

# Agilent Security Module Software

## Guide

<b>What Is the Agilent Security Module Software?</b>	<b>2</b>
<b>Installation of the Fragment Analyzer Security Module Software</b>	<b>4</b>
<b>Initial Tasks When Working With The Security Module</b>	<b>6</b>
Login	6
Setting Up a Project	7
Setting Up Users and Roles	11
<b>Reoccurring Tasks When Working With the Security Module</b>	<b>20</b>
Sample Analysis	20
Data Analysis	21
<b>Other Administrative Elements of the Security Module</b>	<b>22</b>
Activity Log Functionality in the Administration Software	22
Reports In the Administration Software	22
Global Settings	23
<b>Glossary</b>	<b>24</b>
<b>Frequently Asked Questions</b>	<b>26</b>

# What Is the Agilent Security Module Software?

This software edition comes as a standalone package consisting of the Administration Software, Controller software, and ProSize data analysis software.

The Fragment Analyzer Security Module offers a combined installer, which includes the Administration software, Fragment Analyzer controller software and ProSize data analysis software.



**Figure 1** Desktop icon of the Administration Software

The Agilent Security Module software package supports using the parallel capillary electrophoresis systems in regulated laboratory environments by providing a feature set including:

- workflow management
- access control
- e-Signatures
- data reports
- audit trails

After the Security Module package is installed, the Administration Software is installed and visible ([Figure 1](#)) in addition to the standard software elements. See [Table 1](#) on page 3 for a general overview of the software parts and functions.

The Security Module user authentication is enforced and supported by a database stored locally on the system.

Users must log in to be able to use the software. *Projects* represent containers of related work that allow assigning roles with specific permissions associated. *Roles* that 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 Software in the proposed order are illustrated in [Figure 2](#) on page 3.

Some steps are done only occasionally:




- Setting up one or multiple projects
- Setting up users and assigning roles

Other tasks are reoccurring:

- Sample analysis
- Data analysis
- Workflow finalization
- Reporting

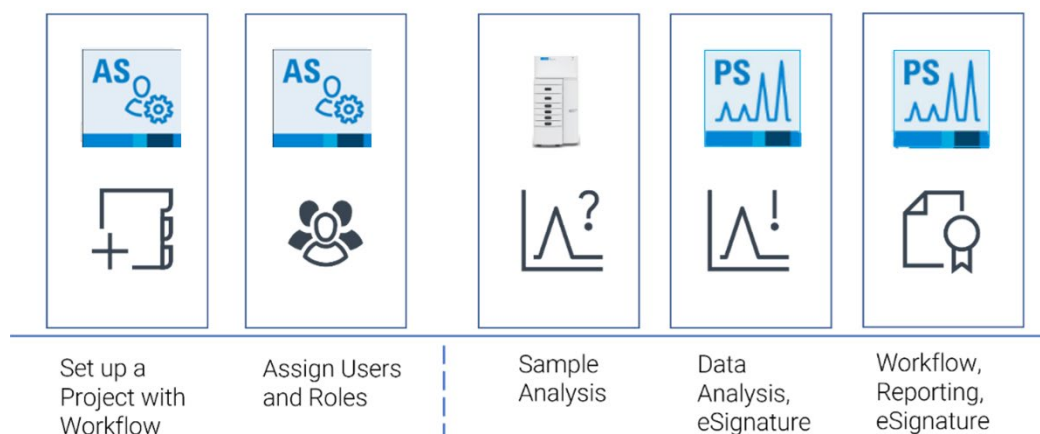
## What Is the Agilent Security Module Software?

**Table 1 Overview on the Agilent Security Module software functions**

Icon	Name	Functions
	Administration Software	<ul style="list-style-type: none"> <li>• User management</li> <li>• Setting up and editing of projects</li> <li>• Creation of customized roles</li> <li>• Assigning of roles to users</li> <li>• Creation of reports on projects, roles, users, system-wide activities</li> <li>• General security settings for the software</li> </ul>
	Fragment Analyzer controller software	<ul style="list-style-type: none"> <li>• Control the instrument during data acquisition</li> <li>• Sample selection and description</li> <li>• Capture of notes</li> <li>• Run of analytical assays</li> <li>• Hardware Maintenance</li> </ul>
	ProSize data analysis software	<ul style="list-style-type: none"> <li>• Data analysis and reporting</li> <li>• Review data as electropherogram and gel image</li> <li>• Integration, peak and region annotation</li> <li>• Size, quantity, molarity, Calculations</li> <li>• Reports</li> <li>• Sample comparison across multiple files</li> </ul>

### Occasional/preparative tasks

### Reoccurring tasks



**Figure 2** Major tasks when using the Security Module

# Installation of the Fragment Analyzer Security Module Software

The Fragment Analyzer systems are typically distributed as a bundle with desktop computers that are tested and fully supported by Agilent. These computers come with preinstalled standard software. The Security Module software requires a dedicated installer.

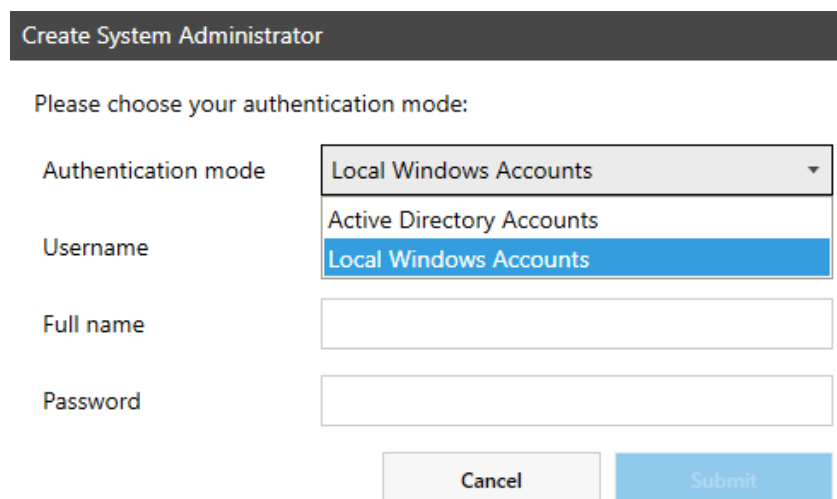
The readme file provides installation advice and useful information on:

- PC Hardware (minimum requirements)
- Operating System Requirements

When opening the Administration Software for the first time, it automatically creates a *user* with **System Administrator** role. For details on setting up further users and administering their roles, see [“Setting Up Users and Roles”](#) on page 11.

During this initial **System Administrator** setup, select between the two **Authentication mode** options (**Local Windows Accounts** or **Active Directory Accounts**). This selection is exclusive, a mixture of the two modes for authentication is not possible.

Choose the **Authentication mode** carefully as it is complicated to revert.



Create System Administrator

Please choose your authentication mode:

Authentication mode: Local Windows Accounts

Username: Local Windows Accounts

Full name:

Password:

Cancel Submit

**Figure 3** Initial System Administrator setup

Key points of the Security Module Software:

- The first user launching the Administration Software (Figure 3) becomes the **System Administrator** of the Security Module Administration Software by default. This role can later be transferred to other users. Always keep at least one **System Administrator** active.
- When installing the Security Module Software, several features in the Controller software and the ProSize data analysis software become restricted. Those features need permissions, which are assigned to user roles.
- The software can be directly upgraded from the standard edition to the Security Module Software edition. However, reverting from the Security Module to standard mode is not supported and it requires a complete uninstallation, PC restart, and new installation of the standard software.
- When uninstalling the Security Module software, 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 computer reestablishes the previous situation. An update path will be provided for future revisions of the Security Module software. This allows the ability to import users, roles, projects, and result data folders.
- ProSize data analysis of the Security Module cannot be installed on standalone without the Controller software. Data review is done exclusively on the system computer. Reviewing on other computers outside the Security Module software can only occur after exporting or importing another Security Module system. This is because projects and roles and Audit Trails are maintained on the computer used for the run itself. After exporting the data file, it becomes a regular file without Audit Trail.

### CAUTION

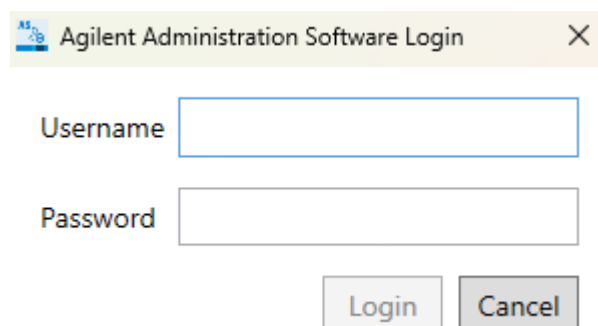
#### Loss of data

**If all System Administrators are removed from the computer or from the Windows Active Directory, the entire Security Module Administration Software becomes unusable and cannot be recovered.**

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

# Initial Tasks When Working With The Security Module

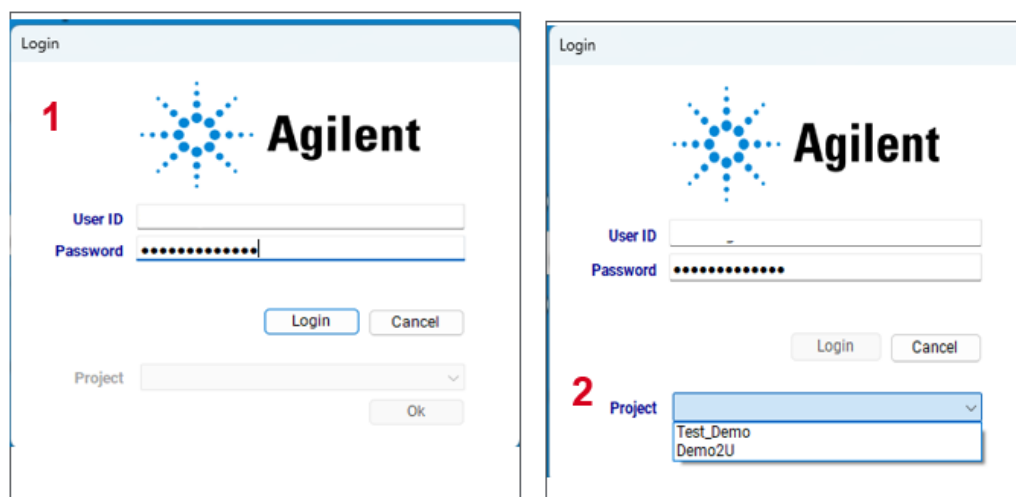
## Login



A screenshot of the 'Agilent Administration Software Login' dialog box. It features a title bar with the Agilent logo and a close button. The main area contains two text input fields: 'Username' and 'Password'. Below these fields are two buttons: 'Login' and 'Cancel'.

**Figure 4** Login screen

Login is required to launch the Security Module software (Figure 4), Fragment Analyzer controller software (Figure 5-1) and ProSize data analysis software (Figure 5-2). It is necessary to enter user ID, password, and select the specific project associated with the run or data analysis. The Administration software can be accessed from both ProSize data analysis software and Fragment Analyzer controller software via the Administration menu.



Two side-by-side screenshots of the 'Login' window illustrating the authentication process. The left screenshot, labeled with a red '1', shows the initial state with the Agilent logo, 'User ID' and 'Password' fields, and 'Login' and 'Cancel' buttons. The right screenshot, labeled with a red '2', shows the 'Project' dropdown menu open, displaying 'Test\_Demo' and 'Demo2U' as options.

**Figure 5** User authentication

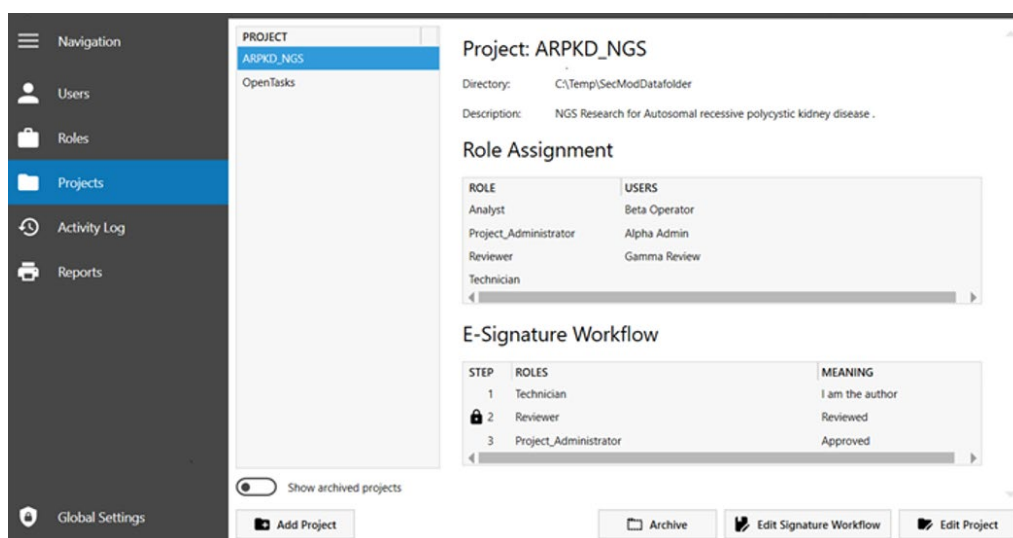
## Setting Up a Project

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, and information (project descriptions, data directory) related to a planned type of work.

Administrators can add, edit, or archive projects. The **Projects** tab (Figure 6) gives an overview on existing projects and their parameters. A project can be selected in the Controller software from the list of active projects prior to sample acquisition and analysis.

Table 2 on page 11 shows predefined **System Roles** and **Project Roles**. This overview helps with understanding the assignments within the project setup. See “Glossary” on page 24 for brief explanations on dedicated terms.



**Figure 6** Projects menu in Administration Software, overview of an existing project

**Project Creators** and **System Administrators** can create new projects, as these are system-wide roles with default permissions to do so. They automatically become the first project administrators for new projects. They can set up further project administrators and assign them project-related roles to manage their projects. They can customize the granted permissions per role, so they may deviate from the default. For more information, see “Setting Up Users and Roles” on page 11.

## Initial Tasks When Working With The Security Module

- 1 To create a new project, click **Add Project**.

The project setup dialog opens. Mandatory fields for new projects are marked with an asterisk:

- **Name**
- **Output Directory**

- 2 Enter a project **Name**. This name is the identifier that is selectable in the Controller software and appears as the identifier in the ProSize data analysis software as well. Short identifiers are recommended while the **Description** field allows the addition of details.
- 3 Select an **Output Directory**. This directory should be a dedicated local data folder accessible by the Administration Software. To protect this folder, a third-party software can be used to control access permissions. Having a secured backend outside the Security Module software (see “[Secure Data Storage](#)” on page 25) completes the system.

### CAUTION

#### Data Integrity

**This software does not provide a content management system. Unauthorized modifications can lead to loss of data.**

- ✓ **Set up and control a compliant data management system. This is the responsibility of the user's organization.**

All users registered within the Security Module (see [Figure 11](#)) are listed and can be assigned to a role in a project ([Figure 7](#)). 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 check boxes) and roles (horizontal, as tabs) depends on the individual setup provided by the administrator.

A user's role assignment can be changed in a project in the **Users** menu in the Administration Software. For example, an existing user can be edited or a new one added (see “[Setting Up Users and Roles](#)” on page 11). Data is not affected by changing a user's role in a project.

While setting up or modifying a project, no other users may be logged in.

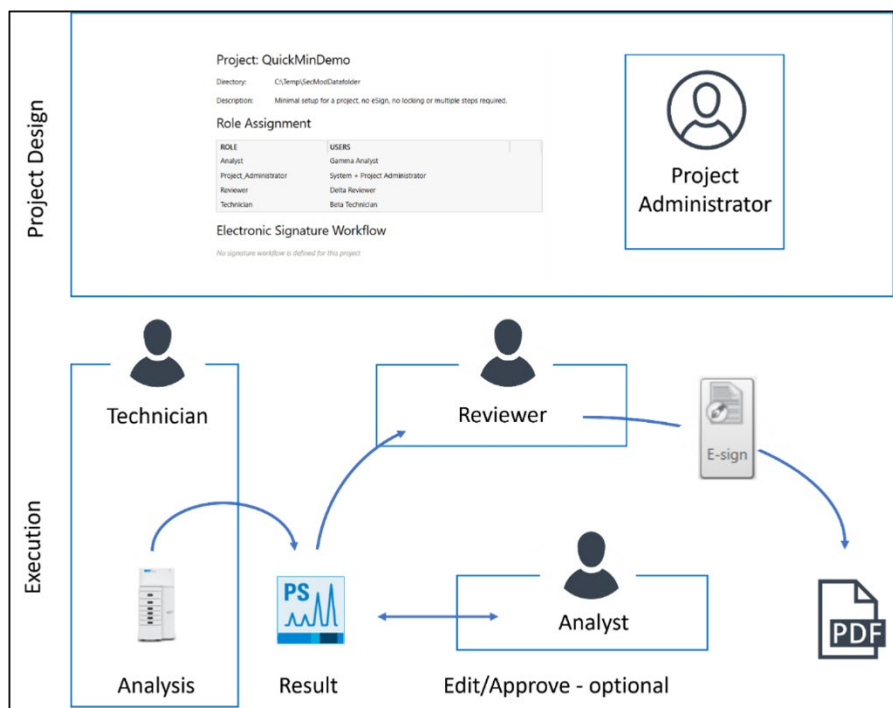
The screenshot shows the 'Add project' dialog box. The 'Name' field is required and contains 'Demo Project'. The 'Description' field is optional and contains 'For Demonstration Purpose only'. The 'Output Directory' field is required and shows a folder icon next to the path 'C:\Temp\SecModDatafolder'. The 'Project Roles' section has four tabs: 'Analyst (1)', 'Project Administrator (1)', 'Reviewer (1)', and 'Technician (1)'. The 'Technician (1)' tab is active, displaying a list of roles with checkboxes. The roles are: Beta Technician (checked), Delta Reviewer, Gamma Analyst, Omega Service Engir, System+Project Adm, and Theta System Validat. To the right of the list, the roles are grouped under their respective category names: Technician, Reviewer, Analyst, and Project Administrator. The 'Add' button is highlighted in blue.

**Figure 7** Project setup window



### Workflow Within Projects

Figure 8 shows a simple example workflow with three users. In the project design phase, the **Project Administrator** assigns respective roles to users. A **System Administrator** previously set up the users in the system.



**Figure 8** Simple example workflow

The **Technician** runs the samples with the Controller software. The ProSize data analysis software creates and shows the results.

The **Analyst** can 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 e-Signature with a reason for any changes.

The **Reviewer** can review and approve the data. These steps are finalized by an e-Signature with a reason for any changes.

### Electronic Signature Workflow

An *Electronic Signature Workflow* forces users to follow a given number of steps in a sequential order.

Defining a signature workflow is optional for a project. Figure 10 on page 10 shows an example workflow with three users.

In the **Projects** menu (Figure 6 on page 7), click **Edit Signature Workflow**. The **Edit Signature Workflow** window opens (Figure 9 on page 10).

If 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 ProSize data analysis software. In the ProSize data analysis software, an **Analyst** edits, analyzes, and reviews the data before a final approval by a **Reviewer**.

Set the **Meaning** to a certain predefined text or to **Any**. The **Meaning** is recorded to the File Lock Records when the respective user executes the required step in the ProSize data analysis software. To customize texts under the **Any** list, see "Global Settings" on page 23. In addition, users can also add free text comments to the **Meaning** once the e-Signature is applied when finalizing the step of the workflow.

## Initial Tasks When Working With The Security Module

Automatically lock a data file from further editing at a defined step (lock symbol). See “Lock status of a file” on page 25.

For good laboratory practice, it is recommended to keep a project workflow as it is once the first analysis is done. If not, two files might be created under different policies, which is correctly documented from the activities log file of the system.

STEP	ROLES	MEANING
1	Technician	I am the author
2	Analyst	Ready for review
3	Reviewer	Approved

Lock file after signing at step: 2

Figure 9 Editing the signature workflow with predefined meanings

## Example Project with signature workflow

Figure 10 shows an example signature workflow with three different users. The following paragraphs give more detailed descriptions.

At this point, the **System Administrator** has already set up the users with the respective roles in the system and defined meanings with which the users can transition the data to the next step. The transition is accompanied by giving their e-Signature.

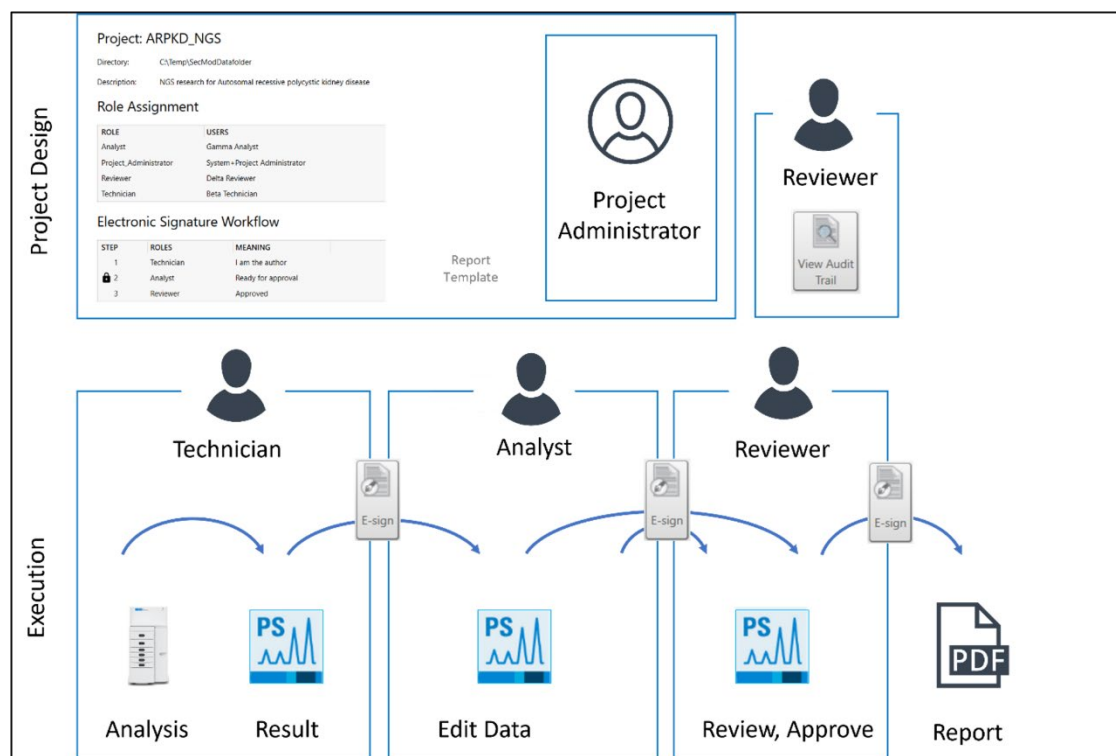


Figure 10 Example signature workflow with three users and three steps

## Initial Tasks When Working With The Security Module

In the project design phase, the **Project Administrator** creates three steps and assigns a different role to each step.

- 1 The **Technician** runs the analysis with the Controller software.

The ProSize data analysis software shows the results. The **Technician** applies the e-Signature and saves data for the next steps.

- 2 The **Analyst** edits the data, adjusts integration boundaries, or peaks, and finalizes the step with an e-Signature.

The **Project Administrator** should lock the file from further modification. This locks the file automatically as defined by the project.

- 3 The **Reviewer** reviews and approves the data.

### NOTE

In this example, the locking event in step 2 blocks the **Reviewer** from reviewing and explicitly signing audit events like integration changes, peak additions, or peak assignments.

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 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 if it was the last e-Signature applied. This might be desired to send the process back to the previous step for corrections. A **Reviewer** can view File Lock Records at any time.

## 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 that a user can have based on the permissions that were granted. The Administration Software has predefined **System Roles** and **Project Roles** (Table 2). For description of available permissions see "Permission Per Role" on page 14 and for customization of roles see "Customization Of Roles" on page 18.

While setting up or modifying users and roles, no other users may be logged in.

Table 2 Predefined System and Project Roles

Role	Role description
<b>System Roles</b>	
Agilent Service Role	Required by Agilent Field 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 validation
<b>Project Roles</b>	
Analyst	Works primarily with Analysis software
Project Administrator	Manages projects
Reviewer	Reviews, approves, and reports data
Technician	Works primarily at the instrument with the Controller software

## Initial Tasks When Working With The Security Module

The **Users** menu in the Administration Software gives an overview on existing users (Figure 11). It lists:

- Username
- Full name
- Assigned **System Roles** and **Project Roles**.

The **User ID** number is unique. A report can be generated on the users.

The **Users** menu allows an administrator to **Add User**, **Deactivate**, and **Edit User**. Add users either from the Active Directory or from local users of this computer. The choice between the two authentication modes is done during the initial user setup (see Figure 3).

Predefined and customized roles per project can be assigned to existing users from the **Users** menu. The **Users** menu gives an overview to which project the respective user was assigned an active role.

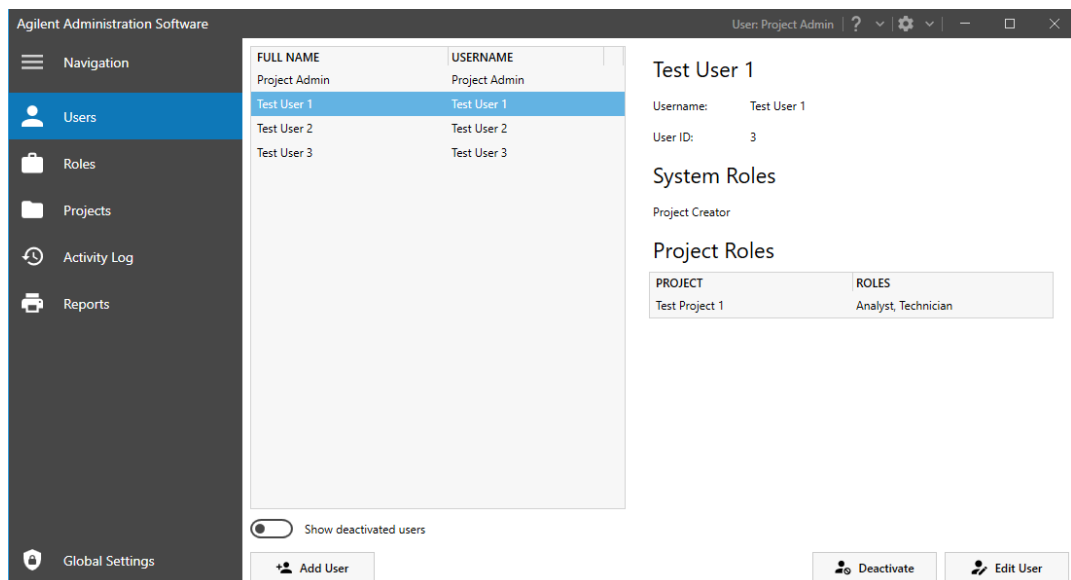


Figure 11 Users menu for the Administration Software

To add users, click **Add User**. Only **Administrators** can add users by searching either the **Full Name** or **Username** in the user repository, see Figure 12. Set up users with their **Full Name** because this information is shown in Electronic Signatures (e-Signature) together with the **Username**.

Users can be assigned any available role for projects that has already been set up depending on the desired workflow. The administrator can change or update this assignment at any point.

Initial Tasks When Working With The Security Module

Add User

Search Users:

Username

starts with

theta

Search

1 result

FULL NAME	USERNAME
(already registered)	Theta

Full Name \*

Username \*

System Roles

☐ Project Creator

☐ System Administrator

☐ System Validator

Project Roles

Analyst (0)

Project Administrator (0)

Reviewer (0)

Technician (0)

☐ ARPKD\_NGS

☐ NoSignatureWorkFlo

☐ OpenTasks

Cancel

Add

Figure 12 Add User window for managing users and their roles

In the following situations, a user is flagged with an exclamation mark:

- A user is locked out for too many failed login attempts.
- The user is not yet assigned to a project.

Agilent Administration Software

User: Project Admin

Navigation

- Users
- Roles
- Projects
- Activity Log
- Reports
- Global Settings

FULL NAME	USERNAME
Project Admin	Project Admin
! Test User 1 (no roles)	Test User 1
Test User 2	Test User 2
Test User 3	Test User 3

Show deactivated users

Add User

Test User 1

Username: Test User 1

User ID: 3

System Roles

No system-wide roles assigned

Project Roles

PROJECT	ROLES
---------	-------

Deactivate

Edit User

Figure 13 User window indicating a user is not yet assigned to a project

Agilent Security Module Software Guide

13

## Initial Tasks When Working With The Security Module

Administrators can select **Unlock User** or **Deactivate User** in the Administration Software. There is no need to remove the windows account to remove a user. Select **Show deactivated users** to review deactivated Users. Click **Reactivate** to add these users again.

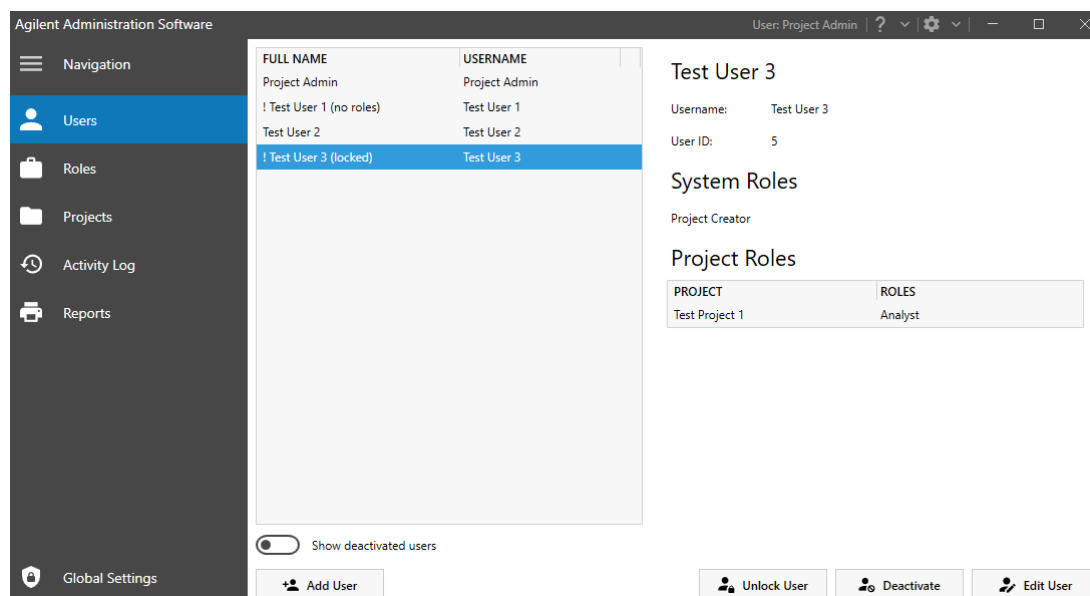


Figure 14 User window showing deactivated list and a locked user

### Permission Per Role

The tables below list all default roles and their permissions for the 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.

## Initial Tasks When Working With The Security Module

**Table 3 System Role permissions**

	System Administrator	Project Creator	System Validator
<b>System Administration</b>			
Create administrative reports	X	-	-
Create project	X	X	-
Create user account	X	-	-
Inactivate and re-activate user account	X	-	-
Manage global settings	X	-	-
Manage projects	X	-	-
Manage roles	X	-	-
Manage security	X	-	-
Manage users	X	-	-
Modify user account settings	X	-	-
Read all users	X	X	-
View error report	X	-	-
View event report	X	-	-
<b>Instrument Maintenance</b>			
Review system maintenance	X	-	X
Maintenance functionality	-	-	X
<b>Project Administration</b>			
Edit project specific settings	X	X	-

X: Role has permission by default

-: Role does not have permission

## Initial Tasks When Working With The Security Module

**Table 4 Project Role permissions**

	Technician	Analyst	Project Administrator	Reviewer
<b>Instrument</b>				
Abort or stop a run	X	-	-	-
Add array length	X	-	X	-
Add array serial number	X	-	X	-
Add or edit reagent lot number	X	-		-
Edit sample description	X	-	X	-
Edit run notes	X	-		-
Edit filename prefix	X	-		-
Edit/change number of capillaries	X	-	X	-
Edit EPG view settings	X	-		-
Add instrument serial number	-	-	X	-
Change automated report application path	-	-	X	-
Change buffer tray and row	-	-	X	-
Edit instrument type	-	-	X	-
Change data analysis software path	-	-	X	-
Change storage solution tray and row	-	-	X	-
<b>System Administration</b>				
View error report	X	X	-	-
View project	X	X	X	-
Manage projects	-	-	X	-
<b>Data Analysis</b>				
Unlock file	-	-	-	X
Lock file	-	X	-	X
Access Administration Software	X	X	X	X
View .raw data	-	X	X	X
View .psda data event log	-	X		X
Export data	-	X	X	X
View .db3 data event log	-	X	X	X
View .db3 data	-	X	X	X
View and analyze .psda data	-	X		X
Modify peak table settings in PDF Generation	-	-	X	-
Create report	-	-	X	X
Create, save, edit, and delete configuration files	-	-	-	-
<b>General Analysis (.psda files only)</b>				
Edit capillary position	-	X	-	-
Edit gel annotation	-	X	-	-
Export data to clipboard	-	X	X	X
Export data to Excel	-	X	X	X
Extract database file	-	X	X	X
Load/apply configuration file	-	X	-	-



## Initial Tasks When Working With The Security Module

**Table 4 Project Role permissions**

	Technician	Analyst	Project Administrator	Reviewer
Save as	-	X	X	X
Edit annotation	-	X	-	-
Change advanced settings – show markers on peak table	-	X	-	-
View capillary position	-	X	X	X
View file comparisons with .psda files	-	X	-	X
View file comparisons with .raw/.db3 files	-	X	X	X
View protein calibration curve	-	X	-	X
Restore default settings for analysis	-	X	-	-
View size calibration curve	-	X	-	X
Create/edit projects for .psda files	-	X	-	-
Create/add annotation (EPG)	-	X	-	-
Access to options menu	-	X	-	-
Add, merge, split, delete peaks	-	X	-	-
Assign/Change RNA Peaks	-	X	-	-
Assign peak as lower marker, assign peak as upper marker	-	X	-	-
Batch processing/view error log	-	X	-	-
Change advanced flag analysis settings	-	X	-	-
Change flag analysis settings	-	X	-	-
Change Genomic Quality Number settings	-	X	-	-
Change inclusion region settings	-	X	-	-
Create/Add gel annotation	-	X	-	-
Change marker analysis settings	-	X	-	-
Change peak analysis settings	-	X	-	-
Change peak start/end points	-	X	-	-
Quantification	-	X	-	-
Change RNA analysis settings	-	X	-	-
Change sample name in analysis software	-	X	-	-
Change advanced settings – mode	-	X	-	-
Change size calibration curve	-	X	-	-
Change smear analysis settings	-	X	-	-
Copy image to clipboard	-	X	X	X
Change advanced settings – minimum RFU for signal processing	-	X	-	-
Help/Create a support package (uncontrolled)	-	X	X	X
<b>System Permissions – Instrument</b>				
Save tray	-	-	X	-
Set bottle volumes	-	-	X	-
View run method	X	-	X	-
Create custom method/edit method	-	-	X	-
Enable auto data processing settings	-	-	X	-

## Initial Tasks When Working With The Security Module

**Table 4** Project Role permissions

	Technician	Analyst	Project Administrator	Reviewer
Access hardware test	X	-	X	-
Open file manager (for .raw and .db3)	-	-	X	-
Save selected row	-	-	X	-
Send stage to park	X	-	-	-
Run sample queue	X	-	-	-
Send stage to storage	X	-	-	-
Set solution levels	X	-	-	-
Send stage to buffer	X	-	-	-
Reset tray	X	-	-	-
Edit run method (add to Queue > Edit Method)	X	-	-	-
Prime gel lines	X	-	-	-
Load sample names	X	-	-	-
Clean reservoir vent valve	X	-	-	-
Change tray name	X	-	-	-
Adjust capillary alignment	X	-	-	-
Add sample to queue	X	-	-	-
Reset row	X	-	-	-

X: Role has permission by default

-: Role does not have permission

To see the permissions of a user who is currently logged in, navigate to the drop-down menu in the Administration Software interface.

### Customization Of Roles

There are default assignments of permissions to a role as shown in [Table 3](#) and [Table 4](#). An Administrator can customize these roles in two ways:

- Changing the permissions of an existing predefined **System Role** or **Project Role**.
  - a** Go to the **Roles** menu.
  - b** Click **Edit Role** (see [Figure 15](#)).
- Creating a new role with a new name and a customized set of permissions.
  - a** Go to the **Roles** menu.
  - b** Click **Add Project Role** or **Add System Role**.

All roles can be deleted except the **System Administrator**, the **Agilent Service Role** and the **System Validator**. These three roles are mandatory and required by the Administration Software. All dialog boxes have a similar interface (see [Figure 16](#)) and allow changing the **Name**, **Description**, and **Permissions**.

Initial Tasks When Working With The Security Module

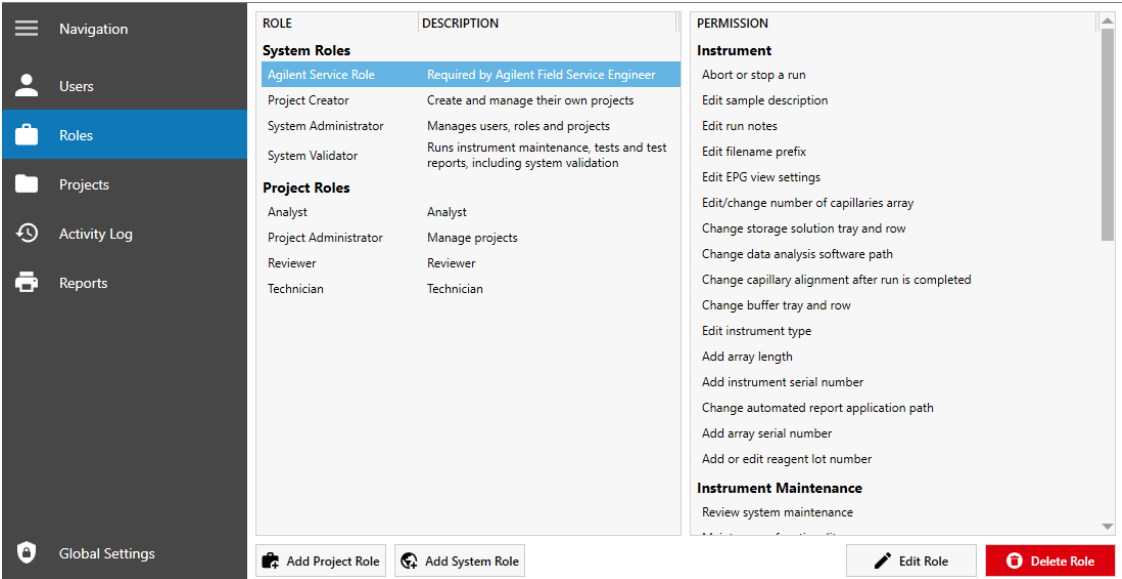


Figure 15 Roles menu

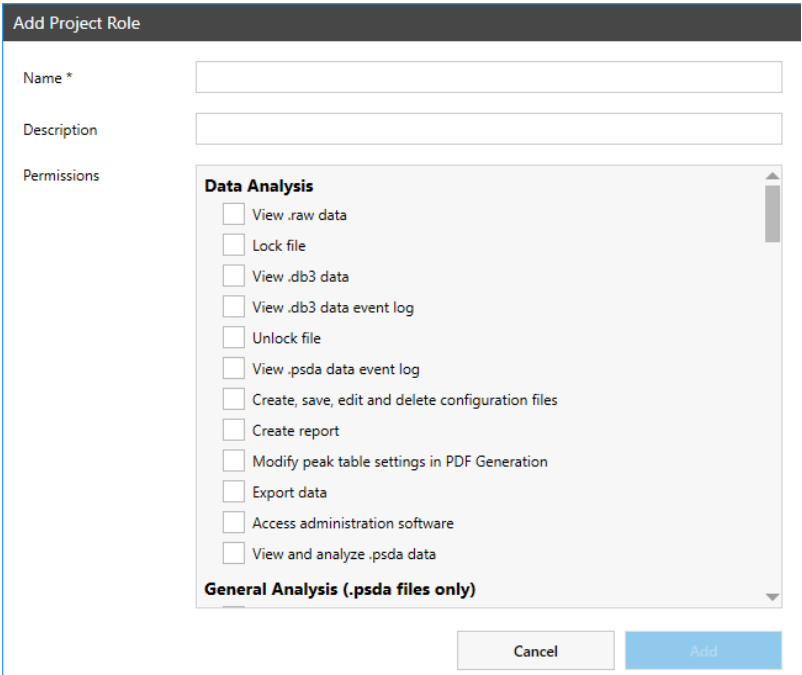


Figure 16 Add Project Role window

# Reoccurring Tasks When Working With the Security Module

## Sample Analysis

Sample analysis with the Agilent Security Module software is similar to analysis with the standard software. Please refer to the kit Quick Guides and the instrument user manuals. The installation and introduction service also introduces the relevant topics:

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

In general, the Controller software is designed to control the instrument during the data acquisition run. The software saves the data files, and they automatically open in the ProSize data analysis software for further processing. The Controller software allows users to select sample location and information, to configure the file save settings, and preselect method parameters. This software reports the instrument status and allows the review of diagnostic counters.

Starting an analytical run does not require an e-Signature. The **Start** button for this becomes active if:

- the *user* who is currently logged on has the permission to start a run,
- a *project* was selected,
- *samples* were selected

Additional features available in the Controller software when using the Security Module:

Access Administration Software: opens Administration Software

Event Report: found in the Administration tab

Project tab: list of available Projects a user can access

Log out: logs out current user

## Data Analysis

The ProSize data analysis software is a simple and intuitive software for data analysis and reporting. Results can be displayed as an electropherogram, as a gel image, or in tabular format for effortless sample comparison. Easily generate reports and save them in PDF format.

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

The **Technician** who records a data file can load and save the file.

The **Analyst** 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 Changes**. When operating without a **Signature Workflow**, manual locking is possible. In **Signature Workflows**, a lock can be placed at a dedicated step when setting up the project is set up, see [Electronic Signature Workflow](#) on page 9.

It is possible to print results of data from unlocked or locked files. This requires a user with **Reviewer** role permissions.

User ID	User's Role	Description	Date	Step Meaning
Test User	Project_Administrator, An		2024-11-19 09:30:48 PM -06:00	I am the author

Data File Name: SW IQOQ.psd

**Figure 17** Saving a data file forces an e-Signature with a reason for changes

Additional features available in ProSize when using the Security Module:

Data Approval:

- Sign Data; option to sign the data that is open in the software

- File Lock Records; opens the File Lock Record as seen in Figure 17 showing the User ID, User's Role, Description (if applicable), Date/Time stamp and Step Meaning

Administration tab:

- Administration Software; option to open the Administration Software

- View Data Event Log; opens the Data Event Log showing any changes made to the data with Date/Time stamp and responsible User

Project tab: List of available Projects a user can access

## Other Administrative Elements of the Security Module

### Activity Log Functionality in the Administration Software

The Activity Log lists which user performed an activity in the Administration Software. The log can be searched for text strings and filtered for the date. See [Reports In the Administration Software](#) on page 22 for creation of a printable report.

### Reports In the Administration Software

Administrative reports can be created individually:

- 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.

The screenshot shows the 'Administrative Report' creation interface. On the left is a dark sidebar with a 'Navigation' menu containing icons and labels for 'Users', 'Roles', 'Projects', 'Activity Log', 'Reports' (highlighted in blue), and 'Global Settings'. The main content area is titled 'Administrative Report' and contains a section 'Select reports for output:' with several checkboxes: 'Projects report' (with a sub-option 'Include archived projects'), 'Users report' (with a sub-option 'Include deactivated users'), 'Roles report', and 'Activity Log Report (for following date range)'. The date range is set from '4/25/2024' to '5/2/2024'. At the bottom right of the main area is a 'Preview Summary' button. At the bottom of the sidebar are 'Export PDF' and 'Print' buttons.

Figure 18 Administrative Report creation

## Global Settings

**Global Settings** reflect security settings applied to the entire Security Module software. In this section it shows the ability to define the duration for when an idle application requests a new log-on (Idle timeout). The ability to set the number of allowed unsuccessful login attempts before disabling a user and the duration of the lock-out.

Administer signature **Meanings** and **Reasons for Change**. These options are available in selection menus of the signature workflow and are applied during data analysis. **Edit settings** also allows for authorization change.

While changing the **Global Settings**, no other users may be logged in

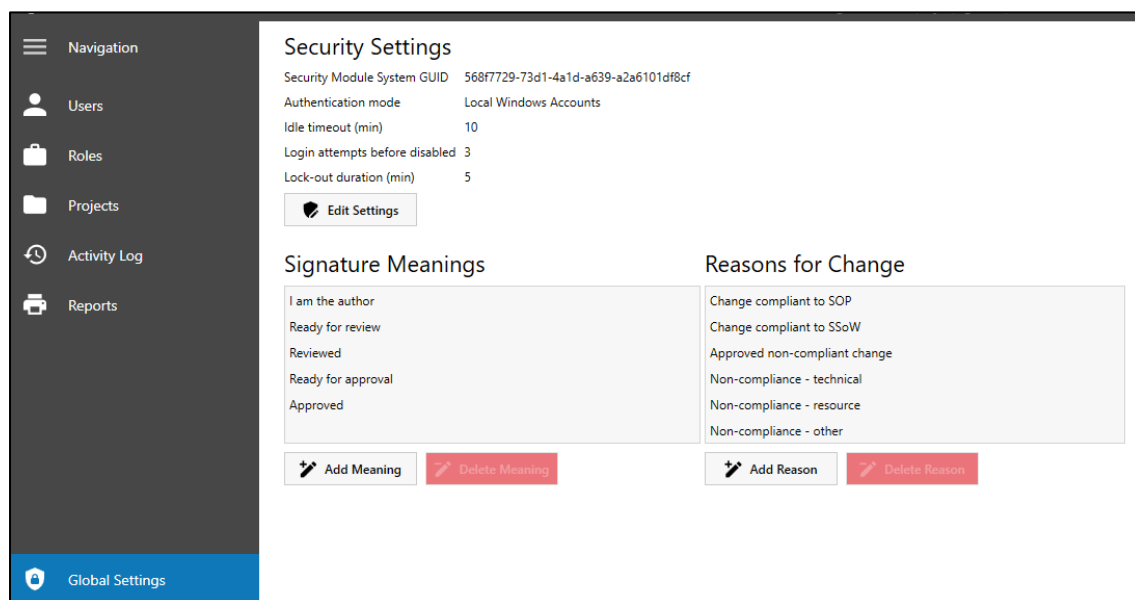


Figure 19 Global Settings offer adjusting **Security Settings**

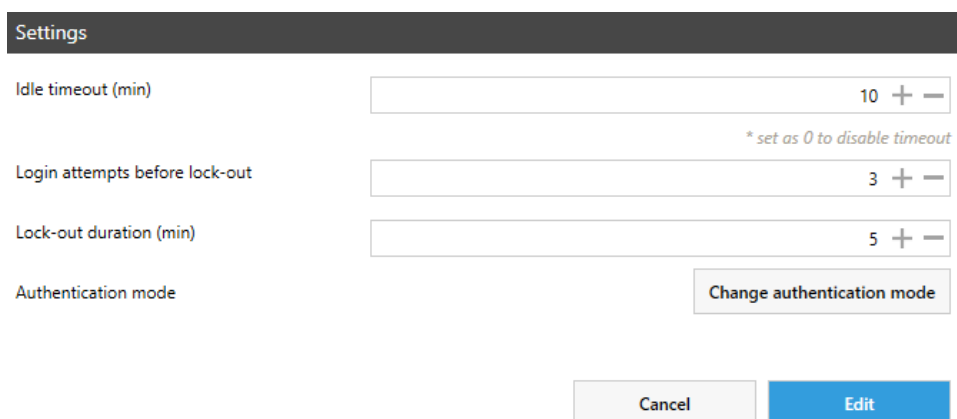


Figure 20 Editing **Global Settings** allows changing parameters and the authorization mode

# Glossary

## Administrator

This Guide mentions three types of administrators. There are **Project Administrators** and **System Administrators**, who are related to the Administration Software, and Windows administrators, who deal with local or domain permissions.

A Windows administrator is typically required to install Administration Software and to set up users either locally on the computer or on domain level, the Windows Active Directory.

Be aware, such Windows administrators must not delete the account of the last **System Administrator** or else the Administration Software becomes inaccessible.

## Activity Log

The **Activity Log** lists which user performed an activity in an Administration Software-related application. For example, it records log-in or log-out events in the Controller or Analysis software, as well as editing of projects, roles, and users in the Administration Software. There is the capability to search the log for text strings and filter by date.

## Authentication method

The term Authentication Method refers to the way a user is identified within the Administration Software. They will choose between the two authentication modes when setting up the first user. Changing it later is complicated. See also "[How to change the authentication mode](#)" on page 28.

## Archive/de-archive project

When archiving a project, it is no longer available from the selection list in the Controller software therefore new data cannot be added to the project. Existing data files become read-only in the ProSize data 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 "[Is archiving of projects and data possible?](#)" on page 28.

## Deactivate/reactivate users

The **System Administrator** can manage users. This includes setup, deactivation, and reactivation of users in the **Users** tab of the Administration Software using the respective buttons.

The function **Show deactivated users** displays deactivated users. A reactivation is possible.

## Electronic signature

Electronic Signatures, in this software referred to as e-Signature, can only be executed by the user logged in and require the user ID and the password. In e-Signature logs, e-Signatures display the full name and a **Meaning** together with a time stamp. Previous e-Signatures are retained after signing new ones.

E-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



### Reject data signature

This can be used for the last e-Signature applied. This is only available for the user who applied the signature. Rejecting data signature allows user to return to a previous step in a Signature Workflow.

### Full name

The username from the Windows Active Directory or local windows account is primarily used to log on and identify a user within the Administration Software. When setting up users, a full name can be given, typically along with more comprehensive details like the person's name or function.

### Lock status of a file

Once a file is locked no further changes can be made. The wording **unlocked/locked** in the ProSize data analysis software indicates the status of the data file currently loaded. Users can define at which stage to lock a file to avoid further changes. Certain activities remain possible for locked files such as:

- Opening and viewing
- Printing with report
- e-Signature
- File lock records

Users can force locking to happen automatically together with the respective e-Signature at predefined steps within a signature workflow (see [Electronic Signature Workflow](#) on page 9). This automated lock will happen for any user even if the current role comes without appropriate permissions, because the workflow forces it.

A locked file can be unlocked by the **Project Administrator**. For details on the required permissions, see [Table 4](#) on page 16. e-Signatures must be revoked before unlocking.

### Reason For Changes

Users can select **Reason For Changes** options from a drop-down menu within the ProSize data analysis software when applying an e-Signature. They are predefined and used when modifying and saving files such as integration changes, region introduction, or marker assignment. Their wording can be edited under **Global Settings**.

### Signature Meanings

Signature **Meanings** can be selected from a drop-down menu within the ProSize data analysis software when applying an e-Signature. They are predefined. They are used at the transition to the next step in a workflow and can be edited under **Global Settings** by a **System Administrator**.

### Secure Data Storage

Secure Data Storage prevents unauthorized access and modification of data outside the Administration 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 systems typically feature measures that make files non-erasable, possibly provide versioning, administrate the permissions to modify, and have general traceability of a file. Such a security software completes the system outside the Security Module software. Secure Data Storage for Administration Software is the responsibility of the user's organization.

A white paper as resource for users of the Agilent Capillary Electrophoresis 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 available.

## Frequently Asked Questions

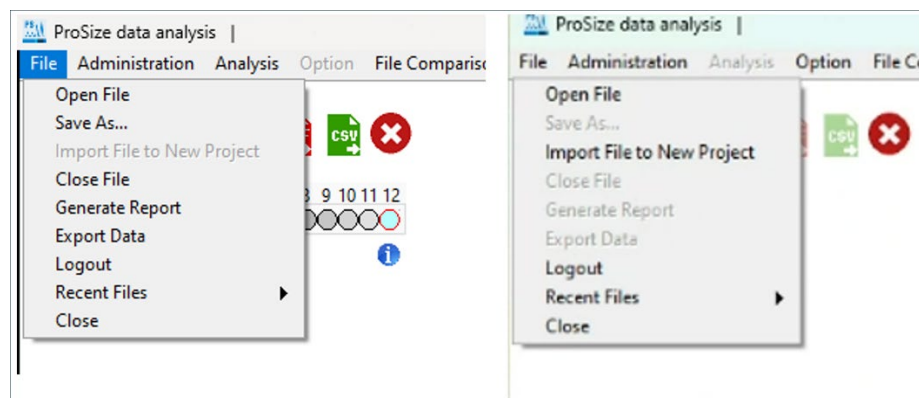
### Why are there no events for review available?

The **System Event Log** leads to a dialog from the Fragment Analyzer controller software that only has content if the respective modifications were not yet reviewed and the event stems from a different user than the one currently logged in. Users cannot review and sign their own modifications.

### Why can't I use some of the buttons?

Some functions require certain roles or permissions to use. This is why some menu icons might be inactive and non-functional. The Administration Software restricts activities stringently in comparison to the regular software edition. For any activity, [Table 3](#) on page 15 and [Table 4](#) on page 16 list which default role has which permissions.

There may be other conditions that leave a menu item inactive even if a user has the required permissions. In this case, refer to the tooltip, save the data, or apply an e-Signature. Consider dependencies from the software logic that prevent using a button or command until another step is done.



**Figure 21** Comparison of active and inactive menu items

### How can data be imported from other installations?

Project Administrators can import data from other installations. When using the **File** dialog, an import step to a dedicated Project is offered (Figure 22). Acknowledge the file name and parameter changes (Figure 23).

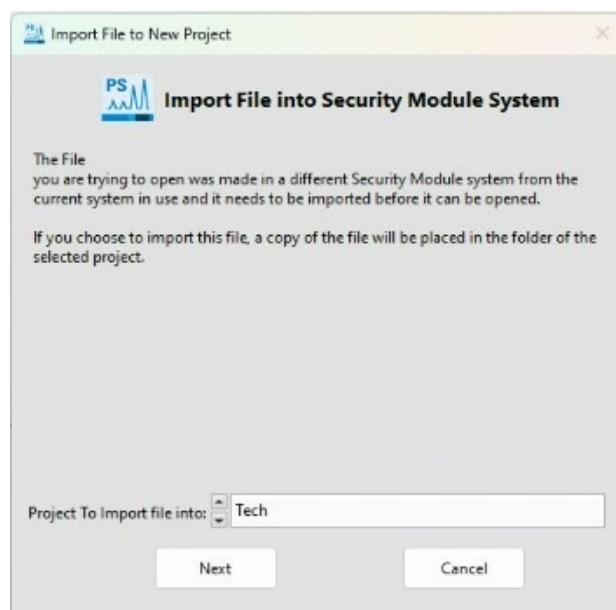


Figure 22 File import

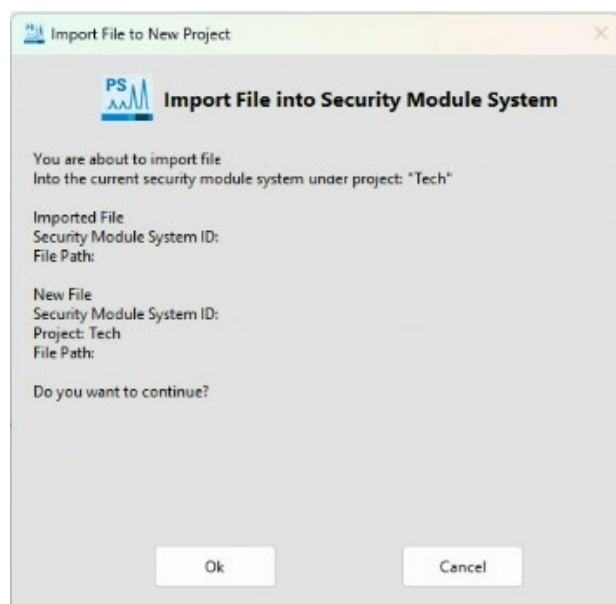


Figure 23 Parameter change overview

All rules of the project to which this file was imported do apply from the import on.

### Is a comparison mode available in Administration Software?

The tab **File Comparison** in the ProSize data 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 event log of a file will subsequently contain the history of both files and continue with recording from the moment it was created. Use check marks to filter for events specific for one initial file of the comparison file.

### Can data be imported that was generated outside of the Administration Software?

Files can be imported from outside the Security Module software as well as legacy \*.db3 data files to a project.

Imported files from outside Secure Module or legacy \*.db3 data file will open in read-only mode.

Data that is imported from another Security Module will lose previous audit logs and only new edits will be recorded. Any .db3 or .raw files only open in read-only mode.

### How to change the authentication mode?

Resetting the authentication mode means changing the repository of users from Windows Active Directory to local accounts and vice versa. Reset the authentication mode under **Global Settings** within the Administration Software. Make sure to choose carefully during the initial setup. It is complicated to align after resetting.

To reset the authorization mode, the previous users must be archived. Subsequently, previous users are 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 e-Signature becomes impossible. However, no data is deleted during this process. New Users can be linked to existing projects.

To process this change of the authentication mode, confirm the decision with a password twice.

### 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, the system can be recreated. Uninstall and reinstall the software and verify its functionality by the build in diagnostics. If they were not affected by the issue, projects, users, and roles are automatically in use again.

Otherwise, all projects, users, and roles will need set up again and manually input the details. Afterwards import the data files to the recreated project. This correction leads to traces in the new system's activity log.

### Is archiving of projects and data possible?

System Administrators have the permission to manage projects and can archive and de-archive data and projects. An archived project will no longer be available for selection in the Controller software.

Data files recorded under an archived project are still present in the data repository. However, all associated permissions of user roles within the project are deactivated, including the permission to open the data file. This makes the data unavailable for project members until an administrator performs the de-archiving.

### What files are traceable?

The traceability files available using the Security Module include the Activity log, Data Event Log and Event Report. The information generated from these logs can be printed and/or exported.

## In This Document

The manual describes the following:

- General description
- Setup of Administration Software
- Setup of users, roles, and projects
- Data analysis
- Reporting
- Administrative elements
- Glossary
- Frequently asked questions