invitrogen

SAE Admin Console

USER GUIDE

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

Publication Number MAN0019446

Revision A.0

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

ThermoFisher SCIENTIFIC

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**.

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

Revision history: Pub. No. MAN0019446

Revision	Date	Description
A.0	25 August 2020	New document

Contents

1 Security, Audit, and Electronic Signature

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 Quant Studio, Attune NxT, andiBright™ 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.

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.

Administrator overview

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 user-name 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.

Example applications

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

- Require users to log in and leave audit disabled
- Allow only certain users to adjust images
- Allow only certain users to perform analysis
- Allow only certain users to annotate images
- Allow only certain users to edit system preferences

2

Manage SAE user accounts and roles

Enable the SAE Admin Console

The SAE Admin Console is available for download from **http://thermofisher.com/ibrightanalysis**.

1. Install the program and launch the application.
2. Enter the Administrator **User Name** and **Password**, then click **Sign in**.

   Note: 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: + & % \

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.
2. Select the **Choose File** option in the pop-up window to select and open the data file for the iBright Imager and Analysis Software.dat. The selected file name will appear by the side of the **Select File** option in the pop-up window.
3. Select **Verify Data File** and then select **Install**.
4. *(Optional)* Select **iBright Imager and Analysis Software** from the list and select **View Details** to see the application details.

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 11.

   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

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

Disable (inactivate) a user account

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

Reset a forgotten password

1. In the **Users** tab, select the affected user account, then click **Edit**.
2. Enter a replacement password for the user 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 12). 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 12 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	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

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. Click on the download report tab in the bottom of the screen to view the report in a new tab of the web browser or to open the location of the downloaded report .pdf on your computer.

3. Use the options available in the .pdf viewer to save and print the report.

4. Close the report.

3

Manage the system security function

Access the system security function screen

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

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

1. See "Configure account setup and security policies" on page 14 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 and password settings.

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

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

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

   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.

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.

4. In the **Other Settings** pane:
   a. Enable or disable **Client offline login**.

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

   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 a SAE file.

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 menu, select **Notifications**.
2. In the **Edit NotificationsSettings** 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**.

4 Manage the audit function

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 when the **Audit mode** is set to **Silent**.

Note: The **Enable Audits** option is not enabled for 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 19 and “Configure audit reason settings” on page 19).
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**
- **Need to change threshold**
- **Need to reanalyze**
- **Entry error**
- **Well anomaly**
- **Calculation error**

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.

Audit histories from the Audit History drop-down menu

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

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

Review the System Configuration

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

Record Type	Action	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

(continued)

Record Type	Action	Description
User Account	Create	Create new user account
	Update	Edit or suspend a user account
Role Assignment	Edit	Assign a different user role to an existing user account
	Create	Create a user account
Auditable Entity Settings	Update	Enable or disable auditing
Auditable Entity	Update	Modify audit settings
Role Permissions	Create	Create a user role **Note:** Creates one role assignment record for each permission in a role.
	Delete	Delete a user role
	Update	Modify user role permissions
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 record log** 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**, and **Action**, then click **Search**.
   The records display in the lower pane.

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

4. Click **Report** to generate an audit history report.
   The report is generated and saved to the default location set by your computer.

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

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

7. *(Optional)* See "Archive, purge, and restore audit records" on page 22 to archive the action records or system configuration records.

8. *(Optional)* See "Archive, purge, and restore audit records" on page 22 to restore purged action records or system configuration records.

Archive, purge, and restore audit records

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

Option	Description
Archive	Makes a copy of audit records.
Purge	Makes a copy of audit records, archives them on the computer, then deletes them from the software.
Restore	Restores audit records from archived files.

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 22.

- Archive records:
  a. Select the records of interest.
  b. Click **Archive**.
  c. Confirm the filter criteria and select **Purge audit records after archival** to purge the records, then click **Archive**.

     The records are archived to the default download location of the computer.
- Restore records:
  a. In the **Action Record** or **System Configuration** view, click **Restore**.
  b. Select the .par file to restore, then click **Open**.

Export audit records

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

1. Display the records of interest as described in "View audit histories from the Audit History drop-down menu" on page 22.
2. In the **Action Records** view or **System Configuration** view, click **Export**.

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

   The .txt file with the audit records downloads to the default location set by your computer.

5 Manage the e-signature function

Access the e-signature function screen

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

Note: The **Enable e-Signature** option is not enabled for the iBright™ Imager and Analysis Software application. The e-Signatures are always enabled irrespective of whether the toggle for **Enable e-Signature** is checked or un-checked

1. Select the **e-Signature** tab.
2. Select **iBright Imager and Analysis Software** from the **Show e-signature configuration for** drop-down menu.
3. See "Configure the meanings of e-signatures" on page 24 to modify your desired e-signature settings
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 SAE module is installed with one default meaning:

- **Reviewed and Approved Image and Data**

Add an e-signature meaning

In the **e-Signature** tab, in the **e-Signature Meanings** pane:

1. 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

In the **e-Signature** tab, in the **e-Signature Meanings** pane:

1. 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**.

6 Manage the SAE export-import function

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

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

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

1. In the **Settings** drop-down menu, select **Export Configuration**.
2. In the **Export Configuration** dialog box,select:
   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 and their associated permissions.
3. Click **Export**.
   The exported file (.dat) is downloaded to the default location of your computer.

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

1. In the **Settings** drop-down menu, select **Import Configuration**.
2. Click **Choose File** to choose the .dat file with the desired configuration settings
3. Select the import options:
   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**.

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

Documentation and support

Related documentation

Document	Publication number	Description
iBright™ Imaging System Help (eGUI help)	MAN0016116	On board help detailing use of instrument with SAE enabled and disabled
iBright™ CL750 Imaging System User Guide	MAN0018652	User guide for iBright™ CL 750 instrument detailing use of instrument with SAE enabled and disabled
iBright™ Imaging Systems User Guide	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

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/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**. If you have any questions, please contact Life Technologies at **www.thermofisher.com/support**.