

# SAE Software Solution for 21 CFR Part 11 Compliance USER GUIDE

for use with Qubit™ Flex Fluorometer

Publication Number MAN0028384

Revision A.0



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](https://thermofisher.com/symbols-definition).

**Revision history: MAN0028384 A.0 (English)**

Revision	Date	Description
A.0	24 October 2022	New document for the Qubit™ Flex Fluorometer.

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

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

**NOTICE TO PURCHASER: DISCLAIMER OF LICENSE:** Purchase of this software product alone does not imply any license under any process, instrument or other apparatus, system, composition, reagent or kit rights under patent claims owned or otherwise controlled by Thermo Fisher Scientific, either expressly, or by estoppel.

**TRADEMARKS:** All trademarks are the property of Thermo Fisher Scientific and its subsidiaries unless otherwise specified.

©2022 Thermo Fisher Scientific Inc. All rights reserved.

# Contents

■	<b>CHAPTER 1</b>	<b>About the software</b>	<b>6</b>
		About the Qubit™ Flex SAE Software Solution for 21 CFR Part 11 compliance	6
		SAE Admin Console overview	7
		Example applications	7
		Network and password security requirements	8
		Network configuration and security	8
		Password security	8
■	<b>CHAPTER 2</b>	<b>Set up SAE user accounts and roles</b>	<b>9</b>
		Enable the SAE Admin Console	9
		How to proceed if a security or warning screen is displayed	10
		Install the Qubit™ Flex Application Profile on the SAE Admin Console	10
		Determine the logged-in user	11
		Create a user account	11
		Edit a user account	11
		Activate a suspended user account	12
		Disable (inactivate) a user account	12
		Reset a forgotten password	13
		Change password	14
		Create or edit a user role	14
		Create a user role	15
		Default permissions and roles	16
		Edit a user role	17
		Delete a user role	17
		Generate, view, and print a user or role report	17
■	<b>CHAPTER 3</b>	<b>Manage the system security function</b>	<b>19</b>
		Access the system security function screen	19
		Configure account setup and security policies	20
		Set up messaging notifications	21
		Set up SMTP configuration	23

■	<b>CHAPTER 4</b>	<b>Manage the audit function</b>	<b>25</b>
	Use the <b>Audit</b> function screen		25
	Enable or disable the audit function		26
	Select items to audit		26
	Configure audit reason settings		26
	Generate audit reports		27
	Display audit histories		28
	Review the system configuration		28
	View audit histories		29
	Use hash key to verify data integrity		30
	Export audit records		30
	Archive audit records		31
■	<b>CHAPTER 5</b>	<b>Manage the e-signature function</b>	<b>32</b>
	Access the e-signature function screen		32
	Configure the meanings of e-signatures		33
	Add an e-signature meaning		33
	Delete an e-signature meaning		33
	Select the actions that require e-signatures		33
■	<b>CHAPTER 6</b>	<b>Manage the SAE export-import function</b>	<b>35</b>
	Export and import user, system security, audit, and e-signature settings		35
	Export user, system security, audit, and e-signature settings		35
	Import user, system security, audit, e-signature settings		36
■	<b>CHAPTER 7</b>	<b>Install and use the SAE module on board the Qubit™</b>	
	Flex instrument		37
	Security, Auditing, and E-signature (SAE) for the Qubit™ Flex instrument		37
	Set up SAE mode on the Qubit™ Flex instrument		38
	Update the Qubit™ Flex software		38
	Generate a license key		38
	Activate a license key		41
	Enable SAE mode on the instrument		44
	Disable SAE mode on the instrument		45
	Configure the SAE functions on the Qubit™ Flex instrument		46
	Disable SAE mode when connection to the SAE Admin Console is lost		46
	Sign in to an instrument in SAE mode		47
	Change password on an instrument in SAE mode		48

■ <b>APPENDIX A</b>	<b>Documentation and support .....</b>	<b>50</b>
	Related documentation .....	50
	Customer and technical support .....	50
	Limited product warranty .....	50

■ About the Qubit™ Flex SAE Software Solution for 21 CFR Part 11 compliance .....	6
■ SAE Admin Console overview .....	7
■ Example applications .....	7
■ Network and password security requirements .....	8

## About the Qubit™ Flex SAE Software Solution for 21 CFR Part 11 compliance

The Invitrogen™ Qubit™ Flex SAE Software Solution for 21 CFR Part 11 (SAE module) supports compliance with 21 CFR Part 11, a regulation that describes the criteria for acceptance by the FDA for electronic records and electronic signatures. Part 11 is composed of procedural and technical requirements. Procedural requirements are the standard operating procedures instituted by the end user, and technical requirements are the technical characteristics of the compliance management software used.

The Qubit™ Flex SAE module includes the following components (see Figure 1):

- **Security, Auditing, and E-signature Administrator Console (SAE Admin Console)**—Used to configure the Security, Audit and e-Signature (SAE) functions of the SAE module
- **Qubit™ Flex SAE License**—Used to activate the SAE functions for the Qubit™ Flex instruments
- **Qubit™ Flex Instrument SAE Mode**—Instrument firmware connected with the SAE Admin Console

The combination of this technical offering does not guarantee 21 CFR part 11 compliance alone. Compliance is the consequence of the end user's work process and systems used.

This guide describes the procedures to set up and manage the SAE mode of the Qubit™ Flex Fluorometer.

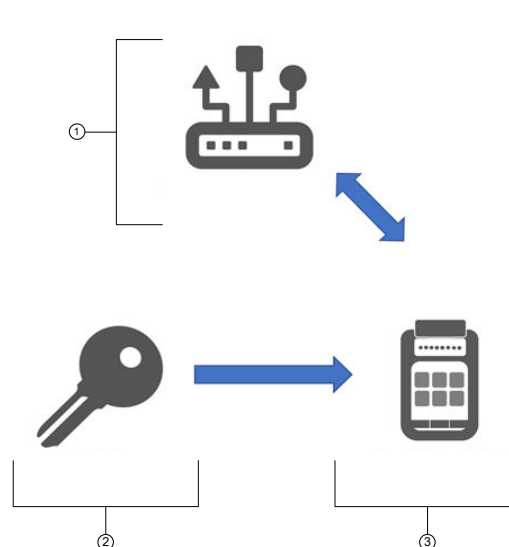


Figure 1 Components of the Qubit™ Flex SAE module

- ① SAE Admin Console
- ② Qubit™ Flex SAE License
- ③ Qubit™ Flex Instrument SAE Mode

## SAE Admin Console overview

The SAE Admin Console is a component of the Qubit™ Flex SAE module that allows an administrator to configure SAE functions on Qubit™ Flex instruments to meet specific requirements.

The SAE Admin Console is available for many instruments and software from Thermo Fisher Scientific, including but not limited to Attune™ NxT and Attune™ CytPix™ flow cytometers, iBright™ Imaging Systems, and Countess™ 3 and 3 FL automated cell counters. For convenience, multiple instruments can be hosted in the same console. Settings for each instrument are imported to the console via the application profile of the instrument.

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

Feature	Description
System security	Controls user access to the software. The following two default user roles are provided; additional user accounts and permissions can be user-defined. <ul style="list-style-type: none"><li>• <b>Qubit™ Flex Administrator role</b>—Includes full privileges on the Qubit™ Flex instrument and the SAE Admin Console</li><li>• <b>Qubit™ Flex Scientist role</b>—Includes most privileges on the Qubit™ Flex instrument, but does not include privileges on the SAE Admin Console</li></ul>
Auditing	Tracks actions performed by users and changes to the SAE module settings. Some actions are automatically audited silently. You can select other items for auditing and specify the audit mode. The auditing function provides reports for audited SAE module changes and actions.
Electronic signature (e-signature)	Determines if users are required to provide a username and password when performing certain functions. E-signature events can be configured to require multiple signatures and to require users with specific permissions to sign.

## Example applications

The SAE module can be configured to support the following functions:

- Leave permissions open to all users but require users to log in for traceability.
- Establish rules-based passwords with defined expirations.
- Track the actions taken to generate results from the time the assay is run to the time it is exported and/or deleted from the instrument.
- Allow only certain users to delete sample reading files.
- Allow only certain users to perform a software update.
- Require users to acknowledge through e-signature the decision to use new or existing standards.

# 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. Password complexity and expiration rules can be configured in the SAE Admin Console (see “Configure account setup and security policies” on page 20).

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





# Set up SAE user accounts and roles

■ Enable the SAE Admin Console .....	9
■ How to proceed if a security or warning screen is displayed .....	10
■ Install the Qubit™ Flex Application Profile on the SAE Admin Console .....	10
■ Determine the logged-in user .....	11
■ Create a user account .....	11
■ Edit a user account .....	11
■ Activate a suspended user account .....	12
■ Disable (inactivate) a user account .....	12
■ Reset a forgotten password .....	13
■ Change password .....	14
■ Create or edit a user role .....	14
■ Generate, view, and print a user or role report .....	17

## Enable the SAE Admin Console

The SAE Admin Console is available for download from [thermofisher.com/qubitresources](https://thermofisher.com/qubitresources).

1. Install the program and launch the application.  
When you start the SAE Admin Console software, it opens the URL for the SAE server in your default web browser. If a security or warning screen is displayed, see “How to proceed if a security or warning screen is displayed” on page 10.
2. Enter the default Administrator **User Name** and **Password**, then click **Sign in**.

---

**Note:** The default user name and password are "Administrator".

---

---

**Note:** After signing in, you will be prompted to change your password. The following symbols cannot be used in the password, because they are not compatible with the Qubit™ Flex instrument: + & % \ ~ ' ^

---

## How to proceed if a security or warning screen is displayed

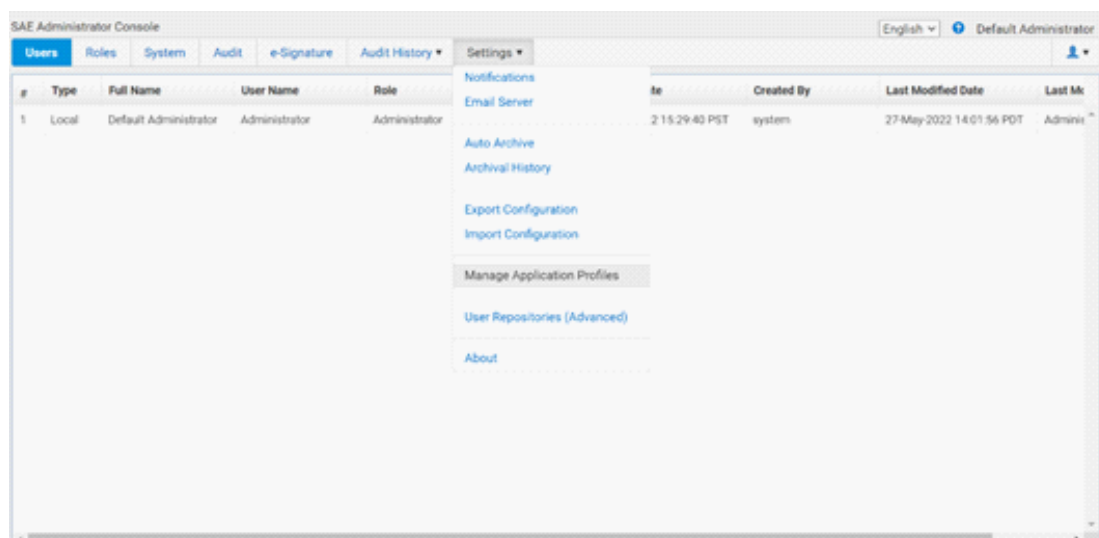
The SAE Admin Console runs locally on your computer. When you start the SAE Admin Console software, it opens the URL for the SAE server in your default web browser. (Google Chrome™ is the recommended browser.) If a security or warning screen is displayed, consult with your local IT representative to generate and install a self-signed certificate for the SAE server URL.

**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 Admin Console 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.

## Install the Qubit™ Flex Application Profile on the SAE Admin Console

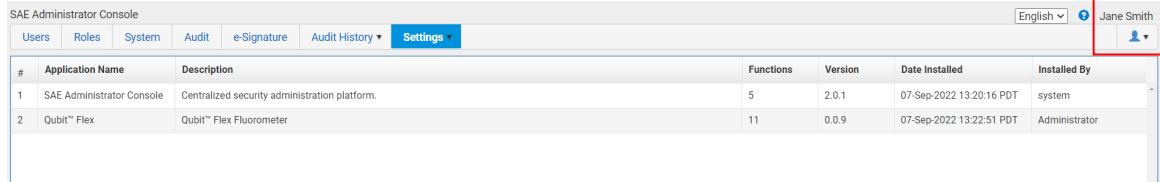
1. To download the Qubit™ Flex Application Profile, go to [thermofisher.com/qubitresources](https://thermofisher.com/qubitresources).
2. In the SAE Admin Console, go to **Settings**, then click **Manage Application Profiles**.



3. Click **Install Application Profile** at the bottom of the page.
4. Select the **Choose File** option in the pop-up window to select and open the data file for **Qubit Flex.dat**. The selected file name appears by the side of the **Select File** option in the pop-up window.
5. Select **Verify Data File**, then select **Install**.

## Determine the logged-in user

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



## Create a user account

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

---

**Note:** First name, MI (middle initial), and last name are used to create the **User Full Name**, which is displayed in the **Action Records** under **Audit History** in the SAE Admin Console.

---

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

---

2. Select **User must set new password at next sign in** to require the user account to specify a new password at first login.

---

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

---

3. Select the **user role** from the **Role** dropdown list. To create custom roles, see “Create or edit a user role” on page 14.

---

**Note:** Two default roles (Qubit™ Flex Administrator and Qubit™ Flex Scientist) are automatically included in the **Application Profile**. For more information on the default settings for these roles, see “Create or edit a user role” on page 14.

---

4. Leave the status set to **Active**.
5. (*Optional*) Enter phone, e-mail (for information only), and comments.
6. Click **Save**.

## Edit a user account

1. In the **Users** tab, select a user account, then click **Edit**.
2. In the **Edit User Account** dialog box, edit the settings as desired.

---

**Note:** You cannot edit the user name of an existing user or delete an existing account.

---

#	Type	Full Name	User Name	Last Modified Date	Last Modified By
1	Local	Default Administrator	Administrator	Sep-2022 13:21:06 PDT	Administrator
2	Local	Jane Smith	flexadmin	Sep-2022 14:54:53 PDT	flexadmin
3	Local	Jane Smith	scientist	Sep-2022 14:54:29 PDT	flexadmin

3. Click **Save**.

## Activate a suspended user account

1. In the **Users** tab, select a user account, then click **Edit**.
2. Change the **Status** from **SUSPENDED** to **ACTIVE**.
3. Click **Save**.

## Disable (inactivate) a user account

1. In the **Users** tab, select a user account, then click **Edit**.
2. Change the **Status** from **ACTIVE** to **INACTIVE**.
3. Click **Save**.

## Reset a forgotten password

**IMPORTANT!** We recommend establishing more than one account with the Administrator role. If one Administrator loses their password or leaves the institution, **there is no way to retrieve the password.** In this case, the user will have to re-install the SAE Admin Console, resulting in the loss of the audit trail and settings. To mitigate this risk, the Administrator password should be properly managed, and multiple Administrator roles should be established as a backup option.

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

Edit User Account

User name

flexadmin

Role

QubitFlex Administrator

Password

Password

Re-enter password

☐ User must set new password at next sign in

\* First name

Jane

MI

\* Last name

Smith

Phone

Email

Status

Active

Comments

Save

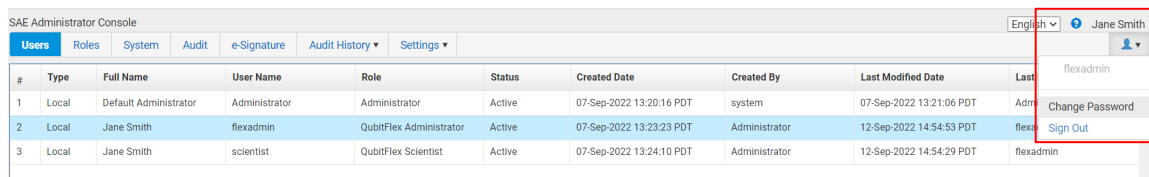
Cancel

4. Click **Save**.

## Change password

1. From the user name dropdown list (👤), select **Change password**.

**Note:** You can access the **Change Password** dialog box from any tab.



2. Enter the old password.
3. Enter a new password, confirm the new password, then click **Update**.

**Note:** The following symbols cannot be used in the password, because they are not compatible with the Qubit™ Flex instrument: + & % \ ~ ' ^

## Create or edit a user role

User roles determine the permissions associated with a user account. The Qubit™ Flex SAE module provides two default SAE user roles with permissions that can be edited by the user:

- **Qubit™ Flex Administrator**—Includes full privileges on the Qubit™ Flex instrument and the SAE Admin Console.
- **Qubit™ Flex Scientist**—Includes most privileges on the Qubit™ Flex instrument, except for updating the software or enabling/disabling SAE mode on the instrument. The Scientist role does not include privileges on the SAE Admin Console.

In addition to the SAE user roles provided by the Qubit™ Flex SAE module, the Qubit™ Flex instrument includes the following user role:

- **Qubit™ Flex local administrator:** The only permissions given to this role are to disable SAE mode and reset instrument settings. **This is not an SAE role and thus, does not appear in the audit trail.** This role should not be used unless absolutely necessary. We recommend using this role only in the following cases:
  - The Qubit™ Flex instrument loses connection to the SAE server and the SAE user role is signed out. Since the SAE mode requires connection to the server, an SAE user role cannot sign in unless connection is re-established. Instead, the Local Administrator can sign out of SAE mode. Once signed out, the user can re-establish network connection and log back in to SAE mode with an SAE user account.
  - The Qubit™ Flex instrument is sent to Customer Service for repair and/or replacement, and the sign-in is still with the SAE user account user name and password. Customer Service must be able to reset the instrument without violating protocol by signing into a customer's SAE account.

**IMPORTANT!** We recommend establishing more than one account with the Administrator role. If one Administrator loses their password or leaves the institution, **there is no way to retrieve the password.** In this case, the user will have to re-install the SAE Admin Console, resulting in the loss of the audit trail and settings. To mitigate this risk, the Administrator password should be properly managed, and multiple Administrator roles should be established as a backup option.

## Create a user role

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

**Note:** Roles assigned to a user account cannot be deleted.

1. In the **Roles** tab, click **Create**.

**Edit Role**

**\* Name** Intern

**Description** This role has permissions to perform runs but not to delete run results, configure the instrument, or access the Admin console.

**Permissions**

- Qubit™ Flex
  - Run
    - Run assay
    - Run fluorometer
    - Run verification assay
  - Results Management
    - View run results
    - Export run results
    - Delete run results
    - Modify run results
  - Instrument Configuration
  - Security Configuration
    - Perform e-signing
  - SAE Administrator Console
    - Security Configuration
    - Audit History

Save Cancel

2. Enter a role name and (optional) description.

3. Select permissions. To select all permissions in a category, select the checkbox next to the category.

---

**Note:** For information on user-configurable permissions and the settings for default user accounts, see “Default permissions and roles” on page 16.

---

4. Click **Save**.

## Default permissions and roles

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

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

---

**Note:** Operations not shown in the table are available to all user roles.

---

**Table 1** Conferrable permissions and default user roles

Permissions			SAE accounts		Local account
Function group	Function category	Specific functions	Administrator	Scientist	Administrator
Run	Run assay	Start assay run Start standards run Re-run standards	Yes	Yes	No
	Run fluorometer	Start fluorometer run	Yes	Yes	No
	Run verification assay	Start verification assay run	Yes	Yes	No
Results management	View run results	View assay run results View fluorometer run results View verification assay run results	Yes	Yes	No
	Export run results	Export assay run results Export fluorometer run results Export verification assay run results	Yes	Yes	No
	Delete run results	Delete assay run results Delete fluorometer run results Delete verification assay run results	Yes	Yes	No
User account management	Reset own password	Update own password	Yes	Yes	Yes



**Table 1** Conferrable permissions and default user roles *(continued)*

Permissions			SAE accounts		Local account
Function group	Function category	Specific functions	Administrator	Scientist	Administrator
Service tools	Perform factory reset	Reset instrument to factory default	No	No	Yes
Instrument configuration	Perform firmware update	Perform firmware update on the instrument	Yes	No	No
	Change system settings	Modifications of the following instrument system settings Network configuration Instrument name Date/Time/Timezone Sleep mode settings Brightness settings	Yes	No	No
Security configuration	Enable/disable SAE	Enable/Disable SAE	Yes	No	Yes

## Edit a user role

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

---

**Note:** Roles assigned to users cannot be deleted.

---

2. Edit settings as needed, then click **Save**.

## Delete a user role

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

## Generate, view, and print a user or role report

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

## Roles Report

Host ID: USEUG-384C163  
Software Name: SAE Administrator Console  
Software Version: 2.1.0

### Roles Summary

#	Role	Description	Privileges	Users	Created Date	Created By	Last Modified Date	Last Modified By
1	Administrator	System role with full privileges	16	1	07-Sep-2022 13:20:13 PDT	system	07-Sep-2022 13:20:13 PDT	system
2	No Privileges Role	System role with no privileges	0	0	07-Sep-2022 13:20:13 PDT	system	07-Sep-2022 13:20:13 PDT	system
3	QubitFlex Scientist		8	1	07-Sep-2022 13:22:51 PDT	Administrator	07-Sep-2022 13:22:51 PDT	Administrator
4	QubitFlex Administrator		15	1	07-Sep-2022 13:22:51 PDT	Administrator	07-Sep-2022 13:22:51 PDT	Administrator
5	Intern	This role has permissions to perform runs but not to delete run results, configure the instrument, or access the Admin console.	7	0	09-Sep-2022 13:47:22 PDT	flexadmin	09-Sep-2022 13:47:22 PDT	flexadmin

## Roles Report

Host ID: USEUG-384C163  
Software Name: SAE Administrator Console  
Software Version: 2.1.0

### 1. Administrator Privileges

#	Application	Privilege
1	Qubit™ Flex	Run assay
2	Qubit™ Flex	Run fluorometer
3	Qubit™ Flex	Run verification assay
4	Qubit™ Flex	View run results
5	Qubit™ Flex	Export run results
6	Qubit™ Flex	Delete run results
7	Qubit™ Flex	Modify run results
8	Qubit™ Flex	Perform firmware update
9	Qubit™ Flex	Perform system reset



# Manage the system security function

■ Access the system security function screen .....	19
■ Configure account setup and security policies .....	20
■ Set up messaging notifications .....	21
■ Set up SMTP configuration .....	23

The following procedures require an SAE Administrator account in the SAE Admin Console.

## Access the system security function screen

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

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

1. See “Configure account setup and security policies” on page 20 to set or modify the system security function settings.
2. Click **Apply Settings**.

The screenshot displays the SAE Administrator Console interface. At the top, there's a navigation bar with tabs: Users, Roles, **System**, Audit, e-Signature, Audit History, and Settings. The **System** tab is active. Below the navigation bar, the main content area is divided into three sections: User Name Settings, Password Policy, and Account Lockout Policy. The User Name Settings section has input fields for Minimum length (8) and Maximum length (32), both labeled 'characters'. The Password Policy section has input fields for Minimum length (8) and Maximum length (64), both labeled 'characters'. It also has a 'May not reuse previous' field set to 3, labeled 'passwords'. Under 'Password complexity', there are radio buttons for 'Forbidden' and 'Allowed' for Alphabets, Uppercase, Lowercase, Numeric, and Special characters. All 'Allowed' options are selected. To the right of these are five 'at least' fields, each labeled 'occurrences', with input fields set to 0. Below these are 'Maximum password age' (120 days) and 'Minimum password age' (0 days) fields. The 'Password expiry reminder' is set to 'Enabled' with a 'Send reminder' field set to 3 days. The Account Lockout Policy section has an 'Account lockout' field set to 'Enabled'. At the bottom right, there are 'Reset to Defaults' and 'Apply Settings' buttons.

## Configure account setup and security policies

In the **Systems** tab, specify user name and password settings.

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

1. In the **User Name Settings** pane, enter the minimum and maximum number of characters for a user name.

---

**Note:** The minimum and maximum number of allowed characters are 1 and 256, respectively.

---

2. In the **Password Policy** pane:

- a. Enter the minimum and maximum number of characters for a password.

---

**Note:** The minimum and maximum number of allowed characters are 1 and 256, respectively.

---

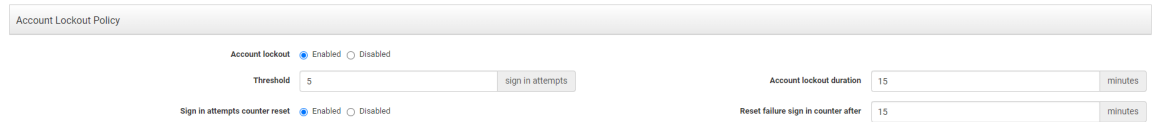
- b. In the **May not reuse previous** field, enter the number of most recent passwords that the software should remember to avoid password reuse.
- c. Select the complexity rules for creating a password, then enter the minimum number of occurrences for that rule.

---

**Note:**

- Ensure that the complexity rules set here are compatible with the Qubit™ Flex instrument.
  - Do not use the following symbols in the password, because they are not supported by the Qubit™ Flex instrument: + % & \ ~ ' ^
- 

- d. Enter the maximum and minimum number of days for which the password is valid.
  - e. Enable or disable the **Password expiry** reminder. If you select **Enabled**, enter the number of days before expiry for the reminder to be sent.
3. In the **Account Lockout Policy** pane, enable or disable the **Account Lockout** feature. If you select **Enabled**:
    - a. Enter the **Threshold** limit for login attempts.
    - b. Enter the **Account lockout duration** in minutes.
    - c. Enable or disable allowing the counter for login attempts to be reset.
    - d. Enter the **Reset account lockout** duration in minutes.



Account Lockout Policy

Account lockout ☒ Enabled ☐ Disabled

Threshold

Sign in attempts counter reset ☒ Enabled ☐ Disabled

Account lockout duration

Reset failure sign in counter after

4. In the **Other Settings** pane:
  - a. Enable or disable **Client offline login**.
  - b. If you select **Enabled**, enter the **Offline login threshold** in minutes.

---

**IMPORTANT!** We strongly recommend that users enable **Client offline login** and set a threshold value of >10 minutes for a stable SAE mode connection. This will minimize the chances of sign-out and workflow interruption if network access is temporarily lost.

---



Client offline sign in ☒ Enabled ☐ Disabled

Offline sign in threshold

---

**Note:** **Automatic screen locking**, **Inactivity duration**, **Open file from non-SAE systems**, and **Report page size** options are not currently enabled through the SAE Admin Console for the Qubit™ Flex instrument. You can set the inactivity period for automatic screen-locking and automatic user log-out on the Qubit™ Flex instrument directly in **Settings** under **Sleep Mode**.

---

5. Click **Apply Settings**.

---

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

---

## Set up messaging notifications

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

1. From the **Settings** dropdown list, select **Notifications** to open the **Edit Notifications Settings** dialog box.

**Edit Notification Settings**

Event	Notify at Administrator Sign In	Notify by Email	Email Address
Security enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<div style="background-color: #d3d3d3; padding: 2px;">Separate multiple emails (max. 5) using comma</div>
Security disabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<div style="background-color: #d3d3d3; padding: 2px;">Separate multiple emails (max. 5) using comma</div>
User did not enter correct password	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<div style="background-color: #d3d3d3; padding: 2px;">Separate multiple emails (max. 5) using comma</div>
User account suspended	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<div style="background-color: #d3d3d3; padding: 2px;">Separate multiple emails (max. 5) using comma</div>
User session timeout	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<div style="background-color: #d3d3d3; padding: 2px;">Separate multiple emails (max. 5) using comma</div>
Role deleted	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<div style="background-color: #d3d3d3; padding: 2px;">Separate multiple emails (max. 5) using comma</div>

Save
Close

2. In the **Edit Notifications Settings** dialog box, select the events for notification:

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

3. Select the notification method:

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

4. Click **Save**.

## Set up SMTP configuration

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

1. Click **Settings** ► **Email Server** to open the **SMTP Configuration** dialog box.

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**.



# 4

## Manage the audit function

■ Use the Audit function screen .....	25
■ Display audit histories .....	28
■ View audit histories .....	29

The following procedures require an SAE Administrator account in the SAE Admin Console.

### Use the Audit function screen

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

- Events that are audited
- List of reasons available to users when the audit mode is set to **Optional** or **Required**

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

---

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

---

1. In the SAE Admin Console home screen, select the **Audit** tab.

SAE Administrator Console

Users Roles System **Audit** e-Signature Audit History Settings

English Jane Smith

**IMPORTANT:** Changing the audit settings can affect opened files/records. Close any opened files/records before making changes to these settings.

☒ Enable Audits

**Audit Settings**

Include	Application	Audit Type	Audit Mode
<input checked="" type="checkbox"/>	Qubit™ Flex	Delete Run	Required
<input checked="" type="checkbox"/>	Qubit™ Flex	Export Run	Optional
<input checked="" type="checkbox"/>	Qubit™ Flex	Fluorometer	Silent
<input checked="" type="checkbox"/>	Qubit™ Flex	Modify Run	Silent
<input checked="" type="checkbox"/>	Qubit™ Flex	Standard/Sample	Silent
<input checked="" type="checkbox"/>	Qubit™ Flex	Verification Assay	Silent

**Audit Reason Settings**

ID	Reason	Edit Delete
1	Manually edited.	Edit Delete
2	Entry error.	Edit Delete
3	Well anomaly.	Edit Delete
4	Calculation error.	Edit Delete
5	Need to change threshold.	Edit Delete
6	Need to reanalyze.	Edit Delete
7	New reason	Edit Delete

[New reason](#)

☐ Require users to select a reason for change from list

**Apply Settings**

2. Set or modify the **Audit Settings** (see “Select items to audit” on page 26 and “Configure audit reason settings” on page 26).
3. Click **Apply Settings**.

## Enable or disable the audit function

1. In the SAE Admin Console home screen, select the **Audit** tab.
2. Select or deselect **Enable Audits**.
3. (Optional) Set or modify the **Audit Settings** and the **Audit Reason Settings**.
4. Click **Apply Settings**.

## Select items to audit

When **Enable Audits** is checked, actions taken to carry out a sample reading and changes to instrument settings are silently audited. For the full list of actions that are audited, see the specific functions column in Table 1.

Non-silent audits require the user to enter the reason for taking an action. Non-silent audits can be optional or required (require a user to select a reason before moving to the next step).

1. Select the **Audit Mode** for each item you include for auditing:

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

2. Click **Apply Settings**.

## Configure audit reason settings

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

The SAE Administrator Console is installed with five default audit reasons. These reasons may not be applicable to every workflow on the Qubit™ Flex Fluorometer and can be updated during SAE Admin Console configuration.

The default reason list:

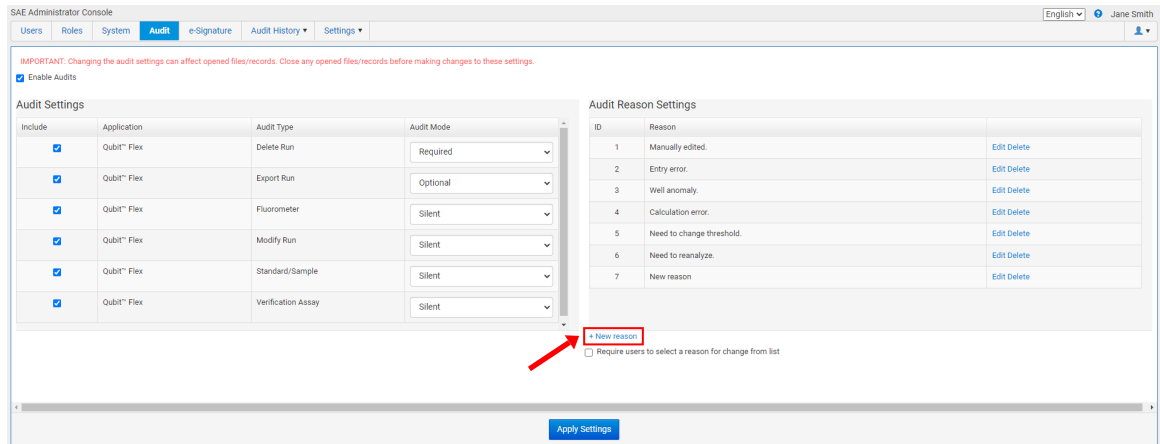
- **Sample dispense error**
- **Wrong input volume**
- **Sample anomaly**
- **New run**
- **Entry error**

1. To add a new audit reason, click **New Reason** in the **Audit Reason Settings** pane to open the **Add New Audit Reason** dialog box.

---

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

---



2. Enter a reason for change, then click **Save**.

Add New Audit Reason

Reason for change

Save

Cancel

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

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

7. Click **Apply Settings**.

## Generate audit reports

Use the **Audit History** dropdown list to generate reports from the **Action Record**, **System Configuration**, or **Application Object Records** views.

**Note:** The **Instrument Run Records** option under the **Audit History** dropdown list is not applicable to the Qubit™ Flex instrument.

## Display audit histories

You can display audit histories from the **Audit history** dropdown list in three different ways:

- **Action Record**—General description of audited events.
- **Application Object Record**—Detailed description of audited events. After selecting an event, details of audit and e-signature events are displayed.
- **System Configuration**—The system security, audit, and e-signature configuration records, including audit history for each user account.

## Review the system configuration

The **System Configuration** view from the **Audit History** dropdown list includes system security, audit, and e-signature configuration records. The following table summarizes the actions that can be audited using the SAE Admin Console.

Record Type	Action	Description
Security settings	Update	Disable, enable, or modify system security policies and session time-out settings
Account settings	Update	Modify password settings, system security policies (password expiration and account suspension), or user name settings
User group manager	Update	Create, delete, or modify reason for change
User role	Create	Create user role
	Delete	Delete user role
	Update	Modify user role
User account	Create	Create new user account
	Update	Edit or suspend a user account
Role assignment	Edit	Assign a different user role to an existing user account
	Create	Create a user account
Auditable entity settings	Update	Enable or disable auditing
Auditable entity	Update	Modify audit settings
Role permissions	Create	Create a user role  <b>Note:</b> One role assignment record is created for each permission in a role.
	Delete	Delete a user role
	Update	Modify user role permissions
Audit reason for change	Create	Create reason for change
	Update	Modify reason for change

(continued)

Record Type	Action	Description
Audit reason for change	Delete	Delete reason for change
Event manager	Update	Update the event manager
E-signature manager	Update	Enable or disable e-signature
E-signature type	Create	Create an e-signature meaning
	Delete	Delete an e-signature meaning
E-signature function	Update	Edit an action requiring e-signature

## View audit histories

- From the **Audit History** dropdown list, select one of the following options:

Option	Description
<b>Action Record</b>	Displays an audit of the actions for each user
<b>System Configuration</b>	Displays updated system configuration settings
<b>Application Object Records</b>	Displays details of each data audit and e-signature record

SAE Administrator Console

Users Roles System Audit e-Signature **Audit History** Settings

English Jane Smith

☒ Enable Action Records Filtering

Date Range:  To

Application:

Instrument:

User Account:

Action:

Search

Date	Account Type	User Name	Full Name	Host ID	Instrument Name	Application	Action	Comment
12-Sep-2022 14:47:12 PDT	Local	flexadmin	Sophia Frantz	USEUG-384C163	NA	SAE Administrator Console	Sign In Success	NA
12-Sep-2022 14:46:47 PDT	Local	Administrator	Default Administrator	USEUG-384C163	NA	SAE Administrator Console	Sign In Failure	NA
09-Sep-2022 13:38:21 PDT	Local	flexadmin	Sophia Frantz	USEUG-384C163	NA	SAE Administrator Console	Sign In Success	NA
09-Sep-2022 13:38:04 PDT	Local	Administrator	Default Administrator	USEUG-384C163	NA	SAE Administrator Console	Sign In Failure	NA
09-Sep-2022 13:37:45 PDT	Local	Administrator	Default Administrator	USEUG-384C163	NA	SAE Administrator Console	Sign In Failure	NA
09-Sep-2022 13:37:35 PDT	Local	Administrator	Default Administrator	USEUG-384C163	NA	SAE Administrator Console	Sign In Failure	NA
09-Sep-2022 13:37:27 PDT	Local	flexadmin	Sophia Frantz	USEUG-384C163	NA	SAE Administrator Console	Sign Out	NA
09-Sep-2022 13:32:25 PDT	Local	flexadmin	Sophia Frantz	USEUG-384C163	NA	SAE Administrator Console	Sign In Success	NA
09-Sep-2022 12:36:00 PDT	Local	flexadmin	Sophia Frantz	USEUG-384C163	NA	SAE Administrator Console	Sign In Success	NA
09-Sep-2022 12:35:51 PDT	Local	flexadmin	Sophia Frantz	USEUG-384C163	NA	SAE Administrator Console	Sign In Failure	NA

- (Optional) Select **Enable Action Records Filtering** to filter or sort the action records.
  - Select the **Date Range**, **User Account**, and **Action**, then click **Search**.  
The records display in the lower pane.
- (Optional) Select **Enable System Configuration Records Filtering** to filter or sort the system configuration records.
  - Select the **Date Range**, **User Account**, **Action**, **Record Type**, and **Record name**, then click **Search**.  
The records display in the lower pane.

- Click **Report** to generate an audit history report.  
The report is generated and saved to the default location set on your computer.
- View the report in the default system viewer or in a new tab of the web browser.
- Use the options in the viewer to manipulate the report as needed, then close the report.
- (Optional) To archive the action records or system configuration records, see “Archive audit records” on page 31.

## Use hash key to verify data integrity

Each time an assay result file or a system verification assay result file is generated, its unique file ID is recorded in the audit trail. The ID is generated based on the date, time, and instrument serial number, ensuring that each file ID is unique.

In addition, each time an assay results file or a system verification assay results file is *exported*, either as a PDF or CSV file, a hash value (checksum value) for the exported file is generated and recorded in the audit trail. A hash value/checksum value is a commonly used property of files that is updated whenever a change is made to a file. The hash value can be displayed using third-party software. If the hash value of the exported file matches the hash value in the audit trail, this means the file was not edited or renamed after leaving the Qubit™ Flex instrument.

Furthermore, the unique file ID of each file that is exported is included in the audit trail next to the export action and hash value. Thus, the actions taken to generate a data file on the Qubit™ Flex instrument can be traced with the unique file ID, and the hash key can be used to ensure that the data was not modified after it was exported from the instrument.

SAE Administrator Console									
<div> <a href="#">Users</a> <a href="#">Roles</a> <a href="#">System</a> <a href="#">Audit</a> <a href="#">e-Signature</a> <a href="#">Audit History</a> <a href="#">Settings</a> </div>									
<div> <div>English</div> <div>Jane Smith</div> </div>									
<div> <div>Enable Application Objects Filtering</div> </div>									
Application	Host ID	Instrument Name	Object Type	Object Name	Last Modified Date	Last Modified By	Last Modification Reason	Last Modification C	
Qubit™ Flex	qubitflex-2332622030093	QubitFlex	Standard/Sample	Run Assay	07-Sep-2022 17:10:29 PDT	flexadmin	NA	NA	
Qubit™ Flex	qubitflex-2332622030093	QubitFlex	Export Run	Export Assay Run	07-Sep-2022 17:09:27 PDT	flexadmin	NA	NA	
Qubit™ Flex	qubitflex-2332622030093	QubitFlex	Standard/Sample	Run Assay	07-Sep-2022 17:08:35 PDT	flexadmin	NA	NA	
Qubit™ Flex	qubitflex-2332622030093	QubitFlex	Delete Run	Delete Assay Run	07-Sep-2022 17:04:42 PDT	flexadmin	New reason	NA	
Qubit™ Flex	qubitflex-2332622030093	QubitFlex	Export Run	Export Assay Run	07-Sep-2022 17:03:10 PDT	flexadmin	NA	NA	
<div> <div>1</div> <div>20</div> <div>Items per page</div> <div>1 - 14 of 14 items</div> </div>									
<div> <div>Data Audits (1)</div> <div>e-Signature Records</div> </div>									
By	Full Name	Record Type	Record Name	Action	Changed Field	Old Value	New Value		
min	Sophia Frantz	Export Run	Export Assay Run	Add	File name	NA	QubitData_07-09-2022_17-09-26...		
					Checksum	NA	b0917eaff7ae0dc5a854e257e95...		
					File type	NA	CSV		
					Run ID	NA	070922-170833		

## Export audit records

You can export audit records to a TXT file for additional reporting outside of the SAE Admin Console.

- Display the records of interest as described. See “View audit histories” on page 29.
- In the **Action Records** view or **System Configuration** view, click **Export**.  
The TXT file with the audit records downloads to the default location set by your computer.

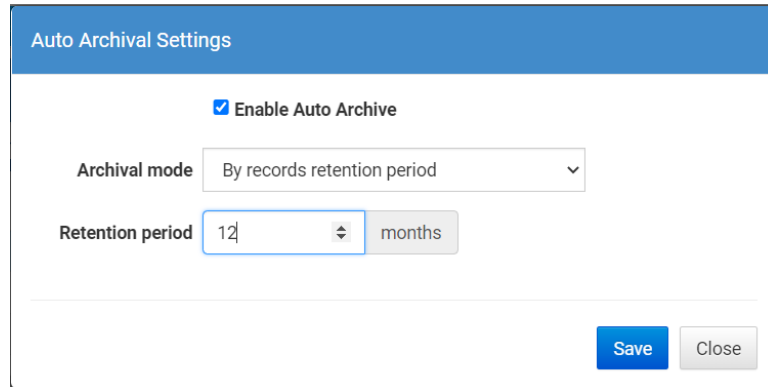
## Archive audit records

Archiving audit records removes the records from the SAE Admin Console and saves them in an internally specified location on the same computer on which the SAE Admin Console is installed.

Archived audit records are accessible for viewing in the SAE Admin Console.

### Archive audit records automatically

1. In the SAE Admin Console home screen, click the **Settings** tab, then select **Auto Archive** to open the **Auto Archival Settings** dialog box.



2. Select the **Enable Auto Archive** checkbox, then select the **Archival mode** and associated settings:
  - By number of records or retention period
  - By number of records
  - By retention period
3. Click **Save**.

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

### Archive audit records manually

1. In the SAE Admin Console home screen, click the **Settings** tab, then select **Archival history**.
2. Click **Ad-hoc Archive**, then select the start and end dates.
3. Click **Archive**.

# Manage the e-signature function

- Access the e-signature function screen ..... 32
- Configure the meanings of e-signatures ..... 33

The following procedures require an SAE Administrator account in the SAE Admin Console.

## Access the e-signature function screen

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

1. In the SAE Admin Console home screen, select the **e-Signature** tab.

SAE Administrator Console

English Jane Smith

Users Roles System Audit **e-Signature** Audit History Settings

IMPORTANT: Changing the e-Signature settings can affect opened files/records. Close any opened files/records before making changes to these settings.

☒ Enable e-Signatures

Show e-signature configuration for

Qubit™ Flex

e-Signature Meanings

Meanings	
Approved to run	Delete

+ New meaning

Data signed for selected meaning

Sign	Data
<input checked="" type="checkbox"/>	Standard/Sample
<input checked="" type="checkbox"/>	Verification Assay

Actions Requiring Signatures

Include	Action
<input checked="" type="checkbox"/>	Standard/Sample
<input checked="" type="checkbox"/>	Verification Assay

Number of signatures required for selected action

Meanings	Administrator	Intern	QubitFlex Administrator	QubitFlex Scientist
Approved to run	0	0	1	0

Apply Settings

2. Select the **Enable e-Signatures** checkbox, then select **Qubit Flex** from the **Show e-signature configuration for** dropdown list.

SAE Administrator Console

Users Roles System Audit **e-Signature** Audit History Settings

IMPORTANT: Changing the e-Signature settings can affect opened files/records. Close any opened files/records before making changes to these settings.

☒ Enable e-Signatures

Show e-signature configuration for

Qubit™ Flex



3. To modify your desired e-signature settings, see “Configure the meanings of e-signatures” on page 33.
4. Click **Apply Settings**.

## Configure the meanings of e-signatures

The e-signature meanings are the text that a user can select to describe a reason for an e-signature. The Qubit™ Flex SAE module is installed with one default meaning: **Approved to run**.

### Add an e-signature meaning

1. In the **e-Signature Meanings** pane of the **e-Signature** tab, click **New Meaning**.
2. Enter an e-signature meaning in the **Name** field, then click **Save**.
3. Click **Apply Settings**.

### Delete an e-signature meaning

1. In the **e-Signature Meanings** pane of the **e-Signature** tab, select a meaning from the **Meanings** list, then click **Delete**.

**Note:** The default meaning (**Review and Approve Image and Data**) cannot be deleted.

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

### Select the actions that require e-signatures

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

Action	The software requires e-signatures when a user...
Standards/sample	Selects new or existing standard calibration to perform an assay run.
Verification assay	Starts a system verification assay run.

Actions Requiring Signatures

Include	Action
<input checked="" type="checkbox"/>	Standard/Sample
<input checked="" type="checkbox"/>	Verification Assay

Number of signatures required for Standard/Sample

Meanings	Administrator	Intern	QubitFlex Administrator	QubitFlex Scientist
Approved to run	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="0"/>
New custom eSignature meaning	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

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

# 6

## Manage the SAE export-import function

- Export and import user, system security, audit, and e-signature settings ..... 35

The following procedures require an SAE Administrator account in the SAE Admin Console.

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

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

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

1. In the **Settings** dropdown list, select **Export Configuration** to open the **Export Configuration** dialog box.

2. In the **Export Configuration** dialog box, select one of the following options:
  - a. **All** to export all configuration settings, including user accounts.

b. **Custom** to export the following:

- **Users & Roles**—Exports all user accounts with "Active" status, as well as all user roles and their associated permissions.
- **System & Roles**—All system settings and all user roles, as well as their associated permissions.

3. Click **Export**.

The exported file (DAT) is downloaded to the default location set on your computer.

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

1. In the **Settings** dropdown list, select **Import Configuration**.

2. Click **Choose File** to choose the DAT file with the desired configuration settings.

3. Select the import options:

a. **All** to import all configuration settings, including user accounts.

b. **Custom** to import the following:

- **Users & Roles**—Imports all user accounts with "Active" status as well as all user roles and their associated permissions.
- **System & Roles**—All system settings and all user roles and their associated permissions.

4. Click **Import**.

---

**Note:** If you have selected **All** or **Users & Roles**, it is possible that the imported user accounts already exist in the SAE module. Select **Skip** or **Overwrite** for each user account, then click **Confirm and Import**.

---



# Install and use the SAE module on board the Qubit™ Flex instrument

■ Security, Auditing, and E-signature (SAE) for the Qubit™ Flex instrument .....	37
■ Set up SAE mode on the Qubit™ Flex instrument .....	38
■ Configure the SAE functions on the Qubit™ Flex instrument .....	46

## Security, Auditing, and E-signature (SAE) for the Qubit™ Flex instrument

---

**IMPORTANT!** 21 CFR part 11 is a regulation that describes the criteria for acceptance by the U.S. Food and Drug Administration (FDA) for electronic records and electronic signatures. Part 11 is composed of procedural and technical requirements. Procedural requirements are the standard operating procedures instituted by the end user (for example, ensuring proper training of personnel), and technical requirements are the functional characteristics of the compliance management software used.

---

This section is intended to provide instructions for using Security, Auditing, and Electronic Signature (SAE) on board the Qubit™ Flex instrument. Security, Auditing, and E-signature (SAE) software provides the tools necessary for supporting 21 CFR Part 11 technical compliance including:

- Creating and maintaining user accounts
- Managing and enforcing password policies of all accounts
- Assigning, managing and enforcing access rights to all accounts
- Documenting and maintaining audit and e-signature histories
- Permitting e-signature approval to proceed with actions

To implement the Qubit™ Flex SAE Software Solution for 21 CFR Part 11 support on Qubit™ Flex instruments, you need the following components installed, activated, and communicating:

- **SAE Admin Console and Qubit™ Flex Application Profile** – This should be downloaded and running on a laptop connected to a stable IP address. The console is opened in a web browser and used to configure the SAE settings for Qubit™ Flex instruments. The console is generalized for use with a variety of Thermo Fisher Scientific instruments, so the settings specific to the Qubit™ Flex Fluorometer must be imported to the SAE console with the **Qubit™ Flex Application Profile (DAT file)**.
- **Qubit™ Flex instrument firmware version 1.7.0 (or later)** – Software update for the Qubit™ Flex instrument that adds the ability to activate security, audit, and e-signature features.
- **Qubit™ Flex SAE License** – The SAE features are provided in firmware version 1.7.0 and later, but a license is needed to activate these features. Ensure that the serial number in the name of the license file matches the serial number of the Qubit™ Flex instrument.

---

**Note:** For details on accessing Qubit™ Flex SAE Software Solution downloads and resources, see “Related documentation” on page 50.

---

## Set up SAE mode on the Qubit™ Flex instrument

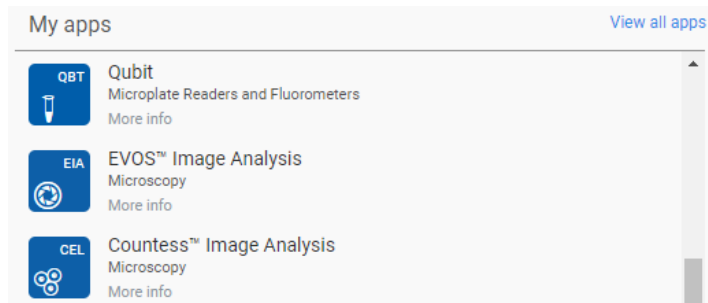
### Update the Qubit™ Flex software

1. Download the most recent Qubit™ Flex software (version 1.7.0 or later) to a USB drive. You can find the software updates on the web page “Technical Resources for Qubit™ Fluorometers” at [thermofisher.com/qubitresources](https://thermofisher.com/qubitresources).
2. Sign in to the local instrument or your Thermo Fisher™ Connect Platform account.
3. Access **Settings**, then click **Software Update**.
4. Insert the USB drive with the Qubit™ Flex software (version 1.7.0 or later) update file.
5. Select the software update file, then click **Install**.

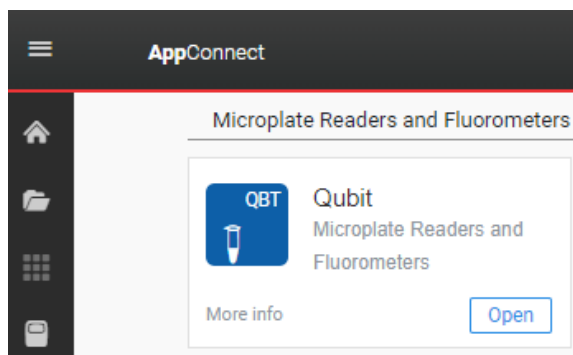
### Generate a license key

1. Purchase a license key at [thermofisher.com/qubitflexcfr](https://thermofisher.com/qubitflexcfr). Check the e-mail linked to your account for the receipt of the purchase, which contains the Order ID needed to download the license.
2. Go to [apps.thermofisher.com](https://apps.thermofisher.com) and sign in to your Thermo Fisher™ Connect Platform account.

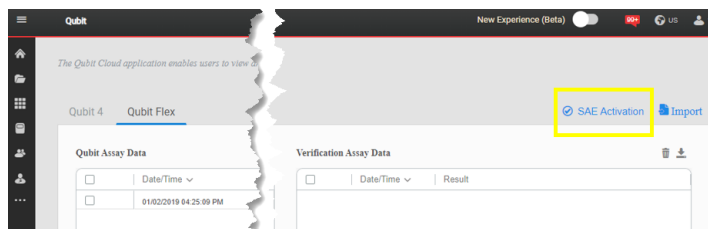
3. Open the **Qubit App** from the **My Apps** pane of the Connect Platform **Home** page.



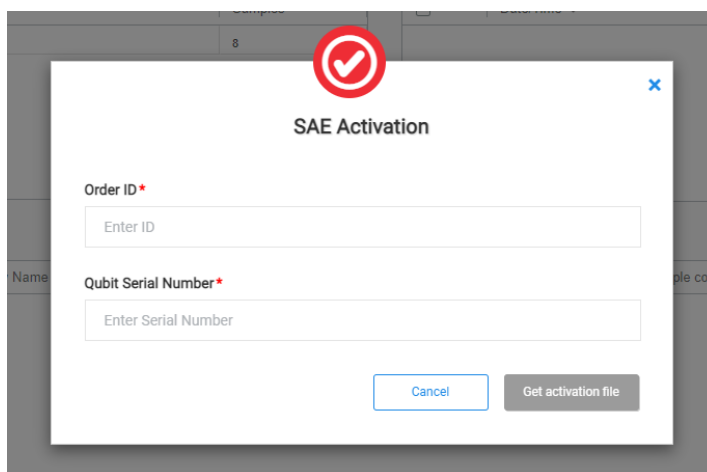
**Note:** If the **Qubit App** has not been opened before and it is not displayed on the Connect Platform **Home** page, click **View All Apps** and locate the **Qubit App** from the list of apps.



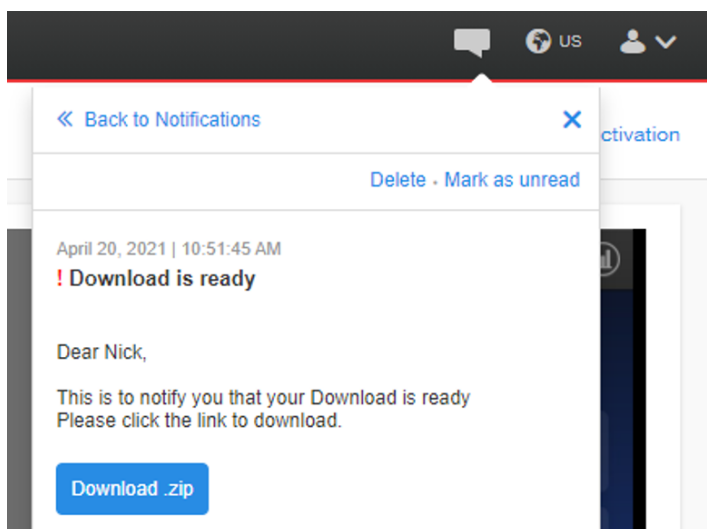
4. Click the **SAE Activation** link in the top-right corner of the page.



5. Enter the Order ID and the Qubit™ Flex instrument serial number into the appropriate fields. Select **Get activation file**. The **Request Submitted** message is displayed when the order information has been validated.

A screenshot of a web form titled "SAE Activation". At the top center is a red circular icon with a white checkmark. Below the title, there are two input fields. The first is labeled "Order ID\*" and contains the placeholder text "Enter ID". The second is labeled "Qubit Serial Number\*" and contains the placeholder text "Enter Serial Number". At the bottom right of the form are two buttons: a blue "Cancel" button and a grey "Get activation file" button.

6. When the file is ready, the **Download is Ready** notification is displayed in the top-right corner. Click on the notification, then select **Download.zip** to begin the license key file download to your computer.





## Activate a license key

This procedure requires a local instrument profile and an SAE Administrator account.

Before SAE mode is enabled on the Qubit™ Flex instrument for the first time, we recommend running an instrument qualification using Installation Qualification/Operational Qualification/Performance Qualification (IQ/OQ/PQ).

1. Back up all data before activating the license key and enabling SAE mode. When enabling SAE mode, data generated in non-SAE mode is deleted.

---

**Note:** When disabling SAE mode, data generated in SAE mode is hidden but not deleted. The data generated in SAE mode is only visible when SAE mode is enabled. This ensures all SAE mode data is accounted for in the audit trail.

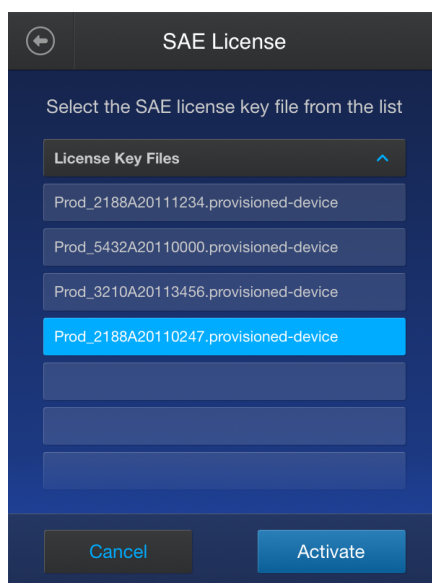
---

2. Sign in to your local instrument profile on the instrument.
3. Tap **Settings** on the bottom-right side of the **Home** screen.
4. Tap **SAE Mode**.
5. Insert a USB device containing your license into a USB port on the instrument, then tap **Next**. For instructions on how to purchase and download your license, see “Generate a license key” on page 38.
6. Select the license key file that matches the serial number of your instrument, then tap **Activate**.

---

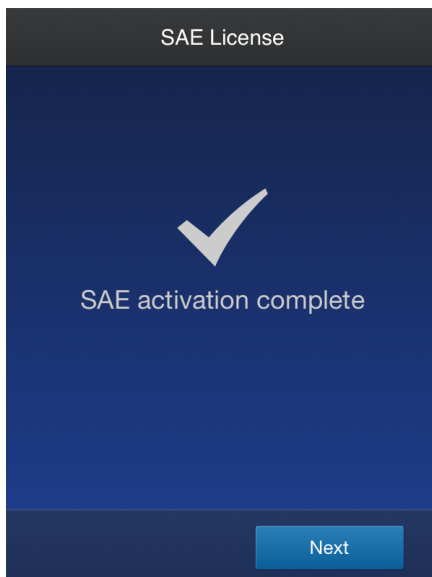
**Note:**

- If you purchased multiple license keys, be sure to choose the correct key. The instrument will verify that the serial number of the instrument matches the serial number in the license key.
  - If you purchased multiple licenses, contact Technical Support.
- 



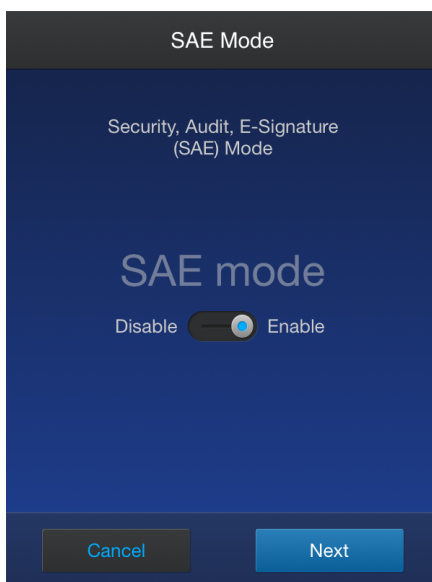
7. Tap **Activate** in the confirmation dialog box to confirm that you want to activate SAE mode using the selected license.

If the activation is successful, the instrument will display **SAE activation complete**. If the activation failed, confirm the instrument serial number in the license matches the serial number of the instrument, then select the correct license key.



8. Tap **Next**.

9. In the **SAE Mode** dialog box, toggle to enable SAE mode, then tap **Next**.



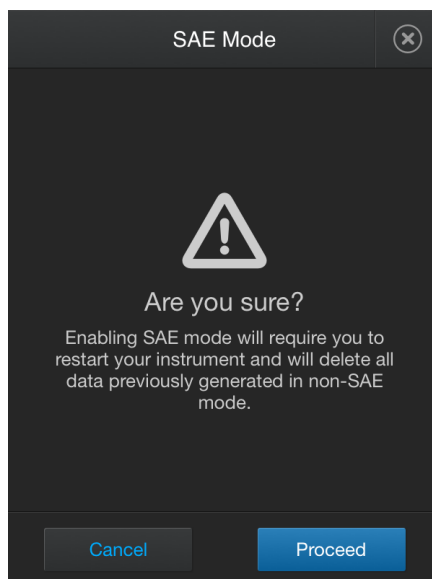
10. Ensure all data previously generated in non-SAE mode is exported from the instrument.

---

**Note:** Data that is generated in non-SAE mode will be deleted after SAE mode is enabled. Conversely, data that is generated in SAE mode is hidden in non-SAE mode but not deleted.

---

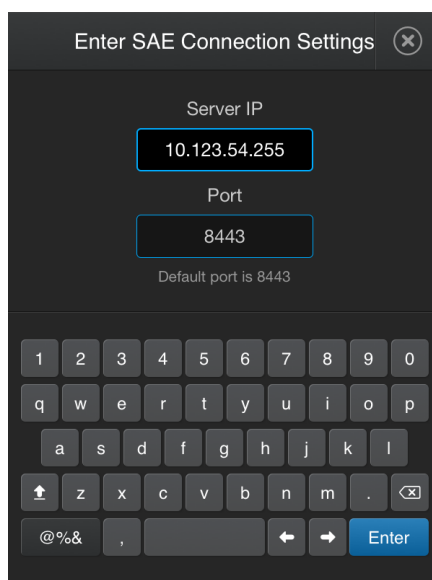
11. In the confirmation dialog box, tap **Proceed**.



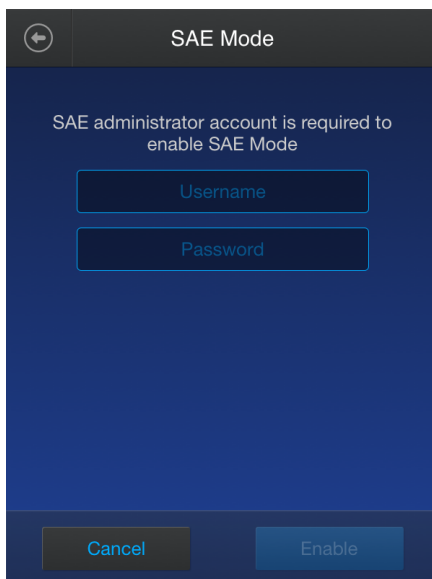
12. Enter the IP address and port number of the SAE Admin Console, then tap **Next**.

**Note:**

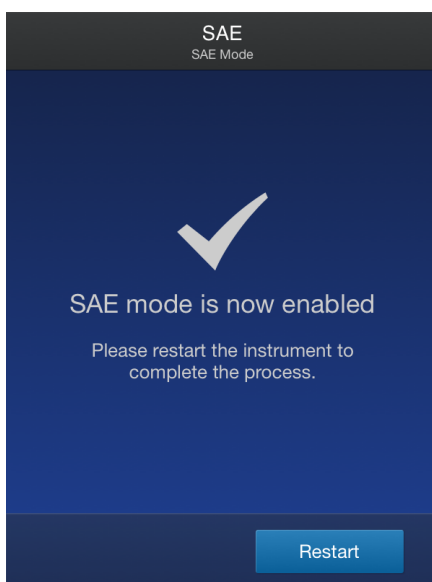
- To find the IP address, enter *ipconfig* on a command prompt or terminal (IPv4), then press **Enter**.
- The SAE Admin Console should be configured with a static IP address to ensure a reliable connection to the instrument.



13. Enter the user name and password of the SAE Administrator, then tap **Enable**. By default, only an SAE Administrator user can activate SAE mode on an instrument.



After successful connection, the instrument will restart.



## Enable SAE mode on the instrument

This procedure requires an SAE Administrator account.

1. Tap **Settings** located on the bottom-right side of the **Home** screen.
2. Tap **SAE mode**.
3. Toggle to enable SAE mode, then tap **Next**.

4. Enter the IP address of the server and the port of the SAE console location, then tap **Next**.

---

**Note:** The IP address and port location are available in the address bar of the SAE Admin Console. Alternatively, the IP address can be found by entering *ipconfig* on a command prompt or terminal (IPv4).

---

**IMPORTANT!** We strongly recommend connecting the computer that is hosting the SAE Admin Console to a stable IP address.

---

5. Enter the user name and password of the SAE Administrator, then tap **Enable**.

---

**Note:** Data that is generated in non-SAE mode will be deleted after SAE mode is enabled.

---

## Disable SAE mode on the instrument

This procedure requires an SAE Administrator account.

1. Sign in to the instrument with an SAE Administrator account.
2. Tap **Settings** on the bottom-right side of the **Home** screen.
3. Tap **SAE mode**.
4. Toggle to disable SAE mode, then tap **Next**.
5. Depending on user-assigned permissions, the SAE Administrator may need to enter their credentials, then tap **Disable** to continue, or **Cancel** to keep the SAE mode enabled.

---

**Note:** When disabling SAE mode, data generated in SAE mode is hidden in non-SAE mode but not deleted.

---

## Configure the SAE functions on the Qubit™ Flex instrument

### Disable SAE mode when connection to the SAE Admin Console is lost

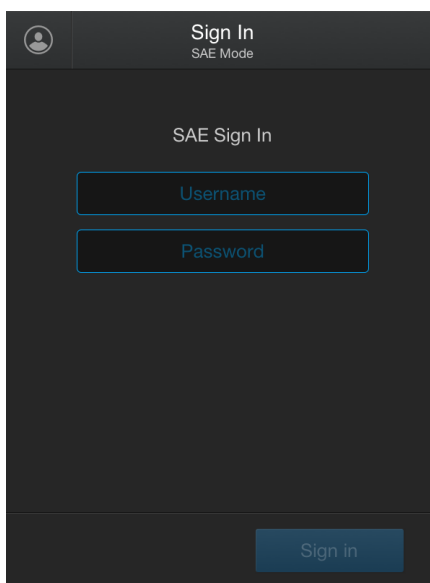
---

**Note:** We recommend using this procedure **only** when it is necessary to disable SAE mode and a network connection cannot be re-established. To maintain a complete audit history, we recommend that you disable SAE mode using an authorized SAE account.

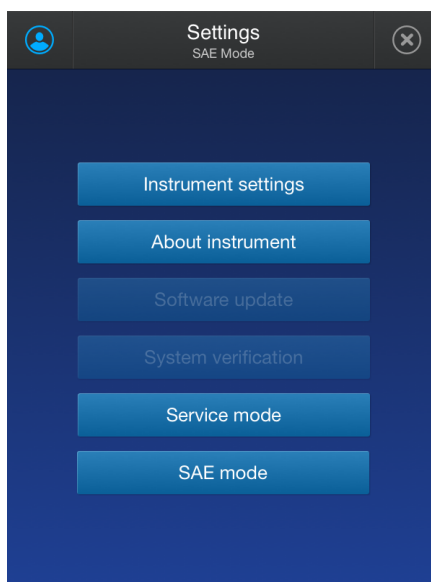
---

Connection to the SAE Admin Console is required to disable SAE mode from an SAE user account. If the connection is lost, use the following procedure to disable SAE mode using a local instrument account.

1. In the **Sign In** screen, tap  (**Profile**).



2. Select your local instrument profile, enter your PIN, then tap **Sign In**.  
Local instrument profiles can only disable SAE mode and reset instrument settings (recommended for service representatives only); all other instrument actions are disabled.



3. Tap **SAE Mode**.
4. Toggle to disable SAE mode, then tap **Next**.

---

**Note:** Data that is generated in SAE mode is hidden in non-SAE mode but not deleted.

---

## Sign in to an instrument in SAE mode

---

**Note:** Your system administrator uses the SAE Admin Console to create SAE accounts. The functions that you can perform in the instrument software are based on the role that an SAE Administrator assigns to your SAE account. For more information, see “Create or edit a user role” on page 14 and “Default permissions and roles” on page 16.

---

In the **Sign in** screen, enter your SAE account user name and password, then tap **Sign in**.

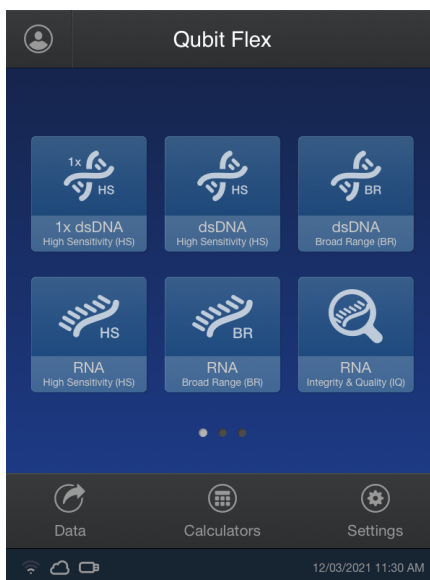
---

**Note:**

- After signing in, you may be prompted to change your SAE password.
  - A password cannot contain the following symbols: + & % \ ~ ' ^
-

## Change password on an instrument in SAE mode

1. In the **Home** screen, tap  (**Profile**).



2. Tap **Edit**, then enter your old password.
3. Enter a new password, then confirm the new password.

---

**Note:**

- A password cannot contain the following symbols: + & % \ ~ ' ^
  - A password must meet the complexity requirements set by an SAE Administrator in the SAE Admin Console.
  - If you exceed the maximum number of sign-in attempts, you will be temporarily locked out of your account. The default permissions for an Administrator role allow sign-in after automatic logout.
  - The functions that you can perform in the instrument software are based on the role that an SAE Administrator assigns to your SAE account.
-



Change Password

SAE Mode

×

Your password has expired. Create a new password to access SAE mode

Username 01

Old password

New password

Confirm password

☐ Show password

Cancel

Update



# Documentation and support

## Related documentation

Document	Publication number	Description
<i>Qubit™ Flex Fluorometer User Guide</i>	MAN0018186	Describes the hardware and software and provides information on preparing, maintaining, and troubleshooting the system.

## Customer and technical support

Visit [thermofisher.com/support](http://thermofisher.com/support) for the latest service and support information.

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

---

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

---

## Limited product warranty

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

