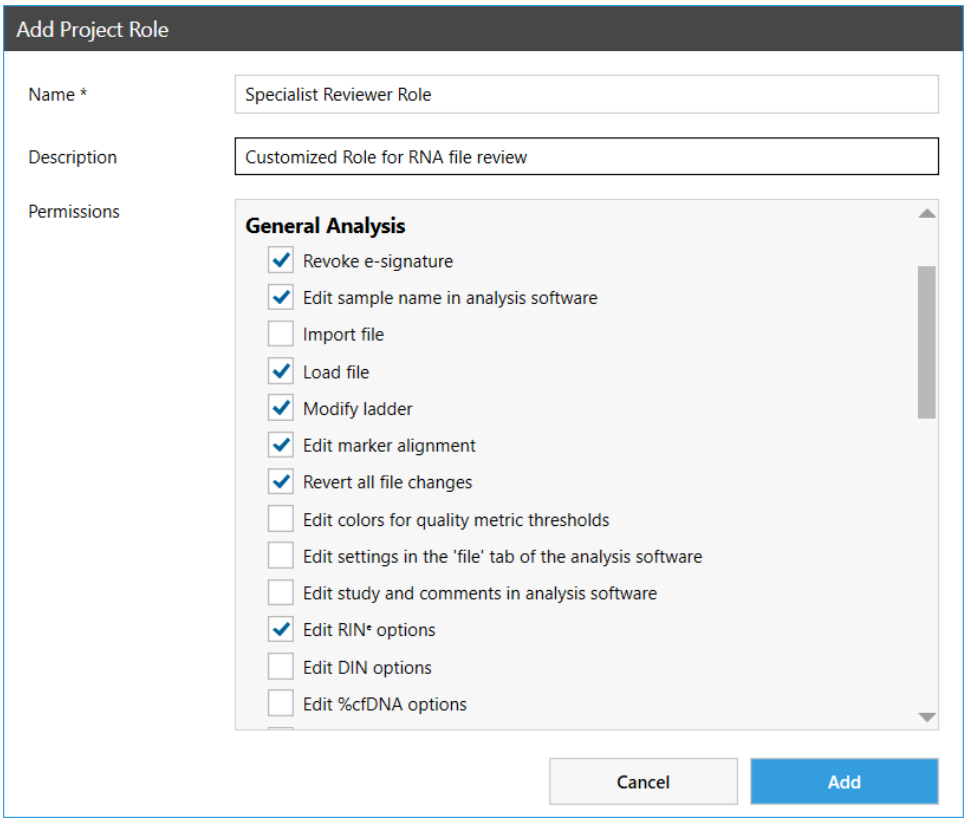


Figure 15 Adding of a customized *Project Role*, *System Role* or Edit *Role* have similar dialogs

Verification Of An Instrument

Prior to using an instrument, an execution of the System Verification test suite by a *System Validator* is needed.

If the System Verification was not performed, the TapeStation Controller software user interface will display a notification about the missing Verification result. This notification is close to the serial number and a request for a Verification, see Figure 16. The Verification is instrument specific. All tests of this Verification (Figure 17, center button, System Verification test suite) need to pass without error or fail otherwise no analysis run is possible. See also Table 5.

The respective test suite can only be run by a *User* with permission to run the verification test. This is typically the *System Validator* or the *Agilent Service Role*. An *Electronic Signature* and *Meaning* must be applied during this process; a comment is optional. See Figure 18. In case of successful *Verification*, the last Verification date is noted with the instrument details at the bottom of the Controller software user interface, see Figure 19.

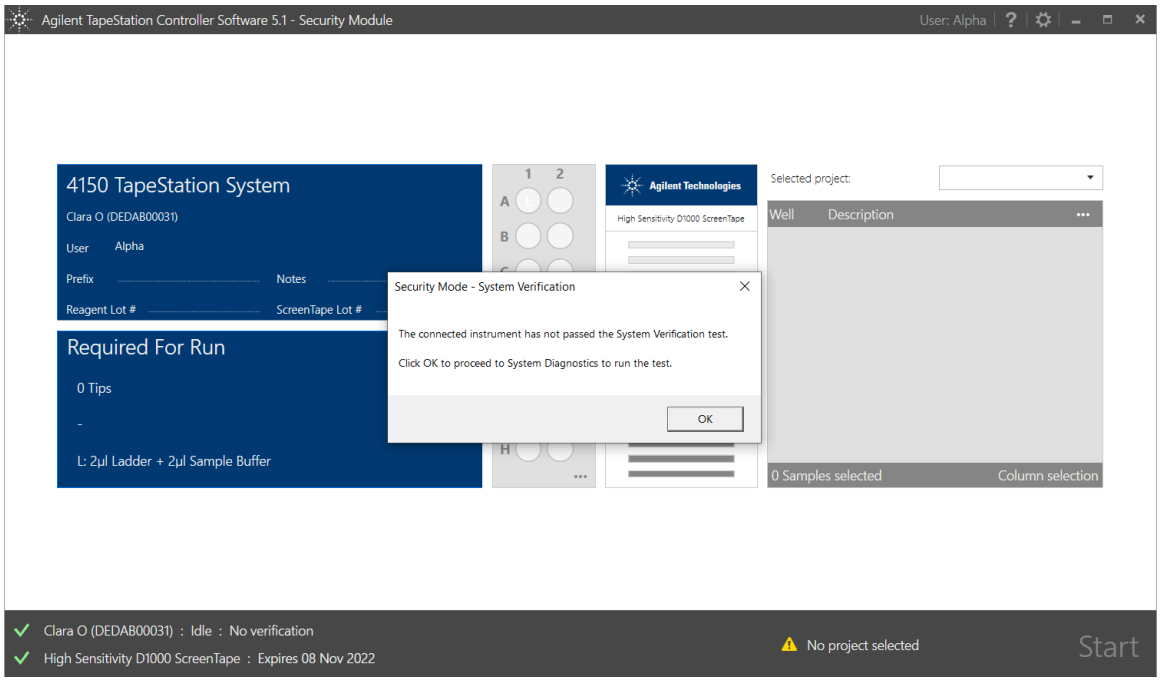


Figure 16 Controller software, requests *System Verification*

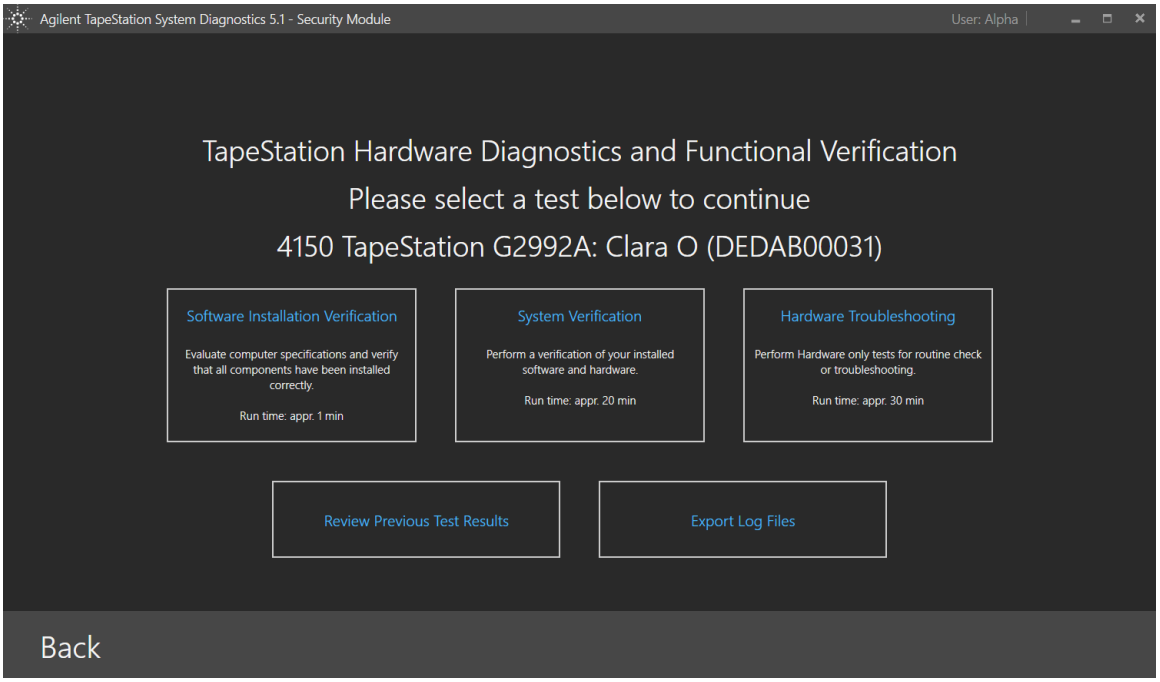


Figure 17 Select *System Verification*, an overall pass in all tests is required to operate the instrument

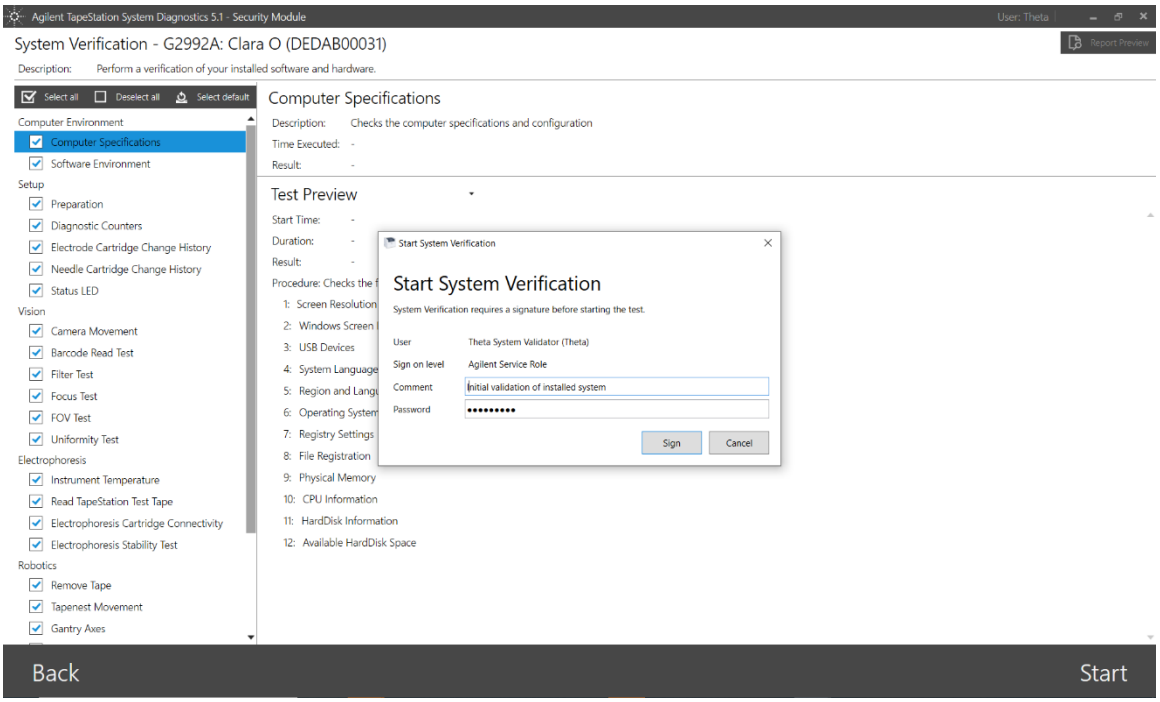


Figure 18 Starting the *System Verification* Test Suite for verification of an instrument

Figure 19 Last Verification date is noted with the instrument details

The execution and results of the Hardware Troubleshooting suite or the Software Installation test suite do not affect the validity of the system regardless of the outcome. The partial execution of the System Verification Test suite of test doesn't either, see Table 5.

A failure of the System Verification Test suite might invalidate the system immediately, for example if the TapeStation Test Tape is meanwhile expired. This is a specific fail that doesn't affect the instrument itself but prevents working further with it. If a subset of tests from the System Verification Test Suite were selected and fail, this doesn't invalidate the instrument. Please select carefully which test suite suits your needs.

Table 5 Test Results affecting the Verification of the system

Test suite	Result affects Status	Availability
Software Installation Verification	No	User and Agilent Personnel
System Verification (all default tests selected)	Pass: verifies; Fail: invalidates	User and Agilent Personnel
System Verification (tests partially selected)	No	User and Agilent Personnel
Hardware Troubleshooting	No	User and Agilent Personnel
Qualification Tests (all default tests selected)	Pass: verifies; Fail: invalidates	Agilent Personnel only
Qualification Tests (tests partially selected)	Any Fail: invalidates	Agilent Personnel only
Service Engineer Tests	No	Agilent Personnel only

Operation Of Non-Verified Instruments

It is not recommended to make use of the following option: Analysis runs can be done with non-verified instruments. If a run start is triggered for a non-verified instrument, a special dialog (Figure 20) will be shown. Processing the analysis regardless of the invalid status requires giving a *Meaning* and an additional electronic signature for the waiver. The waiver is visible in the *Audit Trail* of the analysis, see Figure 42.

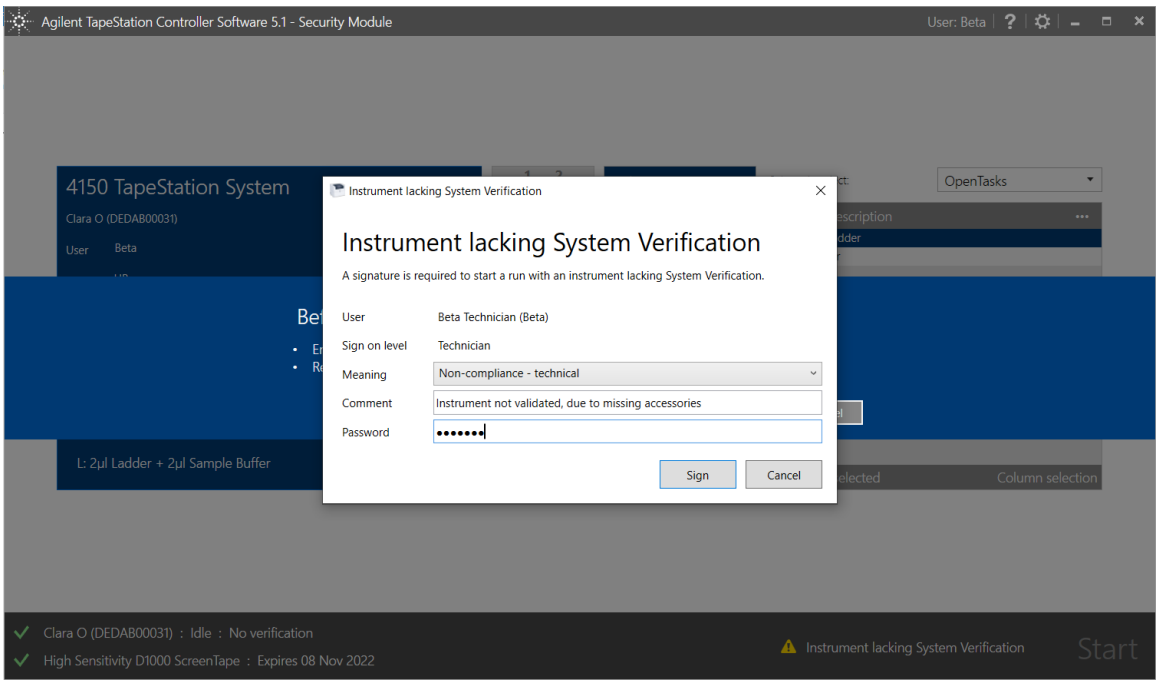


Figure 20 Operation of non-verified instruments requires traceable input

Reocurring Tasks When Working With The Security Module

Sample Analysis

Sample analysis with the Agilent TapeStation Security Module software is similar to the analysis with the regular software. Please refer to the Agilent Information Center, the assay Quick Guides and the instrument user manuals. Also, the installation and introduction service introduces you to the relevant topics:

- Product Description
- Safety
- Legal and Regulatory
- Installation
- Operating Instructions
- Troubleshooting
- Maintenance

In general, the TapeStation Controller software is designed to control the instrument during the analytical run. It allows the automatic connection through USB and controls the robotics and vision system. It runs the desired assay based on the inserted ScreenTape device barcode. Data files are saved by this software and automatically open in the TapeStation Analysis software for further processing. The TapeStation Controller software allows you to select sample location and information, to configure the file save settings and preselect assay parameters. This software reports the instrument status and allows the review of diagnostic counters.

The Security Module edition differences in the user interface are instrument details in the bottom line and the Select a *Project* menu, see Figure 21.

Starting an analytical run does not require an electronic signature. Such Start becomes possible (not dimmed button) if

- the *User* who is currently logged on has the permission to start a run,
- a *Project* was selected,
- samples were selected,
- the ScreenTape device is not expired, and
- the connected instrument is verified.

During the execution of the analysis a check for presence of consumables happens followed by the analysis itself. This is identical to the operation of the standard software edition. The data file is automatically opened in the TapeStation Analysis software which requires a login of the *Technician* at this time.

In case the *Project* allows for running *Expired ScreenTapes Devices*, this *Project*-wide setting can be enabled by the *Project Administrator* only. See for details page 38.

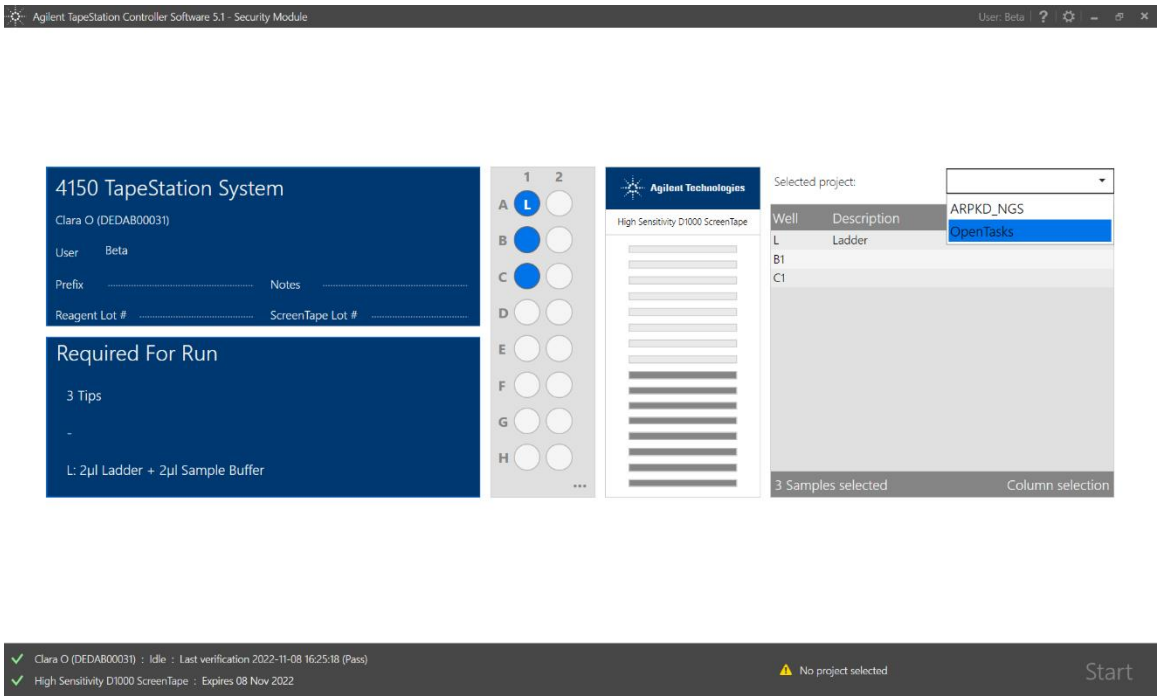


Figure 21 A *Project* must be selected prior to a run. The instrument must have passed verification

Data Analysis

The TapeStation Analysis software is a simple and intuitive software for data analysis and reporting. You can display your results as an electropherogram, as a gel image or in tabular format for effortless sample comparison. Depending on your application, the software automatically determines size, quantity, molarity, purity, RIN^e, DIN, %cfDNA or ribosomal ratios. Reports can easily be generated and saved in PDF format. For context-specific help within the software, press F1 on your keyboard.

In the Agilent Information Center you will find a general description for the TapeStation Analysis software user interface. Two additional groups for traceability and for electronic signatures will be visible in the home ribbon for the Security Module software.

In the file selection menu, data is combined into groups by *Project*. Additionally, an approval status in the sample table can be set by the *Analyst* with appropriate permission.

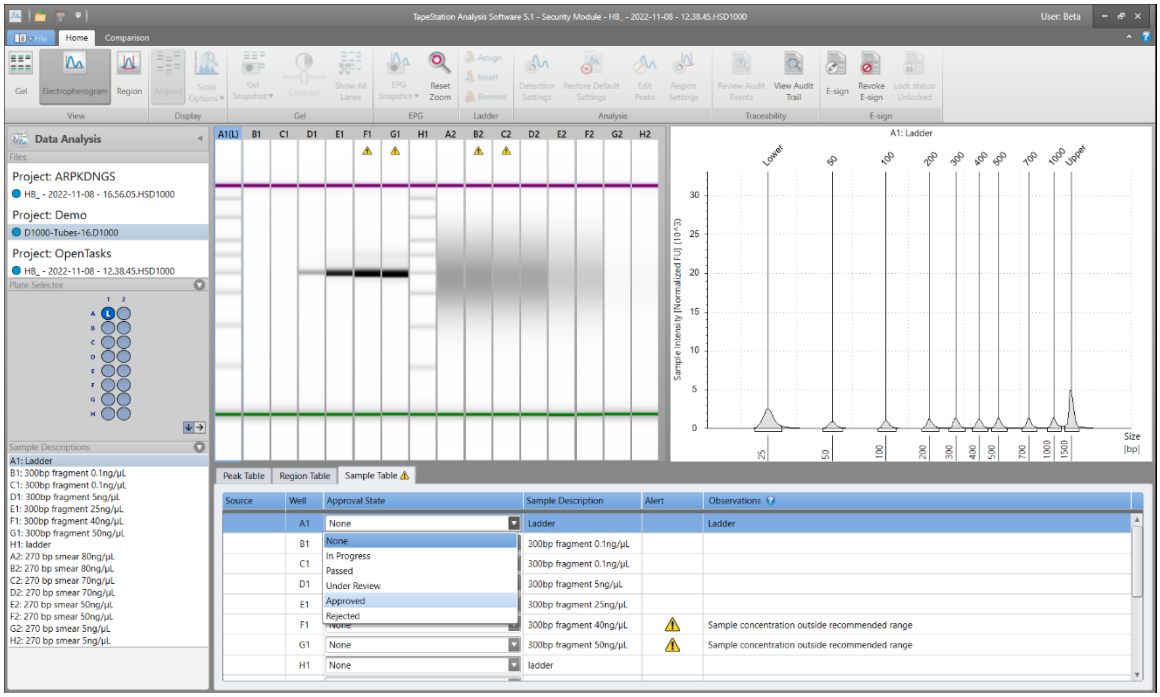


Figure 22 TapeStation Analysis software interface for the Security Module software edition has additional elements

The *Technician* who records a data file can load, save and sign it electronically. The *Analyst*, in contrast, performs tasks like editing of peaks, altering their integration, introduction of regions and setting the approval status in the sample table. All these changes need to be signed electronically before a data file can be saved or finally locked. The saving dialog requests an input for the *Reasons For Change*, see Figure 24. When operating without a *Signature Workflow*, manual locking is possible. In *Signature Workflows*, locking can be forced to happen at a dedicated step by the way the *Project* is set up, see Figure 9. See page 31 for details on electronic signatures and also page 32 for further details on locking of files.

Printing results of data from unlocked or locked files is possible. A *User* with *Reviewer Role* permissions is required for this. Starting to print a report requires the *User* to sign and give a *Meaning*, see Figure 23. Refer to page 34 for information on default *Report Templates* and report template creation.

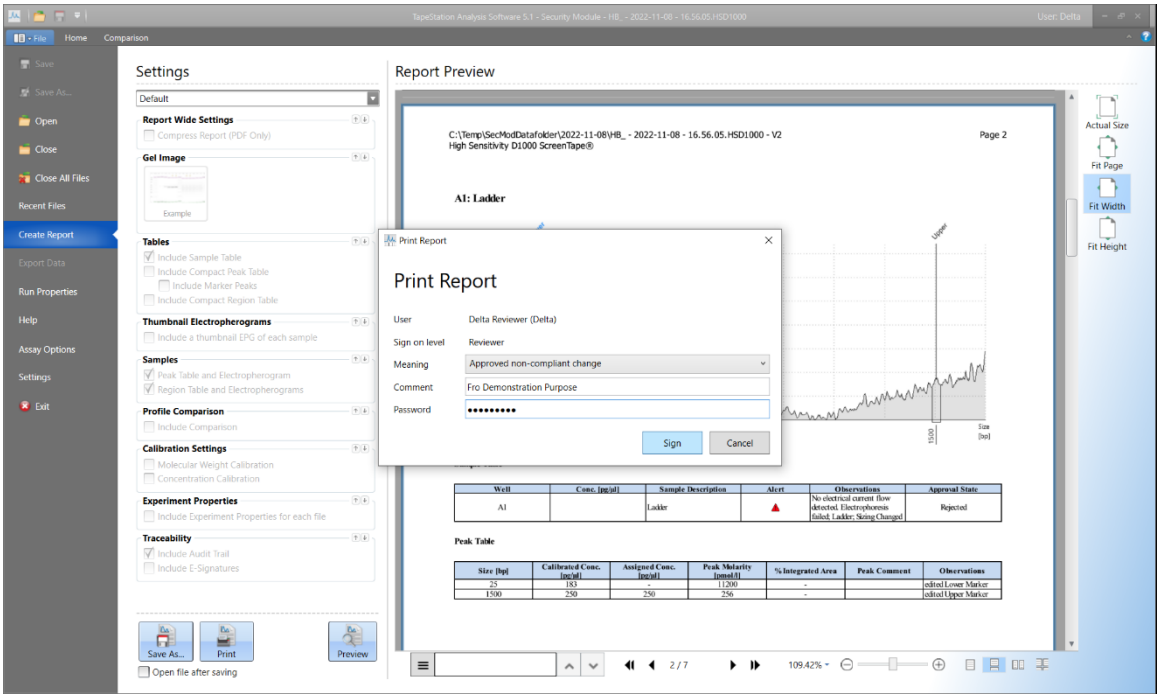


Figure 23 Printing a report with default template

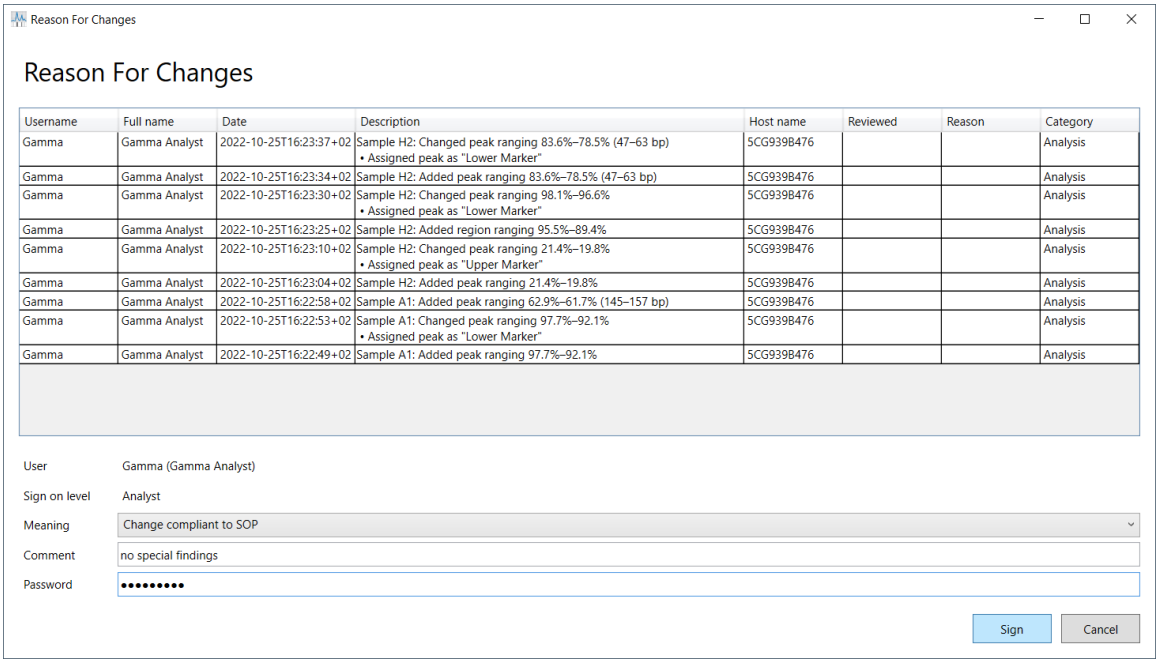


Figure 24 Saving a data file forces an electronic signature with a reason for change

Reporting Of Results

Reports are based on *Reporting Templates*. They are created by the *Reviewer* with appropriate permissions. Reporting within a *Project Workflow* will make use of the linked *Reporting Templates* which are either default (see Figure 25) or templates previously set up by a *Project Administrator* and saved under a specific name (Figure 32). The TapeStation Security Module software does not allow ad hoc modifications by the *Reviewer*.

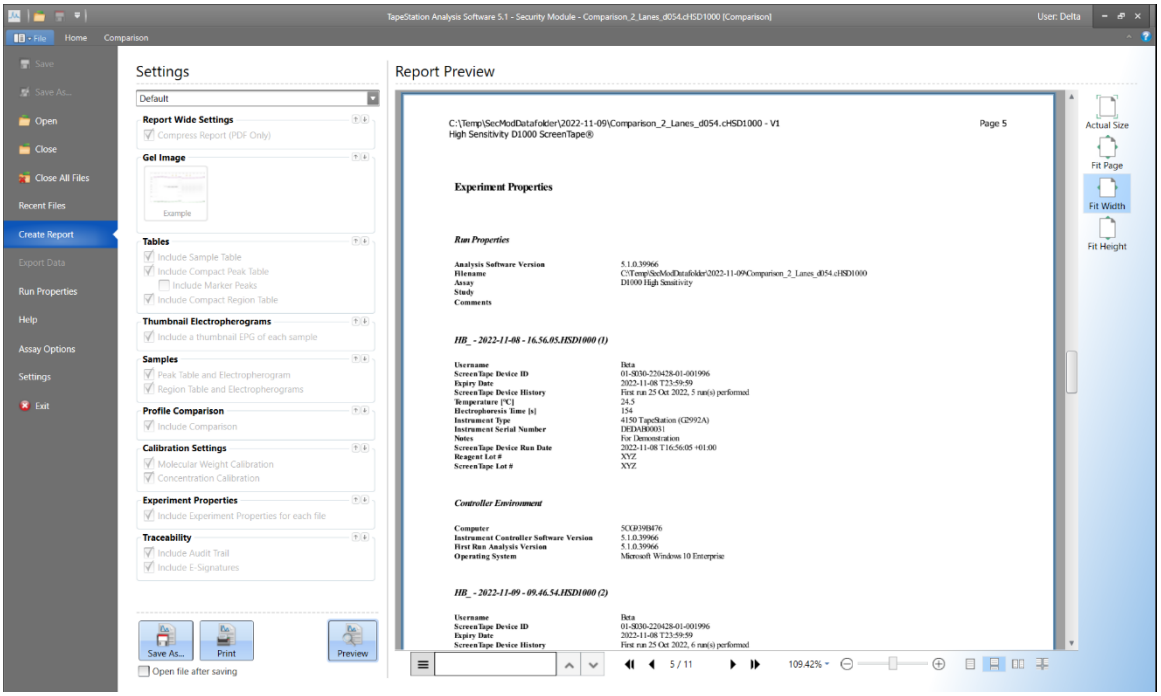


Figure 25 Creation of report based on a default template; preview selected

Other Administrative Elements Of The Security Module software

Activity Log Functionality In The Administration Software

The Activity Log (Figure 26) lists which *User* performed an activity in the TapeStation Administration software. The log can be searched for text strings and filtered for the date. See the Reports sections (Figure 27) for creation of a printable report.

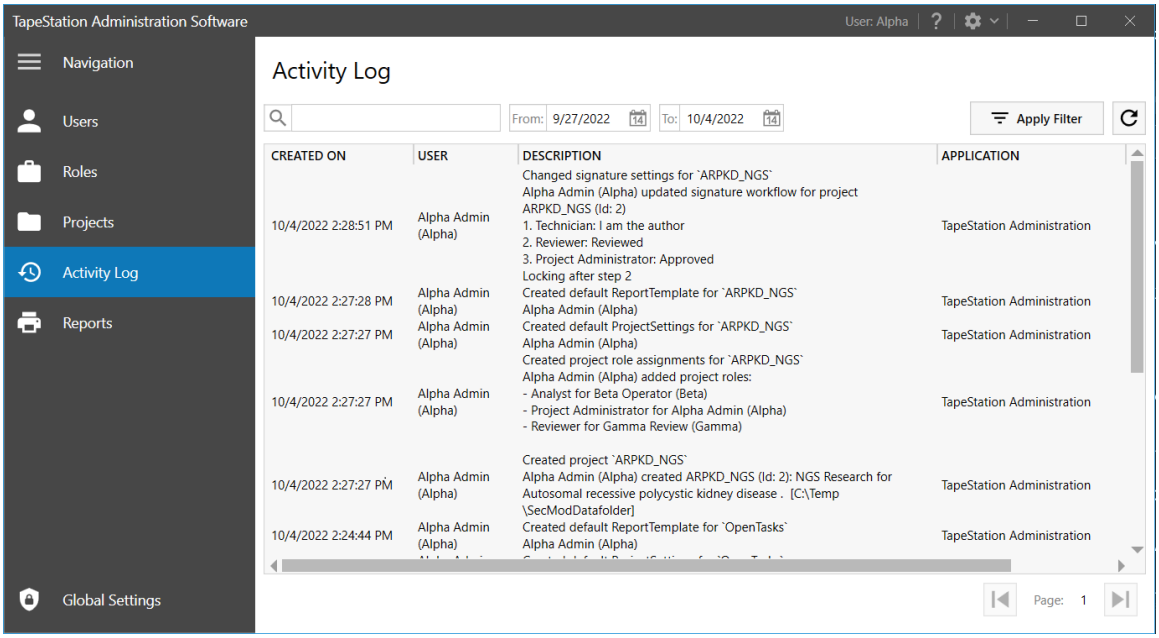


Figure 26 Activity Log of Administration software

Reports In The Administration Software

Administrative reports (Figure 27) can be created individually on the items

- *Projects*
- *Users*
- *Roles*
- *Activity logs* (also filtered)

A combination of any of the four areas collates the information into one report document. Such a report is either saved in PDF format or printed directly.

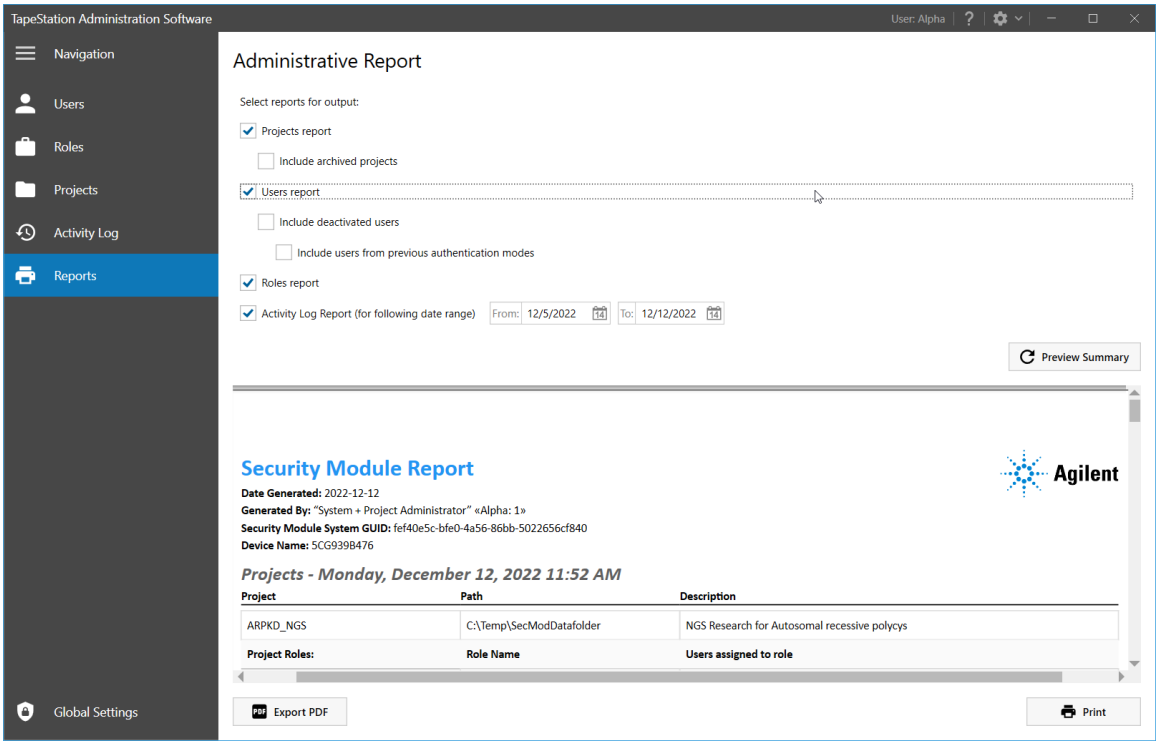


Figure 27 Administrative Report creation

Global Settings

Global Settings (Figure 28) reflect security settings applied to the entire Security Module software. In this section the duration for when an idle application requests a new log-on can be defined (*Idle timeout*). The number of allowed unsuccessful login attempts before disabling a *User* and the duration of the lock-out (Figure 29) can be set.

Signature Meanings and *Reasons For Change* can be administered. The wording choices are made available in selection menus of the *Signature Workflow* and carried out during data analysis, or when working with the *Audit Trail*. Edit settings also allows for authorization change, see page 41.

Let any other user log off while changing the *Global Settings*.

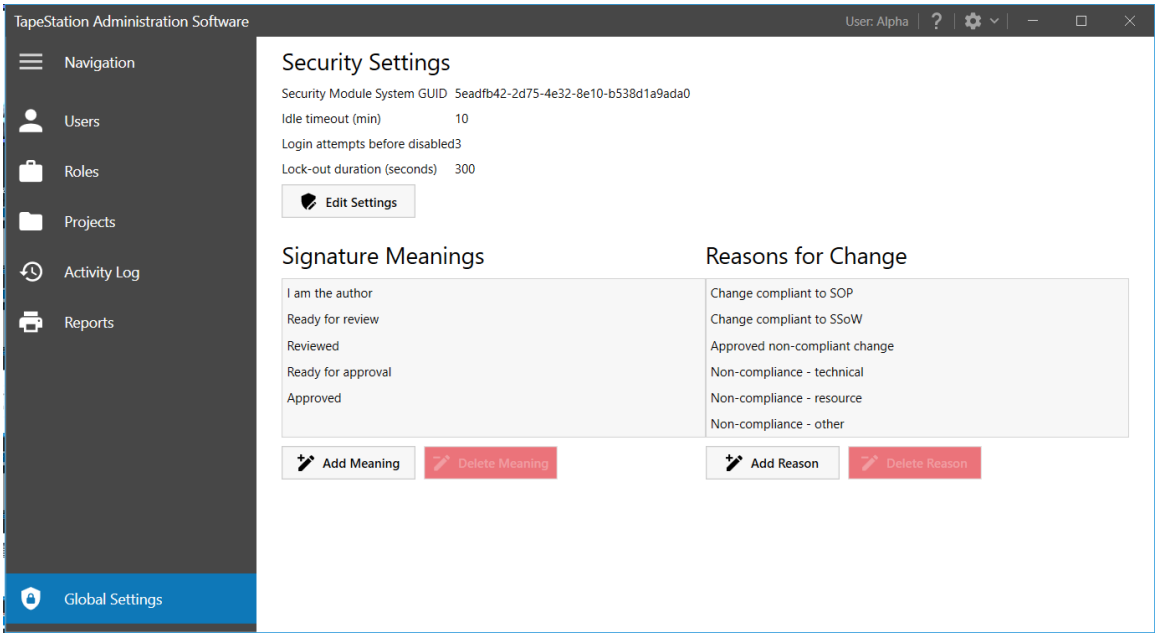


Figure 28 *Global Settings* offer adjusting *Security Settings*

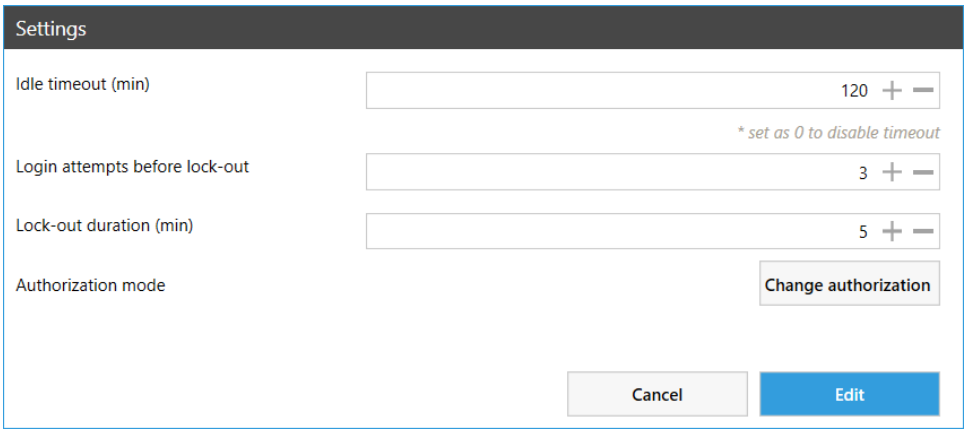


Figure 29 Editing *Global Settings* allows changing parameters and the authorization mode

Glossary

Administrator

Three types of administrators are used in this Quick Guide. There are *Project Administrators* and *System Administrators*, who are related to the Security Module software, and Windows administrators, who deal with local or domain permissions.
A Windows administrator is typically required to install Security Module software and to set up *Users* either locally on the laptop or on domain level, the Windows Active Directory.
Be aware, such Windows administrators must not delete the account of the last *System Administrator* else the Security Module software becomes inaccessible.

Activity Log

The Activity Log lists which *User* performed an activity in Security Module related application. For example, log-in or log-out events in the TapeStation Controller or Analysis software are recorded as well as editing of *Projects*, *Roles* and *Users* in the Administration software. The log can be searched for text strings and filtered for the date.

Authentication Method

The term Authentication Method refers to the way a *User* is identified within the Security Module software. The choice between the two authentication mode options is done with the selection from which source the first user (Figure 3) was selected and is complicated to change. See also page 41 for Resetting the Authentication mode.

Archive/De-archive *Project*

When archiving a *Project*, it is no longer available from the selection list in the Controller software and, therefore, new data cannot be added to a *Project*. Existing data files become read-only in the TapeStation Analysis software. The *Project* Workflow, *Users* and *Roles* are kept in the background and will become active again when de-archiving is done. See also page 42.

Deactivate/Reactivation Of *Users*

The *System Administrator* can manage *Users*. This includes setup and deactivation (Figure 10) or reactivation (Figure 13) of *Users* in the *Users* tab of the Administration software by pressing the respective button.
The function “Show deactivated users” displays such *Users*. A reactivation is possible.

Electronic Signature

Electronic Signatures, in this software referred to as E-sign, can only be executed by the *User* logged in and require the *User* ID and the password. In *Audit Trail*/E-signature logs electronic signatures will display the full name and will display a *Meaning* together with a time stamp. Previous electronic signatures are retained after signing new ones.

Electronic signatures are relevant at multiple occasions when working with data files in the Security Module software such as:

- Saving data files
- Creating and saving comparison file
- Finalizing a step in a signature workflow
- Manual Locking of a data file
- Creating and printing a report

Revoke E-sign can be used for the last electronic signature applied. This is only possible by the *User* who applied the signature and allows to return to a previous step in a *Signature Workflow*. See an example workflow with enforced electronic signatures in Figure 9.

Full Name

The *User* name from the Windows Active Directory or local windows account is primarily used to log on and identify a user within the TapeStation Security Module software. When setting up *Users*, a full name can be given, typically coming with more comprehensive details like the person's name or function. In locations like the Audit Trail *User* name and Full name are used side by side and increase readability.

Lock status of a file

Locking a file prevents further modifications. The lock icon the wording unlocked/locked in the TapeStation Analysis software indicates the status of the data file currently loaded. Certain activities remain possible for locked files such as:

- Opening and viewing
- Printing with *Report Templates*
- Electronic signature
- Review of *Audit Trail*

Locking can be forced to happen automatically together with the respective electronic signature at predefined steps within a *Signature Workflow* (see Figure 9). This automated lock will happen for any *User* even if the current *Role* comes without appropriate permissions because the workflow forces it.

Alternatively, the Lock button in the TapeStation Analysis software can be used and as such a manual locking is done which is also accompanied by an electronic signature. This manual lock can only be performed by *Users* with appropriate permissions. It might require saving first or electronic signing of modification to the data file. In such case the button is dimmed.

A locked file can be unlocked by the *Project Administrator*. Please see Table 4 for details on the required permissions. Eventually an electronic signature must be revoked prior to the unlocking.

Reasons For Change

Reasons For Change can be selected from a dropdown menu within the TapeStation Analysis software when applying an electronic signature. They are predefined and used when modifying and saving files such as integration changes, region introduction, marker assignment. They are visible in the *Audit Trail* for a data file. Their wording can be edited under *Global Settings*, see page 29.

Review Audit Events

With Review Audit Events (Figure 30) all unsigned change events applied to a data file (Figure 31) can be labelled as reviewed and can be signed by an auditor with appropriate permissions. In order to do this the user will highlight the desired rows in the “Review Audit Events” table. You can sign the dialog to apply the indication in the respective column of the *Audit Trail*.

Figure 30 Review Audit Trail icon in TapeStation Analysis Software

The auditor must not be the *User* performing the changes. Change events which were signed off disappear from *Review Audit Events* but are visible in the “View Audit Trail” with an entry in the Reviewed Column (see Figure 35).

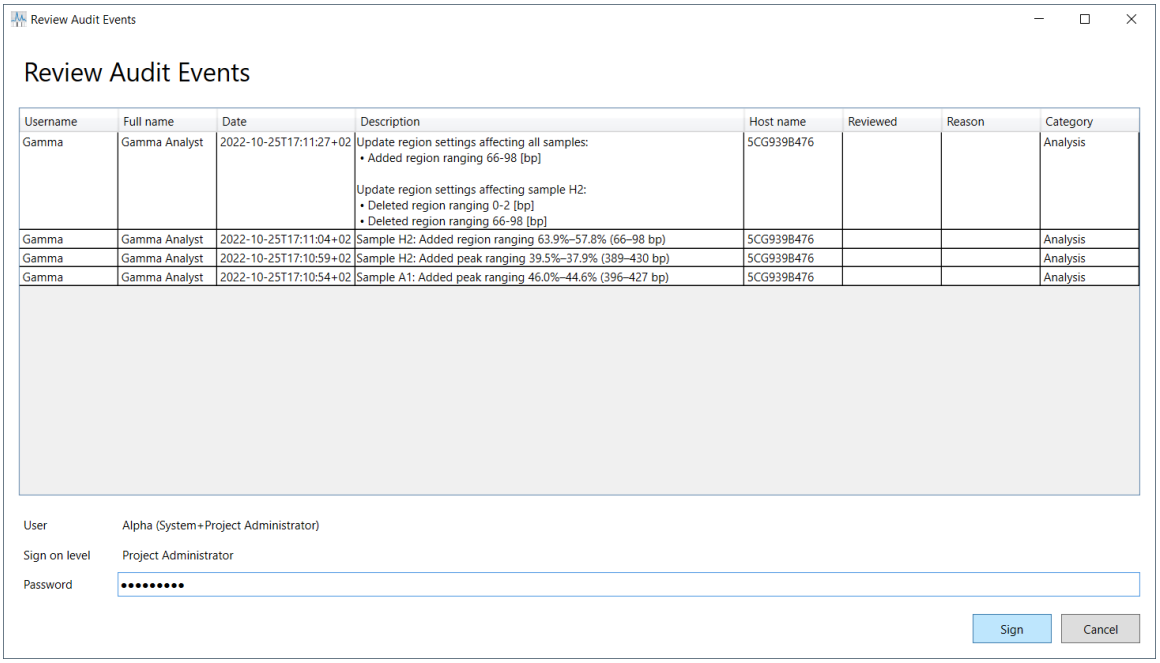


Figure 31 Reviewing the *Audit Trail*

Report Template Creation

It is not possible to change the content of a report ad hoc which is possible in the standard edition of the TapeStation software. For the Security Module software either a default *Report Template* or a created template, specific for the *Project*, can be used.

Creation of a customized template from within the TapeStation Analysis software is shown in Figure 32. Press the " **+** " button. The elements desired are selected by checkboxes and a customized template name can be given. Multiple templates can be saved. A *Project Administrator* might want to provide two types of report for a *Project* such as a full report and a template for reduced content. The default *Report Template* can be modified under the name default and saved per *Project*. There is no option to provide a customized Report Template across all *Projects*. All *Projects* require their own setup.

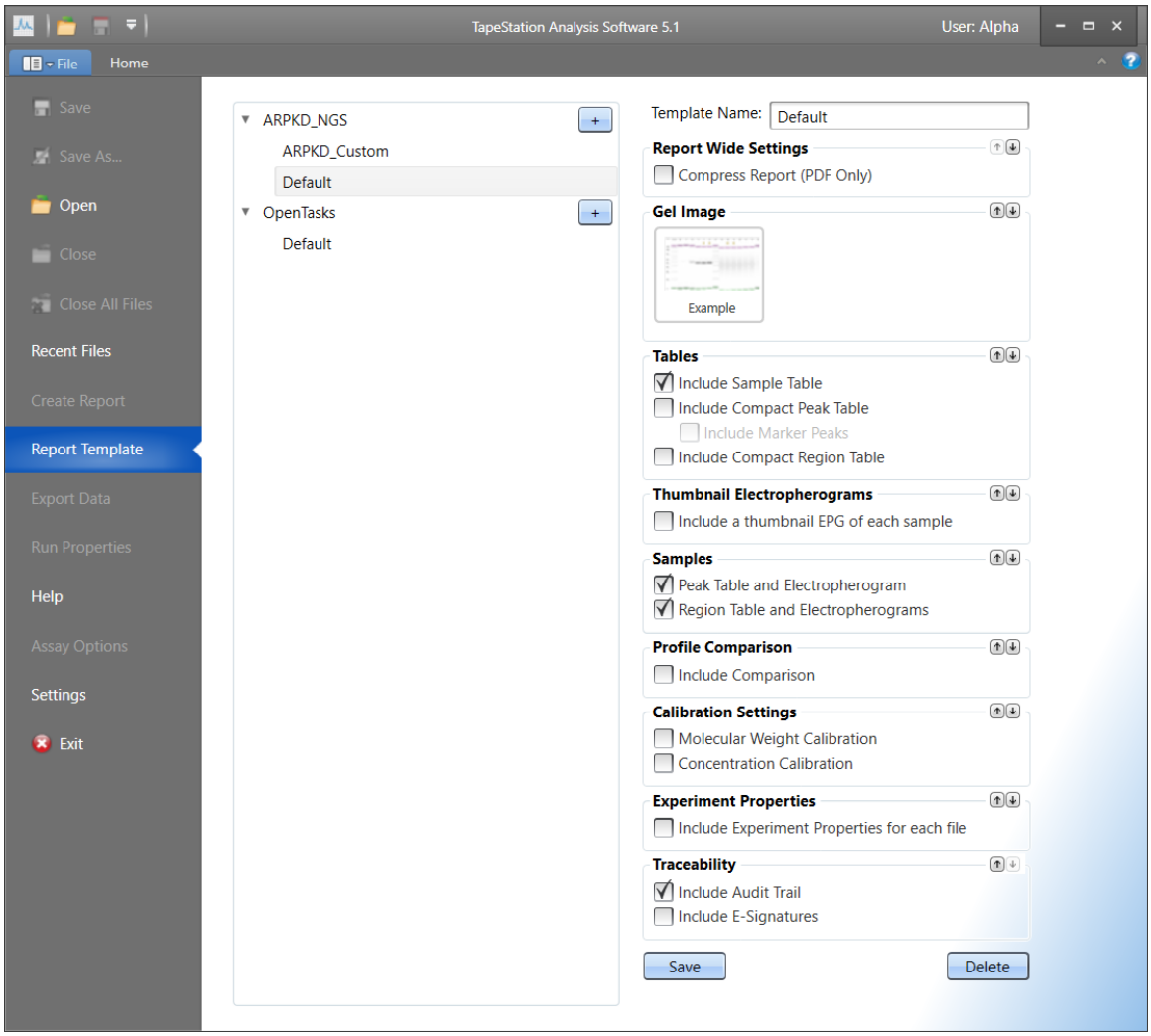


Figure 32 Report Template generation in the TapeStation Analysis software

Signature Meanings

Signature *Meanings* can be selected from a dropdown menu within the TapeStation Analysis software when applying an electronic signature. They are predefined. They are used at the transition to a next step in a workflow and can be edited under *Global settings* by a *System Administrator*, see page 29.

Secure Data Storage

Secure Data Storage prevents unauthorized access and modification of data outside the Security Module software. This might include physical protection of the medium on which the data is stored, as well as dedicated third party security software which applies restrictive policies or blocks access. Depending on laboratory owned policies, such system typically features measures that make files non-erasable, possibly provides versioning, administrates the permissions to modify and have general traceability of container. Such security software completes the system outside the TapeStation Security Module software. Secure Data Storage for TapeStation Security Module software revision 5.1 is the responsibility of the user's organization.
A white paper (document number D0028138) as resource for *Users* of the Agilent TapeStation system whose organizations must comply with US FDA Part 11 in Title 21 of the Code of Federal Regulations (CFR), and its EU analog, Eudralex Chapter 4, Annex 11, is being prepared.

Traceability Group

Traceability Group in the TapeStation Analysis software consisting of

- Review Audit Event, see page 32.
- View *Audit Trail*, see page 34.

It offers an access to the Audit Trail, review its options and printing.

View Audit Trail

Under the Security Module software an *Audit Trail* records all the change events applied to a data file. The *Audit Trail* resides in the data file and is protected from unintended modifications.

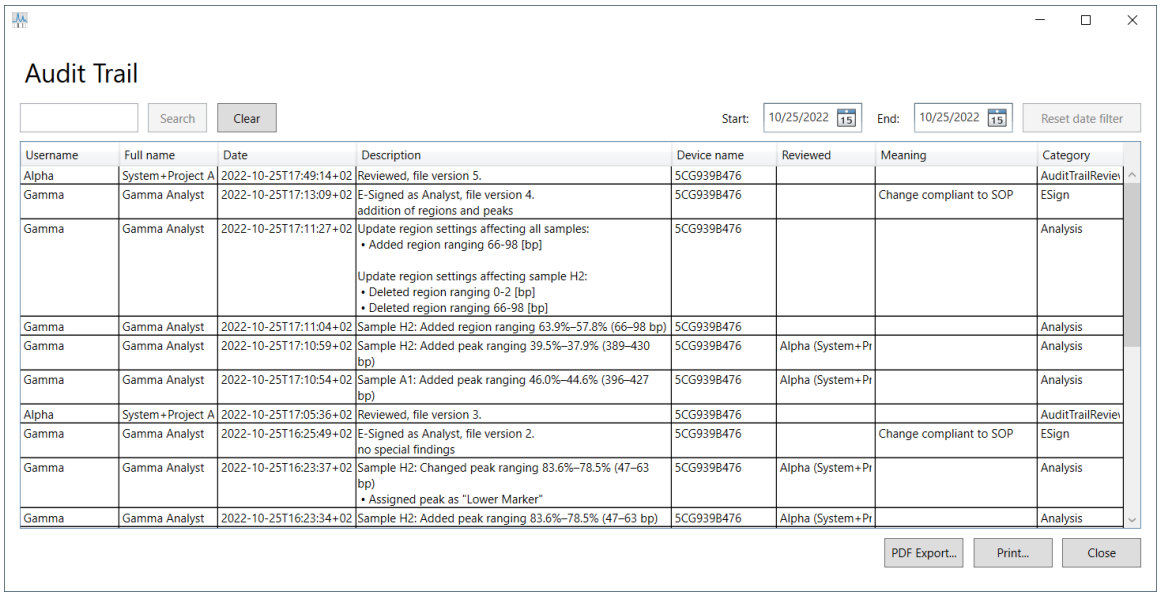
Figure 34 View *Audit Trail* icon in TapeStation Analysis Software

If a data file is loaded, its *Audit Trail* can be opened (Figure 34), and it shows as table (Figure 35). It contains any change event with the columns *Username*, *Full Name*, a *Date*, *Description*, *Host Name*, *Reviewed*, *Meaning*, and *Category*. *Reviewed* and *reason* fields have content after *Review Audit Events* happened (see page 32). Electronic signatures during work on data files will fill the reason field also.

The *Audit Trail* column **Category** includes information on the source or trigger for the respective entry:

- Instrument Operation
- Electronic Signature
- Audit Trail Review
- Analysis
- Saving
- Comparison
- Reporting

The *Audit Trail* can be printed or exported. Search on texts and filter options for date ranges are available.



Username	Full name	Date	Description	Device name	Reviewed	Meaning	Category
Alpha	System+Project A	2022-10-25T17:49:14+02	Reviewed, file version 5.	5CG939B476			AuditTrailReview
Gamma	Gamma Analyst	2022-10-25T17:13:09+02	E-Signed as Analyst, file version 4. addition of regions and peaks	5CG939B476		Change compliant to SOP	ESign
Gamma	Gamma Analyst	2022-10-25T17:11:27+02	Update region settings affecting all samples: • Added region ranging 66-98 [bp] Update region settings affecting sample H2: • Deleted region ranging 0-2 [bp] • Deleted region ranging 66-98 [bp]	5CG939B476			Analysis
Gamma	Gamma Analyst	2022-10-25T17:11:04+02	Sample H2: Added region ranging 63.9%–57.8% (66–98 bp)	5CG939B476			Analysis
Gamma	Gamma Analyst	2022-10-25T17:10:59+02	Sample H2: Added peak ranging 39.5%–37.9% (389–430 bp)	5CG939B476	Alpha (System+Pr		Analysis
Gamma	Gamma Analyst	2022-10-25T17:10:54+02	Sample A1: Added peak ranging 46.0%–44.6% (396–427 bp)	5CG939B476	Alpha (System+Pr		Analysis
Alpha	System+Project A	2022-10-25T17:05:36+02	Reviewed, file version 3.	5CG939B476			AuditTrailReview
Gamma	Gamma Analyst	2022-10-25T16:25:49+02	E-Signed as Analyst, file version 2. no special findings	5CG939B476		Change compliant to SOP	ESign
Gamma	Gamma Analyst	2022-10-25T16:23:37+02	Sample H2: Changed peak ranging 83.6%–78.5% (47–63 bp) • Assigned peak as "Lower Marker"	5CG939B476	Alpha (System+Pr		Analysis
Gamma	Gamma Analyst	2022-10-25T16:23:34+02	Sample H2: Added peak ranging 83.6%–78.5% (47–63 bp)	5CG939B476	Alpha (System+Pr		Analysis

Figure 35 *Audit Trail* dialog with E-sign/*Meaning* and reviewed info

How To Find The Role With Correct Permission?

In case the default set of permissions lacks a permission to complete a task please look up Table 3 and Table 4 to identify the required permission. See Figure 14 for default *Role* permissions within the TapeStation Administration software. Permissions can also be reviewed on the fly per *Project* in the Controller software (Figure 36) or the TapeStation Analysis (Figure 37) from the respective user interface by clicking onto the *User* in the top line and selecting the relevant *Project*.

To correct the missing permission an administrator might add the permission to an existing *Role* or create a new customized *Role* (see page 18).

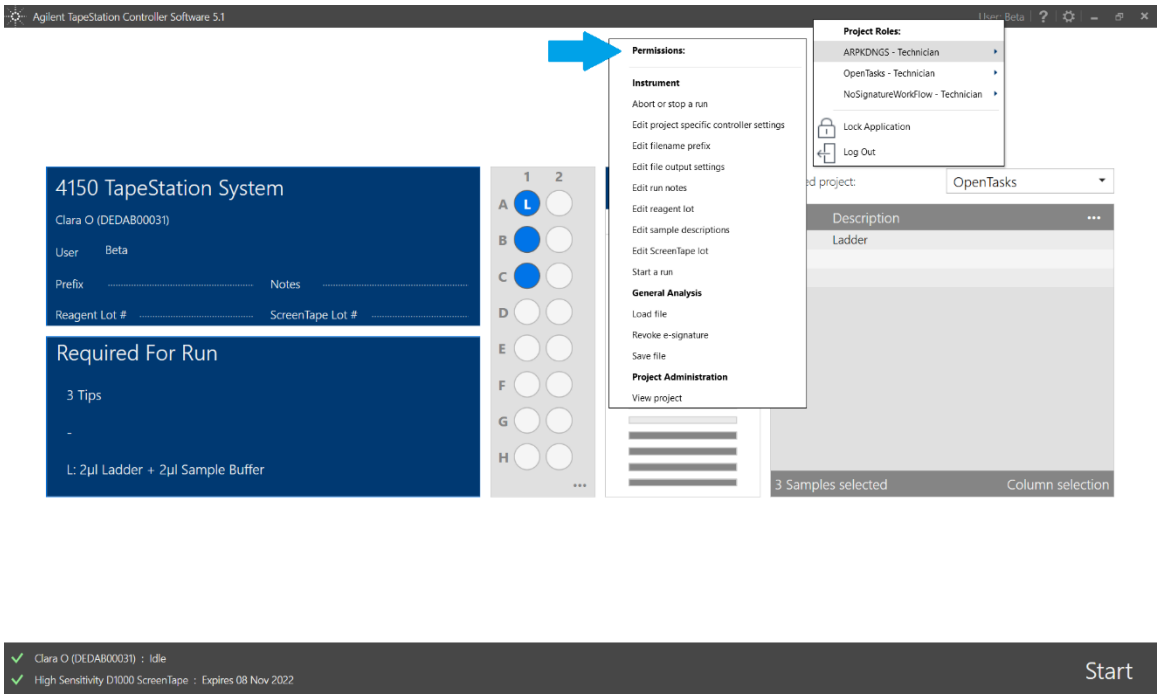


Figure 36 Review Permissions per *Project* of the *User* currently logged on in the Controller software.

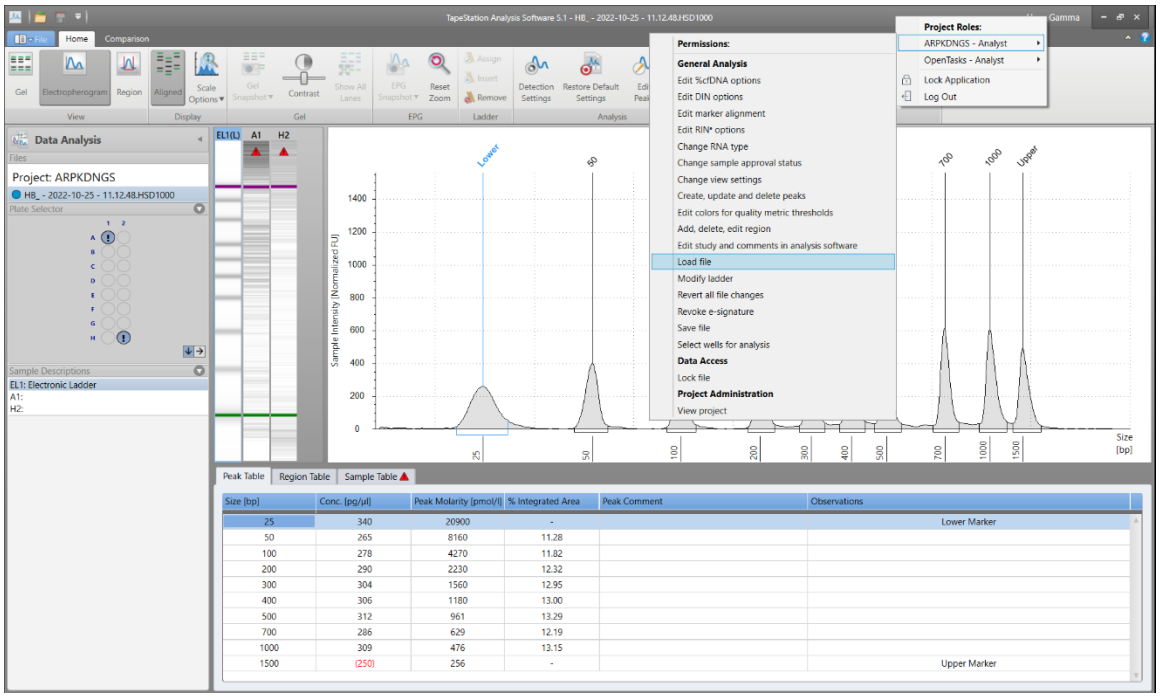


Figure 37 Review Permissions per *Project* of current logged on *User* in TapeStation Analysis software.

Why Are There No Audit Events For Review Available?

In the TapeStation Analysis software the button Review Audit Events will lead to a dialog that only has content if the respective modifications were not yet reviewed and if the event stems from a different *User* than the currently logged on *User*. Modifications which were already reviewed are visible in the *View Audit Trail* dialog with the timestamp and *Meaning*. *Users* cannot review and sign their own modifications.

Why Can't I Use Some Of The Buttons?

Permission to use functions associated with buttons in software dialogues are often bound to certain *Roles* or permissions. Therefore, the button might appear dimmed and non-functional. Please consider that the Security Module software restricts activities stringently in comparison to the regular software edition. For any activity, Table 3 and Table 4 indicate which default *Role* has the permission.

There might be other conditions that leaves a button inactive although permissions are present in principle. In such case, please regard the tool tip, possibly save the data, or even apply an electronic signature. Consider dependencies from the software logic that prevent using a button until another step is done.

How To Enable Usage Of Expired ScreenTapes?

ScreenTapes devices expire according to the date printed onto the barcode label or 14 days after their first insertion to the instrument. It is not recommended to use ScreenTapes devices beyond these dates. You can deviate from this default condition. A *User*, typically the *Project Administrator*,

with the permission to change an instrument setting *Edit allowing expired ScreenTape* is required to do this for a dedicated *Project* from the Controller software (not recommended). This setting is permanently linked to the *Project*, even if the logged on *User* changes or the software is restarted.

How Can Data Be Imported From Other Security Module Installations?

They can be imported by the *Project Administrator*. When using the File Open dialog, an import step to a dedicated *Project* is offered (Figure 38). File name and parameter change needs to be acknowledged (Figure 39). Due to the transfer, the *Audit Trail* will show a warning indication about the file import (Figure 40).

All rules of the *Project* to which this file was imported do apply from the import on. The *Audit Trail* of the file will be continued as of import.

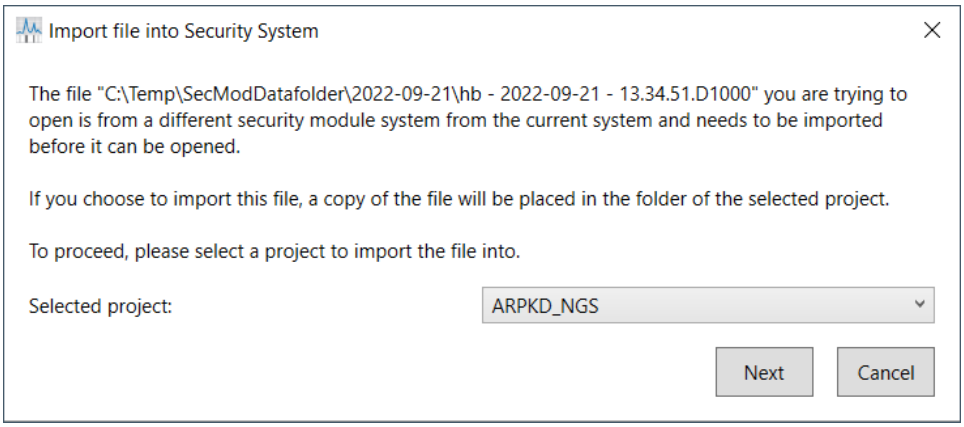


Figure 38 Importing data: select a dedicated *Project*

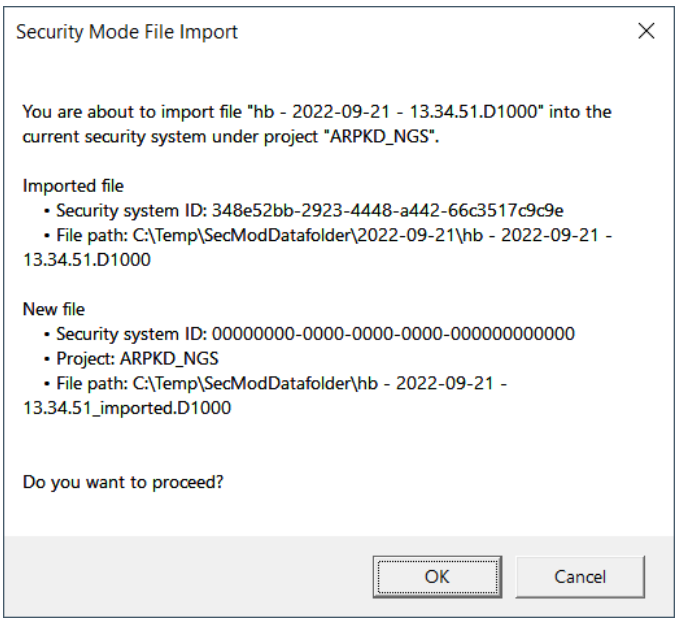


Figure 39 Imported data file details

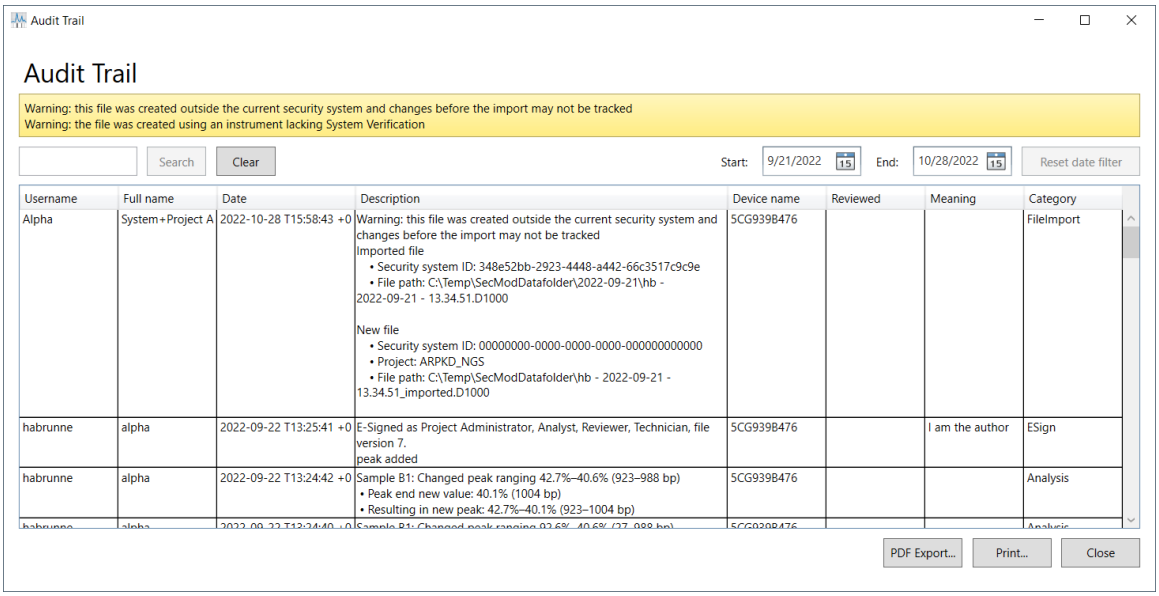


Figure 40 Audit Trail details for imported data

Is A Comparison Mode Available In The Security Module Software?

The tab *Comparison* in the Analysis software allows the *Analyst* to combine two or more lanes from two or more files into one composite file. This is possible for data from the same *Project* only. Data files need to be loaded to the home tab previously. The *Audit Trail* of a composite file will subsequently contain the history of both files and continue with recording from the moment it was created. Use checkmarks to filter for events specific for one initial file of the comparison file (see Figure 41).

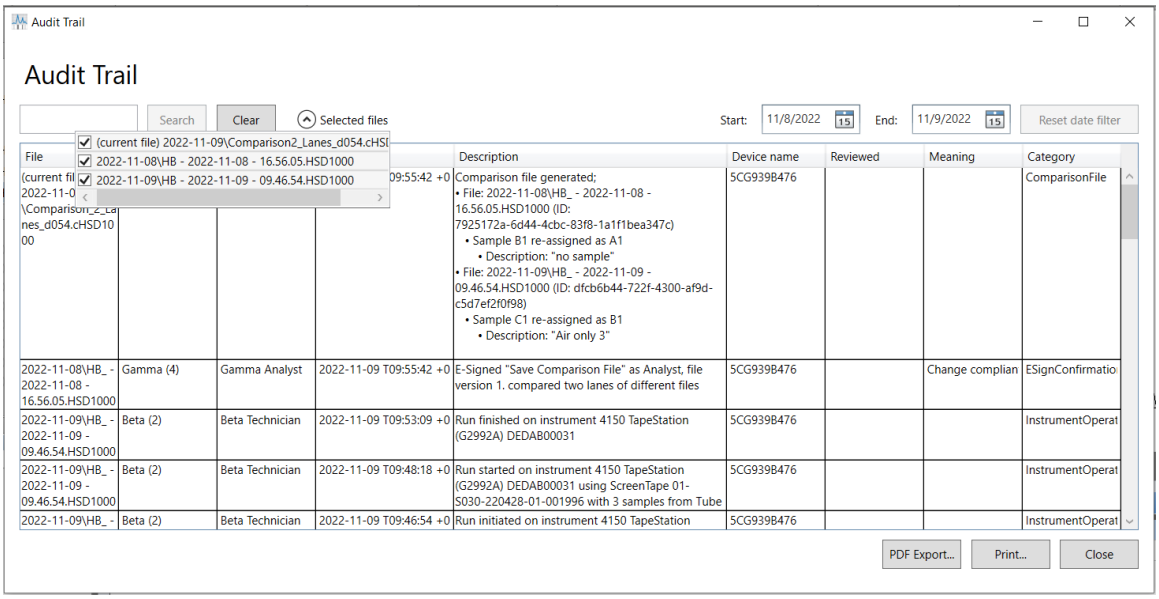


Figure 41 *Audit Trail* for files combined in the *Comparison* Mode

What Impact Have Runs With Non-Verified Systems To The Audit Trail?

It is not recommended to perform analysis runs with non-verified units. The top line of the *Audit Trail* (see Figure 42) will subsequently have a warning that states the file was created using an instrument lacking the *System Verification*. See details for operating a non-verified instrument in Figure 20.

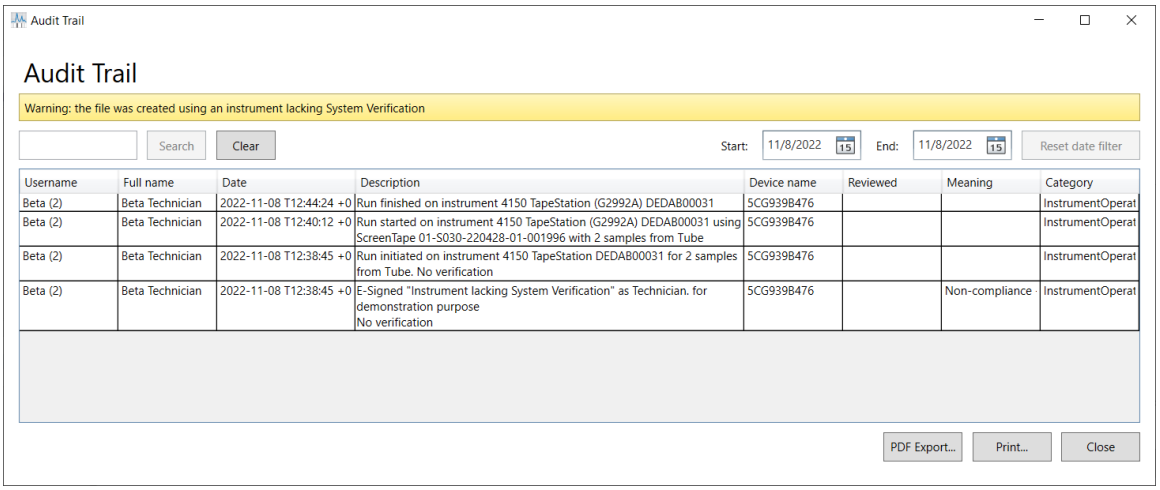


Figure 42 *Audit Trail* details for analysis runs with non-verified systems

Can Data Be Imported That Was Generated Outside Of The Security Module?

Files from outside the Security Module as well as legacy data files can be imported to a *Project*. The import dialogs are equivalent to importing from a different Security Module installation. See Figure 38, Figure 39 and Figure 40.

All rules of the *Project*, to which this file was imported, apply from the import on. The *Audit Trail* of the file will show the import and will be continued as of the import data.

How to Change The Authentication Mode

Resetting the Authentication mode equals changing the repository of *Users* from Windows Active Directory to local accounts or vice versa. Resetting Authentication mode is done under *Global Settings* within the Administration software (Figure 29). The selection at the setup of a system should be done carefully in the first place. Aligning this after resetting can be complicated.

Resetting the authorization mode requires archiving of previous *Users*. Subsequently, previous *Users* will be locked out and it is not possible to link newly added *Users* with their old data. For example, unlocking a data file or reverting an electronic signature becomes impossible. However, no data is deleted during this process. You will be able to link new *Users* to existing *Projects*.

This change on the authentication mode is processed only by confirming the decision with a password, twice.

Are There Special Analysis Software Features?

Selected features of the TapeStation Analysis software are absent from the Security Mode Edition. Additionally, there are some features that are present in the Security Mode edition which are not found in the other TapeStation Analysis software edition.

Absent are features which have an assay wide impact and as such would trigger undesired changes in existing data once these are reopened. Exporting reports to Microsoft Word is unavailable as further modifications of exported data in this secondary software are difficult to prevent.

Two groups (Traceability and E-sign), *Report Template* creation and a field for the approval status in the sample table are additionally present in the Analysis software.

Can Files Be Reverted To An Earlier Version?

Data file version changes are visible in the *Audit Trail*. The actual version is also visible under File > Run Properties. With TapeStation Security Module software revision 5.1 it is not possible to return to one specific intermediate revision of the file. In case an earlier status is desired, the *Analyst* with the permission "revert all files changes" can set back the data file to the initial status and analysis can start over again.

How to rescue data from a broken system

If the system breaks but data files and administrative reports on *Projects* and *Roles* are still present, a system can be similarly recreated. Uninstall and reinstall the software and verify its functionality by the build in diagnostics. In case they were not affected by the issue, *Projects*, *Users* and *Roles* are automatically in use again.
Otherwise all *Projects*, *Users* and *Roles* require to be set up again and require manual input of details. Data files must be imported then to the recreated, similar *Project*. This correction leads to traces in the new *Audit Trail* of files and the new system activity log which is obvious by the nature of the event.

Is Archiving Of Projects And Data Possible?

Archiving and de-archiving is available for a *System Administrator* because of the permission to manage *Projects*. An archived *Project* will not be available for selection in the Controller software any longer.
Data files recorded under a *Project* that was archived are still present in the data repository. However, all associated permissions of a *Users Role* within the *Project* are de-activated including the permission to open of such data file. This makes the data unavailable for *Project* members until an administrator performs the de-archiving.

In This Document

The manual describes the following:

- General description
- Setting up of the Security Module software
- Setting up of Users, Roles and Projects
- Data analysis
- Reporting
- Administrative elements
- Glossary

www.agilent.com

Edition 01/2023
REVISION A.01
This document is subject to change without notice.

Document number D0025074

.....