appliedbiosystems

SAE Administrator Console v2

USER GUIDE

for v2.x

for use with:

QuantStudio™ 7 Pro Real-Time PCR Instrument with QuantStudio™ Design and Analysis Software v2

QuantStudio™ Absolute Q™ Digital PCR Software v6.1 or later

Publication Number MAN0017468

Revision J

ThermoFisher SCIENTIFIC

Life Technologies Holdings Pte Ltd | Block 33 | Marsiling Industrial Estate Road 3 | #07-06, Singapore 739256
For descriptions of symbols on product labels or product documents, go to thermofisher.com/symbols-definition.

Revision history: MAN0017468 J (English)

Revision	Date	Description
J	17 December 2024	The compatibility of the real-time PCR systems was corrected ("Compatibility" on page 32). SAE Administrator Console v2.0 is not compatible with `QuantStudio 7 Pro Instrument (1.3.0).dat` and `Design and Analysis Software (1.3.0).dat`.
H	3 May 2024	• The information about default permissions after upgrading an application profile was corrected. The roles do not receive the permission for the new functions. Only the Administrator role receives the permissions for the new functions ("Default permissions and roles" on page 45). • The functions that can be controlled on the QuantStudio™ 7 Pro Real-Time PCR Instrument were updated to include exporting files, overwriting files, and keeping multiple copies of files ("Functions that are controlled on the QuantStudio™ 7 Pro Real-Time PCR Instrument" on page 41). • The default roles and permissions for data management on the QuantStudio™ 7 Pro Real-Time PCR Instrument were updated ("Default permissions for the QuantStudio™ 7 Pro Real-Time PCR Instrument" on page 46). • The compatibility for the real-time PCR system was updated ("Compatibility" on page 32). • The default roles and permissions for the QuantStudio™ Absolute Q™ Digital PCR System were corrected ("Default permissions and roles" on page 66).
G.0	23 February 2024	• The initial user name and password were added ("Initial user name and password" on page 20). • The information about application profile versions was updated. When an application profile is upgraded, the default permissions of any new functions in the new application profile are not applied. All of the roles receive the permission for the new functions. • The compatibility for real-time PCR systems was updated ("Compatibility" on page 32). • The information about the order of installing the application profiles was updated. The application profile for QuantStudio™ Design and Analysis Software v2.8 or later does not require that the application profile for the QuantStudio™ 7 Pro Real-Time PCR Instrument is installed ("Application profiles" on page 34). • The functions that are controlled on the QuantStudio™ 7 Pro Real-Time PCR Instrument were updated for v1.8 ("Functions that are controlled on the QuantStudio™ 7 Pro Real-Time PCR Instrument" on page 41). • The functions that are controlled in the software were updated for QuantStudio™ Design and Analysis Software v2.8 ("Functions that are controlled in the QuantStudio™ Design and Analysis Software v2" on page 42). • The default roles and permissions were updated for QuantStudio™ 7 Pro Real-Time PCR Instrument v1.8 and QuantStudio™ Design and Analysis Software v2.8 ("Default permissions and roles" on page 45). • Information was added about starting the QuantStudio™ Design and Analysis Software v2 as a Windows™ administrator if a connection cannot be established with the SAE Administrator Console ("SAE error messages and actions" on page 58). • The e-signature option from the **Templates** page was removed ("Sign data in the software" on page 72).
F.0	13 October 2023	The QuantStudio™ Absolute Q™ Digital PCR System information was updated to reflect changes introduced with QuantStudio™ Absolute Q™ Digital PCR Software v6.3.
E.0	10 August 2022	• The content for the SeqStudio™ Genetic Analyzer was removed. The content for the SeqStudio™ Genetic Analyzer is in *SAE Administrator Console v2.1 User Guide for Capillary Electrophoresis Products* (Pub. No. MAN0025849). • The statement covering Limited Use Label Licenses was removed. • Recommendations for passwords were added ("Recommendations for passwords" on page 11). • The descriptions of the SAE components were updated ("Components of the SAE functions" on page 13). • Information was added about the local web browser interface and the file and database locations ("Local web browser interface and database record storage" on page 13 and "File and database locations" on page 14). • A recommendation to use a computer from Thermo Fisher Scientific was added and a requirement to install antivirus software was added ("SAE Administrator Console installation requirements" on page 14). • The computer requirements were corrected ("Minimum computer requirements" on page 15).

Revision	Date	Description
E.0 *(continued)*	10 August 2022	• Information was added about antivirus software ("Antivirus software requirements" on page 15) and third-party software ("Third-party software" on page 16). • The list of features for v2.1 and v2.2 was corrected ("Features of the SAE Administrator Console v2.1 and later" on page 17). • Information was added about a lockout time after 30 minutes of inactivity ("Start the SAE Administrator Console" on page 19). • Information was added about the potential warning messages that are displayed ("Overview of the warning screens" on page 20). • Internet Explorer™ was removed as a browser option. • The information about SSL certificates was updated to indicate that they are installed in Microsoft Edge™ and Google Chrome™. They are not installed in Internet Explorer™ for these browsers. • The instructions to view the terms of use were corrected. • A new chapter was added to cover the use of multiple applications (Chapter 3, "Use the SAE Administrator Console with multiple applications"). • Overviews were added for the system security settings, the audit settings and functions, and the e-signature settings. • The list of functions that are controlled on the QuantStudio™ 7 Pro Real-Time PCR Instrument was updated. A list of functions that are controlled in the QuantStudio™ Design and Analysis Software v2 was added. • Default permissions for each role were added for the QuantStudio™ Design and Analysis Software v2. • The objects and actions that can be audited in the QuantStudio™ 7 Pro Real-Time PCR Instrument and the QuantStudio™ Design and Analysis Software v2 were updated. • The information about functions that can be signed in the QuantStudio™ 7 Pro Real-Time PCR Instrument and the QuantStudio™ Design and Analysis Software v2 was updated. • Instructions were added for the following functions: – Changing the SAE account password in the QuantStudio™ Design and Analysis Software v2 – Entering an audit reason in the QuantStudio™ Design and Analysis Software v2 – Providing an e-signature in the QuantStudio™ Design and Analysis Software v2 – Viewing the audit records for objects on the QuantStudio™ 7 Pro Real-Time PCR Instrument and the QuantStudio™ Design and Analysis Software v2 • The audit information for the QuantStudio™ Absolute Q™ Digital PCR System was updated. • Instructions were added to view e-signatures for the QuantStudio™ Absolute Q™ Digital PCR System. • Information was added to differentiate between audited actions and audited objects ("Overview of the audit settings and functions" on page 87). • Descriptions of each part of the e-signature tab were added. A workflow to set up e-signatures was added and detailed instructions for each step were added. • The e-signature information was updated to indicate that enabling this function applies to all of the applications that are connected to the instance of the SAE Administrator Console. • A new chapter was added to view and report audit and e-signature records (Chapter 10, "View and report audit and e-signature records"). • Instructions were added to export active **Action** or **System Configuration** records ("Export active Action or System Configuration records" on page 103). • A new chapter was added to back up, archive, and restore records (Chapter 11, "Back up, archive, and restore SAE records and files"). • The instructions to edit a role were updated to note that the No Privileges role cannot be edited. • The information about the auditable actions was updated to specify that the records are located in the **System Configuration** audit history. The list of auditable actions was updated to include the purge of audit records. • A troubleshooting appendix was added (Appendix A, "Troubleshooting").

Revision	Date	Description
D.0	4 October 2021	• Added information on static and dynamic IP addresses, and requirements if SAE Administrator Console is installed on a separate computer to "SAE Administrator Console installation requirements" on page 14. • Added information on the firewall ports that must be open on page 16. • Added features and compatibility of SAE v2.1 and SAE v2.2 to "Application profile versions" on page 16. • Added URL information for Google Chrome™ and Internet Explorer™ to "Start the SAE Administrator Console" on page 19. • Added content for the QuantStudio™ Absolute Q™ Digital PCR Software v6.1.0. • Specified the settings that are not used if an external LDAP is used. • Specified that the files are checksum protected.
C.0	2 June 2020	Added functions for using the SAE Administrator Console with the QuantStudio™ 7 Pro Real-Time PCR System and the QuantStudio™ Design and Analysis Software v2.
B.0	3 January 2020	• Added content for the QuantStudio™ 7 Pro Real-Time PCR System and the QuantStudio™ Design and Analysis Software v2. • Added network and password security requirements.
A.0	1 November 2019	New information for SAE Administrator Console v2.0. Adds functionality for the SeqStudio™ Genetic Analyzer, audit archival, instrument run logs, and configuration of user repositories.

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

Contents

1 Product information

Network and password security requirements

Network configuration and security

The network configuration and security settings of your laboratory or facility (such as firewalls, anti-virus software, network passwords) are the sole responsibility of your facility administrator, IT, and security personnel. This product does not provide any network or security configuration files, utilities, or instructions.

If external or network drives are connected to the software, it is the responsibility of your IT personnel to ensure that such drives are configured and secured correctly to prevent data corruption or loss. It is the responsibility of your facility administrator, IT, and security personnel to prevent the use of any unsecured ports (such as USB, Ethernet) and ensure that the system security is maintained.

Password security

Thermo Fisher Scientific strongly recommends that you maintain unique passwords for all accounts in use on this product. All passwords should be reset upon first sign in to the product. Change passwords according to your organization's password policy.

It is the sole responsibility of your IT personnel to develop and enforce secure use of passwords.

Recommendations for passwords

Thermo Fisher Scientific recommends enabling a password policy for SAE user accounts with the following minimum number of characters:

- Administrative users: 12 characters
- Non-administrative users: 8 characters

The use of a password manager is recommended in order to help to create secure passwords.

About the Security, Auditing, and E-signature Administrator Console

The Security, Auditing, and E-signature Administrator Console (SAE Administrator Console) is the tool that you use to configure the Security, Audit, and E-signature functions (SAE functions). The SAE functions can be configured to meet specific requirements for security, audit, and e-signature.

In the SAE Administrator Console, a software or instrument that is configured for the SAE functions is called an "application".

Example applications include the QuantStudio™ Design and Analysis Software v2 and the QuantStudio™ Absolute Q™ Digital PCR Software.

For information on using the SAE Administrator Console with a specific application, see the chapter for the application.

The SAE functions can be configured to provide the following features:

Feature	Description
System security	Controls user access to an application. A default user account assigned the Administrator role is provided at installation. You can set up additional SAE user accounts and permissions.
Auditing	Tracks actions performed by users and changes to the SAE settings. Some actions are automatically audited silently. The following audit functions can be set up: • Audit changes to specific objects and specify the audit mode. • Generate reports for audited user actions and SAE function changes. • Generate reports for software or instrument actions and runs.
Electronic signature (e-signature)	Determines if users are required to fulfill signature requirements before performing specific functions. You can perform the following functions: • Configure e-signature so that a user can perform an action only if the associated data are signed. • Configure each e-signature event to require one or multiple signatures and to require users with specific roles to sign.

Components of the SAE functions

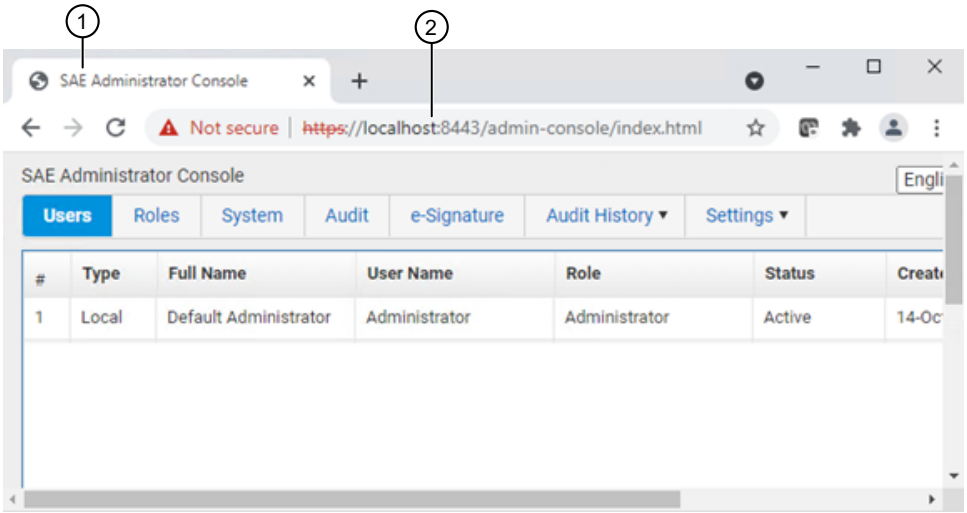
The SAE is a client-server software configuration that includes three components:

- **SAE Administrator Console**—This component is a tool that is used by an SAE administrator to configure the settings. The SAE Administrator Console runs in a web browser, even though it is installed locally on your computer. Google Chrome™ is the recommended web browser, but Mozilla™ Firefox™ or Microsoft Edge™ can be used.
- **SAE server** (server)—This component is a service that runs in the background and stores the settings, user accounts, audit records, and e-signature records. By default, the SAE server is installed on the same computer as the SAE Administrator Console. The communication between the SAE Administrator Console and the SAE server (v2.1 and later) uses the encrypted HTTPS protocol. The SAE server is started automatically when the computer is started.
- **SAE screens** (client)—This component are the screens that are displayed in an application such as the QuantStudio™ 7 Pro Real-Time PCR Instrument. The screens require user input to sign in, provide audit reasons, or provide an e-signature. More than one application can be connected to and controlled by the same instance of the SAE Administrator Console.

Local web browser interface and database record storage

A web browser is typically used to view information on the internet.

The SAE Administrator Console runs in a web browser interface, even though it is installed locally on a computer.



① Web browser tab
② URL indicates that the SAE software is installed on the computer (localhost)

File and database locations

The SAE Administrator Console files are installed in `<…>:\Program Files (x86)\Applied Biosystems\SAE Admin Console`, where <…> is the installation directory.

Records are managed by a relational database management system (RDBMS) in the software.

Database files are stored in `<…>:\Program Files (x86)\Applied Biosystems\SAE Admin Console\SAEDB\seg0`. The database folder is created when the first record is saved. Records for all applications are stored in the same database.

Records that are archived manually or with the automated archive function are stored in `<…>:\Program Files (x86)\Applied Biosystems\SAE Admin Console\automated-archivals`. The archive folder is created when the first automated archive occurs. Date- and time-stamped folders are created for each archive.

IMPORTANT! Do not move or edit files in this directory. For information on backing up and archiving the files and database, see Chapter 11, "Back up, archive, and restore SAE records and files".

SAE Administrator Console installation requirements

The SAE Administrator Console can be installed on a computer purchased from Thermo Fisher Scientific or a customer-supplied computer.

IMPORTANT! We strongly recommend that you use a computer obtained from Thermo Fisher Scientific. These computers are validated for use with Thermo Fisher Scientific software, which may have different operating system settings than a commercially available computer. Specific operating system settings are required for the proper operation of Thermo Fisher Scientific software.

IMPORTANT! Antivirus software must be installed on the computer. See "Antivirus software requirements" on page 15.

If a customer-supplied computer is used, there are minimum requirements (see "Minimum computer requirements" on page 15).

Only one SAE Administrator Console can be installed on one computer.

Multiple applications can connect to the single instance of the SAE Administrator Console.

If the SAE Administrator Console is installed on a different computer than the instrument or software, a static IP address is recommended.

If using a dynamic IP address, enter the **Server** hostname instead of the IP address for the **SAE Connection Settings** to prevent the loss of a connection. Consult your network administrator for help with checking the IP address configuration.

Note: An application software can be installed on the same computer as the SAE Administrator Console or a different computer than the SAE Administrator Console.

- The same computer as the SAE Administrator Console is recommended for a single application
- A different computer than the SAE Administrator Console is recommended for multiple applications

Time difference for server connection

If SAE Administrator Console is installed on a separate computer from the application, the time difference between the application and the separate computer with the SAE Administrator Console must be less than 5 minutes to establish the connection. If the time difference is more than 5 minutes, the application shows an error message.

Minimum computer requirements

The following are the minimum specifications for a customer-supplied computer:

- Operating system—Windows™ 10 (64-bit)
- Intel™ Core™ processor or compatible
- Memory—16 GB RAM minimum
- Hard drive—500 GB minimum free space
- Monitor—1280 × 1024 resolution or higher
- One open Ethernet port for connecting directly to the instrument
- Microsoft™ Excel™ software
- Browser options
  - Google Chrome™ v40 or later (recommended)
  - Mozilla™ Firefox™ v40 or later
  - Microsoft Edge™

Antivirus software requirements

The optional computer that is available from Thermo Fisher Scientific does not include antivirus software because customer preferences and network requirements vary. You are responsible for installing antivirus software of your choice to protect the computer against viruses.

The following antivirus software applications have been tested for use with an optional computer:

- Symantec™ Endpoint Protection
- Norton Internet Security™
- Microsoft™ Defender antivirus software

Firewall ports that must be open

The following ports must be open for the operating system on the computer that is running the SAE Administrator Console.

SAE Administrator Console version	Port	Condition
v2.0	8201	• Instrument-to-SAE Administrator Console server connection • Computer-to-SAE Administrator Console server connection[1]
v2.1 and later	8443	• Instrument-to-SAE Administrator Console server connection • Computer-to-SAE Administrator Console server connection[1]

[1] If the software is installed on a different computer than the SAE Administrator Console.

Firewall ports

To open a port for Microsoft™ Defender, add inbound rules for the port, and apply to all profiles.

To open a port for Norton Internet Security™, use the **Settings** menu to open the port.

No action is required to open a port for Symantec™ Endpoint Protection.

Third-party software

Before installing third-party software on the computer running the product software, confirm that the third-party software will not have either/or of the following effects on the computer:

- Restrict Ethernet communication.
- Interfere with instrument or computer operation.

Application profile versions

The SAE Administrator Console requires an application profile to be installed for each application. For example, in order to use the QuantStudio™ 7 Pro Real-Time PCR Instrument with the SAE Administrator Console, the application profile specific to the instrument must be installed.

Each application profile has a version. For compatibility between the versions of the SAE Administrator Console, the application, and the application profile, see the chapter specific to your application.

Application profiles have the following naming convention:

```
<Application name> (<Application profile version number>).dat
```

The file format for an application profile is DAT.

The following file name is an example of the application profile for the QuantStudio™ 7 Pro Real-Time PCR Instrument. It is version 1.3.0.

```
QuantStudio 7 Pro Instrument (1.3.0).dat
```

Note: When an application profile is upgraded, the default permissions of any new functions in the new application profile are not applied. All of the roles receive the permission for the new functions.

Features of the SAE Administrator Console v2.1 and later

Features of the SAE Administrator Console v2.1 and the SAE Administrator Console v2.2 are listed in the following table:

SAE Administrator Console version	Feature
v2.1	• The URL is converted to HTTPS on port 8443 (see "Start the SAE Administrator Console" on page 19 and "Firewall ports that must be open" on page 16). • The option of an A4 report was added (see "Configure account set up and security policies" on page 85).
v2.2	• The option to select the language is provided (see "Select the language" on page 27). • The option to check that the user name is not used as a password is provided (see "Configure account set up and security policies" on page 85). • The option to check for compromised phrases as passwords is provided (see "Configure account set up and security policies" on page 85).

2 Get started

Workflow: Configure the SAE functions with the SAE Administrator Console

Set up the SAE Administrator Console (before first use)

Start the SAE Administrator Console (page 19)

Install the application profiles (page 22)

Enable the SAE functions in the application (See the chapter for the application)

- Chapter 4, “Configure the SAE functions for the real-time PCR system”
- Chapter 5, “Configure the SAE functions for the QuantStudio™ Absolute Q™ Digital PCR Software”

Configure the settings in the SAE Administrator Console (as needed)

Manage the system security function (page 84) **and Configure account set up and security policies** (page 85)
Complete this step of the workflow to control restrictions and system security policies for all SAE user accounts.

Manage the audit function (page 87)
Complete this step of the workflow to select actions to be audited and view audit reports.

Manage the e-signature function (page 91)
Complete this step of the workflow to select actions that require e-signature and view e-signature reports.

View and report audit and e-signature records (page 99)
Perform the procedures in this chapter as needed.

Back up, archive, and restore SAE records and files (page 105)
Perform the procedures in this chapter as needed.

Start the SAE Administrator Console

Note: In SAE Administrator Console v2.1 and later, the software automatically converts the URL to **https://localhost:8443/admin-console/login**.

1. In the Windows™ desktop, click **Start** ▸ **SAE Admin**.
   A warning screen might be displayed. For more information, see “Overview of the warning screens” on page 20.

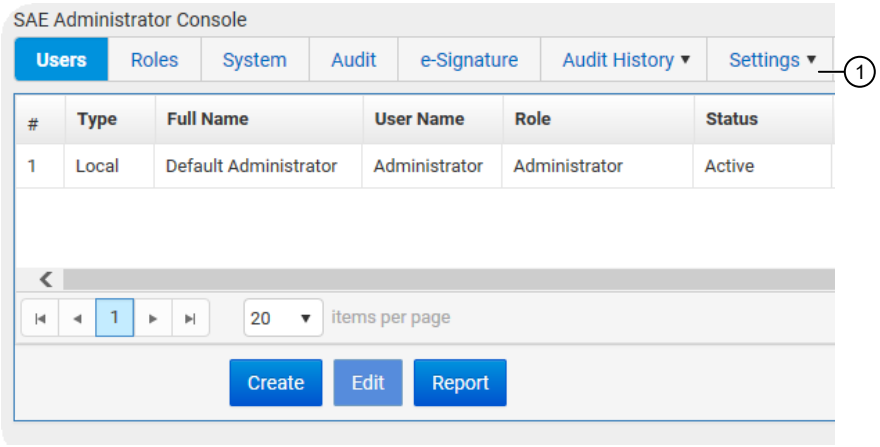
2. Enter the Administrator **User Name** and **Password**, then click **Sign in**.
   If messaging notifications are enabled (see page 25), the **Event Notifications** dialog box is displayed.

   IMPORTANT! The administrator password cannot be recovered after it is set. The software must be uninstalled, then reinstalled.

3. You can do either of the following in the **Event Notifications** dialog box:
   - Select the checkboxes for the events, then click **Acknowledge** to remove the selected events from the list.
   - Click **Close** to close the dialog box and retain the events in the list.

If the notifications are retained, they are displayed the next time a user logs in to the SAE Administrator Console. They can also be viewed from the main screen (see “View the notifications” on page 26).

The SAE Administrator Console main screen is displayed with the URL specified as "local host" in the browser. Click the navigation tabs to display different screens in the software.



1 Navigation tabs

The signed-in user is automatically signed out after 30 minutes of inactivity. This lockout time is not configurable.

Initial user name and password

IMPORTANT! The password must be changed at the first login.

The administrator password cannot be recovered after it has been reset. The software must be uninstalled, then reinstalled. All of the information, including application profiles, permissions, SAE accounts, audit records, and e-signatures are lost when the software is uninstalled.

- Initial user name: ***Administrator***
- Initial password: ***Administrator***

Overview of the warning screens

If a security or warning screen is displayed when you start the SAE Administrator Console, you can bypass the security or warning screen.

See the following sections for more information:

- “Warning for the Google Chrome™ browser” on page 21
- “Warning for the Mozilla™ Firefox™ browser” on page 21
- “Warning for the Microsoft Edge™ browser” on page 22

After you bypass the security or warning screen, the browser may still indicate that the connection is not secure, or that there is a certificate error. It is safe to use the SAE Administrator Console when a security or warning screen is displayed, because the default communication between the client (SAE Administrator Console) and server (SAE server) is encrypted.

The SAE Administrator Console runs locally on your computer, even though it is displayed in a web browser format. Google Chrome™ is the recommended web browser. Mozilla™ Firefox™ or Microsoft Edge™ can be used.

When you start the SAE Administrator Console software, it opens the URL for the SAE server in your default browser.

Note: When any browser accesses a URL that uses the HTTPS protocol, the browser attempts to check the web server certificate with a Certificate Authority (CA). Several well-known and trusted authorities exist, from which a website/URL owner can purchase a certificate that uniquely identifies the URL and verifies its authenticity.
The web server certificate that is provided for the SAE server URL is self-signed (meaning it is not purchased from a CA). Because it cannot be verified by a CA, a security or warning screen is displayed.

If your organization has an internal CA, your IT representative may be able to generate and install a self-signed certificate for the SAE server URL. The certificate is then verified with your internal CA, and the security or warning screen is not displayed when you start the SAE Administrator Console. Adding the URL as a trusted site does not eliminate the security or warning screen.

Warning for the Google Chrome™ browser

Launch the SAE Administrator Console.

The "**Your connection is not private**" warning message is displayed.

Click **ADVANCED ▸ Proceed to <domain name> (unsafe)** to proceed.

The SAE Administrator Console is launched with **Not Secure** displayed in the URL bar. The user can log in.

If a self-signed SSL certificate is installed, the warning message is displayed (for the localhost domain only).

Note: The certificate must be installed in the Google Chrome™ browser.

Warning for the Mozilla™ Firefox™ browser

Launch the SAE Administrator Console.

The "**Warning: Potential Security Risk Ahead**" warning message is displayed.

Click **Advanced ▸ Accept the Risk and Continue** to proceed.

The SAE Administrator Console is launched with **Not Secure** displayed in the URL bar. The user can log in.

If the self-signed SSL certificate is installed in the Mozilla™ Firefox™ browser, the warning message will not be displayed (for the localhost domain only).

Note: The certificate must be installed in Mozilla™ Firefox™ browser.

Warning for the Microsoft Edge™ browser

Launch the SAE Administrator Console.

The "**Your connection isn't private**" warning message is displayed.

Click **Advanced** ▸ **Continue to <domain name> (unsafe)** to proceed.

The SAE Administrator Console is launched with **Not Secure** displayed in the URL bar. The user can log in.

If a self-signed SSL certificate is installed, the warning message will not be displayed (for the localhost domain only).

Note: The certificate must be installed in the Microsoft Edge™ browser.

Install the application profiles

An application profile contains default SAE Administrator Console settings for an application. Example applications include the QuantStudio™ Design and Analysis Software v2 or the QuantStudio™ Absolute Q™ Digital PCR Software.

Before you can use the SAE Administrator Console with an application, you must install a profile for the application. Each application has its own application profile, or set of application profiles.

You can install multiple application profiles in order to support the use of the SAE Administrator Console with multiple applications.

Depending on the application profiles, it might be necessary to install them in a specific order. See the chapter for your application.

For information about the SAE Administrator Console with multiple applications, see Chapter 3, “Use the SAE Administrator Console with multiple applications”.

For information about the versions of the application profiles, see “Application profile versions” on page 16 and the chapter for your application.

1. In the SAE Administrator Console main screen, click **Settings** ▸ **Manage Application Profiles**.
2. Click **Install Application Profile**.
3. In the **Install Application Profile** dialog box, click **Choose File**.
4. Select the application profile.
   The application profile is a DAT file.
5. Click **Verify Data File**.
6. Review the information in the **Install Application Profile** dialog box, then select the **Install new application** checkbox.
7. Click **Install**.
8. Select **Verify Data File** ▸ **Install new application** ▸ **Install**.

The application name and settings are added to the SAE Administrator Console.

An application profile cannot be uninstalled once it has been installed.

Update an application profile

IMPORTANT! Ensure that the new version of the application profile is compatible with your version of the application and the SAE Administrator Console before updating it.

When an application profile is upgraded, the default permissions of any new functions in the new application profile are not applied. All of the roles receive the permission for the new functions.

For information about the versions of the application profiles, see “Application profile versions” on page 16 and the chapter for your application.

1. In the SAE Administrator Console main screen, click **Settings** ▸ **Manage Application Profiles**.
2. Click **Install Application Profile**.
3. In the **Install Application Profile** dialog box, click **Choose File**.
4. Select the application profile.
   The application profile is a DAT file.
5. Click **Verify Data File**.
6. Review the information in the **Install Application Profile** dialog box, then select the **Install new application** checkbox.
7. Click **Install**.
8. Select **Verify Data File** ▸ **Install new application** ▸ **Install**.

The information about the updated application profile is displayed in the list of application profiles.

- Number of functions
- Version
- Date installed
- Installed by

Sign out of the SAE Administrator Console

In the top-right corner of the screen, click ▸ **Sign Out**

Use the application when the SAE server is offline

IMPORTANT! The functionality to use the application when the SAE server is offline is not available for all applications. If is not available, it is noted in the chapter specific to your application.

The SAE server can be offline if the computer running the SAE Administrator Console is not connected to the internet or has been powered off.

If your SAE administrator has set up the settings to allow use of the applications when the SAE server is offline, you can use the application for a specified period of time (see "Configure account set up and security policies" on page 85).

Note: If you have not previously signed into the instrument with your SAE account, you cannot sign in when the SAE server is offline.

All SAE records are retained if the application is disconnected from the SAE server. When the application is reconnected to the SAE server, SAE records are uploaded to the server.

The following functions are not available when the SAE server is offline:

- Account lockout
- Password reminder
- Mandatory password change
- Disable the SAE functions
- Change password

Sign in after automatic screen locking

IMPORTANT! The functionality to set the application to lock after a period of inactivity is not available for all applications. If is not available, it is noted in the chapter specific to your application.

Depending on the way your SAE administrator has configured the settings, the application can be locked after a period of inactivity.

The default permissions for an Administrator role or a Scientist role allow sign-in after automatic lockout.

Optional tasks

Set up notifications

You can specify when and how to be notified when specified events occur in the SAE Administrator Console. The following options are available for notifications:

- In the **Event Notification** dialog box that is displayed when you sign in to the SAE Administrator Console
- By email

Note: The messaging email is not connected to your Thermofisher.com account.

IMPORTANT! You must configure the simple mail transfer protocol (SMTP) server to send email notifications (see "Configure the SMTP server for email notifications" on page 25). If the SMTP server is not configured, email notifications are not sent, even if email addresses are added.

1. In the main screen, click **Settings** ▸ **Notifications**.
2. In the **Edit Notification Settings** dialog box, select **Notify at Administrator sign in** for the events of interest.
3. *(Optional)* Select **Notify by Email** for the events of interest, then specify an email address or multiple email addresses.

   Up to five email addresses can be entered. Separate the email addresses with a comma.
4. Click **Save**, then click **Close**.

Configure the SMTP server for email notifications

Configure the SMTP server so that the SAE Administrator Console can send email notifications.

1. In the main screen, click **Settings** ▸ **Email Server**.
2. In the **SMTP Configuration** dialog box, enter the following:
   - **SMTP host**, **SMTP port**, and **SMTP sender**

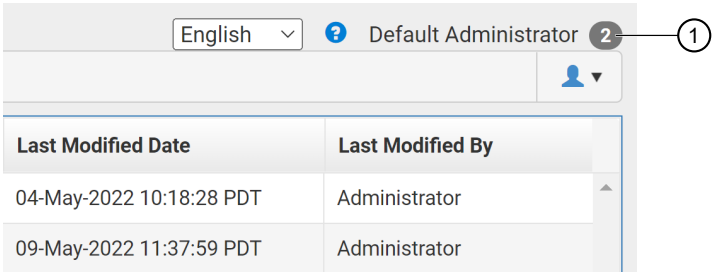
     Note: Select **Authentication required** if the SMTP server requires authentication.
   - **User Name** and **Password**

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

View the notifications

Once the notifications have been acknowledged at sign-in or from the main screen, they are no longer available to view.

If there are notifications available to view, the number of notifications is displayed beside the signed-in user.



① Number of notifications

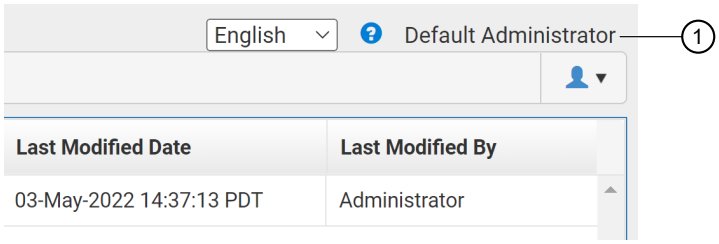
1. In the top-right corner of the screen, click the number that is displayed beside the signed-in user.
   No number is displayed if there are no notifications.
   The **Event Notifications** dialog box is displayed.

2. Perform one of the following steps.

Option	Description
Click **Close**.	The notifications are retained. They are displayed at the next sign-in. They can also continue to be accessed after sign-in.
Select one or all of the notifications, then click **Acknowledge**.	The notifications are cleared. They are not displayed at the next sign-in. They cannot be accessed after sign-in.

Determine the signed-in user

See the top-right corner of the main screen to determine the signed-in user.



① Signed-in user

Display the software version

1. In the main screen, click **Settings** ▸ **About**.
   The software version is displayed in the **About SAE Admin Console** dialog box.
2. Click **Close**.

View the terms of use (EULA)

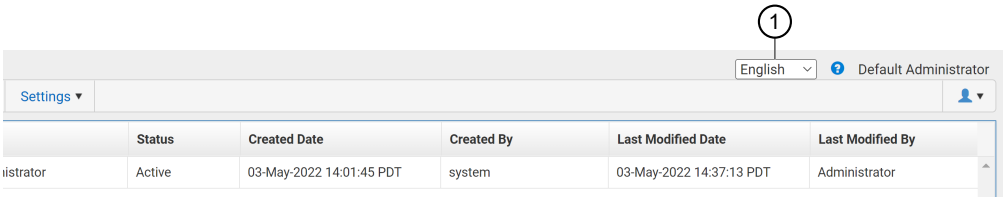
The terms of use is the End User License Agreement (EULA).

1. In the main screen, click **Settings** ▸ **About**.
2. In the dialog box, click **Terms of Use**.
   The EULA is opened as a PDF in a new tab of the browser.
3. In the dialog box, click **Close**.

Select the language

Different languages are available in the SAE Administrator Console v2.2.

The language drop-down list is located at the top-right corner of the SAE Administrator Console.



1 Language drop-down list

Select a language from the drop-down list.

The page reloads in the selected language.

3 Use the SAE Administrator Console with multiple applications

Configuration with multiple applications

Multiple applications can be connected to the same instance SAE Administrator Console.

Note: Some applications require direct connection between the instrument and the computer.

In the example configuration shown below, four instruments/software are connected to the same SAE Administrator Console. Each instrument/software has an application profile that can be configured independently for each user.

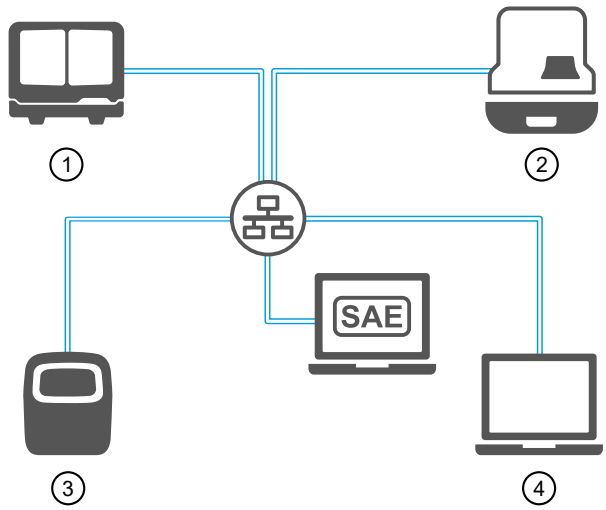


Figure 1 Example SAE configuration connected to multiple applications

① Capillary electrophoresis instrument software 1
② Capillary electrophoresis instrument software 2
③ Real-time PCR instrument
④ Real-time PCR software

Note: For specific instructions for the SAE Administrator Console with capillary electrophoresis applications, see *SAE Administrator Console v2.1 User Guide for Capillary Electrophoresis Products* (Pub. No. MAN0025849).

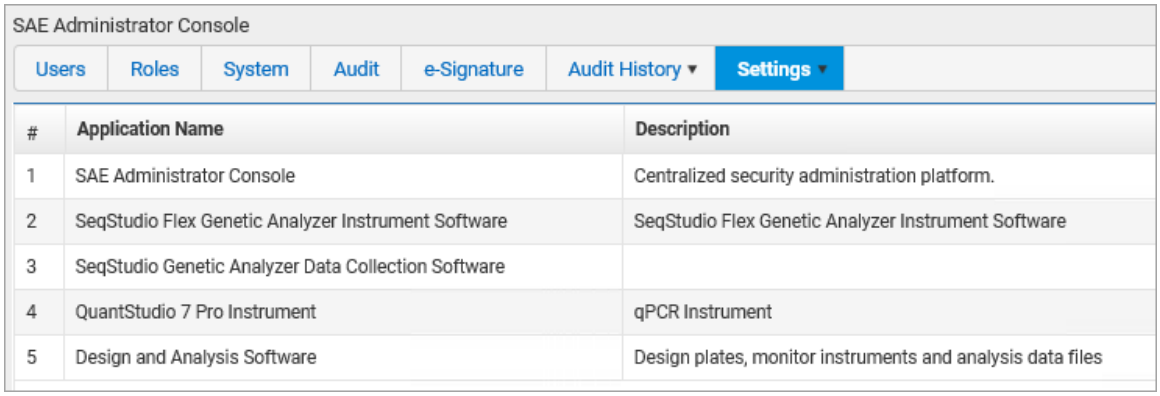


Figure 2 Example application profiles that have been installed in the SAE Administrator Console

An application profile applies to every application. For example, if more than one QuantStudio™ 7 Pro Real-Time PCR Instrument is connected to the same instance of the SAE Administrator Console, the settings apply to all of these instruments. Each individual QuantStudio™ 7 Pro Real-Time PCR Instrument cannot be configured separately.

Some functions set in the SAE Administrator Console apply to all of the applications that are connected to the same instance of the SAE Administrator Console. For example, if e-signatures are enabled or disabled, this selection applies to all of the applications.

Default roles when multiple application profiles are installed

When you install an application profile, the permissions for the application are added to the software. The permissions are listed in the **Create Roles** or **Edit Roles** dialog boxes. These dialog boxes are accessed from the **Roles** tab.

When you install more than one application profile, all of the roles that are common between the applications list the specific permissions for each application.

Some roles might be specific to a particular application. For example, the QuantStudio™ Absolute Q™ Digital PCR Software has an administrator role specific to the application.

Depending on the application profiles, it might be necessary to install them in a specific order. See the chapter for your application.

For information about managing the roles, see the following sections:

- “Create a role” on page 81
- “Edit a role” on page 82
- “Delete a role” on page 82

4 Configure the SAE functions for the real-time PCR system

This chapter covers the use of the SAE Administrator Console with the QuantStudio™ 7 Pro Real-Time PCR Instrument and the QuantStudio™ Design and Analysis Software v2.

System components with the SAE functions enabled

The following system components can be used with the SAE functions enabled:

- QuantStudio™ 7 Pro Real-Time PCR Instrument
- QuantStudio™ Design and Analysis Software v2
- Plate files for the QuantStudio™ 7 Pro Real-Time PCR Instrument—SAE-enabled plate files are created in the QuantStudio™ Design and Analysis Software v2 with SAE functions enabled.
  - If the SAE functions are enabled in the QuantStudio™ Design and Analysis Software v2, you can only create plate files for the QuantStudio™ 7 Pro Real-Time PCR Instrument.
  - If the SAE functions are enabled on the QuantStudio™ 7 Pro Real-Time PCR Instrument, you cannot create or edit a plate file from the instrument touchscreen.
- QuantStudio™ 7 Pro Real-Time PCR Instrument data file—SAE-enabled data files are created on the QuantStudio™ 7 Pro Real-Time PCR Instrument with SAE functions enabled.

We recommend enabling the SAE functions for all system components (see "Enable the SAE functions" on page 34). If one or more of the components have a conflicting SAE status, some features might not be available (see "Compatibility between SAE-enabled and SAE-disabled components" on page 31).

Note: Template and data files are checksum protected.

- Checksum protection helps to ensure that files produced by the instruments are not edited outside of the system.
- Files produced by the software applications are checksum protected by the software, regardless of whether the SAE functions are enabled.

Compatibility between SAE-enabled and SAE-disabled components

We recommend enabling the SAE functions for all system components (for more information, see "Enable the SAE functions" on page 34). If one or more of the components have a conflicting SAE status, some features might not be available. See the following table for more information.

Component	Functionality with an SAE-enabled plate or data file	Functionality with an SAE-disabled plate or data file
QuantStudio™ Design and Analysis Software v2 with SAE functions enabled	• The file can be edited, depending on the SAE configuration. • The audit trail is continued.	• The file is opened in read-only mode. • The file cannot be edited or saved.
QuantStudio™ Design and Analysis Software v2 with SAE functions disabled	• SAE-disabled files allowed—The file is opened and can be edited. The file can be saved as an invalid SAE file only.[1] • QuantStudio™ 7 Pro Real-Time PCR Instrument forbidden—The file cannot be opened.	The file can be opened, edited, and saved.

(continued)

Component	Functionality with an SAE-enabled plate or data file	Functionality with an SAE-disabled plate or data file
QuantStudio™ 7 Pro Real-Time PCR Instrument with SAE functions enabled	• The file can be opened from the run queue, a USB drive, or other sources.[2] • The file cannot be edited. • The audit record is continued.	The file cannot be opened.
QuantStudio™ 7 Pro Real-Time PCR Instrument with SAE functions disabled	• The plate file can be opened and edited. • The file can be saved as an invalid SAE file only.[1] • The file can be used to start a run, but the data file will be an invalid SAE file.[1]	The file can be opened, edited, and saved.

[1] Invalid SAE files contain incomplete audit records.

[2] You cannot import plate files from the Thermo Fisher™ Connect Platform when the instrument has the SAE functions enabled.

Compatibility

Application profile	SAE Administrator Console	QuantStudio™ 7 Pro Real-Time PCR Instrument software version	QuantStudio™ Design and Analysis Software v2 version
`QuantStudio 7 Pro Instrument (1.6.0).dat` `Design and Analysis Software (1.4.0).dat`	v2.2	v1.8.1	v2.8
`QuantStudio 7 Pro Instrument (1.5.0).dat` `Design and Analysis Software (1.4.0).dat`	v2.2	v1.8	v2.8
`QuantStudio 7 Pro Instrument (1.4.0).dat` `Design and Analysis Software (1.3.0).dat`	v2.2	v1.7	v2.7 v2.6.x
`QuantStudio 7 Pro Instrument (1.3.0).dat` `Design and Analysis Software (1.3.0).dat`	v2.2 v2.1	v1.6.x v1.5.x v1.4.x	v2.7 v2.6.x
`QuantStudio 7 Pro Instrument (1.2.1).dat` `Design and Analysis Software (1.2.1).dat`	v2.1 v2.0	v1.4.x	v2.5.1

(continued)

Application profile	SAE Administrator Console	QuantStudio™ 7 Pro Real-Time PCR Instrument software version	QuantStudio™ Design and Analysis Software v2 version
`QuantStudio 7 Pro Instrument (1.2.0).dat` `Design and Analysis Software (1.2.0).dat`	v2.1 v2.0	v1.4.x	v2.5.x
`QuantStudio 7 Pro Instrument (1.1.1).dat` `Design and Analysis Software (1.1.1).dat`	v2.0	v1.3.x	v2.4.x
`QuantStudio 7 Pro Instrument (1.1.0).dat` `Design and Analysis Software (1.1.0).dat`	v2.0	v1.2.1	v2.3.x

Profiles and features when the SAE functions are enabled

Overview of the instrument features when the SAE functions are enabled

The following instrument features are not available when the SAE functions are enabled:

- Facial authentication
- Voice commands
- Linking to the Thermo Fisher™ Connect Platform, including using a Thermo Fisher™ Connect Platform account to log in
- System templates

  Only SAE-enabled plate files that were created in the QuantStudio™ Design and Analysis Software v2 can be opened on the instrument.

Profiles on the QuantStudio™ 7 Pro Real-Time PCR Instrument when the SAE functions are enabled

After the SAE functions are enabled on the QuantStudio™ 7 Pro Real-Time PCR Instrument, the local instrument profiles and the Thermo Fisher™ Connect Platform profiles are not available.

An account from the SAE Administrator Console must be used to sign in to the instrument when the SAE functions are enabled. A local instrument administrator can sign in to the instrument to perform limited administrator functions.

The local instrument profiles and the Thermo Fisher™ Connect Platform profiles are available if the SAE functions are disabled.

Profiles in the QuantStudio™ Design and Analysis Software v2 when the SAE functions are enabled

Sign-in is not required for the software when the SAE functions are not enabled.

When the SAE functions are enabled, sign-in is required with an SAE user account.

Enable the SAE functions

Workflow

Enable SAE functions

1. **Install the application profiles**
   See "Application profiles" on page 34.
2. **Enable the SAE functions on the QuantStudio™ 7 Pro Real-Time PCR Instrument** (page 35)
3. **Connect the QuantStudio™ Design and Analysis Software v2 to the SAE Administrator Console** (page 36)
4. **Enable the SAE functions in QuantStudio™ Design and Analysis Software v2** (page 36)

Application profiles

For detailed instructions to install application profiles, see "Install the application profiles" on page 22.

The application profiles must be installed before the application can be connected to the SAE Administrator Console.

The following application profiles are available:

Application (instrument or software)	Application profile[1]
QuantStudio™ 7 Pro Real-Time PCR Instrument	`QuantStudio 7 Pro Instrument (<…>).dat`
QuantStudio™ Design and Analysis Software v2	`Design and Analysis Software (<…>).dat`

[1] <…> is the version of the application profile. For more information, see "Application profile versions" on page 16.

The application profile for QuantStudio™ Design and Analysis Software v2.8 or later does not require that the application profile for the QuantStudio™ 7 Pro Real-Time PCR Instrument is installed.

For QuantStudio™ Design and Analysis Software v2.7 and earlier, the application profile for the QuantStudio™ 7 Pro Real-Time PCR Instrument must be installed before the application profile for the QuantStudio™ Design and Analysis Software v2.

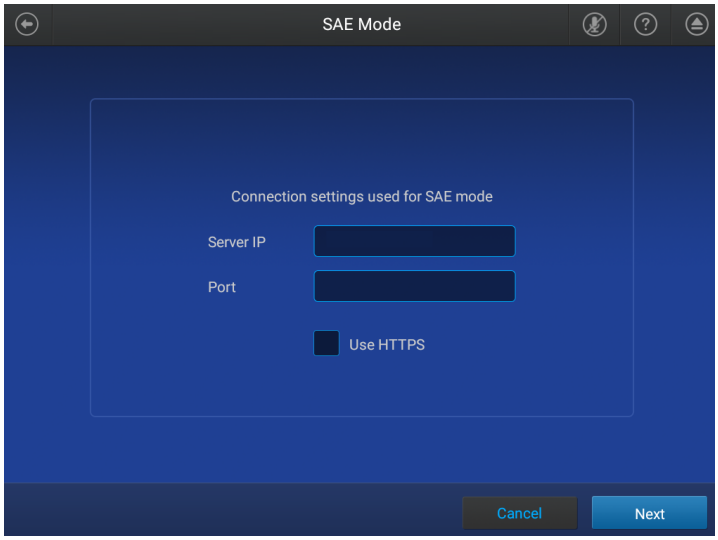
Enable the SAE functions on the QuantStudio™ 7 Pro Real-Time PCR Instrument

This procedure requires a local administrator profile on the instrument and an SAE administrator user account in the SAE Administrator Console.

1. In the home screen, tap ⚙ **(Settings)** ▸ **SAE**.
   The **SAE Mode** screen is displayed.

2. In the **SAE Mode** screen, set the **SAE Mode** slider to **Enable**.

3. Tap the **Server IP** field, then enter the IP address of the SAE server.
   The server IP is the IP address of the computer on which the SAE Administrator Console is installed.



4. Tap the **Port** field, then enter the port.
   The port that is entered is the firewall port.
   It is dependent on the version of the SAE Administrator Console. See “Firewall ports that must be open” on page 16.

5. Tap **Next**.

6. Enter the SAE administrator user name and password when prompted, then tap **Enable**.

The home screen is displayed. The SAE administrator is signed in.

Connect the QuantStudio™ Design and Analysis Software v2 to the SAE Administrator Console

Close all plate files and data files before connecting to the SAE Administrator Console.

Note: Connect the software and instruments to the same instance of the SAE Administrator Console to help ensure that audit records are maintained across system components.

1. In the menu bar, click **System** ▸ **SAE Connection Settings**.
2. Enter the server and port number of the SAE Administrator Console.

   If the SAE Administrator Console is installed on the same computer as the QuantStudio™ Design and Analysis Software v2, enter ***localhost***.

   If the SAE Administrator Console is installed on a different computer from the QuantStudio™ Design and Analysis Software v2, enter the IP address of the computer on which the SAE Administrator Console is installed.

   Note: If using a dynamic IP address, enter the hostname instead of the IP address to prevent the loss of a connection (see "Determine the hostname" on page 36).

   The port number is the firewall port.

   The port number is dependent on the version of the SAE Administrator Console. See "Firewall ports that must be open" on page 16.
3. (*Optional*) Click **Test Connection** to confirm that the connection information is correct.
4. Click **Save**.

Determine the hostname

If the SAE Administrator Console is on a separate computer from the application and a dynamic IP address is used, the hostname is recommended instead of the IP address. This helps to prevent the loss of a connection between the SAE Administrator Console and the application

1. In the Windows™ search bar, enter ***cmd*** to open the **Command Prompt**.
2. Enter ***hostname***, then press **Enter**.

The hostname of the computer is displayed in the **Command Prompt**.

Enable the SAE functions in QuantStudio™ Design and Analysis Software v2

This procedure requires an SAE administrator user account.

Complete the following tasks before you enable the SAE functions in the QuantStudio™ Design and Analysis Software v2:

- Connect to the SAE Administrator Console (see "Connect the QuantStudio™ Design and Analysis Software v2 to the SAE Administrator Console" on page 36).
- Close all plate files and data files.

1. In the QuantStudio™ Design and Analysis Software v2, select ⚙ **System** ▸ **Enable Security**.
2. Enter your SAE administrator account user name and password, then click **Sign In**.

The SAE administrator account is automatically signed into the software after the SAE functions are enabled. The SAE user account name is displayed in the upper-right corner of the software menu bar.

Disable the SAE functions

Disable the SAE functions in the QuantStudio™ Design and Analysis Software v2

This procedure requires an SAE administrator account.

Close all plate files and data files.

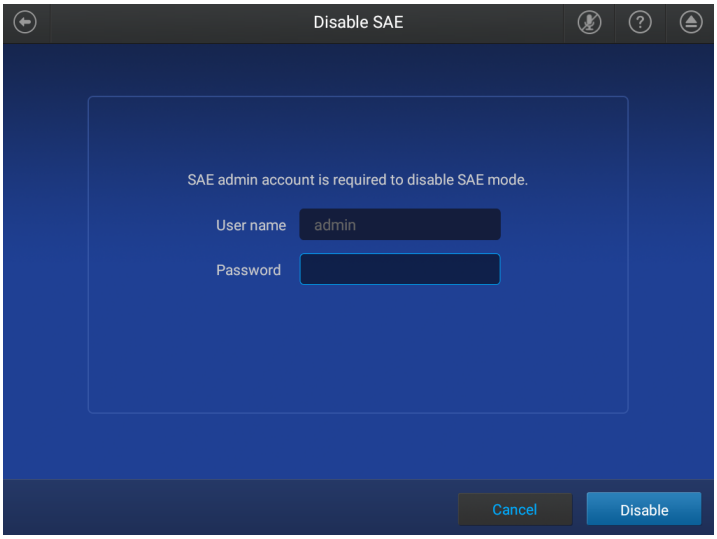
1. In QuantStudio™ Design and Analysis Software v2, select ⚙ **System** ▸ **Disable Security**.
2. Enter the password of the SAE administrator account, then click **Sign In**.

Disable the SAE functions on the QuantStudio™ 7 Pro Real-Time PCR Instrument (administrator only)

This procedure requires a local administrator profile and an SAE administrator user account.

Sign in with a local administrator account (see “Sign in as a local administrator when SAE functions are enabled” on page 38).

1. In the home screen, tap ⚙ **(Settings)** ▸ **SAE**.
   The **SAE Mode** screen is displayed.
2. In the **SAE Mode** screen, set the **SAE Mode** slider to the **Disable** position, then tap **Done**.
3. Enter the password for the SAE administrator account, then tap **Disable**.
   The user name for the SAE administrator account is filled out and cannot be edited.

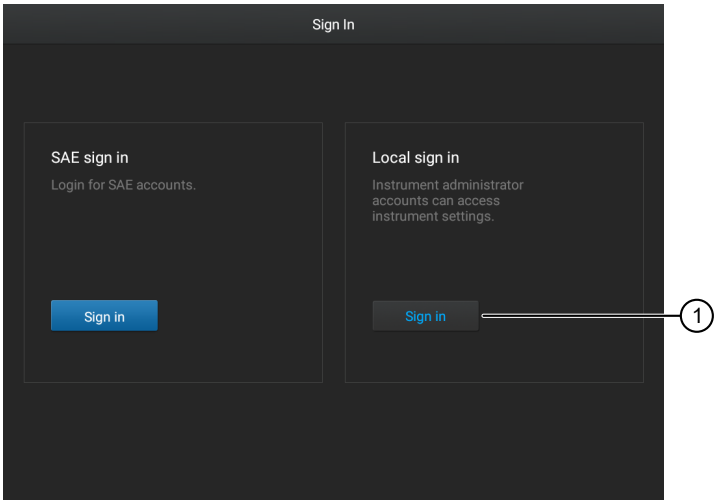


The **Sign In** screen is displayed.

Sign in as a local administrator when SAE functions are enabled

Sign in as a local administrator to access the instrument settings. Plate files are not accessible if you are signed in as a local administrator.

1. In the **Sign In** screen, tap **Sign in** under **Local sign in**.



① Sign in for administrator

The **Local Administrator Sign In** screen is displayed.

2. In the **Local Administrator Sign In** screen, select your local administrator profile.
3. Enter your PIN, then tap **Enter**.

The **Settings** screen is displayed.

Change your password

Overview of a password change

A change to the SAE user account password in one application changes it across all of the applications that are connected to the same instance of the SAE Administrator Console.

The QuantStudio™ Design and Analysis Software v2 and the QuantStudio™ 7 Pro Real-Time PCR Instrument must be connected to the instance of the SAE Administrator Console in order for the SAE user account password to be updated for both the software and the instrument.

Change your SAE user account password on the QuantStudio™ 7 Pro Real-Time PCR Instrument

The SAE functions must be enabled on the instrument.

Sign in to the instrument with your SAE user account.

1. In the home screen, tap **(Profile)**.
   The **My Profile** screen is displayed. The **SAE** button is selected, and the profile that is signed in is listed.

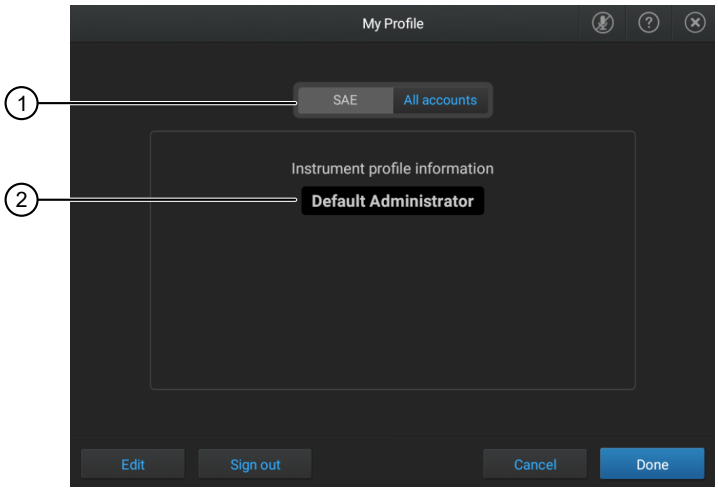


Figure 3 My Profile screen

① **SAE** button is active
② Profile that is signed in

2. Tap **Edit**.
   The **Edit My Profile** screen is displayed.

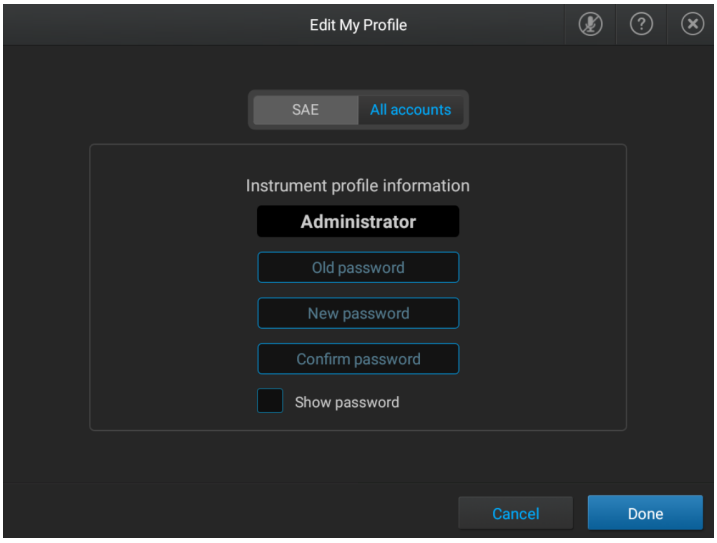


Figure 4 Edit My Profile screen

3. Tap the **Old password** field, enter the current SAE user account password, then tap **Enter**.
4. Tap the **New password** field, enter a new SAE user account password, then tap **Enter**.
   (Optional) Tap the **Show password** checkbox to show or hide the password.
5. Tap the **Confirm password** field, enter the new SAE user account password again, then tap **Enter**.
6. Tap **Done**.

Your SAE user account password is also be changed on the QuantStudio™ Design and Analysis Software v2 if the instrument and the software are connected to the same instance of the SAE Administrator Console.

Change your SAE user account password in the QuantStudio™ Design and Analysis Software v2

The SAE functions must be enabled in the software.

Sign in to the software with your SAE user account.

1. In the top-right corner of the software, click on the user information.

① User information

2. Click **Change password**.

3. In the **Change Password** dialog box, enter the following information:
   - Old password
   - New password
   - New password in the **Confirm password** field
4. Click **OK**.

Your SAE user account password is also changed on the QuantStudio™ 7 Pro Real-Time PCR Instrument if the instrument and the software are connected to the same instance of the SAE Administrator Console.

SAE Administrator Console functions

Functions that are controlled on the QuantStudio™ 7 Pro Real-Time PCR Instrument

The following functions are controlled on the instrument, depending on the user role:

- Setup, including the following functions:
  - Create a new template or run
  - Edit the run method
  - Edit the analysis settings
  - Define, edit, or delete the targets or the assays
  - Assign the target or the assay
  - Define, edit, or delete the sample
  - Assign the samples
  - Define, edit, or delete the reagents
  - Assign the reagents
  - Add a new custom dye
  - Edit the passive reference
- Instrument runs, including the following functions:
  - Start an instrument run
  - Stop an instrument run
- Calibrations, including the following functions:
  - Perform a system dye calibration
  - Perform ROI and uniformity calibration
  - Perform background calibration
  - Perform custom dye calibration
  - Perform custom melt calibration
- Instrument validation (perform an RNase P run)

- Instrument configuration, including the following functions:
  - Perform a firmware update
  - Configure the network
  - Change the instrument name
  - Modify the date and time
  - Modify the sleep mode settings
  - Modify the disk management settings
  - Perform a backup and restore
  - Manage the data, including export locations and import locations
  - Export data files
  - Export general files, including files associated with instrument maintenance
  - Overwrite files that have been previously transferred
  - Keep both files if a file has previously been transferred
  - Delete data files from the instrument
- Security configuration, including the following functions:
  - Log into timed out user sessions
  - Perform e-signing

Functions that are controlled in the QuantStudio™ Design and Analysis Software v2

The following functions are controlled in the software, depending on the user role:

- Instrument management, including the following functions:
  - Add an instrument
  - Delete an instrument
  - Export an instrument
- Template management, including the following functions:
  - Install a template
  - Remove a template
- Setup, including the following functions:
  - Create a plate
  - Edit the run method
  - Edit the analysis settings
  - Add, edit, or delete the targets or the assays
  - Assign the target or the assay
  - Add, edit, or delete the sample
  - Assign the samples
  - Add, edit, or delete the reagents
  - Assign the reagents

  - Add an analysis module
  - Edit the passive reference
- Security configuration, including the following functions:
  - Log into timed out user sessions
  - Perform e-signing
- Plugin management, including the following functions:
  - Install or upgrade a plugin
  - Delete a plugin
- User preferences (edit preferences)
- Edit the file save destination
  - Edit the export destination
  - Edit the RDML export destination
  - Edit the report destination
  - Edit the save as destination

Objects that can be audited

The plate is an audited object for the QuantStudio™ 7 Pro Real-Time PCR Instrument and the QuantStudio™ Design and Analysis Software v2.

The audit function for objects can be enabled or disabled (see “Enable or disable the audit function” on page 88).

The audit mode for objects can be set (see “Set the audit mode” on page 89).

The audit summary for objects is viewed in the QuantStudio™ Design and Analysis Software v2.

Each time one of the following items is changed, it can be audited, depending on the audit function setup:

- Plate layout
- Analysis settings
- Run method
- Samples
- Assays

The user can be required to select a reason if one of the items listed above is edited (see “Set the audit mode” on page 89).

The following reasons are available:

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

A reason can be added, deleted, or edited. See “Configure the audit reason settings” on page 89.

Actions that are audited

The actions are audited and listed in the action records regardless of whether audits are enabled or disabled. The audited actions are viewed in the SAE Administrator Console. They are not viewed in the application.

Note: Enabling and disabling audits only applies to objects that are audited. See “Objects that can be audited” on page 43 .

The following user actions are audited:

- Sign in success
- Sign out
- Sign in failure
- Enable the SAE functions
- Disable the SAE functions
- Add a new instrument
- Remove an instrument
- Add a new plugin
- Remove a plugin
- Install a template
- Remove a template

Actions that require an e-signature in the QuantStudio™ 7 Pro Real-Time PCR Instrument

Certain actions performed on the instrument can be set up to require an e-signature. This depends on how the e-signature settings have been configured in the SAE Administrator Console.

The following actions can be set up to require an e-signature:

- Start a calibration run
- Start a run
- Accept calibration

Each action that requires an e-signature is associated with an e-signature meaning and the data that are signed.

E-signature meaning	Data signed
Reviewed and approved template	• Plate setup • Run method
Accept calibration results	Calibration record

For detailed descriptions of each parameter, see Chapter 9, “Manage the e-signature function”.

Actions that require an e-signature in the QuantStudio™ Design and Analysis Software v2

Certain actions performed in the software can be set up to require an e-signature. This depends on how the e-signature settings have been configured in the SAE Administrator Console.

Printing a report can be set up to require an e-signature.

Each action that requires an e-signature is associated with an e-signature meaning and the data that are signed.

E-signature meaning	Data signed
Reviewed and approved template	• Plate setup • Run method
Reviewed and approved plate results	• Analysis results • Analysis setting

For detailed descriptions of each parameter, see Chapter 9, “Manage the e-signature function”.

Default permissions and roles

The SAE Administrator Console provides the following default roles:

- Administrator
- Scientist
- Technician

Each default role has a set of permissions, depending on the application.

The default roles can be edited (see “Edit a role” on page 82).

Custom roles can be created (see “Create a role” on page 81).

IMPORTANT! SAE permissions for a role apply to all user accounts that are assigned to the role.

When an application profile is upgraded, the default permissions of any new functions in the new application profile are not applied. The roles do not receive the permission for the new functions. Only the Administrator role receives the permissions for the new functions.

The roles and associated user-configurable permissions are listed in the following tables. You can also double-click the role in the **Roles** tab to display the list of permissions.

The Administrator role has full privileges and the permissions cannot be edited.

Note: The **No Privileges** role is used by the software when you set up user repositories. Do not assign this role to a user account.

Default permissions for the QuantStudio™ 7 Pro Real-Time PCR Instrument

Function	Role		
	Administrator	Scientist	Technician
Setup			
Create a new plate file	Yes	Yes	Yes
Edit the run method	Yes	Yes	No
Edit the analysis settings	Yes	Yes	Yes
Define, edit, or delete the targets or the assays	Yes	Yes	Yes
Assign a target or an assay	Yes	Yes	Yes
Define, edit, or delete a sample	Yes	Yes	Yes
Assign a sample A user has permission to assign a sample if they have permission to define, edit, or delete a sample. This applies even if the **Assign Sample** checkbox is not selected in the Security, Auditing, and E-signature (SAE) Administrator Console.	Yes	Yes	Yes
Define, edit, or delete a reagent	Yes	Yes	Yes
Assign a reagent	Yes	Yes	Yes
Add a new custom dye	Yes	Yes	No
Edit the passive reference	Yes	Yes	No
Instrument run			
Start a run	Yes	Yes	Yes
Stop a run	Yes	Yes	Yes
Calibration			
Perform a system dye calibration	Yes	Yes	No
Perform an ROI and uniformity calibration	Yes	Yes	No
Perform a background calibration	Yes	Yes	No
Perform a custom dye calibration	Yes	Yes	No
Perform a custom melt calibration	Yes	Yes	No
Instrument validation			
Perform an RNase P run	Yes	Yes	No

(continued)

Function	Role		
	Administrator	Scientist	Technician
Instrument configuration			
Perform firmware update	Yes	No	No
Configure the network	Yes	No	No
Change the instrument name	Yes	No	No
Modify the date and the time	Yes	No	No
Modify the SAE settings	Yes	No	No
Modify the sleep mode settings	Yes	No	No
Modify the instrument access settings	Yes	No	No
Modify the disk management settings	Yes	No	No
Perform a backup and restore	Yes	No	No
Change data management settings	Yes	Yes	No
Data management			
Allow overwriting of files	Yes	Yes	Yes
Allow deletion of files	Yes	Yes	Yes
Allow keeping both files	Yes	Yes	Yes
Manually export run data	Yes	Yes	Yes
Export general data	Yes	Yes	Yes
Security configuration			
Log into timed-out user sessions	Yes	Yes	No
Perform e-signing	Yes	Yes	No

Default permissions for the QuantStudio™ Design and Analysis Software v2

Function	Role		
	Administrator	Scientist	Technician
Instrument management			
Add instrument	Yes	Yes	No
Delete instrument	Yes	Yes	No
Export instrument	Yes	Yes	No
Template management			
Install template	Yes	Yes	No
Remove template	Yes	Yes	No
Setup			
Create a plate file	Yes	Yes	Yes
Edit run method	Yes	Yes	No
Edit analysis settings	Yes	Yes	Yes
Add, edit, or delete targets and assays	Yes	Yes	No
Assign targets and assays	Yes	Yes	No
Add, edit, or delete samples	Yes	Yes	Yes
Assign samples A user has permission to assign a sample if they have permission to define, edit, or delete a sample. This applies even if the **Assign Sample** checkbox is not selected in the Security, Auditing, and E-signature (SAE) Administrator Console.	Yes	Yes	Yes
Add, edit, or delete reagents	Yes	Yes	Yes
Assign reagents	Yes	Yes	Yes
Add, edit, or delete custom dyes	Yes	Yes	No
Assign an analysis module	Yes	Yes	Yes
Edit passive reference	Yes	Yes	No
Security configuration			
Log into timed-out user sessions	Yes	Yes	No
Perform e-signing	Yes	Yes	No

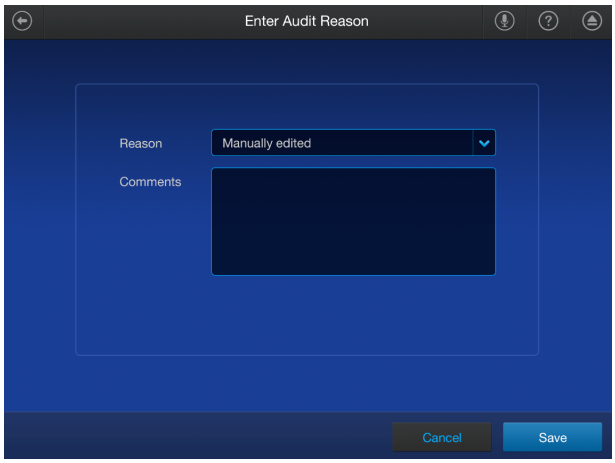
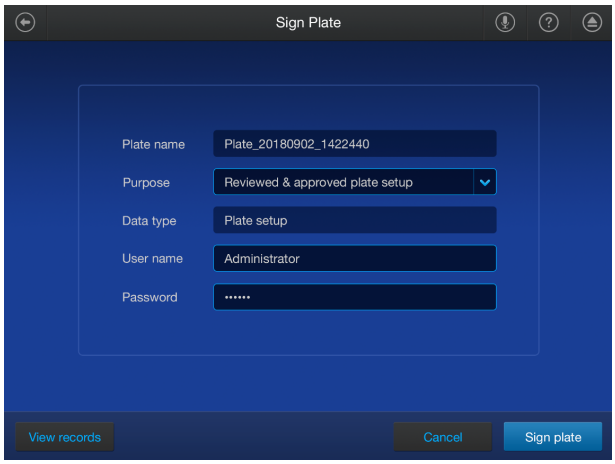
(continued)

Function	Role		
	Administrator	Scientist	Technician
Plugin management			
Install or upgrade a plugin	Yes	No	No
Delete a plugin	Yes	No	No
User preferences			
Edit preferences	Yes	No	No
Edit file save destination			
Edit export destination	Yes	No	No
Edit RDML export destination	Yes	No	No
Edit report destination	Yes	No	No
Edit save as destination	Yes	No	No

Screens and dialog boxes that are displayed in the application when the SAE functions are enabled

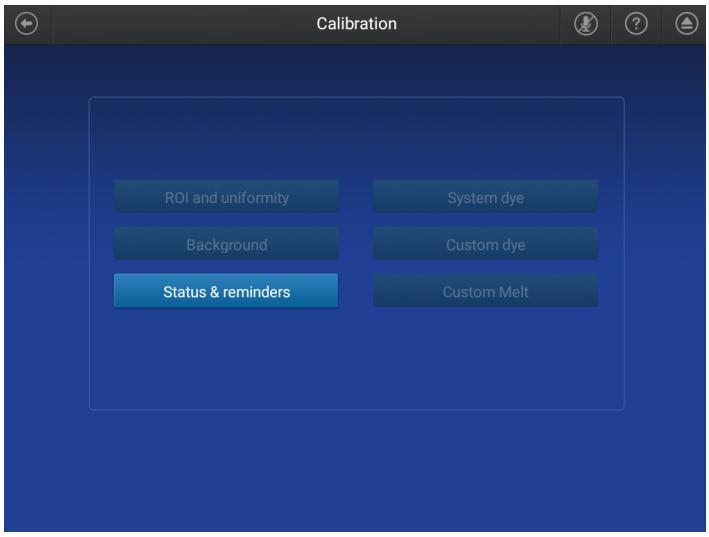
Screens that are displayed on the QuantStudio™ 7 Pro Real-Time PCR Instrument

Some of the screens described might not be displayed. They are dependent on how the SAE administrator has configured the system.

Screen	Description
	This screen is displayed if an object is set up to be audited. See “Objects that can be audited” on page 43.
	This screen is displayed if an action requires an e-signature.

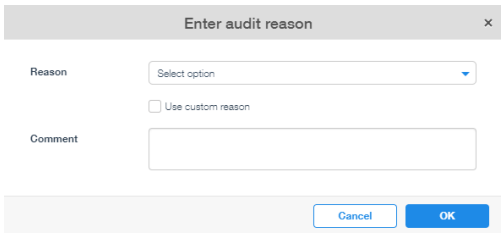
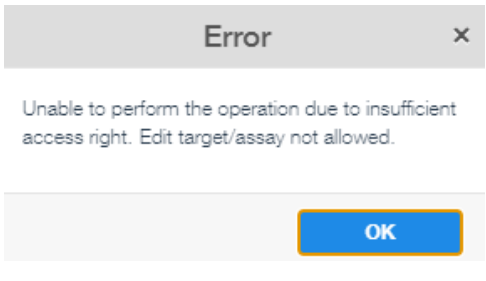
If you do not have access to a function, you cannot select it.

For example, the buttons to start any of the calibrations are inactive if your role does not have permission to perform a calibration.



Dialog boxes that are displayed in the QuantStudio™ Design and Analysis Software v2

Some of the dialog boxes described might not be displayed. They are dependent on how the SAE administrator has configured the system.

Dialog box	Description
	This dialog is displayed if an object is set up to be audited. See “Objects that can be audited” on page 43.
	This screen is displayed if an action requires an e-signature.
	This dialog box is displayed if the function is not permitted for the role.

If you do not have access to a function, you cannot select it. The ⃠ icon is displayed.

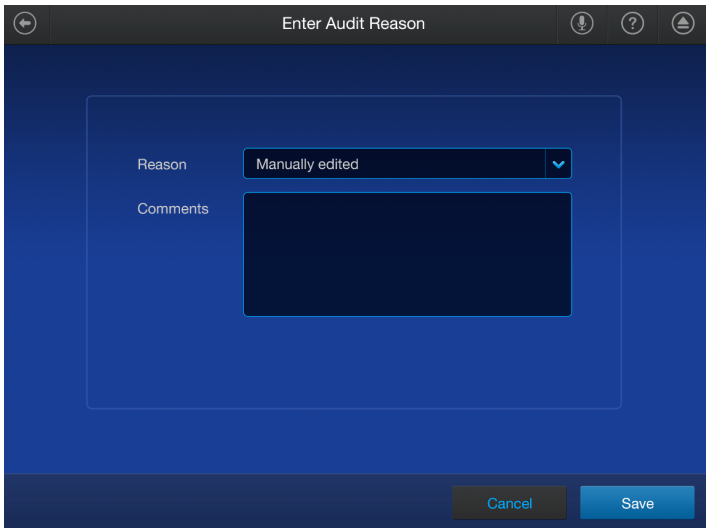
Enter audit reasons and e-signatures

Enter an audit reason on the QuantStudio™ 7 Pro Real-Time PCR Instrument

Depending on the way that the audit settings are configured, the **Enter Audit Reason** screen can be displayed when you make changes to the plate file.

If the audit function is disabled, this screen is not displayed.

If the audit mode is set to silent, this screen is not displayed.



1. Select the reason from the **Reason** dropdown list.
   If the audit mode is set to optional, a reason does not need to be selected.
2. *(Optional)* Enter comments in the **Comments** field.
3. Tap **Save**.

The audit record cannot be viewed on the instrument.

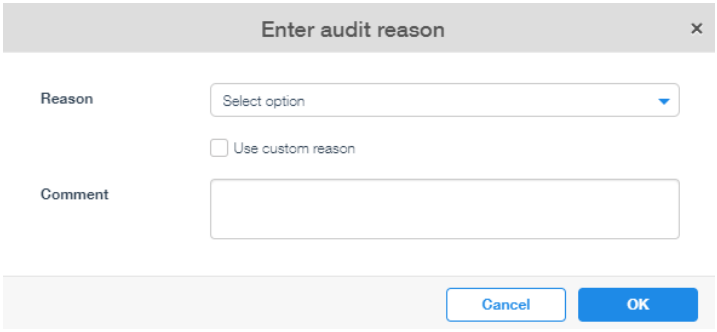
The audit record is displayed in the QuantStudio™ Design and Analysis Software v2 (see “View audit records for objects for the QuantStudio™ Design and Analysis Software v2” on page 56).

Enter an audit reason in the QuantStudio™ Design and Analysis Software v2

Depending on the way that the audit settings are configured, the **Enter audit reason** dialog box can be displayed when you save a plate file that has been edited.

If the audit function is disabled, this screen is not displayed.

If the audit mode is set to silent, this screen is not displayed.



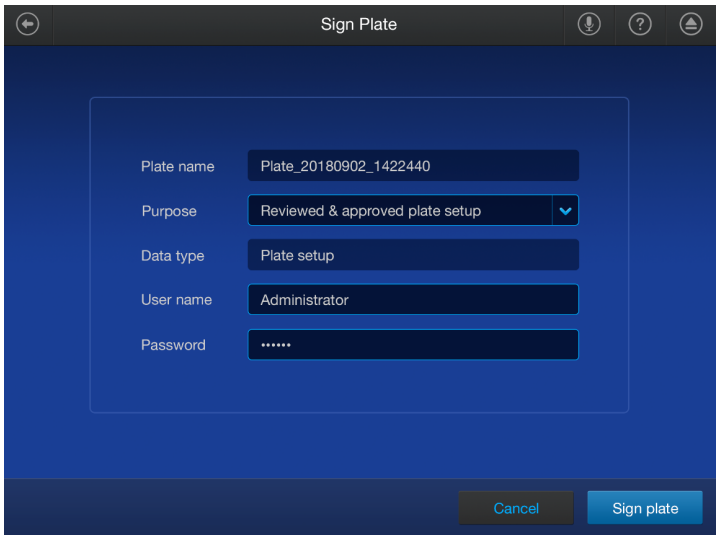
1. *(Optional)* Select the **Use custom reason** checkbox, then enter a reason in the **Reason** field.
   The **Reason** dropdown list changes to a field when the **Use custom reason** checkbox is selected.
2. Select the reason from the **Reason** dropdown list.
   If the audit mode is set to optional, a reason does not need to be selected.
3. *(Optional)* Enter comments in the **Comments** field.
4. Click **OK**.

The audit record is displayed in the **Data Audit** tab (see “View audit records for objects for the QuantStudio™ Design and Analysis Software v2” on page 56).

Enter an e-signature on the QuantStudio™ 7 Pro Real-Time PCR Instrument

The screen to sign depends on action that requires and e-signature and the item that is being signed (see “Actions that require an e-signature in the QuantStudio™ 7 Pro Real-Time PCR Instrument” on page 44).

In the following figure, the plate setup is being signed.



1. Select the e-signature meaning from the **Purpose** dropdown list.
2. Enter your SAE user account name and password.

   Note: The SAE user account must have permissions to perform e-signatures.

3. Tap **Sign <…>**, where <…> is the data signed.

   In the example above, the plate is signed. The button is **Sign plate**.

The e-signature records for a plate setup are viewed on the instrument (see “View e-signature records for a plate file on the QuantStudio™ 7 Pro Real-Time PCR Instrument” on page 56).

The e-signature records for a calibration are not viewed on the instrument. They are included in a calibration report when it is exported from the instrument. They are also included in the EDS file for the calibration and can be viewed if the EDS file is opened in QuantStudio™ Design and Analysis Software v2.

Enter an e-signature in the QuantStudio™ Design and Analysis Software v2

1. In the **Electronic Signature** dialog box, select the meaning from the **Meaning** drop-down list.
2. Enter your SAE user account name and password.

   Note: The SAE user account must have permissions to perform e-signatures.

3. Click **Sign**.

The e-signature record is displayed in the **E-signature** tab (see “View e-signature records in the QuantStudio™ Design and Analysis Software v2” on page 57).

View the audit and e-signature records in the applications

Note: The audit and e-signature records can only be viewed in the real-time PCR applications. They are contained in the template file or the data file. They cannot be viewed in the SAE Administrator Console.

Audit records for actions

The audit records for actions are viewed on the SAE Administrator Console.

For a list of actions that are audited, see “Actions that are audited” on page 44.

For instructions to view the list of actions, see “View the action records audit log” on page 100.

View audit records for objects for the QuantStudio™ Design and Analysis Software v2

The audit records for the object are viewed for each specific object. The plate is the audited object in the QuantStudio™ Design and Analysis Software v2.

Note: The audit record for the object is not viewed on the instrument, even if the change was made on the instrument.

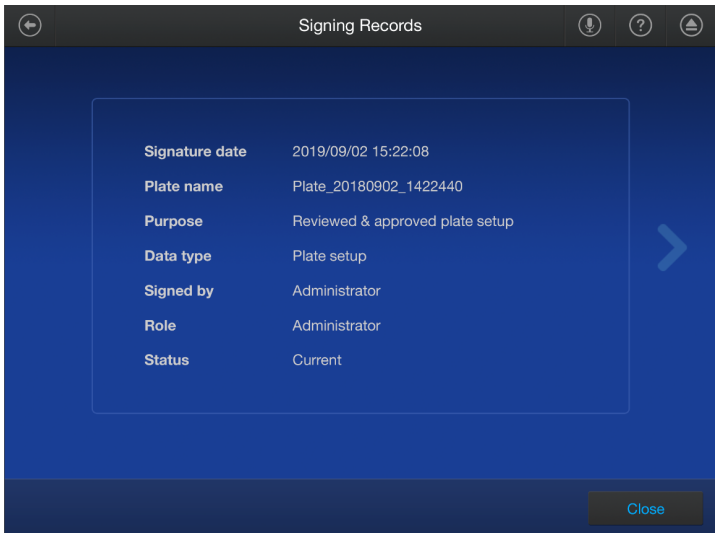
Open the plate file of interest in the software.

1. Navigate to the **Data Audit** tab.
   The audit records are displayed in the **Audit Summary** pane.
2. *(Optional)* Sort by the following parameters:
   - Date
   - User ID
   - Reason

View e-signature records for a plate file on the QuantStudio™ 7 Pro Real-Time PCR Instrument

1. In the home screen, tap one of the following options:
   - **(Load plate file)**
   - **Set up run**
2. Tap the location of the system template or the plate file in the left column.
   - **Run Queue**
   - **Public**
   - **My Instrument**
   - **Network Drive**
   - **USB Drive**
3. Tap the template file name in the right column.
   The **Plate Properties** screen is displayed.
4. In the **Plate Properties** screen, tap **Actions**.
   The **Actions** screen is displayed.
5. Tap **View signing records**.
   The **Signing records** screen is displayed.

6. Tap a row to view the details.



7. Tap **Close** to return to the **Signing records** screen.

View e-signature records in the QuantStudio™ Design and Analysis Software v2

Open the plate file or data file of interest in the software.

Navigate to the **e-Signature** tab.

The e-signatures for the file are displayed.

(Optional) Generate an e-signature report (see “Generate an e-signature report” on page 58).

Generate an e-signature report

View the e-signature records for a plate file or a data file ("View e-signature records in the QuantStudio™ Design and Analysis Software v2" on page 57).

1. Click ··· ▸ **Generate E-signature Report**.
2. *(Optional)* In the **Export E-Sig Report** dialog box, edit the file name.
   The default file name is `Esig_Report_<…>`, where <…> is the date and time stamp.
3. Click **Browse**, then navigate to the location to save the file.
4. Click **Export**.

The e-signature report is saved as a PDF.

SAE error messages and actions

Message	Possible cause	Action
Unable to connect to SAE server.	The SAE server connection settings are incorrect for the QuantStudio™ 7 Pro Real-Time PCR Instrument.	1. In the instrument **Sign In** screen, sign in with a local administrator account. 2. View the settings (see "Enable the SAE functions on the QuantStudio™ 7 Pro Real-Time PCR Instrument" on page 35). 3. Check the SAE server IP address. This is the IP address of the computer that the SAE Administrator Console is installed on. 4. Check the port that is required for your version of the SAE Administrator Console (see "Firewall ports that must be open" on page 16). **Note:** The time difference between the SAE Administrator Console and the instrument must be less than five minutes in order to establish a connection.

(continued)

Message	Possible cause	Action
Unable to connect to SAE server.	The SAE server connection settings are incorrect for the QuantStudio™ Design and Analysis Software v2.	1. Check the SAE server IP address. This is the IP address of the computer that the SAE Administrator Console is installed on. If the SAE Administrator Console and the QuantStudio™ Design and Analysis Software v2 are installed on the same computer, use ***localhost*** as the IP address. 2. Check the port that is required for your version of the SAE Administrator Console (see "Firewall ports that must be open" on page 16). **Note:** If the SAE Administrator Console and the QuantStudio™ Design and Analysis Software v2 are installed on different computers, the time difference between the computers must be less than five minutes in order to establish a connection.
	The option to make the software available to anyone who uses the computer was selected when QuantStudio™ Design and Analysis Software v2 was installed. The computer user enabling SAE settings in the software is a standard Windows™ user and does not have administrator permissions for the computer.	Start QuantStudio™ Design and Analysis Software v2 with the **Run as administrator** option.
	There is a problem with the computer on which the SAE Administrator Console is installed or a problem with the network.	Troubleshoot computer or network problems.
	The computer on which the SAE Administrator Console has a dynamic IP address that is disconnecting the server when the computer is restarted.	Set a static IP address on the computer.

5 Configure the SAE functions for the QuantStudio™ Absolute Q™ Digital PCR Software

Overview of the QuantStudio™ Absolute Q™ Digital PCR Software functionality when SAE functions are enabled

The following features are active when SAE functions are enabled in the QuantStudio™ Absolute Q™ Digital PCR Software.

- Users must sign in with an SAE user account to use QuantStudio™ Absolute Q™ Digital PCR Software.
- Both audit objects and audit actions are tracked in the SAE Administrator Console. Audit actions are tracked automatically, audit objects are viewable when enabled.
- Run setup and software functions for a user are determined by the SAE application profile and user account settings.

Compatibility

QuantStudio™ Absolute Q™ Digital PCR Software v6.1 and later is compatible with SAE Administrator Console v2.2.

SAE functions not supported by the QuantStudio™ Absolute Q™ Digital PCR Software

The following SAE functions are not supported by the QuantStudio™ Absolute Q™ Digital PCR Software.

Function	Option not supported	For more information about a function, see:
System > Other Settings	• Open file from non-SAE system • Client offline sign in • Offline sign in threshold	"Configure account set up and security policies" on page 85.
Audit history	Instrument Run Records	"Types of audit and e-signature history records" on page 99.
e-Signature	• Ability to add e-Signature meanings • Ability to delete e-Signature meanings • Ability to configure actions that require e-Signature • Ability to control/configure e-Signature rights by user role • Ability to control reasons available for e-Signature • Ability to control/configure data to be signed for each e-Signature meaning Signed data in the e-Signature Records PDF report generated by the SAE Administrator Console does not contain any objects. To create a report with this information, print the result report from the QuantStudio™ Absolute Q™ Digital PCR Software. • Ability to control/configure number of signatures (by role) for each action requiring e-Signature	Chapter 9, "Manage the e-signature function".

Enable SAE functions

Workflow

Enable SAE functions

Install the SAE Administrator Console and Absolute Q™ application profile (page 62)

Connect to the SAE server (page 63)

Enable SAE functions in QuantStudio™ Absolute Q™ Digital PCR Software (page 65)

Install the SAE Administrator Console and Absolute Q™ application profile

The following configurations of SAE server and SAE Administrator Console software are supported.

- SAE installed on a stand-alone computer that is connected to the Absolute Q™-dedicated computer and optional Absolute Q™ analysis-dedicated computers

Computer	Function	Software	Provider
SAE stand-alone computer	SAE server	SAE Administrator Console	Customer or Thermo Fisher Scientific
Absolute Q™ dedicated computer	Computer connected to the Absolute Q™ instrument	QuantStudio™ Absolute Q™ Digital PCR Software	Thermo Fisher Scientific
(Optional) Analysis computer(s)	Analyzing digital PCR data	QuantStudio™ Absolute Q™ Digital PCR Software	Customer or Thermo Fisher Scientific

- SAE and Absolute Q™ software that is installed on the Absolute Q™-dedicated computer and is connected to optional Absolute Q™ analysis-dedicated computers

Computer	Function	Software	Provider
Absolute Q™ dedicated computer	SAE server and computer connected to the Absolute Q™ instrument	SAE Administrator Console and QuantStudio™ Absolute Q™ Digital PCR Software	Thermo Fisher Scientific
(Optional) Analysis computer(s)	Analyzing digital PCR data	QuantStudio™ Absolute Q™ Digital PCR Software	Customer or Thermo Fisher Scientific

IMPORTANT! Before installing the application profile, see the release notes for compatibility information to ensure you are installing the Absolute Q™ application profile that is compatible with the version of Absolute Q™ software that you are using.

1. To download the SAE Administrator Console software and Absolute Q™ application profile go to **https://www.thermofisher.com/us/en/home/global/forms/life-science/quantstudio-absolute-q-software.html**.

2. Install the SAE server and SAE Administrator Console software on a computer with a static IP address (*recommended*) or a dynamic IP address.
   a. Unzip the downloaded software.
   b. Double-click **setup.exe**
   c. Follow the **InstallShield Wizard** prompts to install the software.
   d. Select **Typical** as the setup preference, then click **Next**.
   e. Click **Finish**.

   Note: The SAE server and SAE Administrator Console software are installed simultaneously during installation.

3. In the SAE Administrator Console, an SAE administrator must install the application profile for the Absolute Q™ software before SAE can be used.
   The application profile contains default settings for the Absolute Q™ software.
   For information on installing application profiles, see “Install the application profiles” on page 22.

Connect to the SAE server

1. In the QuantStudio™ Absolute Q™ Digital PCR Software, select ⚙ **System ▸ SAE Connection Settings**.

2. Enter the IP address and port number of the SAE Administrator Console.
   If the SAE Administrator Console is installed on the same computer as the QuantStudio™ Absolute Q™ Digital PCR Software, enter ***localhost***.

If the SAE Administrator Console is installed on a different computer from the QuantStudio™ Absolute Q™ Digital PCR Software, enter the IP address of the computer on which the SAE Administrator Console is installed.

Note: If using a dynamic IP address, enter the hostname instead of the IP address to prevent the loss of a connection (see "Determine the hostname" on page 36).

The port number is the firewall port. See "Firewall ports that must be open" on page 16.

3. Click **Test Connection** to confirm that the connection information is correct.
4. Click **Save**.

Determine the hostname

If the SAE Administrator Console is on a separate computer from the application and a dynamic IP address is used, the hostname is recommended instead of the IP address. This helps to prevent the loss of a connection between the SAE Administrator Console and the application

1. In the Windows™ search bar, enter ***cmd*** to open the **Command Prompt**.
2. Enter ***hostname***, then press **Enter**.

The hostname of the computer is displayed in the **Command Prompt**.

Firewall ports that must be open

The following ports must be open for the operating system on the computer that is running the SAE Administrator Console.

SAE Administrator Console version	Port	Condition
v2.0	8201	• Instrument-to-SAE Administrator Console server connection • Computer-to-SAE Administrator Console server connection[1]
v2.1 and later	8443	• Instrument-to-SAE Administrator Console server connection • Computer-to-SAE Administrator Console server connection[1]

[1] If the software is installed on a different computer than the SAE Administrator Console.

Firewall ports

To open a port for Microsoft™ Defender, add inbound rules for the port, and apply to all profiles.

To open a port for Norton Internet Security™, use the **Settings** menu to open the port.

No action is required to open a port for Symantec™ Endpoint Protection.

Enable SAE functions in QuantStudio™ Absolute Q™ Digital PCR Software

This procedure requires an SAE administrator account.

Before you enable SAE functions in the QuantStudio™ Absolute Q™ Digital PCR Software, you must complete the following tasks:

- Connect to the SAE server (see “Connect to the SAE server” on page 63).
- Close all protocol or analyzed run files.

1. In the QuantStudio™ Absolute Q™ Digital PCR Software, select **System** ▸ **Enable Security**.
2. Enter your SAE administrator account user name and password, then click **Sign In**.

The SAE administrator account is automatically signed into the software after SAE functions are enabled. The SAE user name is displayed in the upper-right corner of the software menu bar. All users must sign into the software while SAE functions are enabled.

To sign out of the SAE administrator account in the Absolute Q™ software, see “Sign out of the software using an SAE account” on page 65.

Note: Signing out of the SAE administrator account does not disable SAE functions in the Absolute Q™ software. To disable SAE functions in the Absolute Q™ software, see “Disable SAE functions in QuantStudio™ Absolute Q™ Digital PCR Software” on page 77.

Sign into QuantStudio™ Absolute Q™ Digital PCR Software using an SAE account

Sign in for the QuantStudio™ Absolute Q™ Digital PCR Software is only required if SAE functions are enabled by an SAE administrator (see “Enable SAE functions in QuantStudio™ Absolute Q™ Digital PCR Software” on page 65).

1. In the QuantStudio™ Absolute Q™ Digital PCR Software sign in screen, enter your SAE user name and password.
2. Click **Sign In**.

The user name of the SAE account that is signed in to the software appears in the menu bar.

Sign out of the software using an SAE account

1. In the lower-left corner of the left pane, click .
2. Click **Sign Out**.

Change your SAE account password

Note: External user account (External/Federated LDAP repository accounts) passwords cannot be changed in the QuantStudio™ Absolute Q™ Digital PCR Software, they can only be changed in their respective repository.

1. In the lower-left corner of the left pane, click .
2. Click **Change Password**.
3. Enter the password information, then click **OK**.

Default permissions and roles

The SAE Administrator Console provides the following default permissions and roles. You can use the default roles when you create SAE user accounts or create custom roles in the SAE Administrator Console v2.2 (see “Create a role” on page 81).

- Administrator
- Scientist
- Technician
- Service

IMPORTANT! SAE permissions for a role apply to all user accounts that are assigned to the role.

The roles and associated user-configurable permissions are listed in the following table. You can also double-click the role in the **Roles** tab to display the list of permissions.

Note: The **No Privileges** role is used by the software when you set up user repositories. Do not assign this role to a user account.

Function	Description	Role			
		Administrator	Scientist	Technician	Service
Miscellaneous					
Service access	Access to the instrument service menu.	Yes	No	No	Yes
System settings	Access to the system menu.	Yes	No	No	Yes
Generate report	Create analysis reports.	Yes	Yes	Yes	Yes
E-SIGN run	Place an electronic signature on a run.	Yes	Yes	No	No
E-SIGN study	Place an electronic signature on a study.	Yes	Yes	No	No
Edit notes	Edit notes on plate setup.	Yes	Yes	Yes	Yes

(continued)

Function	Description	Role			
		Administrator	Scientist	Technician	Service
Accept or reject calibration results	Accept or reject the results provided with an instrument calibration.	Yes	No	No	Yes
Presets Management					
Create template	Create a template for a run.	Yes	Yes	Yes	Yes
Import template	Import a template from another system.	Yes	Yes	Yes	Yes
Export template	Export a template to another system.	Yes	Yes	Yes	Yes
Rename template	Rename an existing template.	Yes	Yes	Yes	Yes
Delete template	Delete a template from the system.	Yes	Yes	No	Yes
Save as template	Save a run as a template.	Yes	Yes	Yes	Yes
Create a batch run	Create multiple runs from the same template.	Yes	Yes	Yes	Yes
Edit protocol—templates	Change protocol settings in an existing template.	Yes	Yes	Yes	Yes
Assign samples and groups—templates	Assign samples and groups to wells on the plate in a template.	Yes	Yes	Yes	Yes
Edit groups and dye settings—templates	Modify groups and dye settings in an existing template.	Yes	Yes	Yes	Yes
Edit plate samples and rename samples—templates	Modify samples in an existing template.	Yes	Yes	Yes	Yes
Instrument Control					
Start run	Choose a protocol and start and stop instrument runs.	Yes	Yes	Yes	Yes
Stop run	Stop a run in progress.	Yes	Yes	Yes	Yes
Software or firmware update for instrument	Update the instrument software and firmware.	Yes	No	No	Yes
Pre-Run					
Edit protocol	Change protocol settings on a draft run.	Yes	Yes	Yes	Yes

(continued)

Function	Description	Role			
		Administrator	Scientist	Technician	Service
Assign samples and groups	Assign samples to set groups or load a group set in a run.	Yes	Yes	Yes	Yes
Edit groups and dye settings	Modify groups and dye settings on a draft run.	Yes	Yes	Yes	Yes
Edit plate samples and rename samples	Modify samples on a draft run.	Yes	Yes	Yes	Yes
Run analysis					
Change thresholds	Change channel thresholds in a run.	Yes	Yes	No	Yes
Edit groups and dye settings	Edit group definitions including dye settings in a run.	Yes	Yes	No	Yes
Edit and rename samples	Change sample names in a run.	Yes	Yes	Yes	Yes
Assign samples and groups	Assign samples to set groups or load a group set in a run.	Yes	Yes	Yes	Yes
Omit or include samples	Include or omit samples from an analysis in a run.	Yes	Yes	No	Yes
Run management					
Delete run	Delete a run from the database.	Yes	No	No	Yes
Import run	Import runs to and from ZST or ZIP files.	Yes	Yes	Yes	Yes
Export run	Export runs to and from ZST files.	Yes	Yes	Yes	Yes
Rename run	Change the name of the run.	Yes	Yes	Yes	Yes
Study Analysis					
Change thresholds	Change sample and group thresholds during study analysis.	Yes	Yes	No	Yes
Edit groups	Edit groups contained in a study.	Yes	Yes	No	Yes
Edit plate samples and rename samples	Edit and rename samples in a study.	Yes	Yes	Yes	Yes
Omit or include samples	Include or omit samples from a study.	Yes	Yes	No	Yes
Create a study and add runs to a study	Create and add runs to studies.	Yes	Yes	Yes	Yes

(continued)

Function	Description	Role			
		Administrator	Scientist	Technician	Service
Study Management					
Import study	Import studies from other systems.	Yes	Yes	Yes	Yes
Export study	Export studies to ZIP files.	Yes	Yes	Yes	Yes
Rename study	Change the name of a study.	Yes	Yes	No	Yes
Delete study	Delete a study.	Yes	Yes	No	Yes

Use audit functions

The following sections provide information on using SAE auditing functions.

Specify audit reason

Depending on how the audit settings are configured in the SAE Administrator Console, the **Enter Audit Reason** screen may appear when you make changes to a protocol or an analyzed run in the QuantStudio™ Absolute Q™ Digital PCR Software to prompt you to select an audit reason from the drop down list, or add a custom reason.

Note: **Custom Reason** is not displayed if audit settings are configured to require users to select a reason.

For more information on configuring audit settings, see “Set the audit mode” on page 89.

View audit records

For instructions to view audit action records, see “View the action records audit log” on page 100.

For a list of actions that are audited, see “Actions that are audited” on page 70.

For instructions to view audit object records of a specific run, see “View audit object records” on page 69.

View audit object records

Use the following steps to view the audit object record of a specific run by using the Run ID for the run.

1. In the QuantStudio™ Absolute Q™ Digital PCR Software, select the desired run.
2. In the upper-left corner of the run page, click next to the **Run ID** to copy the **Run ID** to the clipboard.
3. At the SAE Administrator Console perform the following steps.
   a. Select **Audit History > Application Object Records.**

b. Select **Enable Application Objects Filtering**.

c. In the **Object name** field, paste the **Run ID** that you copied in step 2.

d. Click **Search**.

The information regarding the run appears in results area of the **Audit History** screen.

Note: For assistance in interpreting audit history data, contact Technical Support.

Actions that are audited

The actions are audited and listed in the action records regardless of whether audits are enabled or disabled.

The following user actions are audited.

Function	Actions audited
Miscellaneous	• EULA accept or decline • Sign in • Sign out • Save system settings • Update instrument software/firmware version • Open and/or close instrument door (exact action with user name)
Templates	• Create, edit, or save a template • Save as template (when creating/editing a template) • Import or export protocol (when creating/editing a template) • Create a sample group (when creating/editing a template) • Edit dyes (when creating/editing a template) • Change optical settings (when creating/editing a template) • Add, edit, or delete notes in setup • Import template or templates • Export template or templates • Rename template • Delete template or templates • Generate batch runs

(continued)

Function	Actions audited
Runs	• Create, edit, and save a run • Save a run as a template (when creating/editing a run and viewing a completed run) • Import protocol (when creating/editing a run) • Export protocol (when creating/editing a run) • Update sample group assignment • Edit dyes (when creating/editing a run) • Add, edit, or delete notes in setup • Import run or runs • Export run or runs • Rename run • Delete run or runs • Start or stop run on the instrument • Start or stop a calibration run • Add a run or runs to a study
Runs—changes during analysis	• Update sample group assignment • Create or delete a sample group • Export protocol • Edit dyes • Add, edit, or delete notes in setup • Change threshold (both group threshold and threshold for a dye channel) • Omit sample • Pin or unpin threshold • Generate a report for a run • Download data for a run • Accept or reject calibration results • Generate a report for calibration run
Studies	• Create a study • Import study or studies • Export study or studies • Rename study • Delete study or studies • Add a run or runs to a study

(continued)

Function	Actions audited
Studies—changes during analysis	• Update sample group assignment • Create or delete a sample group • Export Protocol • Edit Dyes • Add, edit, or delete Notes in Setup • Change threshold (both group threshold and threshold for a dye channel) • Omit sample • Pin or unpin threshold • Generate a report for a run • Download data for a run • Accept or reject calibration results • Generate a report for calibration run

Export audit records

For information on exporting audit records for a protocol or an analyzed run, see “Export archived audit records” on page 104.

Sign data in the software

An e-signature can optionally be added for plate setup and run results on the **Runs** and **Studies** pages.

1. Chose from the following options to provide an e-signature for plate setup and run results.

Option	Actions
Runs page, **DRAFT**—Signing for plate protocol and setup.	1. From the left pane select to open the **Runs** list page. 2. Use the search field to find a run or select a run from the list.
Runs page, **COMPLETED**—Signing for protocol, setup, and results of the run.	1. From the left pane select to open the **Runs** list page. 2. Select the **COMPLETED** tab. 3. Use the search field to find a run or select a run from the list.
Studies page—Signing for protocol, setup, and results of the study.	1. From the left pane select to open the **Studies** list page. 2. Use the search field to find a study or select a study from the list.

2. Select **E-SIGN**, then select one of the following options from the dropdown list to indicate the meaning of the e-signature.
   - Reviewed & approved setup
   - Reviewed & approved results

3. Enter your user name and password.
4. Click **E-SIGN**.

If a run is signed and unmodified, the signature appears on reports that are created using **GENERATE REPORT**.

For information on how to view e-signature data, see Chapter 10, “View and report audit and e-signature records”.

View and review e-Signatures

For information on how to view e-Signature data, see Chapter 10, “View and report audit and e-signature records”.

The sections that follow provide detailed information for reviewing e-Signature data.

- For information on plate setup e-Signature data, see “Review plate setup e-Signature information” on page 73.
- For information on plate results e-Signature data, see “Review plate results e-Signature information” on page 75.

Review plate setup e-Signature information

The sections that follow provide descriptions of the information provided in the e-Signature plate setup record for draft runs and run templates. Optionally, this information can be printed.

Signature metadata

This section provides information regarding the signature metadata for each e-Signature plate setup record.

Table 1 Signature metadata

Object	Description
Meaning	The e-Signature option selected.
Signed Date	The date of e-Signature.
Signed By	The name of user.
Host ID	The instrument name.
Full Name	The user name.
Status	The status of the signature: • CURRENT: Valid • OBSOLETE: Invalid
Role	The role assigned to the user who performed the run.

Protocol information

This section provides information regarding the **protocol** section of the e-Signature plate setup record.

Table 2 Protocol details

Object	Description
ScanRed	Status of **True** indicates this optical channel was enabled. Status of **False** indicates this optical channel has been disabled.
ScanGreen	Status of **True** indicates this optical channel was enabled. Status of **False** indicates this optical channel has been disabled.
ScanYellow	Status of **True** indicates this optical channel was enabled. Status of **False** indicates this optical channel has been disabled.
ScanDarkRed	Status of **True** indicates this optical channel was enabled. Status of **False** indicates this optical channel has been disabled.
RNAStep_Duration	The duration of RNA-RT step *(optional)*.
RNAStep_Temperature	The temperature of RNA-RT step *(optional)*.
PCRPreheat_Duration	The duration of pre-heat step *(optional)*.
PCRPreheat_Temperature	The temperature of pre-heat step *(optional)*.
PCR_Stage(1/2)_Step(1/2/3)_Duration	The duration of indicated stage and step.
PCR_Stage(1/2)_Step(1/2/3)_Temperature	The temperature of indicated stage and step.
Name	The name of protocol.

Plate channel information for each sample

This section provides information regarding the channels used in the **plate** section of the e-Signature plate setup record. If the channel was not used, the detail will reflect **None** in all data points. The figure that follows depicts a partial record.

Table 3 For each color — blue, green, yellow, red, and dark red

Object	Description
Channel	The name of the target.
Type	The analysis type selected.
Threshold	The predefined analysis threshold.
Selection	The dye selected for the channel.

Additional plate information

This section provides information regarding the additional information provided in the **plate** section of the e-Signature plate setup record.

Table 4 Other plate information

Object	Description
DilutionFactor	Total dilution from sample to reaction mix.
CNVRefNum	The number of copies of the reference genome.
Name	The sample name.
Group	The group name.
GroupType	the group analysis setting

Run metadata

The section provides information regarding the **run name** section of the e-Signature plate setup record.

Table 5 Run metadata

Object	Description
run name	The name given to the run at the instrument.
Columns	Columns enabled for the run.
LastEditedEPOCH	Epoch time stamp of the run.
Barcode	Plate barcode number.

Review plate results e-Signature information

The sections that follow provide descriptions of the information provided in the e-Signature plate results record for completed runs and studies. Optionally, this information can be printed.

Signature metadata

This section provides information regarding the signature metadata for each e-Signature plate results record.

Table 6 Signature metadata

Object	Description
Meaning	E-Signature option selected.
Signed Date	Date of e-Signature.
Signed By	Name of user.
Host ID	Instrument name.

Table 6 Signature metadata *(continued)*

Object	Description
Status	Status of the signature: • CURRENT: Valid • OBSOLETE: Invalid

Results by group

This section provides information regarding the **groups** section of the e-Signature plate results record. A column is included for each dye used.

Table 7 For each group, for each dye

Object	Description
Total	One of the following options: • If replicates, this is the group average of microchambers. • If pooled, this is the total pooled microchambers.
Positive	Group positive microchambers.
Conc.(cp./uL)	Group concentration in copies per microliter.

Results for samples

This section provides information regarding the **samples** section of the e-Signature plate results record. A column is included for each dye used.

Table 8 For each sample, for each dye

Object	Description
Total	Sample total microchambers.
Positive	Sample positive microchambers.
PosThresh	Analysis threshold input by user.

Run metadata

The section provides information regarding the **run name** section of the e-Signature plates result record.

Table 9 Run metadata

Object	Description
run name	The name given to the run at the instrument.
Columns	Columns enabled for run.
LastEditedEPOCH	Epoch time stamp of the run.
Barcode	Plate barcode number.

Disable SAE functions in QuantStudio™ Absolute Q™ Digital PCR Software

This procedure requires an SAE administrator account.

IMPORTANT! Disable SAE functions in the QuantStudio™ Absolute Q™ Digital PCR Software before uninstalling the SAE Administrator Console.

Close all plate files and data files.

1. In QuantStudio™ Absolute Q™ Digital PCR Software, select ⚙ **System** ▸ **Disable Security**.
2. Enter the password of the SAE administrator account, then click **Sign In**.

6 Manage SAE user accounts and roles

Change your SAE user account password

The following instructions are to change the password to log in to the SAE Administrator Console.

The password to log in to an application is changed in the application by the user. See the chapter for the application.

To change a password to log in to an application for a user, see “Reset an SAE user account password” on page 81.

1. At the top right of any screen, click , then select **Change Password**.
2. Enter the old password.
3. Enter a new password, confirm the new password, then click **Update**.

Create an SAE user account

Note: For information on advanced configuration options for user repositories, see “Configure user repositories” on page 111.

1. In the SAE Administrator Console main screen, click the **Users** tab.
2. Click **Create**.

3. In the **Create User Account** dialog box, enter the following information:
   - User name
   - Password
   - First name
   - Middle initial (MI; optional)
   - Last name
   - Phone number (optional)
   - Email address (optional)
   - Comments (optional)

   The field limits are specified in the system security function settings.
   The phone number and email address are for information only.

   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 signed-in user.
   - You cannot change the user name after you save the user account.

   ---

4. Select **User must set new password at next sign in** to require the user to specify a new password the first time they sign in to an application.

   Note: The user account password automatically expires after the number of days that are specified in the system security function settings.

   ---

5. Select the **Role** for the user account.

   Note:
   - Each role grants specific permissions to the user.
   - The **No Privileges Role** is for internal use by the SAE Administrator Console. Do not assign this role to a user account.
   - For the default roles that are provided with the software, see the chapter for the application.

   ---

6. In the **Status** drop-down list, leave the status set to **Active**.
7. Click **Save**.

Edit an SAE user account

1. In the main screen, click the **Users** tab.
2. Select a user account, then click **Edit**.

3. Edit the settings as desired.

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

4. Click **Save**.

Inactivate an SAE user account

1. In the main screen, click the **Users** tab.
2. Select a user account, then click **Edit**.
3. In the **Edit User Account** dialog box, change the status in the **Status** drop-down list to **Inactive**.

   Note: The status of **Suspended** is an option in the **Status** drop-down list. This status is used by the software if the user has reached the number of sign-in attempts defined in the account lockout policy. For more information, see “Configure account set up and security policies” on page 85.

4. Click **Save**.

Activate a suspended or inactive SAE user account

An inactive or suspended SAE user account can be activated.

An SAE user account is set to be inactive by an administrator.

The suspended status is used by the software if the user has reached the number of sign-in attempts defined in the account lockout policy. For more information, see “Configure account set up and security policies” on page 85.

1. In the main screen, click the **Users** tab.
2. Select a user account, then click **Edit**.
3. In the **Edit User Account** dialog box, change the status in the **Status** drop-down list to **Active**.
4. Click **Save**.

Reset an SAE user account password

IMPORTANT! There is no way to recover a forgotten password. If the SAE Administrator forgets their password, the software must be reinstalled. Export all data before reinstalling the software. Otherwise, the data will be lost. For more information, see Chapter 12, “Advanced configuration options”.

1. In the main screen, click the **Users** tab.
2. Select the affected user account, then click **Edit**.
3. Enter a replacement password for the user account, then re-enter the password for confirmation.
4. If you assigned the user account a temporary password, then select **User must set new password at next sign in** to require the user to enter a new password at sign in.
5. Click **Save**.

Manage roles

SAE roles determine the SAE permissions that are associated with an SAE user account.

If your SAE Administrator Console is configured to manage the SAE settings for more than one application, you can create roles that specify permissions for more than one application.

For a list of permissions for a specific application, see the chapter for the application.

IMPORTANT! SAE permissions for a role apply to all user accounts that are assigned to the role.

Create a role

1. In the main screen, click the **Roles** tab.
2. Click **Create**.
3. Enter a name for the role.
4. *(Optional)* Enter a description.
5. Select SAE permissions for the role.
   - The permissions are organized by the application. Select the checkbox next to the application to select all of the permissions for the application.
   - Select the checkbox next to the category to select all SAE permissions in a category.
   - Expand the category to select individual permissions within the category.
6. Click **Save**.

New roles are available for selection when you create or edit a user account, and when you specify e-signature settings.

Edit a role

1. In the main screen, click the **Roles** tab.
2. Select a role, then click **Edit**.

   Note: You cannot edit the Administrator role or No Privileges role.

3. Edit the settings as needed, then click **Save**.

Delete a role

Default roles and custom roles can both be deleted.

Note: If any SAE user account is assigned to a role, that role cannot be deleted.

1. In the main screen, click the **Roles** tab.
2. Select a role, then click **Delete**.
3. In the **Role Deletion** dialog box, click **Delete** to confirm deletion of the role.

View or print a user report

The user report is a PDF. The report contains the following information:

- User type
  For more information about the user type, see “User repository overview” on page 111.
- Full name
- User name
- Role
- Status
- Password pre-expired
  If the user must set a new password the next time they sign in to an application, this value is set to **Yes** (see “Create an SAE user account” on page 78).
- Date created
- Created by
- Date last modified
- Last modified by
- Email
- Phone
- Password last modified
- Comments

1. In the main screen, click the **Users** tab.
2. Click **Report**.
   The user report downloads to the default location set in the web browser.
3. Access the report, save, then print the report.
4. Close the report.

View or print a role report

The role report is a PDF. The report contains the following information:

- Role
- Description
- Number of privileges
- Number of users associated with the role
- Date created
- Created by
- Date last modified
- Last modified by

1. In the main screen, click the **Roles** tab.
2. Click **Report**.
   The role report downloads to the default location set in the web browser.
3. Access the report, save, then print the report.
4. Close the report.

7 Manage the system security function

Overview of the system security settings

The **System** tab contains the settings for the following items:

- User name and password restrictions that apply when you create user accounts. See Chapter 6, “Manage SAE user accounts and roles”.
- Lockout settings (how the software responds when a user tries to sign in multiple times with an incorrect password)
- Other settings such as automatic screen locking and report size

Functions that are controlled in the SAE Administrator Console

Only SAE user accounts with an Administrator role can sign in to the SAE Administrator Console. The Administrator role includes the following functions in the SAE Administrator Console:

- Configure security and auditing
- View action records
- View system configuration records
- View application object records
- View instrument run records

For functions that are controlled in each application, see the chapter for your application.

Enable or disable the system security function

The system security function cannot be enabled and disabled in the SAE Administrator Console. This is performed in the application.

For instructions on how to enable or disable the SAE in an application, see the chapter for the application.

Configure account set up and security policies

Settings in this screen affect all SAE user accounts. Settings are applied the next time that users sign in to an application.

1. In the SAE Administrator Console main screen, click the **System** tab.
2. In the **User Name Settings** pane, specify the minimum length and maximum length for the user names.
3. In the **Password Policy** pane, specify the password requirements.

   The following items are specified:

   - Minimum and maximum length
   - Password reuse
   - Complexity
   - Minimum and maximum age
   - Expiry reminder and length of time before the expiry that the reminder is sent
   - User name check (cannot use a variation of the user name as the password, SAE Administrator Console v2.2 and later only)
   - Check of compromised phrases (SAE Administrator Console v2.2 and later only)
4. *(Optional)* In the **Account Lockout Policy** pane, enable or disable the **Account lockout** feature. If you enable this feature, specify the following settings:

Settings	Description
Threshold and **Account lockout duration**	If a user attempts to sign in with an incorrect user name or password more than the number of times set for the threshold, the user is locked out for the time specified.
Sign in attempts counter reset and **Reset failure sign in counter after**	If the counter reset is enabled, the counter for the number of failed sign-in resets to 0 after the time specified. This setting applies before an account lockout occurs. For example, the threshold is set to 5 sign-in attempts and the counter reset is set to 15 minutes. If the user attempts to sign in with an incorrect user name or password 4 times, then waits for the specified time (15 minutes in this example), the number of failed sign-ins is reset to 0. The account lockout does not occur.

5. *(Optional)* In the **Other Settings** pane, specify the following settings:

Settings	Description when enabled
Automatic screen locking and **Inactivity duration**	The screen is locked if there is no activity for the time specified. A user must enter their user name and password to unlock the screen.
Open file from non-SAE system	The application allows users to access data files that were generated when SAE functions were disabled.
Client offline sign in[1] and **Offline sign in threshold**	When the SAE server is offline, users can sign in and use an application for the time specified.
Report page size	The size of the page when a report is generated by the SAE Administrator Console (SAE Administrator Console v2.1 and later only).

[1] If this setting is not displayed under **Other Settings**, this function is not available for your application.

6. Click **Apply Settings**.

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

8 Manage the audit function

Overview of the audit settings and functions

Use the **Audit** tab to control the following items:

- The objects that are audited
- The list of reasons that are available to users when the audit mode is set to **Optional** or **Required**

Objects can be audited silently, or be set to allow or to require an audit reason.

Note: When the **Audit mode** is set to **Silent**, audit reasons are not available for user selection in an application.

IMPORTANT! Objects and events are audited. The following items apply to auditing of objects:

- Auditing can be enabled or disabled
- The audit mode can be set
- A list of reasons is available to users when the audit mode is set to **Optional** or **Required**

The audit records for objects are viewed in the application or in the SAE Administrator Console. Actions are audited. Auditing of actions cannot be disabled. There is no audit mode or list of reasons available to users. The audit records for the actions are viewed in the SAE Administrator Console.

Auditing of objects is enabled and disabled for all of the applications that are connected to the instance of the SAE Administrator Console.

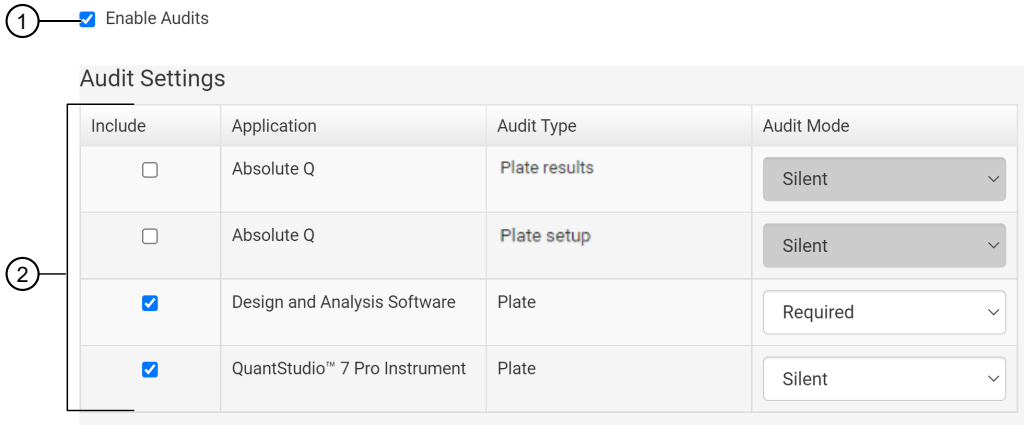
For a list of actions and objects that are audited for your application, see the chapter for your application.

Enable or disable the audit function

Enabling and disabling the audit function applies to objects. Actions continue to be audited even if audits have been disabled.

1. In the SAE Administrator Console main screen, click the **Audit** tab.
2. Select or deselect the **Enable Audits** checkbox.

   Enabling and disabling the audit function with the **Enable Audits** checkbox applies to all of the combinations of applications and audit types.
3. *(Optional)* To enable or disable the audit function for a specific combination of application and audit type, select the **Enable Audits** checkbox, then select or deselect the checkbox that applies to the individual application and audit type.



① **Enable Audits** checkbox
② Checkboxes for the individual combinations of applications and audit types

4. Click **Apply Settings**.

- Set the audit mode (see “Set the audit mode” on page 89).
- Configure the audit reason settings (see “Configure the audit reason settings” on page 89).

Set the audit mode

For the objects that can be audited, see the chapter for the application.

Enable the audit function and ensure that the combination of the application and audit type is selected (see “Enable or disable the audit function” on page 88).

1. 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 continue without entering a reason.
Required	The event is audited, a reason prompt is displayed, and the user must specify a reason.

2. Click **Apply Settings**.

Configure the audit reason settings

If multiple applications are configured for the same instance of the SAE Administrator Console, the reason is edited for all of the applications.

- *(Optional)* Select the **Require users to select a reason for change from list** checkbox to require users to select a pre-defined audit reason from the **Reason** list.

  If this option is not selected, the user can enter a custom reason.

  If the audit mode is set to **Silent**, this setting does not apply.

- Add a new audit reason.
  a. Click **New Reason**.
  b. Enter a reason for change, then click **Save**.
  c. Click **Apply Settings**.

- Edit an existing audit reason.
  a. Click **Edit**.
  b. Edit the reason for change, then click **Save**.
  c. Click **Apply Settings**.

- Delete an existing audit reason.
  a. Click **Delete**.
  b. Click **Delete** to confirm deletion of the audit reason or **Cancel** to exit the dialog box.
  c. Click **Apply Settings**.

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

Auditable actions in the SAE Administrator Console

The records for these actions are located in the **Action Records** or **System Configuration** audit history.

- Sign in to or out of the SAE Administrator Console
- Enable or disable the SAE functions in the application
- Import or export an SAE configuration
- Install an application profile
- Archive or restore audit records
- Manually synchronize with LDAP Directory
- Edit user accounts
- Add, edit, or delete roles
- Edit the audit configuration

9 Manage the e-signature function

Overview of the e-signature settings

Use the **e-Signature** tab to control the following items:

- Actions that require an e-signature check
- Number of e-signatures required for each action
- List of reasons that are available to users when they sign objects in the application

By default, the e-signature function is not enabled, no actions are selected, and no e-signatures are required.

E-signatures are enabled and disabled for all of the applications that are connected to the instance of the SAE Administrator Console.

How the e-signature function works in the application

When the e-signature function is enabled and configured in the SAE Administrator Console, the following steps occur in the application:

- A user with e-signature permission signs in to the application.
- The user performs an action that is configured to require an e-signature.
  The user can also proactively provide an e-signature before the action is performed.
- The software checks the e-signatures associated with the action.
- If an e-signature is required and it has not yet been signed, or does not have the required number of e-signatures, the user is prompted to sign the required object before the action can continue.

- The user selects an e-signature meaning, then enters user name and password.
- When the e-signature requirements are met for the action, the action continues.

For actions that require e-signatures for your application, see the chapter for your application.

Parts of the e-Signature tab

Note: The screens shown in this section are for the real-time PCR application profile and the digital PCR application profile. This example screen is provided to illustrate the parts of the screen. The specific information in each section might be different, depending on which configuration is selected and which application profiles are installed.

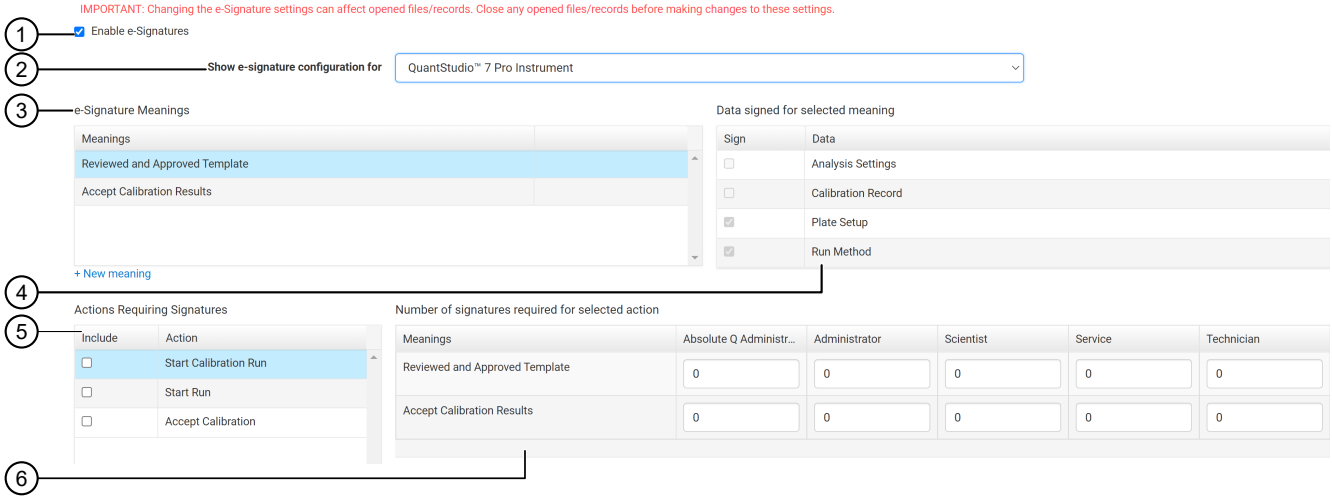


Figure 5 Parts of the e-Signature tab

1. Enable disable the e-signature function
2. The application that the e-signature is being configured for (dropdown list)
3. E-signature meanings that can be applied when the object is signed
4. Objects that can be signed (**Data signed for selected meaning**)
5. Actions that require an e-signature
6. Number of e-signatures required for each action

Enable or disable the e-signature function

This section of the screen allows you to enable or disable the e-signature function. Enabling or disabling the e-signature function applies to all of the applications that are connected to the instance of the SAE Administrator Console.

See Figure 5 on page 92.

E-signature meanings and data signed for a meaning

Note: Ensure that the application that you would like to view and edit is selected in the **Show e-signature configuration for** drop-down list. The values can be different for each application.

See “Enable or disable the e-signature function” on page 92.

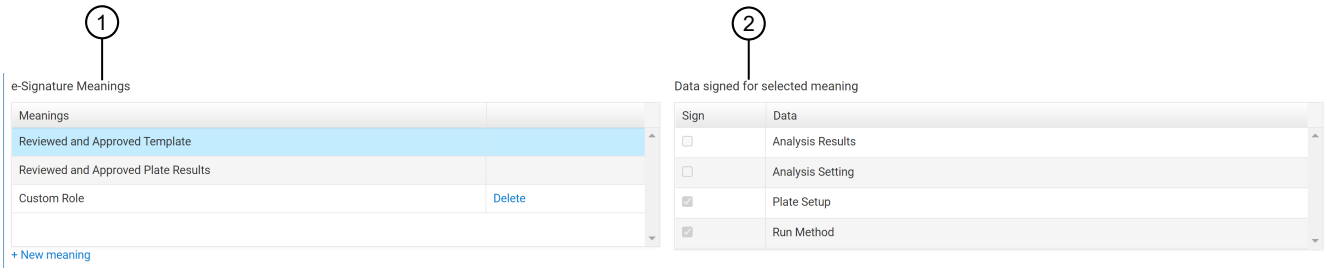


Figure 6 E-signature meanings and data signed for a meaning

(1) E-signature meanings
(2) Data signed for a selected meaning

This section of the screen displays the e-signature meanings and the data that are signed for a selected meaning. Each meaning is linked to specific data that are signed.

The figure above displays the default e-signature meanings and data signed settings for the QuantStudio™ Design and Analysis Software v2. A plate setup and a run method are signed with the meaning of **Reviewed and Approved Template**. The analysis results and analysis settings are not applicable to the template, so they cannot be selected to be signed under the meaning of **Reviewed and Approved Template**.

The e-signature meaning is the value that the user selects when providing an e-signature in the application.

The data signed indicates the items that are associated with an e-signature.

Click a specific e-signature meaning to see the data that are signed for the e-signature meaning. The e-signature meaning is highlighted in blue. The title above the list of data that are signed is updated to display the selected e-signature meaning.

The default e-signature meanings cannot be edited. The data signed associated with each default e-signature meaning cannot be edited.

E-signature meanings can be added. The data signed can be selected for a new e-signature meaning. Items cannot be added to the list of data that are signed. For more information, see “(Optional) Add an e-signature meaning” on page 96.

Note: For the default meanings that are provided with the application profile, the **Sign** checkboxes on the right of the screen are read-only. If you click a checkbox when a default meaning is selected, the ⃠ icon is displayed. Select a default meaning on the left of the screen to see which object is linked to the selected meaning.

Actions that require an e-signature

This section of the screen allows you to select one or more actions that require e-signatures.

For the actions that can be selected for each application profile, see "Actions and objects that require e-signature" in the chapter for the application.

Note: The order of the actions in the **Actions Requiring Signatures** list is not sequential.

The figure below is an example. It shows the actions that can be selected to require e-signatures for the QuantStudio™ 7 Pro Real-Time PCR Instrument.

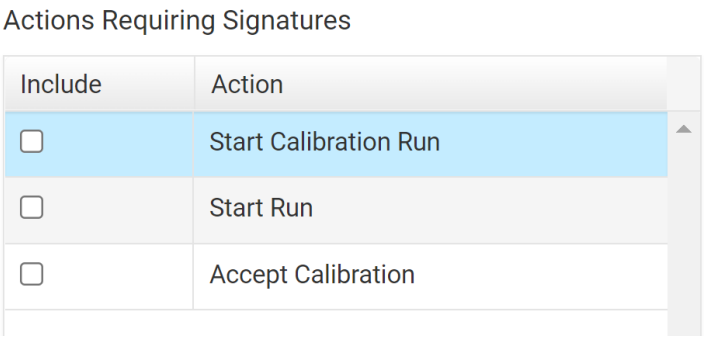


Figure 7 Actions that require e-signatures

Number of e-signatures required for the selected action

This section of the screen allows you to specify the number of e-signatures required from each role and for each meaning for each selected action.

The number of e-signatures applies to the action that is highlighted in blue. The title above the number of e-signatures is updated to display the selected action.

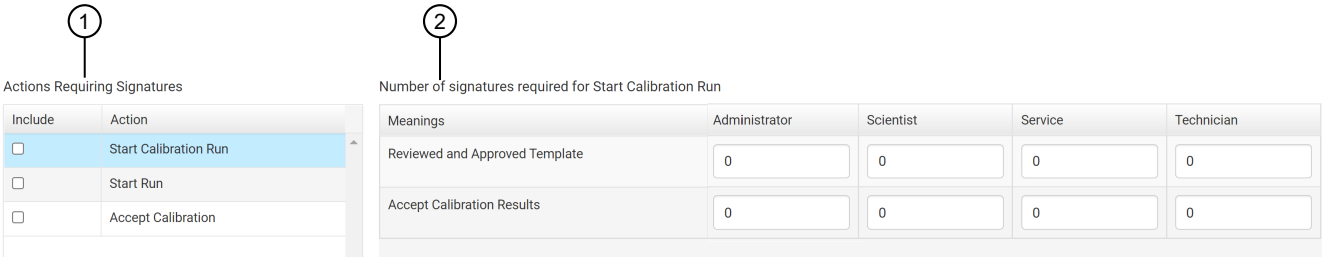


Figure 8 Number of e-signatures required for the selected action

① Actions that require e-signatures
② Number of signatures from each role and for each meaning for the selected action

The left side of the screen lists the actions that can be selected. You cannot add actions to this list. Some applications have only one action. Some applications have multiple actions.

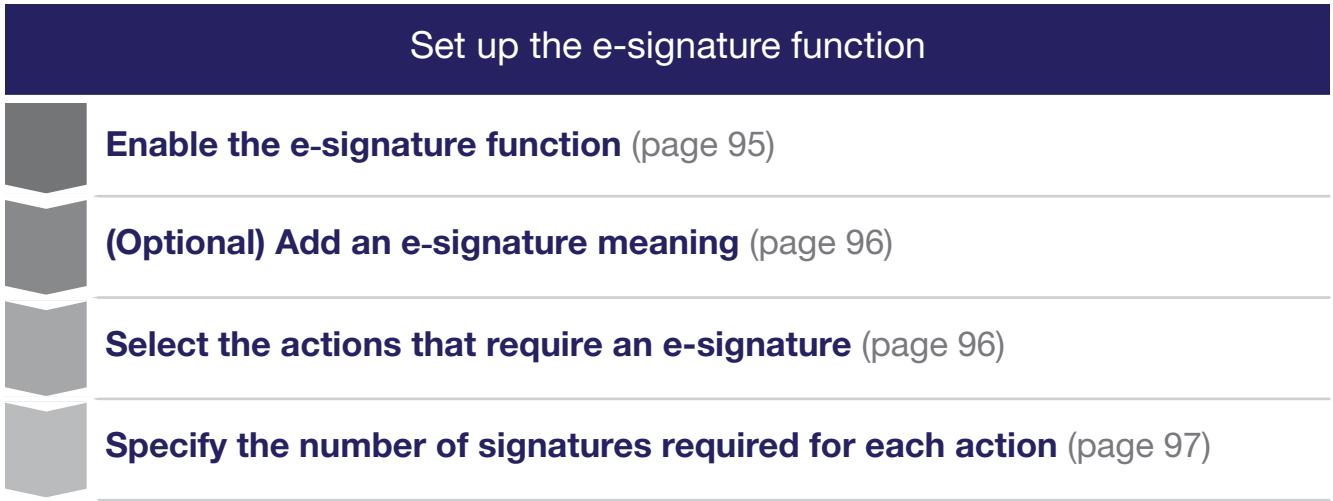
The right side of the screen lists the following information:

- All of the meanings from **e-Signature Meanings** (see "E-signature meanings and data signed for a meaning" on page 92). You can add to this list indirectly by adding to the list of meanings (see "(Optional) Add an e-signature meaning" on page 96).
- All of the roles that are defined in the SAE Administrator Console.

IMPORTANT! Roles are listed regardless of whether they have the e-signature permission enabled. Before specifying a number of signatures for a role, ensure that the role has the e-signature permission enabled.

Workflow to set up the e-signature function

To enable e-signature functions in an application, you must perform three of the four steps in the following workflow diagram. You can optionally perform one of the steps.



Enable the e-signature function

The e-signatures are enabled for all of the applications that are connected to the instance of the SAE Administrator Console.

1. In the SAE Administrator Console main screen, click the **E-signature** tab.
2. Select the **Enable e-signatures** checkbox.
3. *(Optional)* Click **Apply Settings** if no other edits are made.

Use the **Show e-signature configuration for** drop-down list to view the e-signature configuration for each application.

Proceed to one of the following sections:

- "(Optional) Add an e-signature meaning" on page 96
- "Select the actions that require an e-signature" on page 96

(Optional) Add an e-signature meaning

For a description of the e-signature meanings and data that are signed, see "E-signature meanings and data signed for a meaning" on page 92.

Note: The default e-signature meanings for an application cannot be edited. The links to the data that are signed for the default e-signature meanings cannot be edited.

Perform this procedure to add custom e-signature meanings that are available in the application.

Enable the e-signature function ("Enable the e-signature function" on page 95).

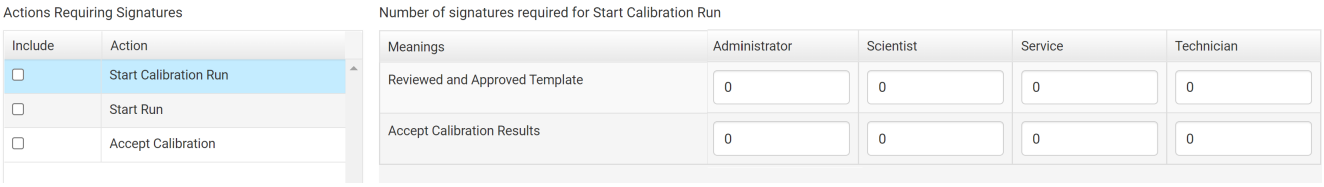
1. In the **e-signature Meanings** pane, click **New meaning**.
2. In the **Create New Meaning** dialog box, enter a name in the **New e-signature meaning** field, then click **Save**.
   The new meaning is listed in the **e-Signature Meanings** pane.
3. Select the new meaning.
   The selected meaning is highlighted in blue.
4. In the **Data signed for <…>** pane, where <…> is the meaning, select the items to be associated with the meaning.
5. *(Optional)* Click **Apply Settings** if no other edits are made.

Select the actions that require an e-signature (see "Select the actions that require an e-signature" on page 96).

Select the actions that require an e-signature

Select the actions that require an e-signature in the application.

1. In the **Actions Requiring Signatures** pane, use the checkboxes select one or more actions that require an e-signature.
   For the actions that can be selected for each application profile, see "Actions and objects that require e-signature" in the chapter for the application.



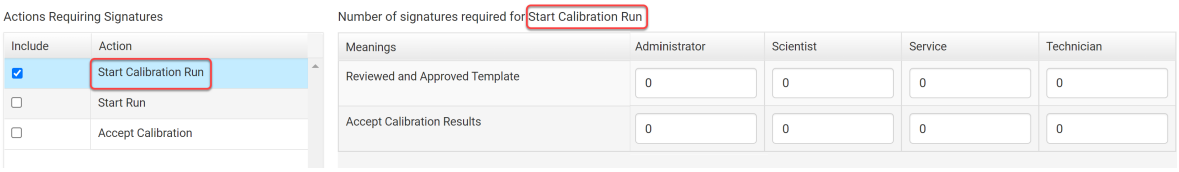
2. *(Optional)* Click **Apply Settings** if no other edits are made.

Specify the number of e-signatures required from each role for an action (see “Specify the number of signatures required for each action” on page 97).

Specify the number of signatures required for each action

1. In the **Actions Requiring Signatures** pane, select an action that requires an e-signature.

   When an action is selected for signatures in the left pane, it is highlighted in blue and the name of the action is displayed above the signature table.



2. For each selected action, enter the number of e-signatures that are required from each role and for each meaning before the associated action can be performed.

   If you specify signatures for an action that is not enabled for e-signature (the checkbox is not enabled), the action does not require an e-signature.

   IMPORTANT! Roles are listed regardless of whether they have the e-signature permission enabled. Before specifying a number of signatures for a role, ensure that the role has the e-signature permission enabled.

3. Click **Apply Settings**.

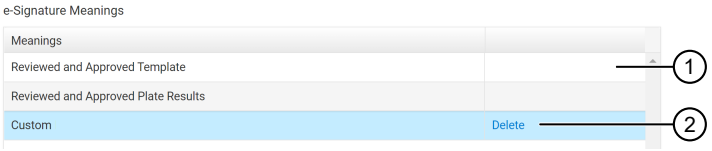
Delete an e-signature meaning

Default e-signature meanings for the application cannot be deleted. Only e-signature meanings that were added can be deleted.

1. In the SAE Administrator Console main screen, click the **E-signature** tab.

2. In the **e-signature Meanings** pane, click **Delete** for the e-signature meaning.

   The **Delete** button is only displayed for the e-signature meanings that can be deleted. The default e-signature meanings for an application cannot be deleted.



① Default e-signature meanings, cannot be deleted
② E-signature meaning that was added, can be deleted

3. Confirm the deletion of the meaning, then click **OK**.
4. Click **Apply Settings**.

Disable the e-signature function

If the e-signature function is disabled, it is disabled for all of the applications that are connected to the instance of the SAE Administrator Console.

1. In the SAE Administrator Console main screen, click the **E-signature** tab.
2. Deselect the **Enable e-signatures** checkbox.
3. Click **Apply Settings**.

10 View and report audit and e-signature records

Types of audit and e-signature history records

The following records are available. Only roles with the appropriate permissions can view the records.

Record type	Description	Contents
Action records	Actions that are set to be audited	Audit records
System configuration	Changes that are made to security, audit, and e-signature settings	Audit records
Application object records	Objects that are set to be audited	Audit and e-signature records
Instrument run records	A summary of the run, objects that have been audited, actions that have been audited, data audits (Information about changes made during a run), and run completion information	Audit records

View the action records audit log

All items in the action records log are audited silently.

For a list of auditable actions in the SAE Administrator Console, see “Auditable actions in the SAE Administrator Console” on page 90.

For a list of auditable actions in a specific application, see the chapter for your application.

1. In the SAE Administrator Console main screen, click **Audit History** ▸ **Action Records**.
2. At the top left of the screen, select the **Enable Action Records Filtering** checkbox.
3. Use one or more of the following filtering tools.
   - **Date Range**
   - **Application** drop-down list
   - **Instrument** drop-down list
   - **User Account** drop-down list

   The **Action** field cannot be edited.
4. Click **Search**.
   The actions that meet the criteria set in step 3 are displayed.
5. *(Optional)* Click **Report** to create a PDF output of the action records.

View the System Configuration audit log

The **System Configuration** audit history contains the audit records for actions performed in the SAE Administrator Console.

1. In the SAE Administrator Console main screen, click **Audit History** ▸ **System Configuration**.
2. At the top left of the screen, select the **Enable System Configuration Records Filtering** checkbox.
3. Use one or more of the following filtering tools.
   - **Date Range**
   - **Action** drop-down list
   - **Record Name**
   - **User Account** drop-down list
   - **Record Type** drop-down list
4. Click **Search**.
   The actions that meet the criteria set in step 3 are displayed.
5. *(Optional)* Click **Report** to create a PDF output of the system configuration records.

View the application objects audit log

In some applications, the audit records are maintained within the template file or the data file. The audit records are not displayed in the SAE Administrator Console. See the chapter for your application for more information.

For a list of objects that can be audited for your application, see the chapter for your application.

The auditing of objects for the application must be set up. See “Enable or disable the audit function” on page 88.

1. In the main screen, click **Audit History** ▸ **Application Object Records**.
2. At the top left of the screen, select the **Enable Application Objects Records Filtering** checkbox.
3. Use one or more of the following filtering tools.
   - **Last modified from**
   - **Application** drop-down list
   - **Last modified by**
   - **Instrument** drop-down list
   - **Object name**
   - **Data audit record name**
   - **Old or new value**
4. Click **Search**.
   The actions that meet the criteria set in the filtering tools are displayed.
5. In the application objects table, select the record you want to view.
   The record that is selected is highlighted in blue.
6. Select the **Data Audits** tab.
7. *(Optional)* Click **Report** to create a PDF output of the application objects.

View the e-signatures

In some applications, the e-signature records are maintained within the template file or the data file. The e-signature records are not displayed in the SAE Administrator Console. See the chapter for your application for more information.

For a list of items that require an e-signature for your application, see the chapter for your application.

1. In the SAE Administrator Console main screen, click **Audit History** ▸ **Application Object Records**.
2. At the top left of the screen, select the **Enable Application Objects Records Filtering** checkbox.

3. Use one or more of the following filtering tools.
   - **Last modified from**
   - **Application** drop-down list
   - **Last modified by**
   - **Instrument** drop-down list
   - **Object name**
   - **Data audit record name**
   - **Old or new value**
4. Click **Search**.
   The actions that meet the criteria set in step 3 are displayed.
5. In the application objects table, select the record you want to view.
   The record that is selected is highlighted in blue.
6. Select the **e-Signature Records** tab, then select the e-signature record that you want to view from the list of available records.
   The **e-Signature Record Details** dialog box opens.
   For information regarding e-signature record details, see your application specific chapter in this guide.
7. *(Optional)* To create a PDF output of **Data Audit and e-Signature** history, click **Report**.
8. *(Optional)* Click **Report** to create a PDF output of the e-signature record.

View the instrument run records

1. In the SAE Administrator Console main screen, click **Audit History** ▸ **Instrument Run Records**.
2. At the top left of the screen, select the **Enable Instrument Run Records Filtering** checkbox.
3. Use one or more of the following filtering tools.
   - **Run date from**
   - **Instrument** drop-down list
   - **File name**
   - **Started by** drop-down list
   - **Run name**
4. Click **Search**.
   The instrument runs that meet the criteria set in step 3 are displayed.
5. In the instrument run records table, select the record you want to view.
   The record that is selected is highlighted in blue.

6. Select one of the following tabs:

Tab	Displays the following information
Run Summary	• The user who started the run • The instrument on which the run was started (**Host ID** and **Instrument name**) • The setup file used for the run and the run name • Run date and duration
Application objects	Information about the objects used in a run (for example, a plate or a template)
Action records	Actions performed during a run (for example, start or cancel a run)
Data audit records	Information about changes made during a run
Run completion outputs	List of objects generated by the run (for example, data files)

7. *(Optional)* Click **Report** to create a PDF output of the instrument run records.

Export active Action or System Configuration records

The **Action** or **System Configuration** tabs provide an export function that allows you to export records in TXT format. The TXT files can be viewed in another program such as Microsoft™ Excel.

The exported file for the action records is `action-records.txt`.

The exported file for the system configuration records is `audit-records.txt`.

IMPORTANT! Exported **Action** or **System Configuration** records cannot be imported back into the **Audit History** tab. To export records that can be restored into the **Audit History** tab, see Chapter 11, “Back up, archive, and restore SAE records and files”.

---

1. In the SAE Administrator Console main screen, select one of the following options.
   - **Audit History ▸ Action Records**
   - **Audit History ▸ System Configuration**
2. *(Optional)* Use the filtering tools.
   When the records are filtered, only the filtered records are exported in the TXT file.
   For more information about the filtering tools, see “View the action records audit log” on page 100 and “View the System Configuration audit log” on page 100.
3. Click **Export**.

View archived audit records

1. In the main screen, click **Settings** ▸ **Archival History**.

   Each row represents an archive event. The **Run Duration** indicates how long the archival event took to complete.

2. Select a row, then select **View Archived Records** to display the records in the archive.

3. As needed, click the **Action Records** tab and the **System Configuration** tab..

   The **Application Object Records** tab and the **Instrument Run Record** tab are visible. These items are not applicable for the QuantStudio™ Design and Analysis Desktop Software.

4. Click the **Back to Archival History** to display the main archive record screen.

Export archived audit records

1. In the main screen, click **Settings** ▸ **Archival History**.

   Each row represents an archive event. The **Run Duration** column indicates how long each archival event took to complete.

2. Select a row, then select **Export** to export a records compressed folder (ZIP folder) that contains the records in the archive.

The exported archived audit records can be imported (see “Restore exported archived audit records” on page 108).

11 Back up, archive, and restore SAE records and files

Archive/backup options and frequency

Several options are available:

- Automatically archive records. SAE records are automatically removed from the database at the frequency you determine. SAE records can be viewed or restored in SAE Administrator Console.

  Note: SAE records can be archived manually at any time.

- Export the settings for the SAE Administrator Console.
- Back up the entire SAE program folder with Windows™ Explorer.

Note: Records that are exported in the **Action** or **System Configuration** tabs cannot be restored. For information, see “Export active Action or System Configuration records” on page 103.

When to archive

The required frequency of archiving depends on your system configuration (such as the number of applications that use the SAE server, the configuration of the audit and e-signature functions). For the optimum performance of the SAE settings, the size of the database should not be large enough to affect SAE performance.

As a starting point, we suggest that you maintain a database size of <50 MB. If you notice a decrease in performance (for example, it takes a long time for the SAE Administrator Console to display records), consider maintaining a smaller database size.

A suggested approach for determining the required frequency is listed below.

- Configure the SAE Administrator Console to automatically archive.
- Check the size of the database monthly.
- If the database size is >50 MB after 3 months, increase the frequency of auto archiving.

Backing up the entire SAE program folder is optional. Perform the back up at a frequency determined by your laboratory/IT protocol.

Set up automatic archive of audit records

Automatically archiving audit records removes the records from the database and saves them in `<…>:/Program Files (x86)/Applied Biosystems/SAE Admin Console/automated_archivals`, where <…> is the installation drive.

Archived audit records can be viewed in the SAE Administrator Console.

1. In the SAE Administrator Console main screen, click **Settings** ▸ **Auto Archive**.
2. In the **Auto Archival Settings** dialog box, select the **Enable Auto Archive** checkbox.,
3. Choose a setting in the **Archival mode** drop-down list.
   - **By number of records or retention period**
   - **By records retention period**
   - **By number of records**
4. Enter the number of records and the retention period.
   The fields that are available depend on the setting that was selected in step 3.
5. Click **Save**.

The software periodically checks the audit record status and archives when the specified archive conditions are met.

Manually archive audit records

Manually archiving audit records removes the records from the database and saves them in `<…>:\Program Files (x86)\Applied Biosystems\SAE Admin Console\automated_archivals`, where <…> is the installation directory. They are saved in a folder named by the date and the time of the archival.

Archived audit records can be viewed in the SAE Administrator Console.

1. In the SAE Administrator Console main screen, click **Settings** ▸ **Archival History**.
2. Click **Ad-hoc Archival**.
3. In the **Archive Records** dialog box, enter a date range.
4. Click **Archive**.

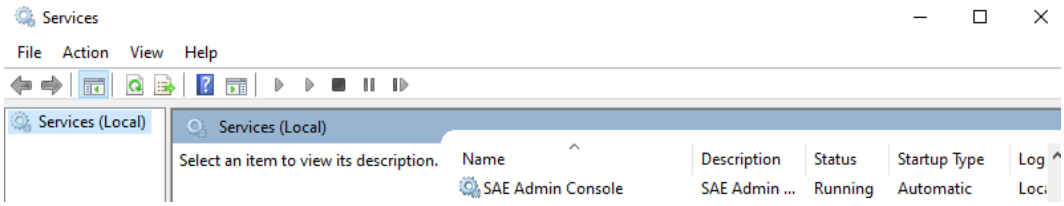
The archive is listed when you click **Settings** ▸ **Archival History**.

Back up the SAE program folder

To obtain a complete copy of all SAE records and settings, you can back up the SAE program folder. Back up the entire program folder, not just the database folder, to ensure compatibility between the SAE server software and the database files.

IMPORTANT! If the backed up files require re-installation or installation on another computer, contact Technical Support.

1. Instruct all users to sign out of the applications and the SAE Administrator Console.
2. Close the SAE Administrator Console.
3. Stop the SAE server.
   a. In the Windows™ desktop, click ⊞, type ***services***, then open the **Services** app.



   b. Scroll down to **SAE Admin Console**, right-click it, then click **Stop**.
4. Copy the `<…>:\Program Files (x86)\Applied Biosystems\SAE Admin Console`, where <…> is the installation directory, to a back up location.
5. Repeat step 3 and click **Start** to start the SAE server.
6. Start the SAE Administrator Console.

Restore archived audit records

1. In the SAE Administrator Console main screen, click **Settings** ▸ **Archival History**.
2. Select an archived audit record to restore, then click **Restore**.
3. In the **Restore Records** dialog box, click **Restore**.
   The **Restore Records** dialog box displays the number of records that were restored.
4. Click **Close**.

The archived audit record remains listed in the SAE Administrator Console.

The folder containing the archived audit records remains in `<…>:\Program Files (x86)\Applied Biosystems\SAE Admin Console\automated_archivals`, where <…> is the installation directory. The folder is named by the date and the time of the archival.

Restore exported archived audit records

Exported archived audit records are stored in a compressed folder (ZIP folder). See “Export archived audit records” on page 104.

1. In the SAE Administrator Console main screen, click **Settings** ▸ **Archival History**.
2. Click **Restore (upload)**.
3. In the **Restore Records** dialog box, click **Choose File**, then navigate to the folder that contains a compressed folder (ZIP folder) with the archived audit records.
4. Click **Restore**.
   The **Restore Records** dialog box displays the number of records that were restored.

12 Advanced configuration options

Export system security, audit, and e-signature settings

Use the export functions to transfer settings from one instance of the SAE Administrator Console to another instance.

1. In the SAE Administrator Console main screen, click **Settings** ▸ **Export Configuration**.
2. In the **Export Configuration** dialog box, select an export option.

Setting	Items exported
All	All settings and user accounts
Custom, **Users & roles**	• Active user accounts • Roles and their associated permissions
Custom, **System & roles**	• Settings • Roles and their associated permissions

3. Click **Export**.

The exported file (DAT format) downloads to the default location of the computer.

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

Settings that were exported from one instance of the SAE Administrator Console can be imported into another instance.

For information about the items that can be exported for import, see “Export system security, audit, and e-signature settings” on page 109.

Export the settings (“Export system security, audit, and e-signature settings” on page 109).

1. In the SAE Administrator Console main screen, click **Settings** ▸ **Import Configuration**.
2. In the **Import Configuration** dialog box, click **Choose File**, then navigate to the file that contains the settings to import.
   The settings are in a DAT file.
3. Select an import option.

Setting	Items exported
All	All settings and user accounts
Custom, **Users & roles**	• Active user accounts • Roles and their associated permissions
Custom, **System & roles**	• Settings • Roles and their associated permissions

   The software imports the items that are in the DAT file. If **All** is selected for import but only **Users & roles** or **System & roles** were exported, the software imports the items that are available in the DAT file.
4. If imported user accounts exist in the SAE Administrator Console, click **Skip** or **Overwrite** for each user account, then click **Confirm and Import**.
   The **Import Configuration** dialog box displays a confirmation message. The number of created accounts and updated accounts is displayed.
5. Click **Close**.

If there are any notifications, the **Event Notifications** dialog box is displayed. Perform one of the following actions:

- Click **Close**.
- Select one or all of the notifications, then click **Acknowledge**.

Configure user repositories

User repository overview

SAE user account information is stored in a "user repository".

The SAE Administrator Console provides the following options for user repositories:

- **Internal**—Allows only SAE user accounts to sign in to an application. SAE user accounts are referred to as "local" accounts in the SAE Administrator Console.
  - SAE user accounts are created in the SAE Administrator Console and are identified as "local" in the **Users** tab.
  - User authentication is based on the accounts that are listed in the **Users** tab and the SAE settings that are specified in the **System** tab.
  - User permissions are determined by the roles that are configured in the SAE Administrator Console.
- **External LDAP**—Enables LDAP based authentication with an LDAP directory. Allows only external user accounts to sign in to an application.
  - User accounts are created in an LDAP (Lightweight Directory Access Protocol) user management system and are identified as "external" in the SAE Administrator Console **Users** tab.
    - The SAE Administrator Console only pulls users from a single Organizational Unit and does not allow aliases or complex filtering.
  - User authentication is based on the accounts that are listed in the SAE Administrator Console **Users** tab and the external LDAP user repository.

    The following settings from the **System** tab are not used for LDAP:
    - **User Name Settings** pane, **Password Policy** pane, and the **Account Lockout Policy** pane.

    The settings that are specified in the **Other Settings** pane are used.
  - User permissions are determined by the roles that are configured in the SAE Administrator Console.
  - All local user accounts except the default Administrator account are set to **Inactive** and cannot sign in to the application.
  - Passwords cannot be changed in the SAE Administrator Console.
- **Federated**—Allows internal (local) and external account sign-in to an application.
  - User accounts are created in the SAE Administrator Console or in an LDAP user management system.
  - User authentication is based on the respective internal or LDAP user repository.

Configure user repositories for SAE or external account access

IMPORTANT! Use this function only with guidance from a service or applications representative.

1. In the SAE Administrator Console main screen, click **Settings ▸ User repositories (advanced)**.
2. Select the **User repository definition**.

Option	Description
Internal User Repository	Allows SAE user accounts to sign in
External LDAP User Repository	Allows external user accounts to sign in
Federated Repositories	Allows SAE user accounts or LDAP accounts to sign in

3. If you selected **External LDAP User Repository** or **Federated Repositories**, click **Next**.
4. Enter the required information in the **LDAP Server Configuration** tab, then click **Next**.
   See “User repository settings” on page 113.
5. Enter the required information in the **User Account Mapping** tab, then click **Next**.
   See “User repository settings” on page 113.
   - New LDAP accounts are listed as **External**, and **Role** is set to the default specified during account mapping. If no default was specified, accounts are set to **No Privileges Role**.
   - SAE user accounts that were previously created in the SAE Administrator Console are listed as **Local**.
   - If you selected LDAP, the **Status** for all accounts except for the default SAE Administrator account is set to **Inactive**.
6. In the **Authentication Verification** tab, enter the user name and password for the LDAP server, then click **Test Authentication**.
7. Click **Test Connection**
8. Click **Apply Settings**.
9. If needed, edit the user accounts to assign roles.
   See Chapter 6, “Manage SAE user accounts and roles”.

The SAE server periodically synchronizes the LDAP accounts with the LDAP server if changes are made to the **User repository definition** or any setting on the LDAP server.

User repository settings

Table 10 External LDAP User Repository and Federated Repositories settings

Setting	Description
LDAP Server Configuration	
Host name, **Port**, and **Use SSL**	LDAP server name or IP address, port, and interface protocol
Bind distinguished name, **Bind password**, **Base distinguished name**	LDAP server attributes required for access
User Account Mapping	
Directory type	LDAP server configuration Click **Set Defaults** after you select the **Directory type** to display typical default parameters for mapping to an LDAP system.
User name	Parameter that maps to the user name in the LDAP system
Default role assignment	The SAE role that will be assigned to all user accounts. You can change the role after the user accounts are imported into the SAE Administrator Console.
User name and other settings	Parameters that correspond to the user name and other fields in the LDAP system
Authentication verification	
User Name and **Password**	LDAP server user name and password

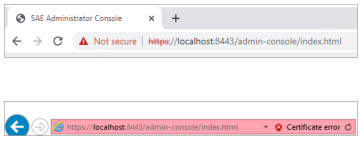
User or administrator sign-in with LDAP or federated user repositories

User repository	User signs in with	Administrator signs in with
Internal	Internal (local) account: User name and password created in the SAE Administrator Console	• User name and password for the default SAE Administrator user account • Any SAE user account that has been assigned the SAE role of Administrator
External	External account: User name and password created in the LDAP user management system. **Note:** Local accounts are set to **Inactive**.	• User name (with local/ prefix) and password for the default SAE Administrator user account Example: local/Administrator • Any external account that has been assigned the SAE role of Administrator

(continued)

User repository	User signs in with	Administrator signs in with
Federated	The account type that they are assigned: • External account • Internal (local) account (with local/ prefix) Example: local/User name	• User name (with local/ prefix) and password for the default SAE Administrator user account Example: local/Administrator • Any external account that has been assigned the SAE role of Administrator

A Troubleshooting

Observation	Possible cause	Recommended action
A security or warning message is displayed when you start the SAE Administrator Console **Details:** Examples of the messages you may see in a browser are shown below. 	The self-signed SSL certificate for the SAE Administrator Console URL cannot be verified by a certification authority.	See "Overview of the warning screens" on page 20.
The SAE Administrator Console automatically signs out after 30 minutes	The software is designed to automatically sign out after 30 minutes of inactivity. This lockout time is not configurable.	Sign in.
The instrument software is not prompting for signatures	The user profile does not have the e-signature permission enabled.	Assign a role that has the e-signature permission enabled. Edit the role to allow e-signatures ("Edit a role" on page 82).
	The e-signature function is not enabled for the application.	Enable the e-signature function for the application ("Enable the e-signature function" on page 95).
	All of the required settings that are required to enable e-signature function are not set.	To enable the function, make all of the following settings (if all settings are not made, the function is not enabled): • Select the **Enable e-signatures** checkbox. • Select an action. • Enter a number of signatures required for a meaning. See "Workflow to set up the e-signature function" on page 95.
An expected permission is not listed for an application when you create a role	A newer version of the application profile may be required.	Check the version of the application profile (**Settings ▸ Manage Application Profiles**), then contact Technical Support.

Observation	Possible cause	Recommended action
Default audit settings are not displayed for an application profile	In the **Audit** tab, the list in the **Audit Settings** pane contains additional rows that are not visible.	Scroll down to see settings for additional application profiles.
The expected audit records are not listed in the audit history screens	The records have been archived.	Select **Settings ▸ Archival History** to view archived records.

Index

F

I

L

M

N

O

P

Q

R

S

T

U

V

W