applied biosystems

Security, Audit, and e-Signature Administrator Console v1.2.x

USER GUIDE

SAE Admin Console

for use with:
QuantStudio™ Design and Analysis desktop Software

Publication Number MAN0010410

Revision A.0

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

ThermoFisher SCIENTIFIC

The information in this guide is subject to change without notice.

DISCLAIMER

TO THE EXTENT ALLOWED BY LAW, LIFE TECHNOLOGIES AND/OR ITS AFFILIATE(S) WILL NOT BE LIABLE FOR SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE, MULTIPLE, OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH OR ARISING FROM THIS DOCUMENT, INCLUDING YOUR USE OF IT.

Revision history

Table 1 Revision history of Pub. no. MAN0010410

Revision	Date	Description
A.0	January 2016	New document

Note: The Security, Audit, and e-Signature (SAE) module is available for QuantStudio™ 5 Systems only.

NOTICE TO PURCHASER: DISCLAIMER OF LICENSE

Purchase of this software product alone does not imply any license under any process, instrument or other apparatus, system, composition, reagent or kit rights under patent claims owned or otherwise controlled by Life Technologies Corporation, either expressly, or by estoppel.

Corporate entity

Life Technologies | Carlsbad, CA 92008 USA | Toll Free in USA 1.800.955.6288

TRADEMARKS

Contents

1 Security, Audit, and Electronic Signature

Note: The Security, Audit, and Electronic Signature (SAE) module is available for QuantStudio™ 5 Systems only.

This guide describes the procedures that an administrator performs to configure and manage the SAE module of the QuantStudio™ Design and Analysis desktop Software.

User interaction with the SAE Admin Console is described in the *QuantStudio™ Design and Analysis desktop Software Help* (Pub. no. MAN0010415).

Administrator overview

The Security, Audit, and Electronic Signature (SAE) module is a component of the QuantStudio™ desktop Software that allows you to configure the QuantStudio™ 5 Real-Time PCR Instrument to meet specific requirements. The module provides the following functionality:

- **System Security** – Controls user access to the software. A default Administrator user account is provided, and additional user accounts and permissions can be user-defined.
- **Auditing** – Tracks actions performed by users, and changes to the SAE module settings. The software automatically audits some actions silently. You can select other items for auditing and specify the audit mode. The auditing function provides reports for audited SAE module changes and actions.
- **Electronic signature (e-signature)** – Determines if users are required to provide a user name and password when performing certain functions. You can configure e-signature so that a user can print a report or start a run only if the associated data are signed. You can also configure each e-signature event to require multiple signatures and to require users with specific permissions to sign.

Example applications

You can configure the Security, Audit, and Electronic Signature (SAE) module in a variety of ways. For example, you can:

- Require users to log in and leave audit disabled.
- Allow only certain users to create or modify protocols.
- Allow only certain users to approve plate setup and results.
- Allow only certain users to modify analysis settings.
- Allow only certain users to edit system preferences.

2 Manage user accounts

Start the SAE Admin Console

The SAE Admin Console is automatically installed along with the QuantStudio™ desktop Software.

1. Click **Start** ▸ **All Programs** ▸ **Applied Biosystems** ▸ **SAE Admin**.
2. Enter the Administrator User Name and Password, then click **Sign in**.

Determine the logged-in user

The name of the logged-in user is displayed in the top-right corner of the SAE Admin Console window.

Create a user account

1. In the Users tab, click **Create**, then enter the user name, password, first name, *(optional)* middle initial, and last name. The field limits are specified in the system security function settings.

   Note: First name, MI (middle initial), and last name are used to create the User Full Name, which is displayed as the name of the logged-in user.

   Note: You cannot change the user name after you save the user account.

2. Select **Password expires at first login** to require the user account to specify a new password at first login. The Password Expires On date is specified in the system security function settings.

3. Select the user role (see “Create or edit a user role“ on page 9) and the e-signature status (determines if a user account has permission to electronically sign objects).

4. Leave the status set to **ACTIVE**.

5. *(Optional)* Enter phone, email (for information only), and comments.

6. Click **Save**.

Edit a user account

1. In the Users tab, select a user account, then click **Edit**.

2. Edit the settings as desired.

   Note: You cannot edit the user name of an existing user.

3. Click **Save**.

Activate a suspended user account

1. In the Users tab, select a user account, then click **Edit**.

2. Change the Status from **SUSPENDED** to **ACTIVE**.

3. Click **Save**.

Disable (inactivate) a user account

1. In the Users tab, select a user account, then click **Edit**.

2. Change the Status from **ACTIVE** to **INACTIVE**.

3. Click **Save**.

Reset a forgotten password

1. In the Users tab, select the affected user account, then click **Edit**.
2. Enter a replacement password for the user, then re-enter the password for confirmation.
3. If you assigned the user a temporary password, then select **Password expires at first login** to require the user to specify a new password at login.
4. Click **Save**.

Change password

1. From the drop-down menu, select **Change Password**.

   Note: You can access the Change Password dialog box from any tab.
2. Enter the old password.
3. Enter a new password, confirm the new password, then click **Update**.

Create or edit a user role

User roles determine the permissions associated with a user account. The SAE module includes three default user roles:

- Administrator (cannot be edited or deleted)
- Technician
- Scientist

In the Roles tab, you can create new roles with customized settings, modify the Technician and Scientist roles, delete roles, and generate a role report as needed.

Create a user role

1. In the Roles tab, click **Create**.
2. Enter a role name and (*optional*) description.
3. Select permissions (see "Permissions and default user roles" on page 10). To select all permissions in a category, select the check box next to the category.

   Note: Operations not shown in the table "Permissions and default user roles" on page 10 are available to all user roles.
4. Click **Save**.

Permissions and default user roles

Note: To determine the permissions for a default role or to edit it: select the role, then click **Edit**.

The following table shows all user-configurable permissions and the settings for the default user accounts.

Permissions		Default user roles		
Category	**Function**	**Technician**	**Scientist**	**Administrator**
Setup	Create and edit an experiment, assign samples, and assign detectors and markers	Yes	Yes	Yes
Run	Start or stop a run	Yes	Yes	Yes
		Yes	Yes	Yes
Targets	Create targets	Yes	Yes	Yes
	Edit targets	Yes		
	Delete targets	No		
Analysis Settings (Library)	Create analysis settings (includes default settings)	Yes	Yes	Yes
	Edit analysis settings (includes default settings)	Yes		
	Delete analysis settings (includes default settings)	No		
Dye (Library)	Create a custom dye	Yes	Yes	Yes
	Delete a custom dye	No		
Preferences	Edit system preferences	No	Yes	Yes
Security Configuration	Log Into Timed Out User Sessions	No	No	Yes
	Perform e-signing	Yes	Yes	Yes
Security Configuration (SAE Admin Console)	Configure Security and Auditing	No	No	Yes

Edit a user role

1. In the Roles tab, select a user role, then click **Edit**.

   Note: You cannot edit the Administrator user role.

2. Edit settings as needed.

3. Click **Save**.

Delete a user role

In the Roles tab, select a user role, then click **Delete**.

Generate, view, and print a user or role report

1. In the Users or Roles tab, click **Report**.
   The user report or role report downloads to the default location of your computer.
2. Click on the download report tab in the bottom of the screen to view the report in a new tab of the web browser or to open the location of the downloaded report .pdf on your computer.
3. Use the options available in the .pdf viewer to save and print the report.
4. Close the report.

3 Manage the system security function

Access the system security function screen

Use the System tab to control restrictions and security policies for all user accounts and to set up notifications when certain security events occur.

Note: The system security is enabled by default, and cannot be disabled.

IMPORTANT! To access the SAE Admin Console, you must enable System security in the QuantStudio™ desktop Software.

---

1. See "Configure account setup and security policies" on page 12 to set or modify the system security function settings.
2. Click **Apply Settings**.

Configure account setup and security policies

In the System tab, specify user name and password settings.

The new settings are applied to the user account the next time that the user logs in.

Note: Click the pane heading to collapse or expand the pane.

1. In the User Name Settings pane, enter the minimum and maximum number of characters for the user name.
2. In the Password Policy pane:
   a. Specify the minimum and maximum number of characters for the password.
   b. In the May not reuse previous field, enter the number of most recent passwords that the software should remember to avoid reuse.
   c. Select the complexity rules for creating a password and enter the minimum number of occurrences for that rule.

   d. Specify the maximum and minimum number of days for which the password can be valid.

   e. Enable or disable the Password expiry reminder.

      Note: If you select Enabled, enter the number of days before expiry for the reminder to be sent.

3. In the Account Lockout Policy pane, enable or disable the Account lockout feature. If you select Enabled:
   a. Enter the Threshold limit for logon attempts.

   b. Enter the Account lockout duration in minutes.

   c. Enable or disable the resetting of counter logon attempts.

   d. Enter the Reset account lockout after period in minutes.

4. In the Other Settings pane:
   a. Enable or disable Automatic screen locking.

      Note: If you select Enabled, enter the Inactivity duration in minutes.

   b. Select **Forbidden** or **Allowed** to prevent or allow, respectively, opening of non-secure data.

   c. Enable or disable Client offline login.

      Note: If you select Enabled, enter the Offline login threshold in minutes.

5. Click **Apply Settings**.

   Note: Click **Reset to Defaults** to reset all the system security settings to their default values.

Set up messaging notifications

You can specify when and how the SAE Admin Console notifies the administrator of certain SAE events.

1. From the Settings drop-down menu, select **Notifications**.
2. In the Edit Notification Settings dialog box, select the events for notification:

Option	Description
System security enabled or disabled	The system security function has been enabled or disabled.
User did not enter correct password	A user attempts to log in with an incorrect password. The message indicates the number of failed authentications.
User account suspended	The user exceeds maximum number of allowed failed authentications (login attempts with an incorrect password).
User session timed out	The user account was inactive for longer than the specified maximum time period.
Role deleted	An existing user role has been deleted.

3. Select the notification method:

Option	Description
Notify Admin at Login	If an event triggers notification, the next time an Administrator logs in, the software lists the security events, along with the time each event occurred and the user who triggered the event. The Administrator has the option of acknowledging the event, which removes it from the notification list.
Email Notification	If an event triggers notification, the SAE Admin Console sends an email to the address(es) in the Email Address fields. The email notification displays the security events, the time each event occurred, and the user who triggered each event.

4. Click **Save**.

Set up SMTP configuration

Use the SMTP Configuration dialog box to configure the SMTP server to which the SAE Admin Console will connect for sending email notifications for security events.

1. Go to **Settings ▸ Email Server**.
2. In the SMTP Configuration dialog box, enter the following:
   - SMTP host
   - SMTP port
   - SMTP sender

   Note: Select **Authentication required** if the intended SMTP server requires authentication.

   - User name
   - Password

   Note: Select **Use SSL** if the SMTP server requires connections via encrypted channel.
3. Click **Save**.

4 Manage the audit function

Access the audit function screen

Use the Audit tab to control the events that are audited and the list of reasons available to users when the audit mode is set to Optional or Required.

Note: Audit reasons are not available when the Audit mode is set to Silent.

Note: The audit function is disabled by default and must be enabled.

1. In the Audits tab, select **Enable Audits**.
2. See "Select items to audit" on page 16 and "Configure audit reason settings" on page 17 to modify your desired audit settings.
3. Click **Apply Settings**.

Select items to audit

1. In the Audit Settings pane, select the items to audit and the mode for each included item.
2. Select the Audit Mode for each item you include for auditing:

Option	Description
Silent	The event is audited, no reason prompt is displayed.
Optional	The event is audited, a reason prompt is displayed, but the user can cancel and continue without entering a reason.
Required	The event is audited, a reason prompt is displayed, and the user must specify a reason.

3. Click **Apply Settings**.

Configure audit reason settings

You can create new reasons, or you can modify and delete the default reasons in the Audit Reason Settings pane.

The SAE module is installed with six default audit reasons:

- Manually edited
- Entry error
- Well anomaly
- Calculation error
- Need to change threshold
- Need to reanalyze

1. In the Audit Reason Settings pane, click **New Reason** to open the Add New Audit Reason dialog box.

   Note: Select **Require users to select a reason for change from list** to ensure users select an auditing reason from the Reason list .

2. Enter a reason for change, then click **Save**.
3. Click **Edit** to open the Edit Audit Reason dialog box.
4. Edit the reason for change, then click **Save**.
5. Click **Delete** to open the Delete Audit Reason dialog box.
6. Click **Delete** to confirm deletion of the audit reason or **Cancel** to exit the dialog box.

   Note: After deleting an audit reason, its ID number is also deleted and is not reused for the next audit reason in the list.

7. Click **Apply Settings**.

Generate audit reports

You can use the Audit History drop-down menu to generate reports from both the Action Records and System Configuration views. You can also generate audit history reports from open templates and experiments in the QuantStudio™ desktop Software.

Audit histories from the Audit History drop-down menu

You can display audit histories from the Audit History drop-down menu in two different ways:

- **Action Record –** Specified audit events.
- **System Configuration –** The system security, audit, and e-signature configuration records, including audit history for each user account.

Review the System Configuration

The System Configuration view from the Audit History drop-down menu lists system security, audit, and e-signature configuration records. The following table summarizes the actions that can be audited using the SAE Admin Console.

Record Type	Action	Corresponds to...
Security Settings	Update	Disable, enable, or modify system security policies and session time-out settings
Account Settings	Update	Modify password settings, system security policies (password expiration and account suspension), or user name settings
User Group Manager	Update	Create, delete, or modify reason for change
User Role	Create	Create user role
	Delete	Delete user role
	Update	Modify user role
User Account	Create	Create new user account
	Update	Edit or suspend a user account
Role Assignment	Edit	Assign a different user role to an existing user account
	Create	Create a user account
Auditable Entity Settings	Update	Enable or disable auditing
Auditable Entity	Update	Modify audit settings
Role Permissions	Create	Create a user role **Note:** Creates one role assignment record for each permission in a role.
	Delete	Delete a user role
	Update	Modify user role permissions

Record Type	Action	Corresponds to...
Audit Reason for Change	Create	Create reason for change
	Update	Modify reason for change
	Delete	Delete reason for change
Event Manager	Update	Update the event manager
E-signature Manager	Update	Enable or disable e-signature
E-signature Type	Create	Create an e-signature meaning
	Delete	Delete an e-signature meaning
E-signature Function	Update	Edit an action requiring e-signature

Review the action log

The Action Record log view in the Audit History drop-down menu lists specified audit events.

All items in the action log are audited silently.

- Auditing Event (Archive, Restore, Purge)
- Configuration (Import, Export)
- Data Audit (Archive, Restore, Purge)
- Login (Success, Failure)
- Logout (Success)
- Run (Start, Stop)

View audit histories from the Audit History drop-down menu

1. From the Audit History drop-down menu, select:

Option	Description
Action Record	Displays an audit of the user's actions
System Configuration	Displays updated system configuration settings

2. *(Optional)* Select **Enable Action Records Filtering** to filter or sort the action records.
   a. Select the Date Range, User Account, and Action, then click **Search**.
   The records are displayed in the lower pane.

3. *(Optional)* Select **Enable System Configuration Records Filtering** to filter or sort the system configuration records.
   a. Select the Date Range, User Account, Action, Record Type, and Record Name, then click **Search**.
   The records are displayed in the lower pane.

4. Click **Report** to generate an audit history report.
   The report is generated at the default location of your computer.

5. View the report in the default system viewer or in a new tab of the web browser.

6. Use the options in the viewer to manipulate the report as needed, then close the report.

7. *(Optional)* See "Archive, purge, and restore audit records" on page 20 to archive the action records or system configuration records.

8. *(Optional)* See "Archive, purge, and restore audit records" on page 20 to restore purged action records or system configuration records.

Archive, purge, and restore audit records

You can selectively archive or purge (delete) system configuration or action records. You can also selectively restore records.

- Archive – Makes a copy of audit records.
- Purge – Makes a copy of audit records on your computer, and then deletes them from the software.
- Restore – Restores audit records from archived files.

1. Archive and purge records:
   a. Display the action records or system configuration records of interest as described in "View audit histories from the Audit History drop-down menu" on page 19.
   b. Select the records of interest.
   c. Click **Archive**.
   d. Confirm the filter criteria and select **Purge audit records after archival** to purge the records, then click **Archive**.
   The records are archived to the default download location of your computer.

2. Restore records:
   a. In the Action Record or System Configuration view, click **Restore**.
   b. Select the .par file to restore, then click **Open**.

Export audit records

You can export audit records to a .txt file for additional manipulation and reporting outside the SAE Admin Console.

1. Display the records of interest as described in "View audit histories from the Audit History drop-down menu" on page 19.

2. In the Action Records view or System Configuration view, click **Export**.

   Note: If you export audit records for samples that have been deleted or moved, an error message is displayed. Return sample data files to their original location, then export again.

   The .txt file is downloaded to the default location of your computer.

5 Manage the e-signature function

Access the e-signature function screen

Use the e-Signature tab to control the e-signature rights of user roles, the reasons available for e-signature, and the data to be signed.

Note: The e-signature function is disabled by default and must be enabled.

1. In the e-Signature tab, select **Enable e-Signature**.
2. See "Configure the meanings of e-signatures" on page 21 to modify your desired e-signature settings.
3. Click **Apply Settings**.

Configure the meanings of e-signatures

The e-signature meanings are the text that a user can select to describe a reason for an e-signature. The SAE module is installed with three default meanings:

- Reviewed and Approved Results
- Reviewed and Approved Plate Set Up
- Reviewed and Approved Template

Add an e-signature meaning

1. In the e-Signature tab, in the e-Signature Meanings pane, click **New meaning**.
2. Enter an e-signature meaning in the Name field, then click **Save**.
3. Select a meaning. Then, in the Data signed for the selected meaning, select the data that is signed for the meaning.
4. See "Select the actions that require e-signature" on page 22 to set the actions that require e-signature and the number of e-signatures required for that action.
5. Click **Apply Settings**.

Delete an e-signature meaning

1. In the e-Signature tab, in the e-Signature Meanings pane, select a meaning from the Meanings list, then click **Delete**.
2. Confirm you want to delete the meaning, then click **OK**.
3. Click **Apply Settings**.

Select the actions that require e-signature

IMPORTANT! Do not change e-signature function settings during calibration.

1. In the Actions Requiring Signatures pane, select each action for which you want to require e-signatures (see below). The software displays an e-signature prompt if a user performs the action on a data file that does not have the required signatures.

Action	The software requires e-signatures when a user...
Print report	Prints a report from an experiment or template.
Start run	Initiates a run from the QuantStudio™ desktop Software.

2. For each meaning of each selected action, enter the number of e-signatures required from each user role before the software can execute the associated action.
3. Click **Apply Settings**.

6 Manage the export-import function

Export and import user, system security, audit, and e-signature settings

Use the export/import feature to back-up or replicate identical SAE settings across multiple computers. You can create a standard SAE settings "image" for the SAE module and then import the settings "image" to other computers to bypass manual setup.

Export user, system security, audit, and e-signature settings

1. In the Settings drop-down menu, select **Export Configuration**.
2. In the Export Configuration dialog box, select:
   - **All** to export all configuration settings, including user accounts.
   - **Custom** to export the following:
     - **Users & Roles** – Exports all user accounts with "Active" status as well as all user roles and their associated permissions.
     - **System & Roles** – All system settings and all user roles and their associated permissions.
3. Click **Export**.
   The exported file (.dat) is downloaded to the default location of your computer.

Import user, system security, audit, e-signature settings

1. In the Settings drop-down menu, select **Import Configuration**.
2. Click **Choose File** to choose the .dat file with the desired configuration settings.
3. Select the import options:
   - All
   - Custom
     - Users & Roles
     - System & Roles
4. Click **Import**.
5. If you selected All or Users & Roles, it is possible the imported user accounts already exist in the SAE module. Select **Skip** or **Overwrite** for each user account, then click **Confirm and Import**.

Documentation and support

Related documentation

Document	Publication number	Description
QuantStudio™ 3 and 5 Real-Time PCR Systems Installation, Use, and Maintenance Guide	MAN0010407	Describes the QuantStudio™ 3 and 5 Real-Time PCR Systems hardware and software and provides information on preparing, using, maintaining, and troubleshooting the system.
QuantStudio™ Real-Time PCR System Help	MAN0010422	Describes the QuantStudio™ 3 and 5 Real-Time PCR Systems touchscreen and provides procedures for configuration, calibration, and performing a run.
QuantStudio™ Design and Analysis desktop Software Command-Line Application Guide	MAN0010409	Describes how to use the command-line interface of the QuantStudio™ Design and Analysis desktop Software and provides the procedure to automate the creation of new experiment files and export data from existing files.
QuantStudio™ Design and Analysis desktop Software User Guide	MAN0010408	Describes how to perform the six different experiments on the QuantStudio™ Design and Analysis desktop Software
QuantStudio™ Design and Analysis desktop Software Help	MAN0010415	Describes the QuantStudio™ Design and Analysis desktop Software and provides procedures for common tasks.
SAE Admin Console Help	MAN0010417	Describes the Security, Audit, and e-Signature Administrator Console and provides procedures for common tasks.
SAE Admin Console User Guide	MAN0010410	Describes how to use the Security, Audit, and e-Signature Administrator Console.

Document	Publication number	Description
QuantStudio™ Design and Analysis cloud Software Help	MAN0010414	Describes the QuantStudio™ Design and Analysis cloud Software and provides procedures for common tasks.
QuantStudio™ 3 and 5 Real-Time PCR Systems Site Preparation Guide	MAN0010405	Explains how to prepare your site to receive and install the QuantStudio™ 3 and 5 Real-Time PCR Systems. Intended for personnel who schedule, manage, and perform the tasks required to prepare the site for installation of the QuantStudio™ 3 and 5 Real-Time PCR Systems.

Note: For additional documentation, see "Customer and technical support" on page 25.

Obtain information from the Help System

The SAE Admin Console has a Help system that describes how to use each feature of the user interface. Click ⓘ to access the Help system.

Customer and technical support

Visit **thermofisher.com/support** for the latest in services and support, including:

- Worldwide contact telephone numbers
- Product support, including:
  - Product FAQs
  - Software, patches, and updates
- Order and web support
- Product documentation, including:
  - User guides, manuals, and protocols
  - Certificates of Analysis
  - Safety Data Sheets (SDSs; also known as MSDSs)

    Note: For SDSs for reagents and chemicals from other manufacturers, contact the manufacturer.

Limited product warranty

Life Technologies Corporation and/or its affiliate(s) warrant their products as set forth in the Life Technologies' General Terms and Conditions of Sale found on Life Technologies' website at **www.thermofisher.com/us/en/home/global/terms-and-conditions.html**. If you have any questions, please contact Life Technologies at **www.thermofisher.com/support**.

Index

T

U

W