

SAE Admin Console v2.2

USER GUIDE

for use with iBright™ Imaging Systems and iBright™ Analysis
Software – Secure

Publication Number MAN0019446

Revision B



Thermo Fisher Scientific | 3747 N. Meridian Road | Rockford, Illinois 61101 USA

For descriptions of symbols on product labels or product documents, go to thermofisher.com/symbols-definition.

Revision history: MAN0019446 B (English)

Revision	Date	Description
B	9 April 2025	Updated guide due to software updating from version 2.0 to version 2.2.
A	28 August 2020	New document for SAE Admin Console for iBright™ Imaging Systems and iBright™ Analysis Software – Secure.

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.

Important Licensing Information: This product may be covered by one or more Limited Use Label Licenses. By use of this product, you accept the terms and conditions of all applicable Limited Use Label Licenses.

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.

©2020-2025 Thermo Fisher Scientific Inc. All rights reserved.

Contents

■ CHAPTER 1	Security, Audit, and Electronic Signature	6
	Network and password security requirements	6
	iBright™ SAE Software Solution for 21 CFR Part 11 compliance	7
	SAE Administrator Console	7
	Components of the SAE functions	8
	SAE Admin Console v2.2 features	8
	Additional information	8
	Firewall ports	9
	Third-party software	9
	Local web browser interface and database record storage	10
	File and database locations	10
■ CHAPTER 2	Manage SAE user accounts and roles	11
	Enable the SAE Admin Console	11
	Overview of warning screens	12
	Installation of iBright™ Imager and Analysis Software profiles	14
	SAE Administrator Console installation requirements	15
	Determine the logged-in user	15
	Create a user account	15
	Edit a user account	16
	Activate a suspended user account	16
	Disable (inactivate) a user account	16
	Reset a forgotten password	17
	Change password	17
	Create or edit a user role	17
	Create a user role	17
	Permissions and default user roles	18
	Edit a user role	18
	Delete a user role	19
	Generate, view, and print a user or role report	19

■	CHAPTER 3	Manage the system security function	20
		Access the system security function screen	20
		Configure account setup and security policies	20
		Set up messaging notifications	22
		Set up SMTP configuration	23
■	CHAPTER 4	Manage the audit function	24
		Use the Audit function screen	24
		Select items to audit	25
		Configure audit reason settings	25
		Generate audit reports	26
		Display audit histories	26
		Review the system configuration	26
		Review the action log	27
		View audit histories from the Audit History drop-down menu	28
		When to archive records	28
		Archive and restore audit records	29
		Set up an automatic archive of audit records	30
		Archive/backup options and frequency	30
		Restore archived audit records	30
		Restore exported archived audit records	31
		Archive/backup options and frequency	31
		When to archive records	31
		Set up an automatic archive of audit records	32
		Manually archive audit records	32
		Back up the SAE program folder	33
		Restore archived audit records	33
		Restore exported archived audit records	34
■	CHAPTER 5	Manage the e-signature function	35
		Access the e-signature function screen	35
		Configure the meanings of e-signatures	35
		Add an e-signature meaning	35
		Delete an e-signature meaning	36
		Select the actions that require e-signature	36
■	CHAPTER 6	Manage the SAE export-import function	37
		Export and import user, system security, audit, and e-signature settings	37
		Export user, system security, audit, and e-signature settings	37
		Import user, system security, audit, e-signature settings	38

Documentation and support 39

 Related documentation 39

 Obtain information from the Help System 39

 Customer and technical support 39

 Limited product warranty 40



Security, Audit, and Electronic Signature

■ Network and password security requirements	6
■ iBright™ SAE Software Solution for 21 CFR Part 11 compliance	7
■ SAE Administrator Console	7
■ Additional information	8
■ Firewall ports	9
■ Third-party software	9
■ Local web browser interface and database record storage	10
■ File and database locations	10

The Security, Audit, and Electronic Signature (SAE) Administrator Console (Admin Console) is available for many instruments and software from Thermo Fisher Scientific, including but not limited to QuantStudio™, Attune™ NxT, and iBright™ Imaging Systems.

This guide describes the procedures that an administrator performs to configure and manage the SAE features of the iBright™ Imaging Systems and iBright™ Analysis Software-Secure.

User interaction with the SAE Admin Console is described in *iBright™ CL750 Imaging System User Guide* (Pub. No. MAN0018652), *iBright™ Imaging Systems User Guide* (Pub. No. MAN0018592) and *iBright™ Analysis Software-Secure Help Guide* (Pub. No. MAN0019528).

Network and password security requirements

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.

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 into 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, however, 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

Note: We recommend using a password manager to help in creating secure passwords.

iBright™ SAE Software Solution for 21 CFR Part 11 compliance

21 CFR part 11 is 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 Invitrogen™ iBright™ SAE Software Solution for 21 CFR Part 11 consists of:

- **SAE Administrator Console**— Used to configure the Security, Audit and e-Signature settings on SAE module
- **iBright™ SAE License**— Used to activate the SAE settings for the iBright™ instrument and iBright™ Analysis Software-Secure
- **iBright Instrument SAE mode**— Instrument firmware connected with SAE Administrator Console
- **iBright Analysis Software – Secure**— Desktop analysis software connected with SAE Administrator 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.

SAE Administrator Console

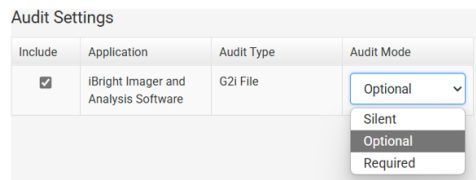
The SAE Admin Console is a component of the iBright™ Imaging and Analysis System 21 CFR Part 11 support software that allows you to configure the iBright™ Imager and Analysis Software to meet specific requirements. The SAE Admin Console provides the following functionality:

- **System Security** – Controls user access to the software. Two default Administrator user accounts are provided, one with full privileges and the other with no privileges. Additional user accounts and permissions can be user-defined.
- **Auditing** – Tracks actions performed by users, and changes to the SAE module settings. The software automatically audits some actions silently. You can select other items for auditing and specify the audit mode. The auditing function provides reports for audited SAE module changes and actions.
- **Electronic signature (e-signature)** – Determines if users are required to provide a username and password when performing certain functions. You can configure e-signature so that a user can export a signed g2i file and print a signed report. You can also configure the e-signature event to require multiple signatures and to require users with specific permissions to sign.

Components of the SAE functions

The SAE is a client-server software configuration that includes 4 components:

- **Enable Audits:** By default, audits are enabled. If unchecked, the user can open and edit on-board the imager but cannot commit any of the changes.
- **Audit Settings:** By default, the iBright™ Imager and Analysis Software is enabled. When the selection box is unchecked, there is no noticeable difference.



- **Audit Mode:** By default, the audit mode is set to optional.
- **SAE screens (client):** 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.

SAE Admin Console v2.2 features

SAE Admin Console v2.2 software adds the following options:

- Convert the URL to an **https://** address prefix on port 8443 (see “Enable the SAE Admin Console” on page 11 and “Firewall ports” on page 9).
- Create an A4 report (see “Configure account setup and security policies” on page 20).
- Select a language (see the SAE Admin Console top toolbar for language choices selectable from a dropdown list).
- Verify the username and password are not the same for any user (see “Configure account setup and security policies” on page 20).
- Check for compromised phrases as passwords (see “Configure account setup and security policies” on page 20).

Additional information

Time difference for server connection	• The time difference between the SAE Administrator Console and the iBright Analysis Software (computer) must be less than 5 minutes to login to the software. If the time difference is more than 5 minutes, an error will display. • The time difference between the SAE Administrator Console and the iBright Imaging System must be less than 5 minutes to enable SAE mode on board the iBright instrument. If the time difference is greater than 5 minutes, an error message will display: Clock Skew Error: Unable to connect to server. Client clock skew is too large. Check and synchronize client and server clock.
---------------------------------------	--

Minimum computer requirements	• Operating system: Windows™ 10 (64-bit version) • Intel™ Core processor or compatible • Memory with minimum of 16 GB RAM • Hard drive with minimum of 20 GB storage • Monitor with 1,280 x 1,024 or greater pixel resolution • Ethernet port for directly connecting to instrument • Microsoft™ Excel™ Software • Browser options: – Google™ Chrome™ Software (v40 or later) – Mozilla™ Firefox™ Software (v40 or later) – Microsoft™ Edge™ Antivirus Software • IMPORTANT! The optional computer available from Thermo Fisher Scientific does not include antivirus software because customer preferences and network requirements vary. You are responsible for installing the antivirus software of your choice to protect the computer against viruses.
Antivirus software options	The following software has been tested for use with the optional computer: • Symantec™ Endpoint Protection • Norton™ Internet Security • Microsoft™ Defender Antivirus Software

Firewall ports

The firewall ports must be open on the server computer to establish a connection between the SAE Admin Console and the iBright™ analysis software or instrument. The port selection is dependent on the version of SAE Admin Console being used:

- For SAE Admin Console v2.0, use port 8201.
- For SAE Admin Console v2.2, use port 8443.

Opening a firewall port on the SAE Admin Console depends on which anti-virus software is installed:

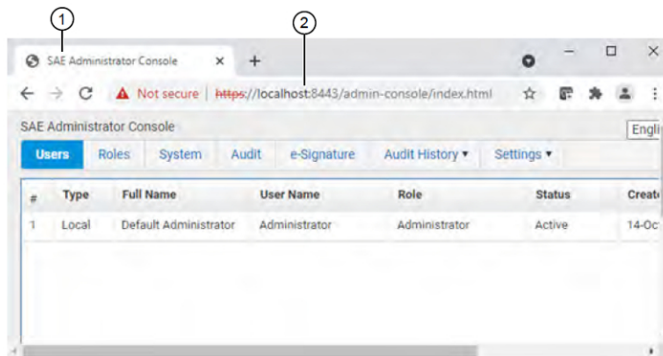
- For Symantec™ Endpoint Protection, no further action needed.
- For Norton™ Internet Security, use the Settings menu to open the port.
- For Microsoft™ Defender Antivirus Software, add inbound rules for the port and apply to all profiles.

Third-party software

Before installing third-party software on the computer running the SAE Admin Console software, confirm the third-party software does not restrict Ethernet communication or interfere with instrument or computer operation.

Local web browser interface and database record storage

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



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

File and database locations

- The SAE Administrator Console files are installed in <C:\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 C:\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 C:\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 “Archive/backup options and frequency” on page 30.



Manage SAE user accounts and roles

■ Enable the SAE Admin Console	11
■ Installation of iBright™ Imager and Analysis Software profiles	14
■ SAE Administrator Console installation requirements	15
■ Determine the logged-in user	15
■ Create a user account	15
■ Edit a user account	16
■ Activate a suspended user account	16
■ Disable (inactivate) a user account	16
■ Reset a forgotten password	17
■ Change password	17
■ Create or edit a user role	17
■ Generate, view, and print a user or role report	19

Enable the SAE Admin Console

The SAE Admin Console is available for download from thermofisher.com/ibright-sae-component-download.

1. Install the program and launch the application.

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

Note: Make a note of the server or local host IP address if on your computer.

2. Enter the Administrator **User Name** and **Password**, then click **Sign in**.

Note: The initial username and password are both "Administrator". After signing in, you will be prompted to change your password. The following symbols cannot be used in the password as they are not compatible with the iBright™ Instruments: + & % \

IMPORTANT! The administrator password cannot be recovered after being set. If you cannot remember the password, the software must be uninstalled, then reinstalled. All of the information, including application profiles, roles, permissions, SAE accounts, audit records, and e-signatures are lost when the software is uninstalled.

Note: A warning screen can display. See "Overview of warning screens" on page 12 for more information.

3. If messaging notifications are enabled (see "Set up messaging notifications" on page 22), the **Event Notifications** dialog box is displayed. With the dialog box displayed:
 - a. Select the checkboxes for the events, then click **Acknowledge** to remove the selected events from the list.
 - b. Click **Close** to close the dialog box and retain the events in the list.

Note: If the notifications are retained, they will be displayed the next time a user logs in to the SAE Administrator Console. They can also be viewed from the main screen (see "Set up messaging notifications" on page 22).

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

Overview of warning screens

If a security or warning screen is displayed at start up, that screen can be bypassed. See the following sections for more information:

- "Warning for the Google Chrome™ browser" on page 13
- "Warning for the Mozilla™ Firefox™ browser" on page 13
- "Warning for the Microsoft™ Edge™ browser" on page 14

After bypassing the security or warning screen, the browser can 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 also 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" message displays.
 - Click **Advanced** ▶ **Proceed to <domain name> (unsafe)** to proceed to the next steps.
- 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" message displays.
 - Click **Advanced** ▶ **Accept the Risk** ▶ **Continue** to proceed to the next steps.
- 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 in the Microsoft™ Edge™ browser, the warning message is not displayed (for the localhost domain only).

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

Warning for the Microsoft™ Edge™ browser

- Launch the SAE Administrator Console. The "Your connection isn't private" message displays.
- Click **Advanced** ► **Continue** to <domain name> (unsafe) to proceed to the next steps.
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 not displayed (for the localhost domain only).

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

Installation of iBright™ Imager and Analysis Software profiles

The iBright™ Imager and Analysis Software application profile is available for download from <http://thermofisher.com/ibrightanalysis>.

1. Download the iBright™ Imager and Analysis Software application profile.
 - Application profiles have the following naming convention: **<Applicationname>(<Applicationprofileversionnumber>).dat**
 - File format for an application profile is DAT.
 - The following file name is an example of the application profile for v1.0.0 of the iBright™ Imager and Analysis Software:
iBright™ Imager and Analysis Software (1.0.0).dat
2. In the SAE Administrator Console main screen, click **Settings** ► **Manage Application Profiles**.
3. Click **Install Application Profile**.
4. In the **Install Application Profile** dialog box, click **Choose File**.
5. Select the application profile. The application file is a DAT file.
6. Click **Verify Data File**.
7. Review the information in the **Install Application Profile** dialog box, then select the **Install new application** checkbox.
8. Click **Install**.
9. Click **Verify Data File** ► **Install new application** ► **Install**.

SAE Administrator Console installation requirements

- For the SAE Administrator Console, we recommend using a dedicated computer that meets minimum requirements. See “Additional information” on page 8 for more information.
- Only one SAE Administrator Console can be installed per 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 single application software can be installed on the same computer as the SAE Administrator Console. For multiple application softwares, a separate computer is recommended.

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 recorded in the **Action Records** under **Audit History** in 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 drop down menu by **Role**. To create custom roles, see “Create or edit a user role” on page 17.

Note: Two default roles (iBright Administrator and iBright Scientist) are automatically included in the **Application Profile**.

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

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

Edit a user account

1. In the **Users** tab, select a user account, then click **Edit**.
2. Edit the settings as desired.

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

3. Click **Save**.

Activate a suspended user account

Suspended status is applied to a user account to disable access for a brief period (account suspended if number of sign-in attempts exceeds the threshold or if the console administrator suspends that 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

Inactive status is applied to a user account to disable access for an extended time. For example, it is used when a user role has changed and the new role is not approved for SAE system use.

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! 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 to prevent loss of the data after reinstallation. For more information, see Chapter 9, “Advanced configuration options”.

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.
4. Click **Save**.

Change password

1. From the  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 as they are not compatible with the iBright™ Instruments: + & % \

Create or edit a user role

User roles determine the permissions associated with a user account. The iBright™ Imager and Analysis Software SAE module provides two default user roles:

- iBright Administrator
- iBright Scientist

Create a user role

In the **Roles** tab, you can create new roles with customized settings, modify the **iBright Administrator** and **iBright 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**.
2. Enter a role name and (*optional*) description.

3. Select permissions (see “Permissions and default user roles” on page 18). To select all permissions in a category, select the check box next to the category.

Note: Operations not shown in the table “Permissions and default user roles” on page 18 are available to all user roles.

4. Click **Save**.

Permissions and default user roles

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

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

Table 1 Conferrable permissions and default user roles

Permissions		Default roles		
Category	Function	SAE Admin	iBright Admin	iBright Scientist
Image Management on iBright Instrument	Acquire, Adjust, Analyze, Delete, and Export image	Yes	Yes	Yes
Image Management on iBright Analysis Software	Import non-SAE File, Adjust, Analyze, Crop, Delete, Annotate and Export image	Yes	Yes	Yes
iBright™ Instrument and Analysis Software Security configuration	Sign g2i file, unlock g2i file	Yes	Yes	Yes
	Enable SAE mode on instrument	Yes	No ^[1]	No
	Disable SAE mode on instrument	Yes	Yes	No
Instrument configuration	Administer instrument, Update instrument System Configuration	Yes	Yes	No
Service tools	Instrument Diagnostic, Pixel Mapping, and Export Workspace	Yes	Yes	No
SAE Administrator Console	Configure Security and Auditing, View and manage audit History	Yes	No	No

^[1] By default the iBright™ Admin role cannot enable SAE mode on board the iBright Imager. The iBright™ Admin Role can be given this privilege if the SAE Admin Console Administrator changes their role privileges.

Edit a user role

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

Note: The Administrator and No Privileges roles cannot be edited.

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. Access the report, save, then print the report.
3. Close the report.



Manage the system security function

■ Access the system security function screen	20
■ Configure account setup and security policies	20
■ Set up messaging notifications	22
■ Set up SMTP configuration	23

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**.

Configure account setup and security policies

In the **Systems** tab, specify **User Name Settings**, **Password Policy**, **Account Lockout Policy**, **Other Settings**, and **Password Settings**.

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

1. In the **Username Settings** pane, enter the minimum and maximum number of characters for a username.

Note: The minimum and maximum number of allowed characters are 1 and 256, respectively. Care must be taken to ensure that the user name restrictions are similar on both the SAE Admin Console and the iBright™ instrument and Analysis Software.

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. Care must be taken to ensure that the password restrictions are similar on both the SAE Admin Console and the iBright™ Instrument and Analysis Software.

- 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 and enter the minimum number of occurrences for that rule.

Note: Ensure that the complexity rules set here are compatible with the iBright™ Instrument and Analysis Software.

Note: Do not use the following symbols in the password as they are not supported by iBright™ Instrument and/or iBright™ Analysis Software: + % & \

- d. Enter the maximum and minimum number of days for which the password is valid.
- e. Enable or disable the **Password expiry** reminder.

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

- f. **Username check:** Enabled/disabled to prevent the user from using the username as a password.
- g. **Compromised phrase check:** Enabled/disabled to prevent the user from using an unsafe phrase as a password.

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 Account lockout. If enabled, when the threshold for sign-in attempts is reached, the account will lockout for the specified lockout duration.
- d. Enter the **Reset account lockout** duration in minutes.

4. In the **Other Settings** pane:

- a. Enable or disable **Client offline sign in**.

Note: If you select **Enabled**, enter the **Offline sign-in threshold** in minutes

- b. The report page size can be toggled between A4 and Letter sizes.

Automatic screen locking, Inactivity duration, and Open file from non-SAE systems options are not currently enabled through SAE Admin Console for the iBright™ instrument and Analysis Software.

The inactivity period for automatic screen locking and automatic user log out can be set on the iBright™ instrument directly.

iBright™ Analysis software is a desktop-based application that uses the computer settings for screen locking.

Files from non-SAE systems cannot be opened on the iBright™ instrument however, these file(s) can be imported into the iBright™ analysis software after confirming the intent. Upon import, the file is converted to an SAE file.

5. In the SAE Admin Console title bar, select the language.
6. 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 menu, select **Notifications**.
2. In the **Edit Notifications Settings** dialog box, select the events for notification:

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

3. Select the notification method:

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

4. Click **Save**.

Set up SMTP configuration

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

1. Click **Settings**, then **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**.



Manage the audit function

■ Use the Audit function screen	24
■ Display audit histories	26
■ View audit histories from the Audit History drop-down menu	28
■ Archive/backup options and frequency	31
■ Set up an automatic archive of audit records	32
■ Manually archive audit records	32
■ Back up the SAE program folder	33
■ Restore archived audit records	33
■ Restore exported archived audit records	34

Use the Audit function screen

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

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

Note: The **Enable Audits** option does not apply to iBright™ Imager and Analysis Software applications. Audits are always enabled in this application even if the **Enable Audits** option is deselected.

1. Select the **Audit** tab.
2. Set or modify the **Audit Settings** (see “Select items to audit” on page 25 and “Configure audit reason settings” on page 25).
3. Click **Apply Settings**.

Select items to audit

There is only one audit object, g2i file, available for auditing in iBright™ Imager and Analysis Software.

IMPORTANT! It is essential to check the check box under **Include** in **Audit Settings** for Audit to work on iBright™ Instrument and Analysis Software. Deselection of this check box will prevent export of images from iBright™ Instrument and iBright™ Analysis Software – Secure.

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 cancel and 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 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 six default audit reasons. These reasons may not be applicable to the iBright™ imager and the analysis software and can be updated during SAE Admin Console configuration. The reasons can be updated anytime without having an impact on performance of iBright™ imager and iBright™ Analysis Software – Secure.

The default reason list:

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

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

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

2. Enter a reason for change, then click **Save**.
3. Click **Edit** to open the **Edit Audit Reason** dialog box.
4. Edit the reason for change, then click **Save**.

5. Click **Delete** to open the **Delete Audit Reason** dialog box.
6. Click **Delete** to confirm deletion of the audit reason or **Cancel** to exit the dialog box.

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

7. Click **Apply Settings**.

Generate audit reports

Use the **Audit History** drop-down menu to generate reports from both the **Action Records** and **System Configuration** views.

Note: **Application Object Records** and **Instrument Run Records** under the **Audit History** drop down menu are not applicable to iBright™ Imager and Analysis Software application.

Display audit histories

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

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

Review the system configuration

The **System Configuration** view from the **Audit History** 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

(continued)

Record Type	Action	Description
Role assignment	Create	Create a user account
Auditable entity settings	Update	Enable or disable auditing
Auditable entity	Update	Modify audit settings
Role permissions	Create	Create a user role Note: 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
	Delete	Delete reason for change
Event manager	Update	Update the event manager
E-signature manager	Update	Enable or disable e-signature
E-signature type	Create	Create an e-signature meaning
	Delete	Delete an e-signature meaning
E-signature function	Update	Edit an action requiring e-signature

Review the action log

Select **Audit History ▶ Action Records** to view a log of the specified audit events.

All items in the action log are audited silently, including:

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

View audit histories from the Audit History drop-down menu

1. From the **Audit History** dropdown menu, select:

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

2. (Optional) Select **Enable Action Records Filtering** to filter or sort the action records.
 - a. Select the **Date Range**, **User Account**, **Application**, **Action**, and **Instrument**, then click **Search**.
The records display in the lower pane.
 - b. Click **Export** to export the action-records as a Text Document to the default location on your computer (usually the Download folder).
 - c. Click **Report** to generate an “Action Records History” report (PDF). The report is generated and saved to the default location set by your computer (usually in the Download folder).
3. (Optional) Select **Enable System Configuration Records Filtering** to filter or sort the system configuration records.
 - a. Select the **Date Range**, **User Account**, **Action**, **Record Type**, and **Record name**, then click **Search**.
The records display in the lower pane.
4. Click **Export** to export a filtered audit-records (Text Document) to default location (usually the **Download** folder).
5. Click **Report** to generate a filtered System Configuration History report (PDF).
The report is generated and saved to the default location set by your computer (usually the **Download** folder).

When to archive records

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, it is recommended to 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.

Archive and restore audit records

You can selectively archive audit records from the Audit History or automatically archive records by using a set number of records, a set records retention period, or both. The Audit records are removed from the Audit History and saved as an archive (.par) file in the Archival History. Audit records consist of Action records and System Configuration Records. You can also selectively restore archived records back to the audit history. You can also selectively restore archived records back to the Audit History.

Option	Description
Archive	Removes the records from the Audit History for the selected date range and places the archive file (.par) into the Archival History.
Restore	Restores audit records from an archived file (.par).

Display the action records or system configuration records of interest as described in “View audit histories from the Audit History drop-down menu” on page 28.

- Archive and export audit records:
 - a. Go to **Settings ▶ Archival History**.
 - b. Click **Ad-hoc Archival** and select the date range to archive.
 - c. Click **Archive**.
A dialog box will appear with button **Confirm to Archive**. Click this action to archive and remove the audit records dated between **date 1** and **date 2** from the system. Confirm by clicking **Archive** again.

Note: Although the individual records are removed from the system, the archived files are retained in the Archival History.

- d. Select an archive file and click **Export**. The archive file will be downloaded as a zip file, typically to the “Download” folder on your computer. Note: Although archived files can be exported from the console, they are not removed the archival history.

Note: Although archived files can be exported from the console, they are not removed from the Archival History.

- Restore archived audit records:
 - a. Select **Settings ▶ Archival History ▶ Restore (Upload)** to upload and archive records to the Archival History.
 - b. Select **Settings ▶ Archival History**, then select the archive record to restore. Click **Restore** to restore the archived audit records (actions and configuration) back into the system..

Set up an automatic archive of audit records

Automatically archiving audit records removes the records from the database and saves them in <C:/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** dropdown list.
4. Enter the number of records and the retention period. The available fields are dependent 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.

Archive/backup options and frequency

Options 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 manually archived 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.

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 <C:\Program Files (x86)\Applied Biosystems\SAE Admin Console\automated_archivals>, where <...> is the installation directory. The folder is named by the date and time of the archival.

Restore exported archived audit records

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.

Archive/backup options and frequency

Options 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 manually archived 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.

When to archive records

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, it is recommended to 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 an automatic archive of audit records

Automatically archiving audit records removes the records from the database and saves them in <C:/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** dropdown list.
4. Enter the number of records and the retention period. The available fields are dependent 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 <C:\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 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**.

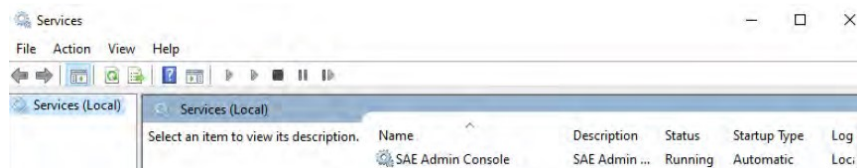
The archive is listed when you click **Settings ▶ Archival History**.

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 only the database folder) to ensure compatibility between the SAE server software and the database files.

IMPORTANT! If the backed up files require reinstallation 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, type "services", then open the **Services** app.



- b. Scroll to **SAE Admin Console**, right-click, then click **Stop**.
4. Copy <C:\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 <C:\Program Files (x86)\Applied Biosystems\SAE Admin Console\automated_archivals>, where <...> is the installation directory. The folder is named by the date and time of the archival.

Restore exported archived audit records

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.



Manage the e-signature function

■ Access the e-signature function screen	35
■ Configure the meanings of e-signatures	35

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. Select the **e-Signature** tab.
2. Uncheck **e-Signature** toggle to disable e-Signature. Check the toggle to enable.
3. Select **iBright Imager and Analysis Software** from the **Show e-signature configuration for** drop-down menu.
4. See “Configure the meanings of e-signatures” on page 35 to modify your desired e-signature settings
5. Click **Apply Settings**.

Configure the meanings of e-signatures

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

- **Reviewed and Approved Image and Data**

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-signature

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...
Sign file	Exports a signed report

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**.



Manage the SAE export-import function

- Export and import user, system security, audit, and e-signature settings 37

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

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

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

1. In the **Settings** drop-down menu, select **Export Configuration**.
2. In the **Export Configuration** dialog box, select:
 - a. **All** to export all configuration settings, including user accounts ("Users & Roles" and "System & Roles").
 - 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 and their associated permissions.
3. Click **Export**.

The exported file (.dat) is downloaded to the default location of your computer.

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

1. In the **Settings** 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**.

Documentation and support

Related documentation

Document	Publication number	Description
iBright™ Imaging System Help (eGUI help)	MAN0016116	On board help detailing use of instrument with SAE enabled and disabled
<i>iBright™ CL750 Imaging System User Guide</i>	MAN0018652	User guide for iBright™ CL 750 instrument detailing use of instrument with SAE enabled and disabled
<i>iBright™ Imaging Systems User Guide</i>	MAN0018592	User guide for iBright™ CL1500/FL1500 instruments detailing use of instrument with SAE enabled and disabled
iBright™ Analysis Software – Secure Help	MAN0019528	Help for SAE enabled iBright™ Analysis Software – Secure
SAE Migration from Version 2.0 to 2.2	thermofisher.com/SAE_Migration	User guide with procedures to move from version 2.0 to version 2.2 of the SAE Admin Console.

Obtain information from the Help System

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

Note: This Help is not specific for the iBright™ Imager and Analysis Software and should only be used as a general guide.

Customer and technical support

Visit 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 its affiliates 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. If you have questions, contact Life Technologies at www.thermofisher.com/support.

