invitrogen

SAE Administrator Console

USER GUIDE

for use with:

Attune™ NxT Software

Publication Number MAN0019099

Revision A.0

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

ThermoFisher SCIENTIFIC

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

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: These products may be covered by one or more Limited Use Label Licenses. By use of these products, 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.

Revision history: Pub. No. MAN0019099

Revision	Date	Description
A.0	05 May 2020	New document

Contents

1

Get started

Network and password security requirements

Network configuration and security

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

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

Password security

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

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

About the SAE Administrator Console

The SAE Administrator Console is the tool that you use to configure the Security, Audit, and Electronic Signature (SAE) module. The SAE module can be configured to meet specific requirements for security, audit, and e-signature (such as 21 CFR Part 11 compliance).

In the SAE Administrator Console, a software or instrument that is configured for the SAE module is called an "application". An example application is the Attune™ NxT Software.

The SAE module can be configured to provide the following functionality:

Function	Description
System security	Controls user access to the Attune™ NxT application. A default user account with the Administrator role is provided at installation that has access to both SAE Administrator Console and the Attune™ NxT Software. Other default SAE user roles include Advanced user, User, Reviewer, and No Privileges roles. You can set up additional SAE user accounts with specific permissions.
Auditing	Tracks actions performed by users, changes to the SAE module settings, and changes made to application objects (i.e., Experiments). You can: • Enable or disable audits, select actions and application objects to be audited, specify the audit mode, and require users to provide a reason for changes made to auditable application objects. • View specific audit logs and generate printable audit records. • Archive the audit records or configure auto archive settings.
Electronic signature (e-signature)	Determines if users are required to fulfill signature requirements before performing specific functions. You can: • Configure e-signature so that a user can export data, print data, and save experiment as a template only if the required e-Signatures are provided. • Configure each e-signature event to require multiple signatures and to require users with specific roles to sign.

IMPORTANT! 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 software used. The SAE Module of the Attune™ NxT Software does not automatically guarantee 21 CFR part 11 compliance. Compliance is the consequence of the end user’s work process and systems used. Attune™ NxT Software in the SAE mode enables 21 CFR part 11 compliance for the flow cytometry data collection and analysis steps within the workflow.

SAE module components

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

- **SAE Administrator Console**—Tool that is used by an SAE administrator to configure the SAE module.
- **SAE server** (server)—Service that runs in the background and stores SAE settings, user accounts, audit records, and e-signature records. By default, the SAE server is installed on the same computer as the SAE Administrator Console.
- **SAE screens** (client)—Screens that are displayed in an application (sign in, audit, and e-signature) and that require user input. The Attune™ NxT Software runs on the client.

Install the Attune™ NxT Software with the SAE module

The SAE Administrator Console is installed optionally as part of the Attune™ NxT Software on the same computer that controls the Attune™ NxT instrument. When installing the Attune™ NxT Software, select the **Attune™ NxT Software with Security, Audit, E-Signatures** option.

Note: For detailed instructions on how to install the Attune™ NxT Software with the Security, Audit, and e-Signature functions, refer to the *Attune™ NxT Software User Guide*, available for download at **thermofisher.com/attune**.

IMPORTANT! A license control mechanism in the form of a SAE-specific DESkey device is required to access the SAE Administrator Console from the Attune™ NxT Software and to use the Attune™ NxT Software in the SAE mode.

Workflow: Configure the SAE module using the SAE Administrator Console

Set up the SAE Administrator Console (before first use)

Open the SAE Administrator Console (page 11)

▼

Use the SAE module (as needed)

Chapter 2, “Manage SAE user accounts and roles” and

“Create an SAE user account” on page 14

A default Administrator user account is provided at installation. Complete this step of the workflow to add more users.

▼

Chapter 3, “Manage the system security function” and

“Configure account setup and security policies” on page 25

Complete this step of the workflow to control restrictions and system security policies for all SAE user accounts.

▼

Chapter 4, “Manage the audit function”

Complete this step of the workflow to select actions to be audited and view audit reports.

▼

Chapter 5, “Manage the e-Signature function”

Complete this step of the workflow to select actions that require e-signature and view e-signature reports.

IMPORTANT! Ensure that audit settings are configured before using the Attune™ NxT Software in SAE mode, because changes to audit object settings can result in audit gaps if the changes are made after the experiments have been created.

Configure the SAE server from the client application

The SAE server is a service that runs in the background and stores SAE settings, user accounts, audit records, and e-Signature records. By default, the SAE server is installed on the same computer as the SAE Administrator Console. Before you enable the SAE mode, ensure that the SAE server is configured correctly in the Attune™ NxT Software.

Note: By default, the SAE server is setup to run locally. If you wish to use a remote server for the user repositories, see Chapter 6, “Advanced configuration options”.

1. Launch the Attune™ NxT Software and sign in as **Administrator**.
2. Click the **Options** button on the **Quick Access** toolbar to open the **Options** dialog, then select the **Administrator** tab.
3. In the **SAE Configuration** section of the **Administrator** tab, ensure that **Local Server** is selected for Server Configuration.

   When **Local Server** is selected, the **Port Number** is automatically set to ***8201*** and the **Server IP Address** is set to ***localhost*** by default.

   Note: The SAE Configurations options are only visible if the SAE-specific DESkey device is present to allow access to the SAE mode in the Attune™ NxT Software, and they are only enabled if the SAE mode is disabled (i.e., the **Enable SAE Mode** checkbox is unchecked).
4. (*Optional*) Click **Test Connection** to confirm that the connection information is correct.
5. Click **OK**.

Enable the SAE Administrator Console

Before you can start using the Attune™ NxT Software in the SAE mode, you must first access the SAE Administrator Console to change your SAE password, then enable the SAE mode in Attune™ NxT Software. This procedure requires a local administrator profile on the instrument and an SAE administrator account in the SAE Administrator Console.

IMPORTANT! A license control mechanism in the form of a SAE-specific DESkey device is required to access the SAE Administrator Console from the Attune™ NxT Software and to use the Attune™ NxT Software in the SAE mode.

1. Launch the Attune™ NxT Software and sign in as **Administrator**.

   Note: When signing into the Attune™ NxT Software for the first time after installation, you must sign in as an Administrator. The default username and password for the Administrator are both ***admin***. After you sign in for the first time, the software will prompt you to change the password.

2. Click the **Options** button on the **Quick Access** toolbar to open the **Options** dialog, then select the **Administrator** tab.

3. In the SAE Configuration section of the Administrator tab, click **Setup** to open the **SAE Administrator Console** in your system's default web browser, then sign in to the SAE Administrator Console using the default SAE Administrator credentials.

   Note: The SAE Configurations options are only visible if the SAE-specific DESkey device is present to allow access to the SAE mode in the Attune™ NxT Software.

4. When prompted, enter the new SAE Administrator password in the SAE Administrator Console, then click **Update**.

   Note: By default, the SAE Administrator password is set to expire after the first sign in. To enable the SAE mode for the Attune™ NxT Software, you must first update the password for the SAE Administrator.

5. Configure the SAE Console. For detailed instructions, see the following pages:
   - Manage the SAE user accounts and roles Chapter 2, "Manage SAE user accounts and roles"
   - Manage the system security function Chapter 3, "Manage the system security function"
   - Manage the audit function Chapter 4, "Manage the audit function"
   - Manage the e-Signature function Chapter 5, "Manage the e-Signature function"
   - Setup advanced configuration options Chapter 6, "Advanced configuration options"

   IMPORTANT! Changing audit settings after experiments have been created may result in audit gaps. Ensure that audit settings are configured before using the Attune™ NxT Software in SAE mode.

   Note: For detailed information on the SAE Console configuration, refer to the *Attune™ NxT Software User Guide* (Part. No. 100024236), available for download at **thermofisher.com/attune**.

6. In the Attune™ NxT Software, select **Options dialog ▸ Administrator tab ▸ Enable SAE Mode**.

7. When prompted, enter your SAE Administrator credentials, then click **OK**.

8. The software displays the **SAE Enabled** notification, which prompts you to log out of the Attune™ NxT Software and sign in with your SAE credentials to make the changes go into effect.

9. Click **OK** to close the notification, then click **OK** to close to **Options** dialog

10. Log out of the The Attune™ NxT Software, then sign in again using your SAE credentials. You can now use the Attune™ NxT Software in the SAE mode.

    IMPORTANT! When signing into the Attune™ NxT Software after the SAE mode is enabled, you must use your SAE account username and password, and not your Attune™ NxT username and password. In cases where the SAE server is unavailable or you need service repair of your instrument, you can sign in to your local Attune™ NxT Software account using the **Sign in with local account** drop down option. This option is only available if you have an Administrator, System Administrator, or Service account. Users and Advanced Users are not allowed to login to the local account once SAE is enabled.

Open the SAE Administrator Console

After you have enabled the SAE Administrator Console on the Attune™ NxT Software, open the SAE Administrator Console to manage SAE functions.

1. In the Attune™ NxT Software, select the SAE tab, then click View SAE Console.

   The SAE Administrator Console opens in the system's default web browser.

2. Click the navigation tabs to display different screens in the software.

Optional SAE Administrator Console tasks

Set up SAE messaging notifications

You can specify when and how to be notified when specified events occur in the SAE Administrator Console.

1. In the SAE Administrator Console main screen, click the **Settings** tab.

2. Select **Notifications**.

3. In the **Edit Notification Settings** dialog box, select **Notify at Administrator sign in** for the events of interest.

4. *(Optional)* Select **Notify by Email**, then specify an email address.

5. Click **Save**.

Configure the SMTP server for email notifications

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

1. In the SAE Administrator Console main screen, click the **Settings** tab.

2. Select **Email Server**.

3. 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.
4. Click **Save**.

Determine the signed-in user

The name of the signed-in user is displayed in the top-right corner of the SAE Administrator Console main screen.

Display the software version

1. In the SAE Administrator Console main screen, click the **Settings** tab.
2. Select **About**.
   The SAE Administrator Console software version is displayed.

Change your SAE user account password

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

2 Manage SAE user accounts and roles

The SAE Administrator Console has an Attune™ NxT-specific security profile that defines users, user roles, and application permissions, which are managed using the **Users** and **Roles** tabs.

The **Users** tab displays a list of the current SAE accounts in the SAE server, and allows the SAE Administrator to create additional SAE users, edit current users, and to create Users reports. There are three action buttons in the **Users** tab:

- **Create**: Allows the SAE Administrator to create additional SAE users.
- **Edit**: Allows the SAE Administrator to edit the settings for the selected SAE user.
- **Report**: Allows the SAE Administrator to create a PDF report that lists the current SAE accounts saved in the SAE server.

The **Roles** tab allows SAE Administrators to create, edit, and delete custom roles, and to create roles reports. SAE roles determine the SAE permissions that are associated with an SAE user account. There are four action buttons in the **Roles** tab:

- **Create**: Allows the SAE Administrator to create custom SAE roles that give granular permissions to the Attune™ NxT Software features.
- **Edit**: Allows the SAE Administrator to edit the settings for the selected custome SAE role.

  Note: The default SAE roles (Administrator, Advanced User, User, Reviewer, and No Privileges) are non-modifiable and are fixed with the functions they can perform.
- **Delete**: Allows the SAE Administrator to delete selected custom SAE roles.
- **Report**: Allows the SAE Administrator to create a PDF report that lists the available SAE roles.

Create an SAE user account

The **Users** tab of the SAE Administrator Console displays a list of the current SAE accounts in the SAE server, and allows the SAE Administrator to create additional SAE users, edit current users, and to create Users reports.

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

2. Click **Create** to open the **Create User Account** dialog, then enter the user name, password, first name, *(optional)* middle initial, and last name.

   The field limits are specified in the system security function settings.

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

   Note: You cannot change the user name or delete a user after you have saved the user account.

3. *(Optional)* Deselect **User must set new password at next sign in**. By default, this option is selected and users must specify a newe password the first time they sign in to an application.

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

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

   Available default options are **Administrator**, **Advanced User**, **User**, and **Reviewer**. For more information, see “Default SAE account types” on page 17.

   Note: Each role grants specific SAE permissions to the user. You can also create a custom role with specific privileges in the **Roles** tab. For more information, see “Manage roles” on page 16.

   Note: The No Privileges Role is for internal use by the SAE Administrator Console. Do not assign this role to a user account.

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

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

7. Click **Save**.

Edit an SAE user account

1. In the SAE Administrator Console main screen, click the **Users** tab.
2. Select a user account, then click **Edit** to open the **Edit User Account** dialog.
3. Edit the settings as desired.

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

4. Click **Save**.

Activate a suspended SAE user account

1. In the SAE Administrator Console main screen, click the **Users** tab.
2. Select a user account, then click **Edit** to open the **Edit User Account** dialog.
3. Change the **Status** from **SUSPENDED** to **ACTIVE**.
4. Click **Save**.

Disable (inactivate) an SAE user account

1. In the SAE Administrator Console main screen, click the **Users** tab.
2. Select a user account, then click **Edit** to open the **Edit User Account** dialog.
3. Change the **Status** from **ACTIVE** to **INACTIVE**.
4. Click **Save**.

Reset an SAE user account password

IMPORTANT! There is no way to recover a forgotten password. If the SAE Administrator forgets their password, the software must be reinstalled. Export all data before reinstalling the software. Otherwise, the data will be lost. For more information, see Chapter 6, “Advanced configuration options”.

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

Manage roles

SAE roles determine the SAE permissions that are associated with an SAE user account. For the default permissions and roles in the Attune™ NxT Software, see .

SAE roles are managed from the **Roles** tab of the SAE Administrator Console, which allows SAE Administrators to create, edit, and delete custom roles, and to create roles reports. If your SAE Administrator Console is configured to manage the SAE module for more than one application, you can create roles that specify permissions for more than one application.

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

Note: Changes made to a role in the SAE Administrator Console are reflected in the client application (i.e., Attune™ NxT Software) within 10 seconds.

Default SAE account types

The SAE module for the Attune™ NxT Software provides the following default SAE account types:

- **Administrator:** System administrator role with full access to the software and full privileges, including the ability modify SAE configuration and define the system security policy.
- **Advanced User:** Similar to Attune™ NxT advanced user.
- **User:** Similar to Attune™ NxT user.
- **No Privileges Role:** This role is for internal use only by the SAE Administrator Console when you set up user repositories. Do not assign this role to a user account.

For the permissions assigned to each default SAE account type, see the Default permissions and roles on page 18. To create a custom role with specific privileges, see Create a role on page 23.

Default SAE permissions and roles

Permission	Administrator	Advanced User	User	Reviewer
SAE Administrator Console				
Security Configuration				
Configure Security and Auditing	Yes	No	No	No
Audit History				
View Action Records	Yes	No	No	Yes
View System Configuration Records	Yes	No	No	Yes
View Application Object Records	Yes	No	No	Yes
View Instrument Run Records	Yes	No	No	Yes
Attune™ NxT Software				
Acquisition Control				
Copy and paste run protocols settings	Yes	Yes	Yes	No
Modify collect options	Yes	Yes	Yes	No
Modify run protocol settings	Yes	Yes	Yes	No
Record over (overwrite) existing sample data	Yes	Yes	Yes	No
Run and record samples/plates	Yes	Yes	Yes	No
Compensation				
Apply compensation	Yes	Yes	Yes	No
Create compensation	Yes	Yes	Yes	No
Delete compensation	Yes	Yes	Yes	No
Edit compensation channels	Yes	Yes	Yes	No
Export compensation	Yes	Yes	Yes	No
Import compensation	Yes	Yes	Yes	No
Modify compensation values	Yes	Yes	Yes	No
Experiment Management				
Change experiment and group colors	Yes	Yes	Yes	No
Create experiments	Yes	Yes	Yes	No
Create experiments from templates	Yes	Yes	Yes	No

Permission	Administrator	Advanced User	User	Reviewer
Create samples and groups	Yes	Yes	Yes	No
Create templates	Yes	Yes	Yes	No
Delete experiments	Yes	Yes	Yes	No
Delete samples	Yes	Yes	Yes	No
Delete templates	Yes	Yes	Yes	No
Duplicate experiments	Yes	Yes	Yes	No
Export experiments	Yes	Yes	Yes	No
Export FCS files	Yes	Yes	Yes	No
Export sample list	Yes	Yes	Yes	No
Export templates	Yes	Yes	Yes	No
Import experiments	Yes	Yes	Yes	No
Import FCS files	Yes	Yes	Yes	No
Import sample list	Yes	Yes	Yes	No
Import templates	Yes	Yes	Yes	No
Modify experiment annotation	Yes	Yes	Yes	No
Modify templates	Yes	Yes	Yes	No
Open experiments	Yes	Yes	Yes	No
Remove FCS files	Yes	Yes	Yes	No
Show/Hide experiment and group colors	Yes	Yes	Yes	No
Update keywords in exported FCS files	Yes	Yes	Yes	No
Filter Configuration				
Create and edit filters	Yes	Yes	No	No
Manage filter configurations	Yes	Yes	No	No
Modify filter mapping	Yes	Yes	No	No
View filter configuration	Yes	Yes	Yes	No
Instrument Control				
Run auto sampler calibration	Yes	Yes	Yes	No
Run debubble and unclog	Yes	Yes	Yes	No

Permission	Administrator	Advanced User	User	Reviewer
Run deep clean and shutdown	Yes	Yes	Yes	No
Run recover sample	Yes	Yes	Yes	No
Run rinse, SIP sanitize	Yes	Yes	Yes	No
Run startup	Yes	Yes	Yes	No
Run system decontamination	Yes	Yes	No	No
Run system self test	Yes	Yes	No	No
Instrument Settings				
Copy and paste instrument settings	Yes	Yes	Yes	No
Export instrument settings	Yes	Yes	Yes	No
Import instrument settings	Yes	Yes	Yes	No
Modify advanced instrument settings	Yes	Yes	No	No
Modify parameter on/off states	Yes	Yes	Yes	No
Modify parameter target and label names	Yes	Yes	Yes	No
Modify system instrument settings	Yes	No	No	No
Modify thresholds	Yes	Yes	Yes	No
Modify voltages	Yes	Yes	Yes	No
Options				
Create and edit plates	Yes	Yes	No	No
Create and edit user keywords	Yes	Yes	Yes	No
Manage global keywords	Yes	No	No	No
Modify administrator options	Yes	No	No	No
Modify configuration options	Yes	No	No	No
Modify default colors	Yes	Yes	Yes	No
Modify default font options	Yes	Yes	Yes	No
Modify default gate options	Yes	Yes	Yes	No
Modify default plot options	Yes	Yes	Yes	No
Modify default sample and group name	Yes	Yes	Yes	No
Modify default statistics options	Yes	Yes	Yes	No
Modify display options	Yes	Yes	Yes	No

Permission	Administrator	Advanced User	User	Reviewer
Modify export options	Yes	Yes	Yes	No
Performance Test				
Reset baseline	Yes	Yes	No	No
Run performance test	Yes	Yes	No	No
View performance test report	Yes	Yes	Yes	Yes
Workspace and Overlay Gates				
Change gate color	Yes	Yes	Yes	No
Change gate coordinates	Yes	Yes	Yes	No
Change gate name	Yes	Yes	Yes	No
Change gate opacity	Yes	Yes	Yes	No
Change gate type	Yes	Yes	Yes	No
Create gates	Yes	Yes	Yes	No
Delete gates	Yes	Yes	Yes	No
Export gate to FCS file	Yes	Yes	Yes	No
Modify gate equation	Yes	Yes	Yes	No
Modify gate Z order	Yes	Yes	Yes	No
Show/Hide gate name	Yes	Yes	Yes	No
Workspace and Overlay Plots				
Change density plot color and mode	Yes	Yes	Yes	No
Change legend text	Yes	Yes	Yes	No
Change overlay opacity	Yes	Yes	Yes	No
Change overlay plot color	Yes	Yes	Yes	No
Change percent of displayed events	Yes	Yes	Yes	No
Change plot axes labels	Yes	Yes	Yes	No
Change plot parameters	Yes	Yes	Yes	No
Change plot range	Yes	Yes	Yes	No
Change plot resolution	Yes	Yes	Yes	No
Change plot scale	Yes	Yes	Yes	No
Change plot title	Yes	Yes	Yes	No

Permission	Administrator	Advanced User	User	Reviewer
Change plot types	Yes	Yes	Yes	No
Create overlays	Yes	Yes	Yes	No
Delete overlays	Yes	Yes	Yes	No
Delete plots	Yes	Yes	Yes	No
Format plot text	Yes	Yes	Yes	No
Hide tick marks on overlays	Yes	Yes	Yes	No
Insert plots	Yes	Yes	Yes	No
Modify histogram properties	Yes	Yes	Yes	No
Modify overlay 3D options	Yes	Yes	Yes	No
Modify plot statistics	Yes	Yes	Yes	No
Perform overlay calculations	Yes	Yes	Yes	No
Reorder overlay plot members	Yes	Yes	Yes	No
Save plot as image	Yes	Yes	Yes	No
Show/Hide overlay plots	Yes	Yes	Yes	No
Show legend on overlays	Yes	Yes	Yes	No
Workspace Layout				
Align objects	Yes	Yes	Yes	No
Change workspace grid size	Yes	Yes	Yes	No
Modify workspace mode	Yes	Yes	Yes	No
Move and resize objects	Yes	Yes	Yes	No
Other Workspace Objects				
Copy objects to clipboard	Yes	Yes	Yes	No
Delete images	Yes	Yes	Yes	No
Delete statistics	Yes	Yes	Yes	No
Delete text boxes	Yes	Yes	Yes	No
Edit text box text	Yes	Yes	Yes	No
Format statistics	Yes	Yes	Yes	No
Format text box	Yes	Yes	Yes	No

Permission	Administrator	Advanced User	User	Reviewer
Insert images	Yes	Yes	Yes	No
Insert statistics	Yes	Yes	Yes	No
Insert text boxes	Yes	Yes	Yes	No
Modify statistics box statistics	Yes	Yes	Yes	No
Other				
Export workspace	Yes	Yes	Yes	No
Import workspace	Yes	Yes	Yes	No
Modify heatmap settings	Yes	Yes	Yes	No
Printing and page layout	Yes	Yes	Yes	No
View system logs	Yes	Yes	Yes	No
View user logs	Yes	No	No	No
Security Configuration				
Perform e-signing	Yes	Yes	No	No

Create a role

1. In the SAE Administrator Console main screen, click the **Roles** tab.
2. Click **Create** to open the **Create Role** dialog.
3. Enter the Name and (optional) Description for the new role.
4. Select SAE and Attune permissions for the role (See “Default SAE permissions and roles” on page 18). To select all SAE permissions in a category, select the checkbox next to the category.
5. Click **Save**.

   The newly created role is displayed in the **SAE Roles** list in the **Roles** tab, and it becomes available in the **Role** dropdown in the **Create User Account** dialog.

Edit a role

1. In the SAE Administrator Console main screen, click the **Roles** tab.
2. Select a role, then click **Edit** to open the **Edit Role** dialog.

   Note: You cannot edit the default Administrator, Advanced User, and User roles.
3. Edit settings as needed, then click **Save**.

Delete a role

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

1. In the SAE Administrator Console main screen, click the **Roles** tab.
2. Select a role, then click **Delete**.

   Note: Changes to a role will be reflected in the client application (i.e., Attune) within 10 seconds.

View or print a user or role report

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

3

Manage the system security function

The **System** tab of the SAE Administrator Console allows the SAE Administrator to modify SAE configuration and define the system security policy. In this tab, the SAE Administrator can:

- Configure user name settings
- Set password policy
- Define account lockout policy
- Configure other system settings

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

Enable or disable the system security function

The system security function cannot be disabled in the SAE Administrator Console. To disable SAE user sign in to the Attune™ NxT Software, you must disable SAE in the **Administrator** tab of the **Options** dialog in the Attune™ NxT Software. For more information, refer to the Attune™ NxT Software User Guide (Pub. No. 100024236).

Configure account setup and security policies

The **System** tab allows the SAE Administrator to modify SAE configuration and define the system security policy. Settings in this screen affect all SAE user accounts. Settings are applied the next time that users sign in to an application.

1. In the SAE Administrator Console main screen, click the **System** tab.
2. In the **User Name Settings** pane, specify the user name requirements and limits (user name length, and so on).

   Note: The Attune™ NxT Software only allows a maximum user name length of 50 characters. If a user name length greater than 50 characters is chosen, the SAE user will not be able to login into the Attune™ NxT Software.

3. In the **Password Policy** pane, specify the password requirements and limits (password required characters, and so on).

4. *(Optional)* In the **Account Lockout Policy** pane, enable or disable the **Account lockout** feature. If you enable this feature, specify the following settings:

Settings	Description
Threshold and **Account lockout duration**	If a user attempts to sign in with an incorrect user name or password more than the number of times set for the threshold (by default, 3 failed attempts), the user is locked out for the time specified (by default, 24 hours).
Sign in attempts counter reset and **Reset failure sign in counter after**	If the counter reset is enabled, the counter resets to 0 after the time specified. For example, if a user is locked out because of exceeding the number of failed sign-in attempts, the user will be able to attempt to sign in after the time specified.

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

Settings	Description when enabled
Automatic screen locking and **Inactivity duration**	The screen is locked if no mouse or keyboard input is detected. An actively signed-in user or SAE administrator must enter their user name and password to unlock the screen.
Open file from non-SAE system	The application allows users to access data files that were generated when SAE functions were disabled. By default, this is set to Forbidden.
Client offline sign in and **Offline sign in threshold**	When the SAE server is offline, users can sign in and use the Attune™ NxT Software for the time specified.

Note: When set to **Allowed**, the **Open file from non-SAE system** function also allows you to:

- Open an Experiment altered outside of an application and continue with that Experiment.
- Open, duplicate, or export Experiments where an audit gap or tampering was detected.

However, depending upon what has been changed in the data files, continuing with a tampered Experiment could result in an Audit gap. If there are audit gaps in the audit history or the audit settings are modified on the SAE console, the Attune™ NxT Software displays the **File Modification Detected** warning dialog to notify you that you are trying to open an Experiment that has an invalid audit history and ask if you want to continue.

6. Click **Apply Settings**.

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

4 Manage the audit function

The Audit function allows you to track user actions, changes to SAE settings, and changes made to application objects (i.e., Experiments). Manage the audit function using the **Audit** and **Audit History** tabs.

The **Audit** tab has the following functional groups:

- **Audit Settings** (consists of the **Enable Audits** checkbox and the **Audit Settings** panel)
- **Audit Reason Settings**

Use the **Audit** to enable or disable audits, control which actions and application objects are audited, and require users to provide a reason for changes made to auditable application objects.

Use the **Audit History** tab to access audit record logs for the auditable transactions. The audit logs available for viewing are:

- *Action Records*
- *System Configuration Records*
- *Application Object Records*
- *Instrument Run Records* (this function is not used by the Attune™ NxT Software)

Note: For detailed information on the **Audit** and **Audit History** tabs, refer to the *Attune™ NxT Software User Guide* (Part. No. 100024236), available for download at **thermofisher.com/attune**.

IMPORTANT! Changing audit settings after experiments have been created may result in audit gaps. Ensure audit settings are configured before using the software in SAE mode.

Enable or disable the audit function

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

Select items to audit and set the Audit Mode

Use the **Audit Settings** panel of the **Audit** tab to select the items to audit and the **Audit Mode**. The **Audit Settings** panel has four columns:

- **Include**: Selects the items to include in the audit.
- **Application**: Displays the application to which the audit applies.

  If your SAE Administrator Console is configured to manage the SAE module for more than one application, you can audit more than one application (for example, Attune™ NxT Software and SeqStudio™ Genetic Analyzer).
- **Audit Type**: Lists what is included in the audit (for example, Compensation, Compensation Channel, etc.).
- **Audit Mode**: Allows you to select one of the three audit modes (Silent, Optional, Required).

  The default audit mode for Attune™ NxT Software application objects is **Silent**.

1. In the SAE Administrator Console main screen, click the **Audit** tab.
2. In the **Audit Settings** panel, select the items to audit.
3. Select the **Audit Mode** for each item you include for auditing:

Option	Description
Silent *(Default)*	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.

Note: When the **Audit mode** is set to **Silent**, audit reasons are not available for user selection in the Attune™ NxT Software.

Note: When the **Audit mode** is set to **Optional** or **Required**, the **Enter Audit Reason** dialog is displayed each time a change is made that results in an audit.

4. Click **Apply Settings**.

Configure audit reason settings

Configure audit reason settings in the **Audit Reason Settings** panel of the **Audit** tab.

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

  The SAE console is preloaded with the following defined audit reasons:

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

- Add new audit reason:

  a. Click **New Reason**.

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

  c. Click **Apply Settings**.

- Edit an existing audit reason:

  a. Click **Edit**.

  b. Edit the reason for change, then click **Save**.

  c. Click **Apply Settings**.

- Delete an existing audit reason:

  a. Click **Delete**.

  b. Click **Delete** to confirm deletion of the audit reason or **Cancel** to exit the dialog box.

  c. Click **Apply Settings**.

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

View audit logs (audit history)

Audit History

The **Audit History** tab allows users with permission to view **Audit History** to access the audit logs for auditable transactions. The permission to view the entire **Audit History** or specific audit logs is granted in the **Roles** tab. The audit logs available for viewing are:

- *Action Records*
- *System Configuration Records*
- *Application Object Records*
- *Instrument Run Records* (this function is not used by the Attune™ NxT Software)

View the Action Records audit log

Action Records are always audited and cannot be turned off. All items in the action records log are audited silently.

1. In the SAE Administrator Console main screen, click the **Audit History** tab.
2. Select **Action Records** to view a log of the specified audit events.
3. To display a list of items that are audited for your application:
   a. Select **Enable Action Records Filtering**.
   b. Select your application from the **Application** list.
   c. In the **Action** field, click ⌄.
      The list of auditable actions is displayed.
4. *(Optional)* Perform the following actions:
   - Specify other filtering settings.
   - Click **Report** to generate a PDF file of the log.
   - Click **Export** to generate a TXT file of the log.

Auditable actions in the SAE Administrator Console

- Enable or disable security, audit, or e-signature
- Sign in to or out of the SAE Administrator Console
- Import or export an SAE configuration
- Install an application profile
- Archive, purge, or restore audit records
- Manual Sync with LDAP Directory

Auditable client application actions

Table 1 Auditable client application actions

Action	Description
Stop	Stop function (if in acquisition, Stop Acquisition) (via Ribbon tab or Collection panel)
Startup	Run Startup function (via Ribbon tab, Collection panel, or PT view)
Recover Sample	Recover Sample (via Ribbon tab or Collection panel)
Rinse	Run Rinse function
Deep Clean	Run Deep Clean function
Shutdown	Run Shutdown function
SIP Sanitize	Run SIP Sanitize function
Decon	Run System Decontamination function
Unclog	Run Unclog function
Debubble	Run Debubble function
Calibrate AAS	Calibrate autosampler
Calibrate PZT	Calibrate PZT
Run Self Tests	Run Self Tests
Run Performance Test	Action logged when a Performance Test is initiated
Performance Test Passed	Action logged at the completion of a passing Performance Test
Performance Test Failed	Action logged at the completion of a failed Performance Test
Run Baseline Test	Action logged when a Baseline Test is initiated
Baseline Test Passed	Action logged at the completion of a passing Baseline Test
Baseline Test Failed	Action logged at the completion of a failed Baseline Test
Run Sample in Setup Mode	Action recorded when Tube or Manual well is run in Setup mode
Record Sample	Action recorded when Tube or Manual well is run in Record mode (Record button clicked)
Clear Data	Action recorded when the Clear button is clicked and data is cleared
Stop Run	Action recorded when the Stop button is clicked while acquisition is in progress
Record Compensation	Action recorded when the Compensation controls are recorded
Record Plate	Action recorded when Plate is recorded or Record All is selected
Pause Plate	Action recorded when Plate run is paused
Resume Plate	Action recorded when Plate run is resumed from pause
Activate Experiment	Action audited when Experiment is activated
Activate Sample	Action audited when Sample is activated
Export Experiment	Action audited when Plate or Tube Experiment is exported
Import Experiment	Action audited when Plate or Tube Experiment is imported

Action	Description
Export FCS Files	Action audited when FCS Files are exported
Import FCS Files	Action audited when FCS Files are imported
Export Statistics	Action audited when statistics are exported

View the System Configuration audit log

System Configuration is always audited and cannot be turned off.

1. In the SAE Administrator Console main screen, click the **Audit History** tab.
2. Select **System Configuration** to view a log of the system security, audit, and e-signature configuration records.
3. To display a list of items that are audited:
    a. Select **Enable System Configuration Records Filtering**.
    b. In the **Record type** field, click ⌄.
    The list of auditable system configuration objects is displayed.
4. *(Optional)* Perform the following actions:
    - Specify other filtering settings.
    - Click **Report** to generate a PDF file of the log.
    - Click **Export** to generate a TXT file of the log.

View Application Object Records audit log

Application objects are auditable items such as plate setups, templates, or other items that you create in an application.

1. In the SAE Administrator Console main screen, click the **Audit History** tab.
2. Select **Application Object Records**.
3. To display a list of items that are audited for your application:
    a. Select **Enable Application Object Records Filtering**.
    b. Select your application from the **Application** list.
    c. In the **Having data audit record type** field, click ⌄.
    The list of auditable objects is displayed.
4. *(Optional)* Perform the following actions:
    - Specify other filtering settings.
    - Click **Report** to generate a PDF file of the log.

    Note: Export is not supported for this audit log.

View Instrument Run Records audit log

Instrument Run Records audit history allows you to view a log of the instrument run, including a summary of the run, the application objects used and the actions performed in the run, any changes made during the run, and a list outputs at the completion of the run.

IMPORTANT! Instrument Run Records audit log is not used by the Attune™ NxT Software. Therefore, the Instrument Run Records audit history is not available for the Attune™ NxT Software application.

Archive and restore audit records

Archive audit records

Archiving audit records removes the records from the SAE Administrator Console and saves them in an internally specified location on the same computer on which the SAE Administrator Console is installed. You can archive audit records in the **Settings** tab. You have two options to archive audit records: automatically (Auto Archive) or manually (Ad-hoc Archive).

Note: Archived audit records are accessible for viewing in the SAE Administrator Console.

- To archive audit records automatically:
  a. In the SAE Administrator Console main screen, click the **Settings** tab.

  b. Select **Auto Archive**.

  c. Select **Enable Auto Archive**, then select the **Archival mode** and associated settings:
     – By number of records or retention period
     – By number of records
     – By retention period

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

- To archive audit records manually:
  a. In the SAE Administrator Console main screen, click the **Settings** tab.

  b. Select **Archival history**.

  c. Click **Ad-hoc Archive**, select the start and end dates, then click **Archive**.

View or export archived audit records

1. In the SAE Administrator Console main screen, click the **Settings** tab.
2. Select **Archival history**.
3. Select a record, then click **View Archived Records** or **Export**.

Restore archived audit records

1. In the SAE Administrator Console main screen, click the **Settings** tab.
2. Select **Archival history**.
3. Select a restore option:
    - **Restore**—Restores an archived record. Click a record, then click **Restore**.
    - **Restore (upload)**—Restores a ZIP file that was exported from the archival history. Click **Restore (upload)**, then select the ZIP file.

5 Manage the e-Signature function

About e-Signatures

Actions that require signatures to be completed cannot be performed unless the required signatures are provided.

The **e-Signature** tab allows you to control the e-Signature rights of SAE roles, the actions requiring signatures, the reasons available for e-signature, and the data to be signed.

There are three built-in Actions Requiring Signatures for the Attune™ NxT Software that you can select in the **e-Signature** tab:

- Export Data
- Print Data
- Save As Template

Signatures represent the state of the Experiment at the time of signing. If any modifications are made to the Experiment after signing, actions that require signatures cannot be performed unless new signatures are provided.

You can view the log of e-Signatures and the status of the signatures (Current or Obsolete) by selecting **Audit History ▸ Application Object Records ▸ e-Signature Records**.

Note: For detailed information on the **e-Signature** and **Audit History** tabs, refer to the *Attune™ NxT Software User Guide* (Part. No. 100024236), available for download at **thermofisher.com/attune**.

Enable or disable the e-Signature function

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

IMPORTANT! Changing the e-Signature settings can affect opened files or records. Close any opened files or records before making changes to e-Signature settings.

1. In the SAE Administrator Console main screen, click the **e-Signature** tab.
2. Select or deselect **Enable e-Signatures**.
3. From the **Show e-Signature configuration for** dropdown, select **Attune™ NxT Software**.

   Note: If your SAE Administrator Console is configured to manage the SAE module for more than one application, you can configure the e-Signature settings for more than one application (for example, Attune™ NxT Software and SeqStudio™ Genetic Analyzer).
4. *(Optional)* Set or modify the e-Signature settings.
5. Click **Apply Settings**.

Select the actions that require e-Signature

1. In the SAE Administrator Console main screen, click the **e-Signature** tab.
2. In the **Actions Requiring Signatures** panel, select each action that requires an e-Signature.
3. For each meaning of each selected action, enter the number of e-Signatures that are required from each SAE role before the associated action can be performed.

   Note: If the selected user does not have permission to perform an e-Signature, then the action's required signature workflow will not be completed.
4. Click **Apply Settings**.

   Note: Actions that require e-Signatures to be completed cannot be performed unless the required e-Signatures are provided.

Configure the meanings of e-Signatures

The e-Signature meanings are the stated reason for an e-Signature. There are two built in e-Signature meanings for the Attune™ NxT application:

- Require and Approve Experiment for Template
- Review and Approve Data

If desired, you can add custom e-Signature meanings.

Add an e-Signature meaning

1. In the SAE Administrator Console main screen, click the **e-Signature** tab.
2. In the **e-Signature Meanings** panel, click **New Meaning**.
3. In the **Create New Meaning** dialog, enter an e-Signature meaning in the **Name** field, then click **Save**.
4. In the **e-Signature Meanings** panel, select a meaning from the **Meanings** list.
5. In the **Data signed for the selected meaning** list, select the item with which to associate the meaning.
6. Set the actions that require e-Signature and the number of e-Signatures that are required for that action.
7. Click **Apply Settings**.

Delete an e-Signature meaning

1. In the SAE Administrator Console main screen, click the **e-Signature** tab.
2. In the **e-Signature Meanings** panel, select a meaning from the **Meanings** list, then click **Delete**.

   Note: Default meanings cannot be deleted.
3. Confirm the deletion of the meaning, then click **OK**.
4. Click **Apply Settings**.

6

Advanced configuration options

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

Use the export and import functions to transfer settings from one installation of the SAE Administrator Console to another.

- To export settings:
  a. In the SAE Administrator Console main screen, click the **Settings** tab.

  b. Select **Export Configuration**.

  c. In the **Export Configuration** dialog box, select an export option:

Setting	Exports
All	SAE settings and SAE user accounts
Custom Users & Roles	– SAE user accounts with **Active** status – SAE roles and their associated permissions
Custom System & Roles	– SAE settings – SAE roles and their associated permissions

  d. Click **Export**.
  The exported file (DAT format) downloads to the default location of the computer.

- To import settings on another installation of the SAE Administrator Console:
  a. In the SAE Administrator Console main screen, click the **Settings** tab.

  b. Select **Import Configuration**.

  c. Click **Choose File** to select the DAT file with the desired configuration settings.

  d. Select an import option.

  e. Click **Import**.

f. If imported user accounts exist in the SAE Administrator Console, click **Skip** or **Overwrite** for each user account, then click **Confirm and Import**.

Configure user repositories

User repository overview

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

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

- **Internal**—Allows only SAE user accounts to sign in to an application. SAE user accounts are referred to as "local" accounts in the SAE Administrator Console.
  - SAE user accounts are created in the SAE Administrator Console and are identified as "local" in the **Users** tab.
  - User authentication is based on the accounts that are listed in the **Users** tab and the SAE settings that are specified in the **System** tab.
  - User permissions are determined by the roles that are configured in the SAE Administrator Console.
- **External LDAP**—Enables LDAP based authentication with an LDAP directory. Allows only external user accounts to sign in to an application.
  - User accounts are created in an LDAP (Lightweight Directory Access Protocol) user management system and are identified as "external" in the SAE Administrator Console **Users** tab.
  - User authentication is based on the accounts that are listed in the SAE Administrator Console **Users** tab and the external LDAP user repository. The SAE settings that are specified in the SAE Administrator Console **System** tab are not used.
  - User permissions are determined by the roles that are configured in the SAE Administrator Console.
  - All local user accounts except the default Administrator account are set to **Inactive**.
  - Passwords cannot be changed in the SAE Administrator Console.
- **Federated**—Allows internal (local) and external account sign-in to an application.
  - User accounts are created in the SAE Administrator Console or in an LDAP user management system.
  - User authentication is based on the respective internal or LDAP user repository.

Configure user repositories for SAE or external account access

1. In the SAE Administrator Console main screen, click the **Settings** tab.

2. Select **User repositories (advanced)**.

3. Select the **User repository definition**:

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

4. If you selected **External LDAP User Repository** or **Federated Repositories**, click **Next**, then enter the required information (see “User repository settings” on page 41).

5. Click the **Users** tab to display the list of accounts added to the SAE Administrator Console.

   - New LDAP accounts are listed as **External**, and **Role** is set to the default specified during account mapping. If no default was specified, accounts are set to **No Privileges Role**.
   - SAE user accounts that were previously created in the SAE Administrator Console are listed as **Local**.
   - If you selected LDAP, the **Status** for all accounts except for the default SAE Administrator account is set to **Inactive**.

6. Click **Test Connection** to synchronize the new accounts with the LDAP server.

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

7. If needed, edit the user accounts to assign roles.

User repository settings

Table 2 External LDAP User Repository and Federated Repositories settings

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

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

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

Index

thermofisher.com/support | thermofisher.com/askaquestion
thermofisher.com

5 May 2020