gibco

CTS™ Xenon™ Electroporation System SAE

USER GUIDE

for use with: SAE Administrator Console v2.1 or later

Publication Number MAN0025673

Revision A.0

For Research Use or Manufacturing of Cell, Gene, or Tissue- Based Products.

ThermoFisher SCIENTIFIC

Life Technologies Holdings Pte Ltd | Block 33 | Marsiling Industrial Estate Road 3 | #07-06, Singapore 739256

Revision history: Pub. No. MAN0025673

Revision	Date	Description
A.0	18 August 2023	New document for CTS™ Xenon™: *SAE Admin Console User Guide*.

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.

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

SAE Administrator Console version	Port	Condition
v2.1 and later	8443	Instrument-to-SAE Administrator Console server connection

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.

Contents

■ Product information 6

About the Security, Auditing, and E-signature Administrator Console 6

Security, Audit, and Electronic Signature (SAE) module components 7

View the terms of use 7

Network and password security requirements 7

Network configuration and security 7

Password security 8

SAE Administrator Console installation requirements 8

Upgrade to Clinical Manufacturing mode 8

Instrument-to-SAE Administrator Console server connection 8

Minimum computer requirements 9

Firewall ports that must be open 9

Compatibility of SAE versions and application profiles 9

Features of SAE v2.1 9

■ Get started 10

Overview of the SAE Administrator Console 10

Start the SAE Administrator Console 11

Open the SAE Administrator Console in the Google Chrome™ browser 11

Open the SAE Administrator Console in the Mozilla™ Firefox™ browser 11

Open the SAE Administrator Console in the Microsoft Edge™ browser 12

Install the application profiles 12

Configure application profiles 12

Optional tasks 13

Set up messaging notifications 13

Configure the SMTP server for email notifications 13

Identify signed in user 13

Display the software version 14

Change password 14

■ SAE Functions for the CTS™ Xenon™ Electroporation Instrument 15

Overview of the instrument features when the Security, Audit, and Electronic Signature (SAE) module is enabled 15

Profiles when the Security, Audit, and Electronic Signature (SAE) module is enabled ... 15

Sign in as a local administrator when SAE functions are enabled 16

SAE Administrator Console functions 16
- Functions that are controlled 16
- Functions that can be audited 17
- Functions that can be signed 17
- Default permissions and roles 18
- Dialog boxes in SAE mode 19

CTS™ Xenon™ Electroporation Instrument Operation in Clinical Manufacturing Mode . . . 21
- Create a Protocol 21
- Enter an audit reason 22
- Run a Protocol 23

■ Manage SAE user accounts and roles 28

Create an SAE user account 28

Edit a user account 29

Activate a suspended user account 29

Disable (inactivate) a user account 29

Reset a forgotten password 30

Manage user role 30
- Create a role 30
- Edit a role 31
- Delete a role 31

Generate, view, and print a user or role report 31

■ Manage the system security function 32

Change an SAE user account password from the instrument 32

Expired passwords 33

Enable or disable the system security function 34
- Enable SAE on the instrument and specify the SAE server (Administrator only) 34
- Disable SAE on the instrument (Administrator only) 36

Configure account setup and security policies 36

■ Manage the audit function 38

Enable or disable the **Audit** function 38
- Add new audit reason 38

Select items to audit and set the **Audit Mode** 38

Configure audit reasons 39
- Add new audit reason 40
- Edit an existing audit reason 40
- Delete an existing audit reason 40

View audit logs (Audit history) 41
View the System Configuration audit log 41
View the Action Records audit log 41
View Application Object Records audit log 42
View Instrument Run Records audit log 42
Archive and restore audit records 43
Archive audit records 43
View or export archived audit records 44
Restore archived audit records 44

■ Manage the e-signature function 45

E-signature requirements to use a protocol 45
Enable or disable the e-signature function 45
Select the actions that require e-signature 46
Configure the meanings of e-signatures 46
Add an e-signature meaning 47
Delete an e-signature meaning 47

■ Advanced Configuration Options for the SAE Administrator Console 48

Export and import user, system security, audit, and e-signature settings 48
Export settings to another installation of the SAE Administrator Console 48
Import settings from another installation of the SAE Administrator Console 48
Archive and restore audit records 49
User repository overview 49
Configure user repositories for SAE or external account access 49
User repository settings 50
User or administrator sign-in with LDAP or federated user repositories 51

Troubleshooting 52

SAE error messages and actions 52

Documentation and support 55

Customer and technical support 55
Limited product warranty 55

Product information

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

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

The Security, Audit, and Electronic Signature (SAE) module can be configured to provide the following functionality:

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

Security, Audit, and Electronic Signature (SAE) module components

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

- **SAE Administrator Console**—This component is a tool used by an SAE administrator to configure the Security, Audit, and Electronic Signature (SAE) module. The SAE Administrator Console runs in a web browser, even though it is installed locally on your computer. Google Chrome™ is the recommended web browser, but Mozilla™ Firefox™ or Microsoft Edge™ can be used.
- **SAE server** (server)—This component is a service that runs in the background and stores the settings, user accounts, audit records, and e-signature records. By default, the SAE server is installed on the same computer as the SAE Administrator Console. The communication between the SAE Administrator Console and the SAE server (v2.1 and later) uses the encrypted HTTPS protocol. The SAE server is started automatically when the computer is started.
- **SAE screens** (client)—This component are the screens displayed by the embedded Graphical User Interface (eGUI) of the CTS™ Xenon™ Electroporation Instrument during instrument use. The screens (sign in, audit, and e-signature) require user input. More than one application can be connected to and controlled by the same instance of the SAE Administrator Console.
- **OPC UA server**—This component is the instrument server responsible for relaying instrument data via OPC UA protocol to an OPC UA client. The SAE Administrator Console acts as the client for the internal OPC UA server of the CTS™ Xenon™ Electroporation Instrument.

  As part of the upgrade to Clinical Manufacturing mode for SAE, options to connect with other OPC UA clients are removed. The CTS™ Xenon™ Electroporation Instrument has been validated to operate with only a single OPC UA client.

View the terms of use

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

To view the terms of use, click **Settings ▸ About terms of use**.

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.

Thermo Fisher Scientific cannot retrieve lost passwords.

SAE Administrator Console installation requirements

For Xenon™ and DynaCellect™ systems, the SAE Administrator Console should be installed to a customer-supplied computer.

See "Minimum computer requirements" on page 9.

Only one SAE Administrator Console can be installed on one computer. Multiple Xenon™ instruments can connect to the single instance of the SAE Administrator Console.

The SAE Administrator Console runs on the Windows™ Operating System, and 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.

Upgrade to Clinical Manufacturing mode

To enable SAE functions on the CTS™ Xenon™ Electroporation Instrument, the instrument must be upgraded to Clinical Manufacturing (CM) mode.

Note: The CM mode upgrade process is irreversible.

⚠ **WARNING!** To preserve information and data stored on the CTS™ Xenon™ Electroporation Instrument, it is critical to perform protocol and data backup before upgrading the instrument to CM mode.

- If an OPC-UA client was configured for the instrument, this connection is lost following the upgrade.
- Install the SAE Administrator Console and the SAE server on a computer with a static IP address (recommended) or a dynamic IP address.

Instrument-to-SAE Administrator Console server connection

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

Minimum computer requirements

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

- Pentium® 4 processor or compatible
- Operating system—Windows™ 10 (64-bit)
- Memory—16 GB RAM minimum
- Monitor—1280 × 1024 resolution or higher
- Hard drive—500 GB minimum free space

Firewall ports that must be open

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

SAE Administrator Console version	Port	Condition
v2.1 and later	8443	Instrument-to-SAE Administrator Console server connection

Compatibility of SAE versions and application profiles

Thecompatibility of SAE versions and applications are listed in the following table:

Application	SAEversion
CTS™ Xenon™ Electroporation System	SAE v2.1

Features of SAE v2.1

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

SAE Administrator Console version	Feature
SAE v2.1	Converts the URL to HTTPS (see “Start the SAE Administrator Console” on page 11).

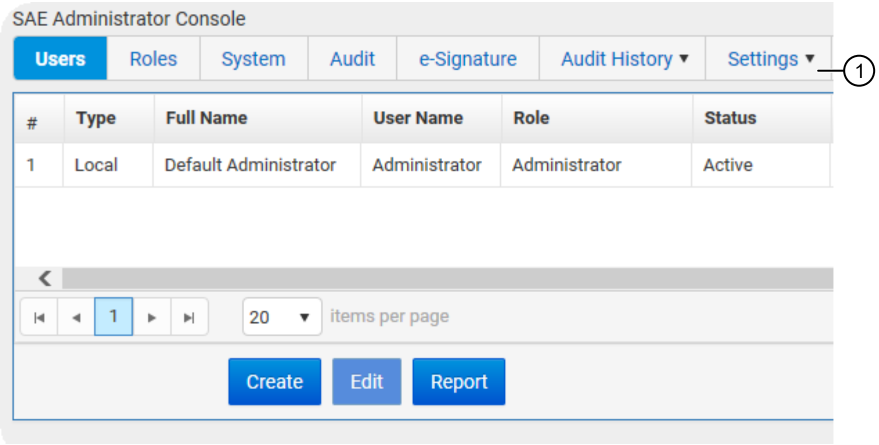
Get started

Overview of the SAE Administrator Console

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, but Mozilla™ Firefox™ or Microsoft Edge™ can be used.

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

The SAE Administrator Console main screen is used to access the various functions of the software. Click the navigation tabs at the top to display different screens in the software.



#	Type	Full Name	User Name	Role	Status
1	Local	Default Administrator	Administrator	Administrator	Active

① Navigation tabs

Start the SAE Administrator Console

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

For more information, see "Open the SAE Administrator Console in the Google Chrome™ browser" on page 11 or "Open the SAE Administrator Console in the Microsoft Edge™ browser" on page 12.

Contact Support for additional questions.

1. During the upgrade to Clinical Manufacturing mode, a shortcut to launch the SAE Administrator Consoleis placed on the Windows™ desktop. If this shortcut has been removed, the default directory to launch the Console is located under `C:\Program Files (x86)\Applied Biosystems\SAE Admin Console`.

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

   If messaging notifications are enabled (see page 13), the **Event Notifications** dialog box is displayed.

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

3. Two options are available in the **Event Notifications** dialog box:

   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.

Open the SAE Administrator Console in the Google Chrome™ browser

If the URL of the SAE Administrator Console has not been added as a trusted site in the Google Chrome™ browser, "**Not secure**" is displayed in the URL bar, but the user can still sign in.

If the URL of the SAE Administrator Console is added as a trusted site in the Google Chrome™ browser, the same user interface will be displayed as if the URL was not added as a trusted site.

Open the SAE Administrator Console in the Mozilla™ Firefox™ browser

If the URL of the SAE Administrator Console has not been added as a trusted site in the Mozilla™ Firefox™ browser, "**Warning: Potential Security Risk Ahead**" is displayed.

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

The SAE Administrator Console will be launched with **Not Secure** displayed in the URL bar. The user can still sign in.

If the URL of the SAE Administrator Console is added as a trusted site in the Mozilla™ Firefox™ browser, the warning message will not be displayed (for the localhost domain only).

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

Open the SAE Administrator Console in the Microsoft Edge™ browser

If the URL of the SAE Administrator Console has not been added as a trusted site in the Microsoft Edge™ browser, "**Your connection isn't private**" is displayed.

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

The SAE Administrator Console will be launched with **Not Secure** displayed in the URL bar. The user can still sign in.

If the URL of the SAE Administrator Console is added as a trusted site in the Microsoft Edge™ browser, the warning message will not be displayed (for the localhost domain only).

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

Install the application profiles

An application profile contains default SAE Administrator Console settings for an application.

Before the SAE Administrator Console can be used to configure the Security, Audit, and Electronic Signature (SAE) module for an application, a Thermo Fisher Scientific representative will install a profile for the CTS™ Xenon™ Electroporation System application. Each instrument application has its own application profile or set of application profiles.

1. In the SAE Administrator Console main screen, click **Settings ▶ Manage Application Profiles ▶ Install Application Profile**, then select the appropriate application profile (.dat file).

2. Click **Verify Data FileInstall new applicationInstall**.

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

Configure application profiles

Configuring application profiles in the SAE Administrator Console requires an SAE administrator account. See “Install the application profiles” on page 12.

In the SAE Administrator Console, an application profile contains default settings for an application. Before using the SAE Administrator Console, a Thermo Fisher Scientific representative will install, then configure profiles for the CTS™ Xenon™ Electroporation Instrument.

Optional tasks

Set up 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 select the **Settings** tab, then click **Notifications**.
2. In the **Edit NotificationsSettings** dialog box, select **Notify at Administrator sign in** for the events of interest.
3. (*Optional*) Select **Notify by Email**, then specify an email address.
4. Click **Save**.

Configure the SMTP server for email notifications

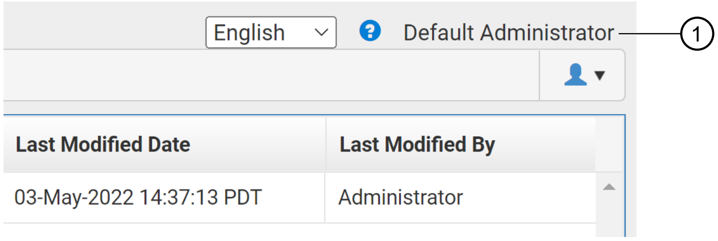
Configure the SMTP server so that the SAE Administrator Console can send email notifications.

1. In the SAE Administrator Console select the **Settings** tab, then click **Email Server**.
2. In the **SMTP Configuration** dialog box, enter the following:
   a. **SMTP host**, **SMTP port**, and **SMTP sender**
      Select **Authentication required** if the SMTP server requires authentication.

   b. **User name** and **Password**
      Select **Use SSL** if the SMTP server requires an encrypted channel connection.
3. Click **Save**.

Identify signed in user

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



Default Administrator

Last Modified Date	Last Modified By
03-May-2022 14:37:13 PDT	Administrator

① Signed in user

Display the software version

1. In the SAE Administrator Console select the **Settings** tab.
2. Click **About** to display the SAE Administrator Console software version.

Change password

1. 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**.

SAE Functions for the CTS™ Xenon™ Electroporation Instrument

Overview of the instrument features when the Security, Audit, and Electronic Signature (SAE) module is enabled

SAE Administrator Console functions:

- Create all SAE user accounts
- Manage password policies of accounts
- Assign access rights to accounts
- Import instrument profiles
- Configure audit reasons and settings
- Storing audit logs
- Configure e-signature settings

CTS™ Xenon™ Electroporation Instrument functions in Clinical Manufacturing (CM) mode:

- Process and enforce SAE policies
- Send audit logs for user actions to SAE server
- Perform e-signing
- Maintain connection to server for policies update

The following instrument features are not available when the Security, Audit, and Electronic Signature (SAE) module is enabled:

- Addition of other OPC-UA clients
- Linking to the Connect Platform, including using a Connect Platform account to sign in.

Profiles when the Security, Audit, and Electronic Signature (SAE) module is enabled

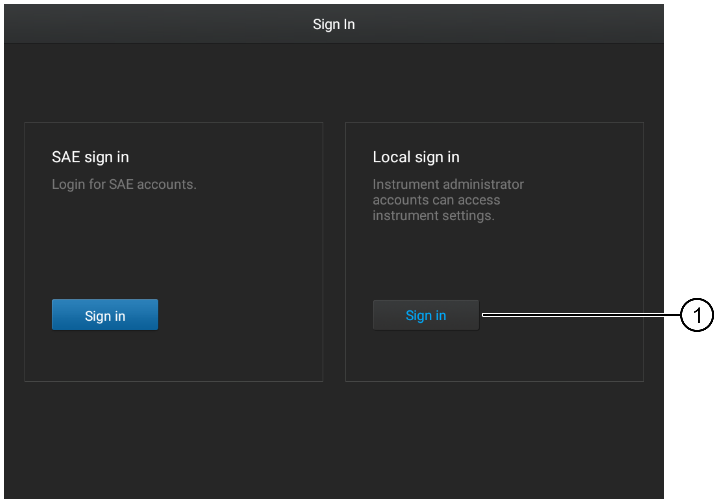
After the Security, Audit, and Electronic Signature (SAE) module is enabled on the instrument, the local instrument profiles and the Connect Platform profiles will not be available. An account from the SAE Administrator Console must be used to sign-in to the instrument when theSecurity, Audit, and Electronic Signature (SAE) module is enabled.

A local instrument administrator can sign in to the instrument to perform limited functions.

Sign in as a local administrator when SAE functions are enabled

Sign in as a local administrator to access the instrument settings.

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



Sign In

SAE sign in

Login for SAE accounts.

Local sign in

Instrument administrator accounts can access instrument settings.

① Sign in for administrator

2. In the **Local Administrator Sign In** screen, select your local administrator profile.

3. Enter your PIN, then select **Enter**.

SAE Administrator Console functions

Functions that are controlled

The following functions are controlled, depending on the user role. Role-based permissions can be modified at any time.

Controllable functions	
Start SingleShot run	View/export instrument logs
Start/Pause/Resume/Abort MultiShot run	Reset instrument to factory default
Creation (cloning) of new custom run modules	Performing firmware update on the instrument
Creation/editing of custom run modules	• Modifications of the following instrument system settings: – Network configuration – Instrument name
Viewing of available EP protocols	
Searching of available EP protocols	
Modification of EP protocols	

(continued)

Controllable functions	
Saving of modifications	– Date/time/time zone – Sleep mode setting – Brightness settings – Manage process details – SAE settings
Deletion of custom EP protocols	
Update own password	
Perform instrument self-diagnostics test	
Export of custom EP protocols from USB/Cloud/Network	e-Signature access

Functions that can be audited

Certain instrument functions can be audited. This depends on how the SAE administrator has configured the audit settings.

Table 1 Auditable functions

Application Objects	User Actions	
SingleShot protocol creation	Disable Security	Export protocol
MultiShot protocol creation	Enable Security	Protocol imported
—	Sign In Success	Run aborted
—	Sign Out	Run completed
—	Sign In Failure	Run error
—	Firmware upgrade started	Run paused
—	Instrument settings modified	Run resumed
—	Protocol exported	Run started

Functions that can be signed

Certain instrument functions can be signed. This depends on how the SAE administrator has configured the e-signature settings.

The following functions can be signed with an e-signature:

- SingleShot Protocol creation – Apply approvals to the creation of a SingleShot Protocol, as needed.
- MultiShot Protocol creation – Apply approvals to the creation of a MultiShot Protocol, as needed.

The following User Actions can be audited:

Default permissions and roles

The SAEmodule provides the following default permissions and roles. You can use the default roles when you create SAE user accounts or create custom roles.

- Administrator
- Scientist
- Technician

A "**Default Administrator**" role always exists and is given default access to application functions.

IMPORTANT! SAE permissions for a role apply to all user accounts that are assigned to the role. The roles and associated user-configurable permissions are listed in the following table. You can also double-click the role in the **Roles** tab to display the list of permissions.

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

Table 2 Conferrable permissions and default user roles

Permissions		Default roles [1]			Local account
Function Group	Function	Xenon™ Admin	Xenon™ Scientist	Xenon™ Technician	Admin
Run	Run protocol	Yes	Yes	Yes	No
	Run others protocol	Yes	Yes	Yes	No
Protocol management	Create EP protocol	Yes	Yes	No	No
	View EP protocol	Yes	Yes	No	No
	View others EP protocol	Yes	Yes	Yes	No
Protocol Management	View others unsigned EP protocol	Yes	Yes	Yes	No
	Edit EP protocol	Yes	Yes	No	No
	Edit others EP protocol	Yes	Yes	No	No
	Delete EP protocol	Yes	Yes	No	No
	Delete others EP protocol	Yes	Yes	No	No
	Import EP protocol	Yes	Yes	No	No
	Export EP protocol	Yes	Yes	No	No
User Account Management	Reset own password	Yes	Yes	Yes	Yes
Service Tools	Run diagnostics checks	Yes	No	No	Yes

Table 2 Conferrable permissions and default user roles *(continued)*

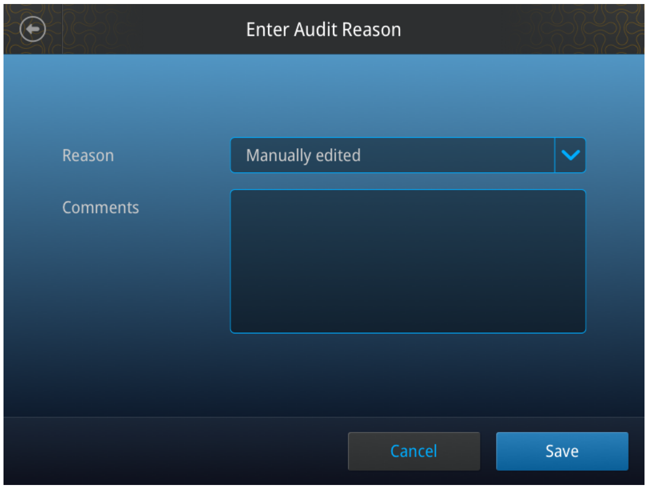
Permissions		Default roles [1]			Local account
Function Group	Function	Xenon™ Admin	Xenon™ Scientist	Xenon™ Technician	Admin
Service Tools	View instrument logs	Yes	No	No	No
	Perform factory reset	No	No	No	Yes
Instrument Configuration	Perform firmware update	Yes	—	—	—
	Change system settings	Yes	—	—	—
Security Configuration	Perform e-signing	Yes	—	—	—

[1] Default, can be modified

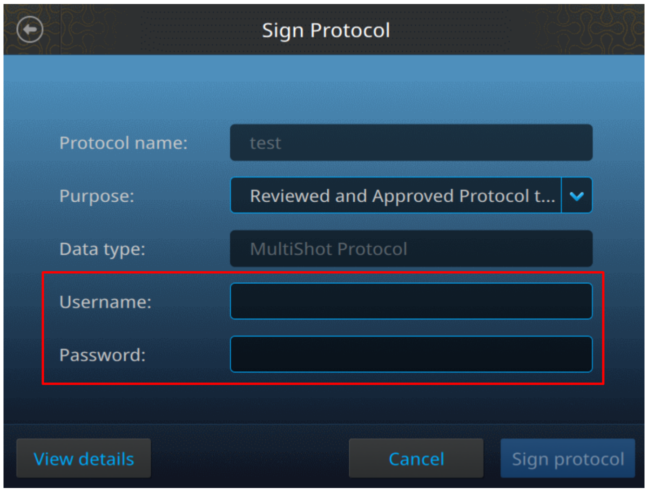
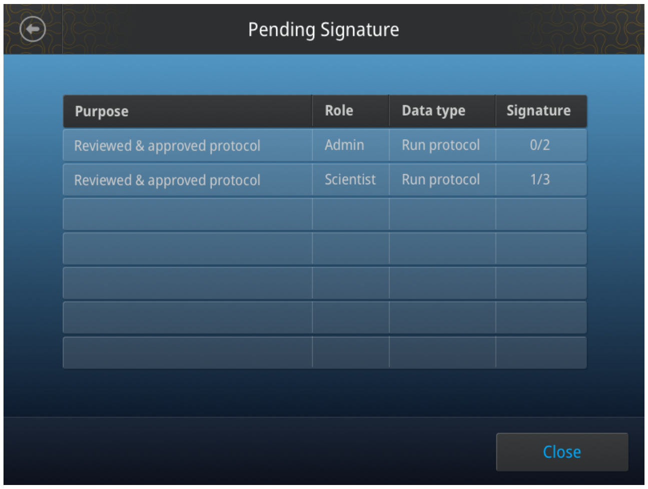
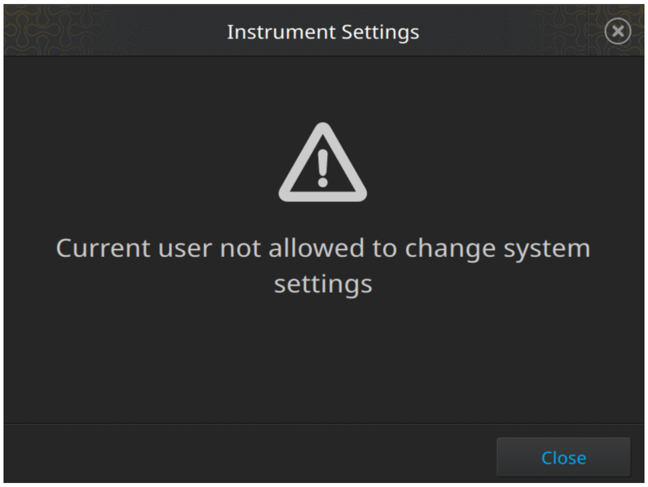
Dialog boxes in SAE mode

New dialog boxes have been added with the upgrade to Clinical Manufacturing mode for SAE.

Note: The appearance of the screens depends on the configurations set in the SAE Administrator Console. Some of the features and functions described in this section might not be accessible to if the Administrator has not configured these settings.

Dialog box	Description
 Enter Audit Reason Reason: Manually edited Comments 	An action is set up for auditing and requires you to specify a reason for the action. Configurations for this screen are located under the **Audit** tab of SAE Administrator Console.

(continued)

Dialog box	Description
 Sign Protocol Protocol name: test Purpose: Reviewed and Approved Protocol t... Data type: MultiShot Protocol Username: Password: 	An action is set up for electronic signature and allows you to enter your password to allow the action. Configurations for this screen are located under the **e-signature** tab of SAE Administrator Console. Additionally, the Role must be configured to perform e-signing.
 Pending Signature Purpose | Role | Data type | Signature Reviewed & approved protocol | Admin | Run protocol | 0/2 Reviewed & approved protocol | Scientist | Run protocol | 1/3 	Review the list of e-signatures using the View Details button of the **Sign Protocol** screen. The right column displays the number of e-signatures accepted versus total number required.
 Instrument Settings Current user not allowed to change system settings 	A notification is displayed if you select an action but do not have the allowed permissions.

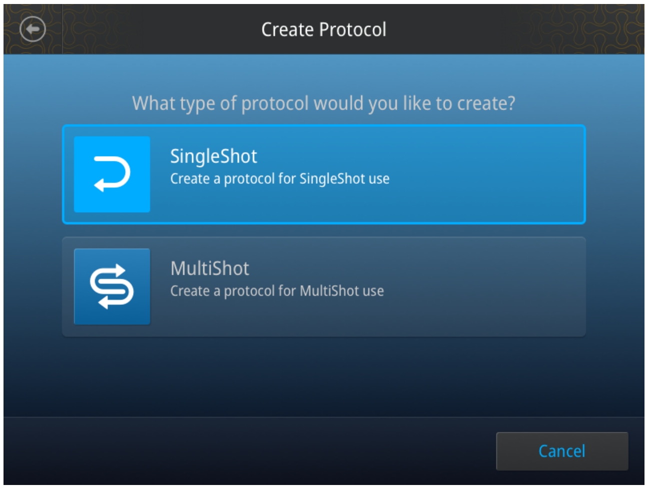
CTS™ Xenon™ Electroporation Instrument Operation in Clinical Manufacturing Mode

Create a Protocol

1. In the **Home** screen, select **Create protocol**.

   The steps for SingleShot and MultiShot protocol creation are similar. The following procedure, uses the SingleShot protocol as an example.

2. Select the protocol type you want to create.

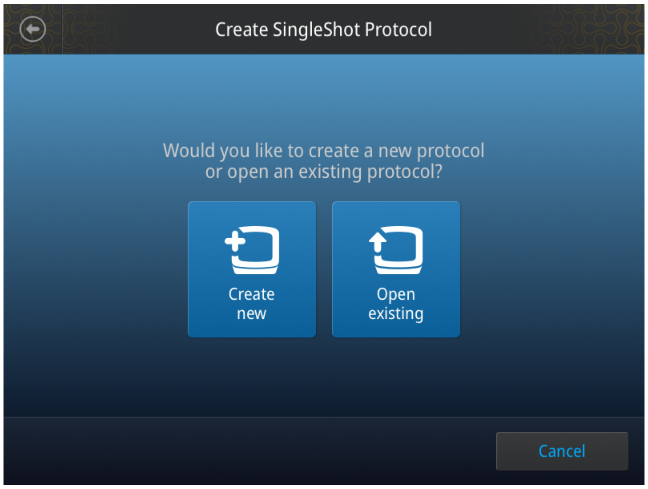


Create Protocol

What type of protocol would you like to create?

SingleShot
Create a protocol for SingleShot use
MultiShot
Create a protocol for MultiShot use
Cancel

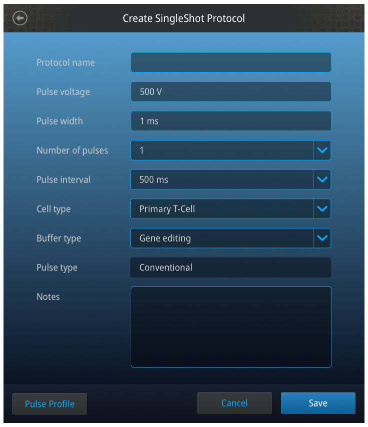
3. Select **Create new**.



Create SingleShot Protocol

Would you like to create a new protocol or open an existing protocol?

4. Configure the protocol details.



Create SingleShot Protocol

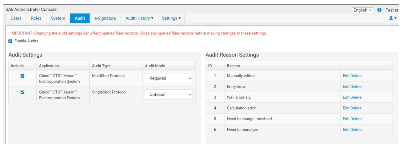
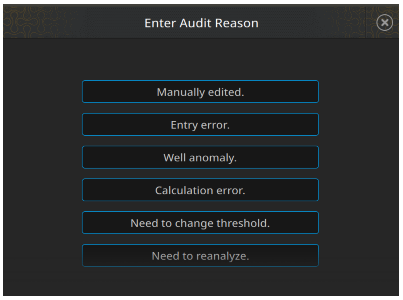
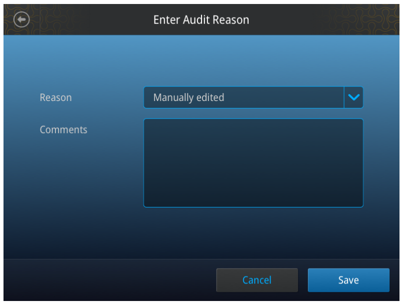
Protocol name:
Pulse voltage: 500 V
Pulse width: 1 ms
Number of pulses: 1
Pulse interval: 500 ms
Cell type: Primary T-Cell
Buffer type: Gene editing
Pulse type: Conventional
Notes:

5. Choose the Audit Reason then select **Save**. The Audit Reason configuration is set in SAE Administrator Console. If this prompt is not seen, the Audit Reason has been set to "Silent."

Enter an audit reason

Depending on the way that your SAE administrator configures audit settings, the **Enter Audit Reason** screen may be displayed when you change one of the following items:

- Create or modify a SingleShot protocol
- Create or modify a MultiShot protocol

Appearance of Enter Audit Reason screens		
		

SAE Administrator Console

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

☑ Enable Audits

Audit Settings

Include	Application	Audit Type	Audit Mode
☑	Gibco™ CTS™ Xenon™ Electroporation System	MultiShot Protocol	Required
☑	Gibco™ CTS™ Xenon™ Electroporation System	SingleShot Protocol	Optional

Audit Reason Settings

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

Enter Audit Reason

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

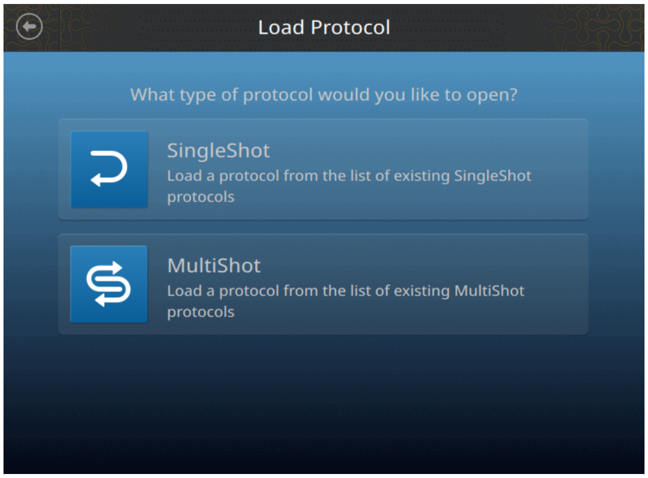
Enter Audit Reason

Reason: Manually edited
Comments:

Run a Protocol

1. In the home screen, select on **Load Protocol** to run an existing protocol.

   The steps for SingleShot and MultiShot protocol creation are similar.



Load Protocol

What type of protocol would you like to open?

SingleShot
Load a protocol from the list of existing SingleShot protocols

MultiShot
Load a protocol from the list of existing MultiShot protocols

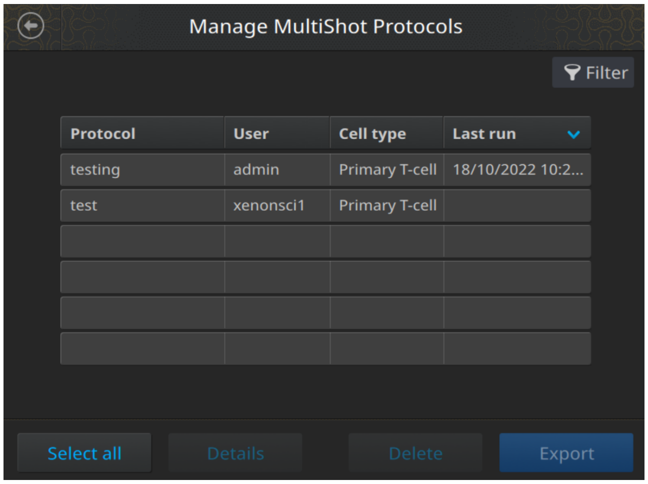
2. Select the protocol type you want to run.

   The following procedure, uses the MultiShot protocol as an example.

3. A list of protocols is displayed. To proceed with the run, select a protocol.

   a. Navigate to **Load Protocol** ▸ ▸ **MultiShot / SingleShot** ▸ ▸ **Actions** ▸ ▸ **Manage protocol** to **Delete** or **Export** protocols.

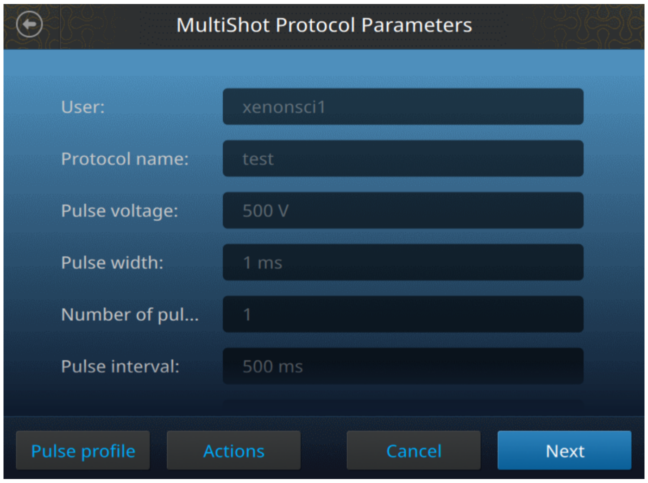
   b. Navigate to **Load Protocol** ▸ ▸ **MultiShot / SingleShot** ▸ ▸ **Actions** to **Import** protocols.



Manage MultiShot Protocols

Protocol	User	Cell type	Last run
testing	admin	Primary T-cell	18/10/2022 10:2...
test	xenonsci1	Primary T-cell	

4. The user can view the protocol details, and click **Next** to proceed with the run.



MultiShot Protocol Parameters

User: xenonsci1

Protocol name: test

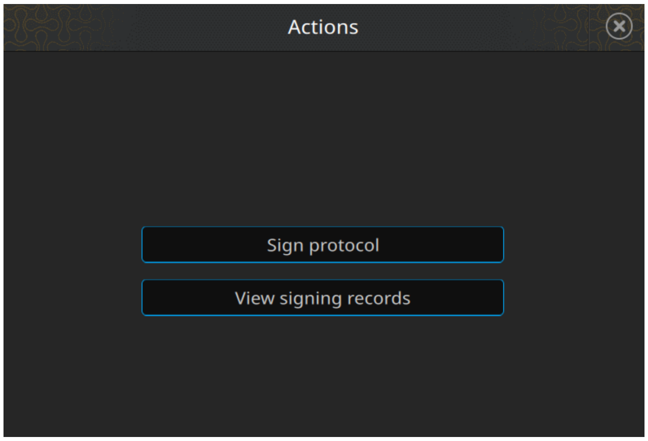
Pulse voltage: 500 V

Pulse width: 1 ms

Number of pul... 1

Pulse interval: 500 ms

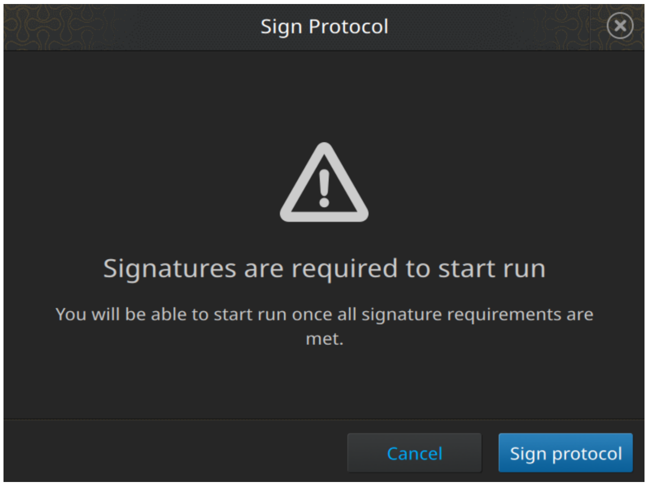
5. Select **Actions** to sign the protocol or view signing records.



Actions

6. A message is displayed if the protocol e-signature requirements have not been met. Select **Sign protocol** to apply e-signatures.

Note: If the e-Signature requirements are not met, the protocol cannot be used until they are satisfied. Once a protocol has all e-signatures required, the protocol can be run without further approvals unless further modified.

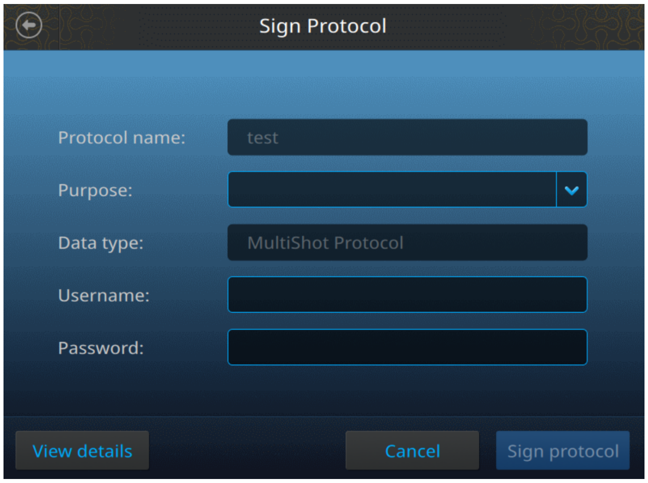


Sign Protocol

Signatures are required to start run

You will be able to start run once all signature requirements are met.

7. Select the **Purpose** field to view and select the e-signature meanings.



Sign Protocol

Protocol name: test

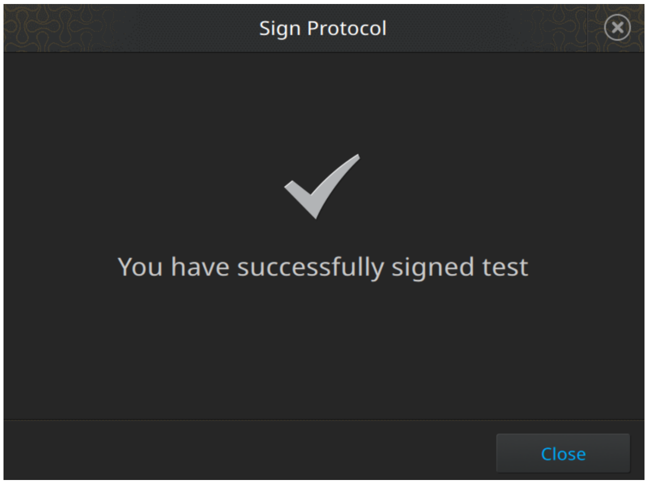
Purpose:

Data type: MultiShot Protocol

Username:

Password:

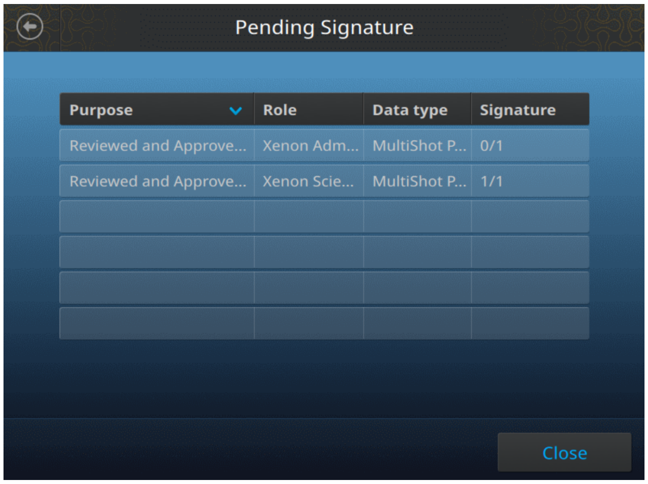
8. Enter the approver SAE credentials to sign off on the protocol then select **Sign Protocol**.



Sign Protocol

You have successfully signed test

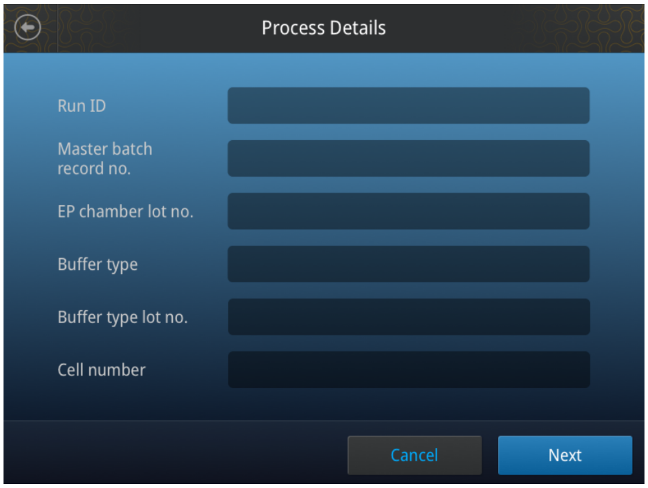
9. Select **View Details** from the **Sign Protocol** screen to display the list of e-signatures received and number of signatures collected versus the number required.



Pending Signature

Purpose	Role	Data type	Signature
Reviewed and Approve...	Xenon Adm...	MultiShot P...	0/1
Reviewed and Approve...	Xenon Scie...	MultiShot P...	1/1

10. Once all required e-signatures have been entered, the protocol can be used. The user will be taken to the **Process Details** screen, where batch details can be added.



11. Select **Next** once data has been entered to begin the run.

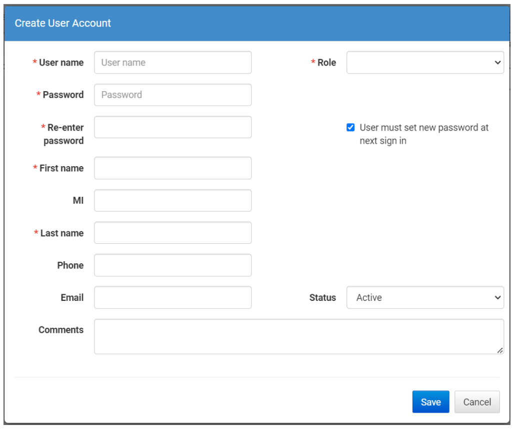
Manage SAE user accounts and roles

Create an SAE 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 the SAE Administrator Console.

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



Create User Account

* User name: User name

* Role:

* Password: Password

☑ User must set new password at next sign in

* Re-enter password:

* First name:

MI:

* Last name:

Phone:

Email:

Status: Active

Comments:

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**.

   Note: Each roles grants specific SAE permissions to the user.

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

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.

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**.

Manage user role

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

If your SAE Administrator Console is configured to manage the Security, Audit, and Electronic Signature (SAE) module for more than one application, you can create roles that specify permissions for more than one application.

Reference the chapter for the application for a list of permissions.

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

Create a role

1. In the SAE Administrator Console main screen, click the **Roles** tab.
2. Click **Create**.
3. Enter a role name and (*optional*) description.
4. Select one or more applications to which the role applies.
5. Select SAE permissions for the role. To select all SAE permissions in a category, select the checkbox next to the category.
6. Click **Save**.

Edit a role

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

   Note: You cannot edit the Administrator role.

3. Edit the 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**.

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.

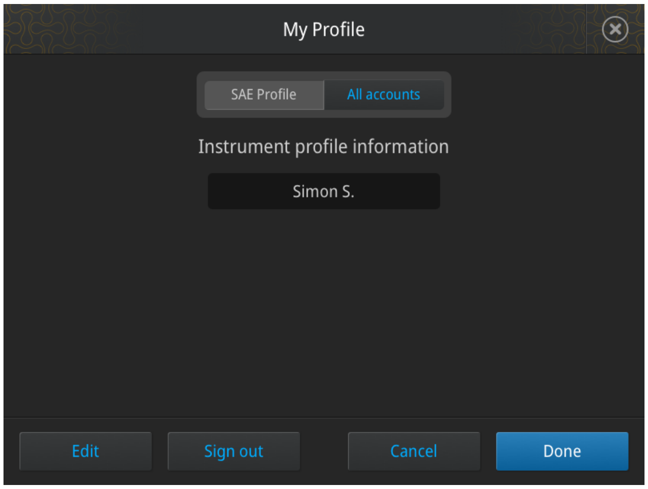
Manage the system security function

Change an SAE user account password from the instrument

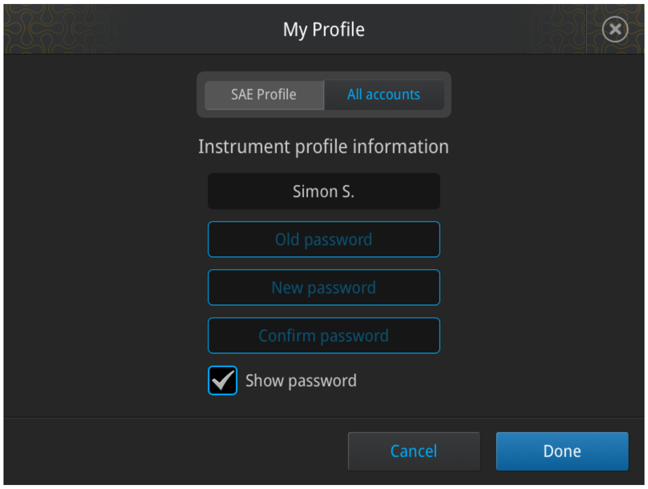
IMPORTANT! The CTS™ Xenon™ Electroporation Instrument must be connected to the SAE server in order for the SAE account password to be updated for both the SAE Administrator Console and instrument.

To update your password, you must be signed in with the instrument in SAE mode.

1. In the home screen, select 👤 **(Profile)** to diplay the **My Profile** screen.



2. Select **Edit** to diplay the **Edit My Profile** screen.



My Profile

Instrument profile information

Simon S.

Old password

New password

Confirm password

☑ Show password

3. Select the **Old password** field, enter the current SAE account password, then select **Enter**.

4. Select the **New password** field, enter a new SAE account password, then select **Enter**.

   (*Optional*) Select the **Show password** checkbox to show or hide the password.

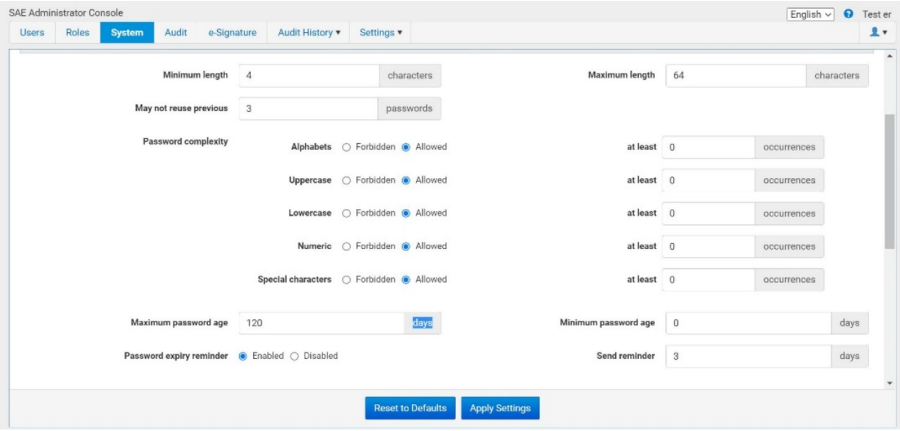
5. Select the **Confirm password** field, enter the new SAE account password again, then select **Enter**.

6. Click **Done**.

Your SAE password is changed on the SAE server as well.

Expired passwords

Password expiry reminders can be configured by an Administrator through the SAE Administrator Console.



SAE Administrator Console

Minimum length 4 characters

Maximum length 64 characters

May not reuse previous 3 passwords

Password complexity

Alphabets ○ Forbidden ● Allowed at least 0 occurrences

Uppercase ○ Forbidden ● Allowed at least 0 occurrences

Lowercase ○ Forbidden ● Allowed at least 0 occurrences

Numeric ○ Forbidden ● Allowed at least 0 occurrences

Special characters ○ Forbidden ● Allowed at least 0 occurrences

Maximum password age 120 days

Minimum password age 0 days

Password expiry reminder ● Enabled ○ Disabled

Send reminder 3 days

If a set number of days is configured, a reminder is shown when the current date is within the set number of days to the user account password expiration date.

This reminder is only shown during the initial login. Subsequent login due to session timeout will not show the same reminder message.

If a user password has expired, the user will be brought to a screen to change his/her password during login. This is a mandatory change. If the change is not performed, the user will not be able to complete the sign in process.

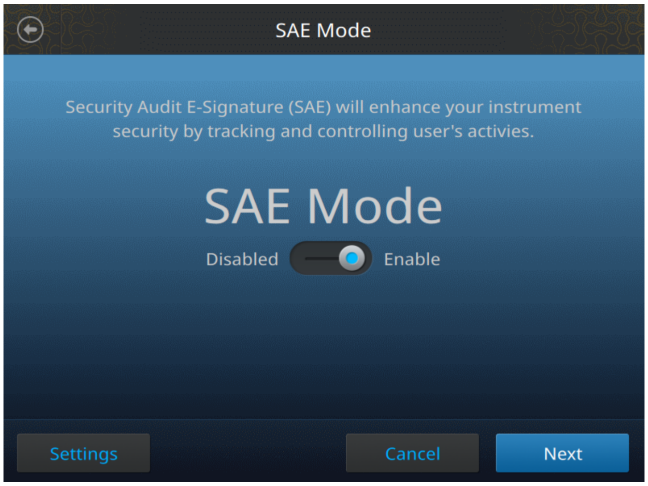
Enable or disable the system security function

The system security function cannot be disabled in the SAE Administrator Console. To disable user sign in to an application, you must disable SAE in the application.

Enable SAE on the instrument and specify the SAE server (Administrator only)

This procedure requires a local administrator profile on the CTS™ Xenon™ Electroporation Instrument as well as an administrator account in the SAE Administrator Console.

1. Sign in with a local administrator account (see “Sign in as a local administrator when SAE functions are enabled” on page 16).
2. In the home screen, select ⚙ **(Settings)** ▸ **SAE Mode** to display the **SAE Mode** screen.
3. In the **SAE Mode** screen, set the **SAE Mode** slider to **Enable**.



Security Audit E-Signature (SAE) will enhance your instrument security by tracking and controlling user's activies.

4. Select the **Settings** field to enter the IP address of the SAE server.
5. Select the **Port** field, enter the port, then select **Next**.
6. Enter the SAE administrator username and password when prompted, then select **Enable**.

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

Requirements to enable SAE on the CTS™ Xenon™ Electroporation Instrument

Rules for enabling SAE on the instrument are as follows:

- Enabling SAE can only be done by SAE user accounts with administrative privilege. The user is required to provide an SAE administrator account username and password to enable SAE.
- Enabling SAE requires a connection to the SAE server. The instrument will then send:
  - An authentication for admin request is sent to the SAE server.
  - If provided credentials are valid and the specified SAE user account is authorized to enable SAE, the server returns a success status code.
  - Upon successful admin authentication, the following will be performed:
    - Log out the current instrument user.
    - Initiate an SAE user session for specified admin account.
    - All relevant security, audit, and e-signature configuration will take effect immediately on the instrument.
    - Two audit records will appear in the SAE Administrator Console:
      - Enable Security
      - Login Success
    - Instrument will return to the home screen.
  - If step (b) is not successful, an error message, depending on the error type will be displayed accordingly:
    - Unable to reach SAE Server, please check SAE server settings.
    - Unable to sign in. The username or password is incorrect.
    - Account is disabled. Account needs to be enabled by SAE admin to sign-in to this instrument.
    - You have reached the maximum sign-in attempts. Your account will be temporarily locked out. Please try again later.
    - Current user is not allowed to update SAE configuration.
- After SAE has been enabled:
  - Only SAE user accounts can access the instrument to perform runs.
  - Users will not be able to login to the instrument via the local instrument profiles that were in use previously.

    Note: local instrument administrator accounts will still be able to login via the login home page to access the instrument settings.

    - The local instrument profiles and their associated data are not deleted via this action of enabling SAE.
    - The action of disabling SAE enables these local instrument profiles to be accessible again.

Disable SAE on the instrument (Administrator only)

This feature is intended to discontinue OPC UA communication with the SAE Administrator Console, if needed (e.g., for server pr network modifications). To resume operation with the instrument, SAE will need to be reenabled.

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

1. Sign in with a local administrator account (see "Sign in as a local administrator when SAE functions are enabled" on page 16).
2. In the home screen, select ⚙ **(Settings)** ▸ **SAE Mode** to display the **SAE Mode** screen.
3. In the **SAE Mode** screen, set the **SAE Mode** slider to **Disable**, then select **Done**.
4. Enter the password for the SAE administrator account, then select **Disable**.

The **Sign In** screen is displayed. All relevant security, audit, and e-signature configuration will no longer have any effect on the instrument and two audit records will appear in the SAE Administrator Console:

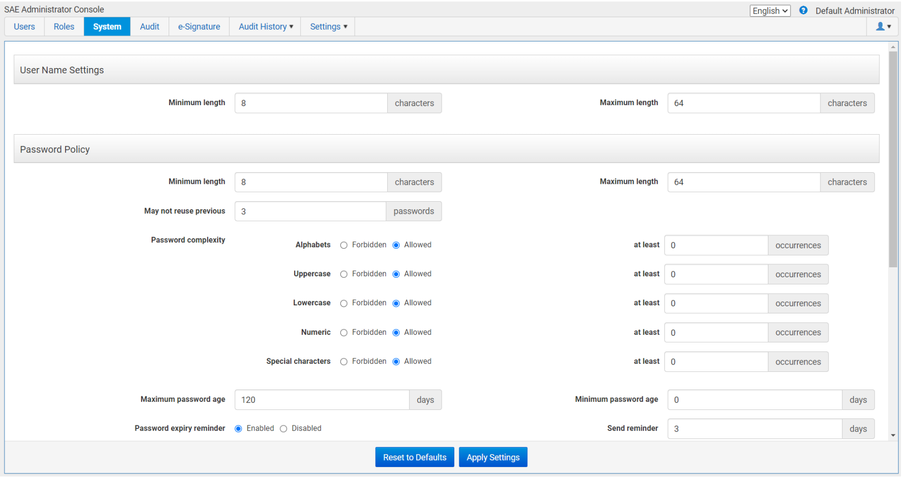
- Disable SAE
- Logout

Configure account setup and security policies

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

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

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



User Name Settings

Minimum length 8 characters
Maximum length 64 characters

Password Policy

Minimum length 8 characters
Maximum length 64 characters
May not reuse previous 3 passwords

Password complexity
Alphabets ○ Forbidden ● Allowed at least 0 occurrences
Uppercase ○ Forbidden ● Allowed at least 0 occurrences
Lowercase ○ Forbidden ● Allowed at least 0 occurrences
Numeric ○ Forbidden ● Allowed at least 0 occurrences
Special characters ○ Forbidden ● Allowed at least 0 occurrences

Maximum password age 120 days
Minimum password age 0 days
Password expiry reminder ● Enabled ○ Disabled
Send reminder 3 days

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

2. In the **User Name Settings** pane, specify the username requirements and limits (username length, and so on).

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 select **Enabled**:

Feature	Description
Set **Threshold** limit for login attempts Set **Account lockout duration** in minutes	If a user attempts to sign in with an incorrect username or password more than the number of times set for the threshold, the user is locked out for the time specified.
Enable or disable reset of **Sign in attempts counter** Set **Reset account lockout** duration in minutes	If the counter reset is enabled, the counter resets to zero 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:

Feature	Description when enabled
Set **Automatic screen locking** in minutes Set **Inactivity duration** in minutes	The screen is locked if there is no activity for the time specified. A user must enter their username and password to unlock the screen.
Enable **Open file from non-SAE system**	The application allows users to access data files that were generated when SAE functions were disabled.
Enable **Client offline sign in** [1] Enable **Offline sign in threshold**	When the SAE server is offline, users can sign in and use an application for the time specified.

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

6. Click **Apply Settings**.

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

7. Enable the offline login again and set a sufficiently high threshold value (>30 minutes) after reset.

Manage the audit function

Enable or disable the Audit function

Use the **Audit** tab to control the events that are audited and provide a list of reasons that are available to users when the audit mode is set to **Optional** or **Required** (see "Select items to audit and set the Audit Mode" on page 38).

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

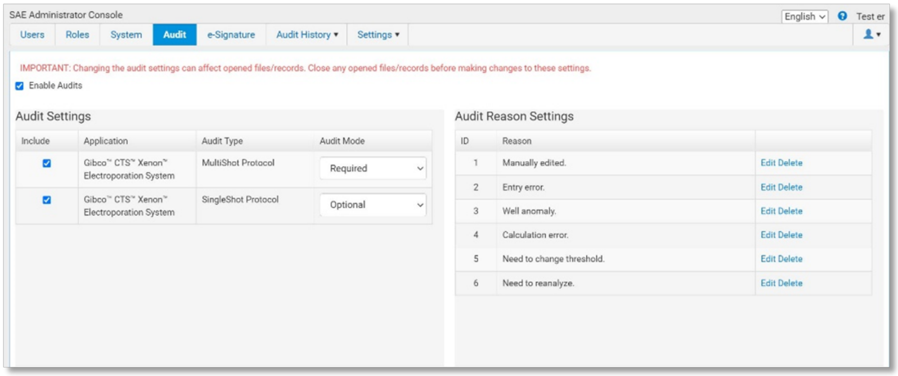
1. In the SAE Administrator Console main screen, click the **Audit** tab.
2. Select or deselect **Enable Audits**.
3. (*Optional*) Set or modify the **Audit Settings** and the **Audit Reason Settings**.
4. Click **Apply Settings**.

Add new audit reason

1. Click **New Reason**.
2. Enter a reason for change, then click **Save**.
3. Click **Apply Settings**.

Select items to audit and set the Audit Mode

1. In the SAE Administrator Console main screen, click the **Audit** tab.
2. In the **Audit Settings** pane, select the items to audit.



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

☑ Enable Audits

Audit Settings

Include	Application	Audit Type	Audit Mode
☑	Gibco™ CTS™ Xenon™ Electroporation System	MultiShot Protocol	Required
☑	Gibco™ CTS™ Xenon™ Electroporation System	SingleShot Protocol	Optional

Audit Reason Settings

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

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

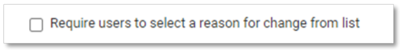
Option	Description
Silent	The event is audited. No reason prompt is displayed.
Optional	The event is audited. A reason prompt is displayed but the user can select Cancel to continue without entering a reason.
Required	The event is audited. A reason prompt is displayed, and the user must specify a reason to proceed.

4. Click **Apply Settings**.

Configure audit reasons

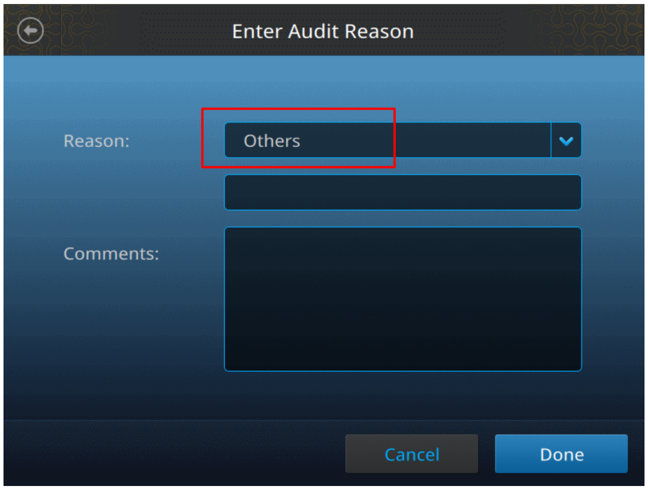
Configure the CTS™ Xenon™ Electroporation Instrument dropdown list of audit reasons in the **Audit** tab of the SAE Administrator Console.

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.



☐ Require users to select a reason for change from list

If this option is selected, the "Others" option and its manual entry field will not be displayed.



Add new audit reason

1. Click **New Reason**.
2. Enter a reason for change, then click **Save**.
3. Click **Apply Settings**.

Edit an existing audit reason

1. Click **Edit**.
2. Edit the reason for change, then click **Save**.
3. Click **Apply Settings**.

Delete an existing audit reason

1. Click **Delete**.
2. Click **Delete** to confirm deletion of the audit reason or **Cancel** to exit the dialog box.
3. Click **Apply Settings**.

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)

View the System Configuration audit log

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 ⌄ to show a list of auditable system configuration objects.

View the Action Records audit log

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 ⌄ to show a list of auditable actions.
4. (*Optional*) Perform the following actions:
   a. Specify other filtering settings.
   b. Click **Report** to generate a PDF file of the log.
   c. 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

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 ⌄ to show a list of auditable objects.
4. (*Optional*) Perform the following actions:
    a. Specify other filtering settings.
    b. 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

CTS™ Xenon™ Electroporation Instrument runs are logged in the **Application Object Records**.

1. In the SAE Administrator Console main screen, click the **Audit History** tab.
2. Select **Instrument Run Records** to show the following records.

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

3. (*Optional*) Perform the following actions:
   a. Select **Enable Instrument Run Records Filtering** to limit the records that are displayed.

   b. Click **Report** to generate a PDF file of the log.

Note: Export is not supported for this audit log.

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.

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

Archive audit records automatically

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

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

2. Select **Auto Archive**.

3. 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

4. Click **Save**.

Archive audit records manually

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

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

2. Select **Archival History**.

3. Select **Ad-hoc Archive**, select the start and end dates, then click **Archive**.

View or export archived audit records

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

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

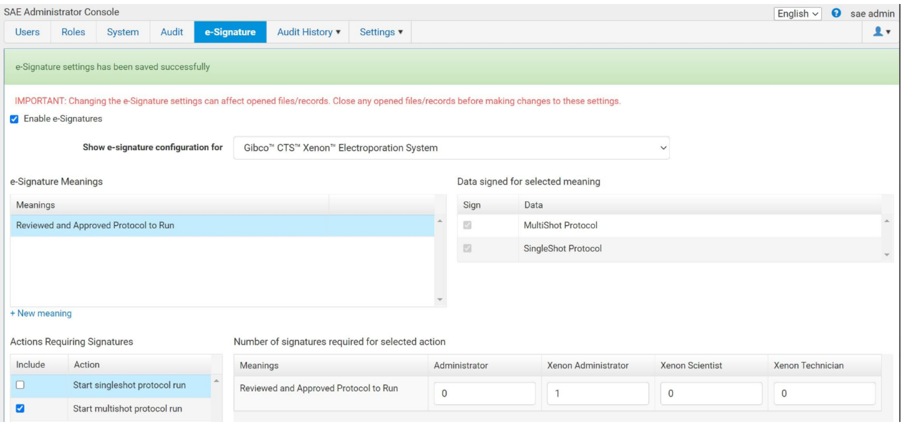
1. In the SAE Administrator Console main screen, click the **Settings** tab.
2. Select **Archival History**.
3. Select a restore option:
    a. Click a record, then click **Restore** to restore an archived record.

    b. Click **Restore (upload)**, then select a ZIP file to restore a ZIP file that was exported from the archival history.

Manage the e-signature function

E-signature requirements to use a protocol

E-signatures requirements can be configured for protocols prior to use in the SAE Administrator Console.



e-Signature settings has been saved successfully

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

☑ Enable e-Signatures

Show e-signature configuration for Gibco™ CTS™ Xenon™ Electroporation System

e-Signature Meanings

Meanings
Reviewed and Approved Protocol to Run

+ New meaning

Data signed for selected meaning

Sign	Data
☑	MultiShot Protocol
☑	SingleShot Protocol

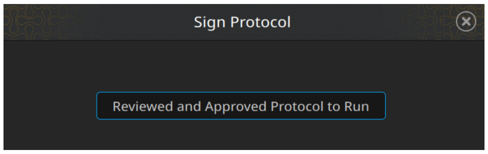
Actions Requiring Signatures

Include	Action
□	Start singleshot protocol run
☑	Start multishot protocol run

Number of signatures required for selected action

Meanings	Administrator	Xenon Administrator	Xenon Scientist	Xenon Technician
Reviewed and Approved Protocol to Run	0	1	0	0

If e-signature requirements have been set for a protocol, a message is displayed before the protocol can be used.



Enable or disable the e-signature function

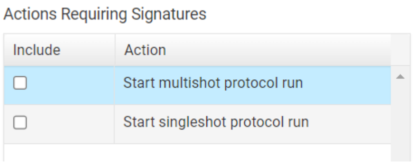
Use the **e-Signature** tab to control the e-signature rights of SAE roles, the reasons available for e-signature, and the data to be signed.

1. In the SAE Administrator Console main screen, click the **e-Signature** tab.
2. Select or deselect **Enable e-signature**.
3. (*Optional*) Set or modify the e-signature settings.
4. Click **Apply Settings**.

Select the actions that require e-signature

1. In the SAE Administrator Console main screen, click the **e-Signature** tab.

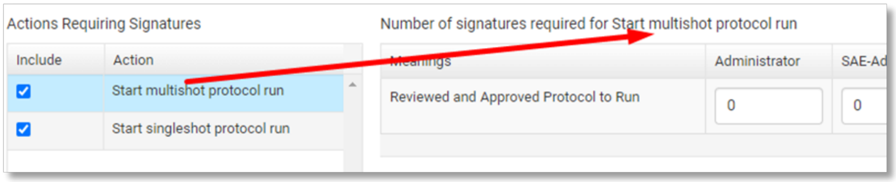
2. In the **Actions Requiring Signatures** pane on the bottom left, select each action that requires an e-signatures.



Actions Requiring Signatures

Include	Action
☐	Start multishot protocol run
☐	Start singleshot protocol run

3. For each meaning of each selected action, enter the number of e-signatures required from each SAE role before the associated action can be performed.



Actions Requiring Signatures

Include	Action
☑	Start multishot protocol run
☑	Start singleshot protocol run

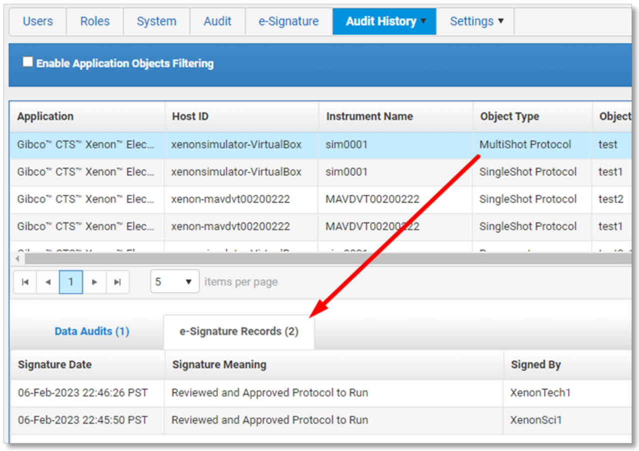
Number of signatures required for Start multishot protocol run

Meanings	Administrator	SAE-Ad
Reviewed and Approved Protocol to Run	0	0

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. This text will appear in the **Application Object Records** of the audit history.



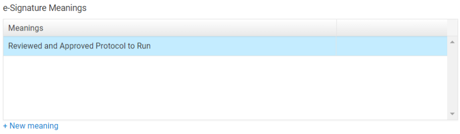
☐ Enable Application Objects Filtering

Application	Host ID	Instrument Name	Object Type	Object
Gibco™ CTS™ Xenon™ Elec...	xenonsimulator-VirtualBox	sim0001	MultiShot Protocol	test
Gibco™ CTS™ Xenon™ Elec...	xenonsimulator-VirtualBox	sim0001	SingleShot Protocol	test1
Gibco™ CTS™ Xenon™ Elec...	xenon-mavdvt00200222	MAVDVT00200222	SingleShot Protocol	test2
Gibco™ CTS™ Xenon™ Elec...	xenon-mavdvt00200222	MAVDVT00200222	SingleShot Protocol	test1

Signature Date	Signature Meaning	Signed By
06-Feb-2023 22:46:26 PST	Reviewed and Approved Protocol to Run	XenonTech1
06-Feb-2023 22:45:50 PST	Reviewed and Approved Protocol to Run	XenonSci1

Add an e-signature meaning

1. In the SAE Administrator Console main screen, click the **e-Signature** tab.
2. In the **e-Signature Meanings** pane on the upper right, click **New Meaning**.

   
   e-Signature Meanings

Meanings
Reviewed and Approved Protocol to Run

3. Enter an e-signature meaning in the **Name** field, then click **Save**.
4. Select a meaning, then select the item with which to associate the meaning from the **Data signed for the selected meaning** list.
5. Set the actions that require e-signature and the number of e-signatures that are required for that action.
6. 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** pane on the upper right, select a meaning from the **Meanings** list, then click **Delete**.
3. Confirm the deletion of the meaning, then click **OK**.
4. Click **Apply Settings**.

Advanced Configuration Options for the SAE Administrator Console

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

Export settings to another installation of the SAE Administrator Console

Use the export function to transfer settings from one installation of the SAE Administrator Console to another.

1. In the SAE Administrator Console main screen, click the **Settings** tab.
2. Select **Export Configuration**.
3. 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

4. Click **Export**.

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

Import settings from another installation of the SAE Administrator Console

Use the import function to transfer settings from one installation of the SAE Administrator Console to another.

1. In the SAE Administrator Console main screen, click the **Settings** tab.
2. Select **Import Configuration**.
3. Click **Choose File** to select the .dat file with the desired configuration settings.
4. Select an import option.
5. Click **Import**.

Archive and restore audit records

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

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

Configure user repositories for SAE or external account access

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

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

3. Select a **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 50).

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 Console account is set to **Inactive**.

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

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

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

User repository settings

Table 3 External LDAP User Repository and Federated Repositories settings

Setting	Description
LDAP Server Configuration	
Host name, Port, and 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.
Username	Parameter that maps to the username 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.

Table 3 External LDAP User Repository and Federated Repositories settings *(continued)*

Setting	Description
Username and other settings	Parameters that correspond to the username and other fields in the LDAP system.
Authentication verification	
Username and Password	LDAP username and password.

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

Table 4 External LDAP User Repository and Federated Repositories settings

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

SAE error messages and actions

Message	Possible cause	Action
Unable to connect to SAE server. Check current connections.	The SAE server connection settings are incorrect for the CTS™ Xenon™ Electroporation Instrument.	**1.** Check the SAE server IP address. **2.** In the instrument **Sign In** screen, sign in with a local administrator account. **3.** Set the correct IP address (see page 34).
	There is a problem with the computer on which the SAE Administrator Console is installed or a problem with the network.	Troubleshoot computer or network problems.
	The computer on which the SAE Administrator Console has a dynamic IP address that is disconnecting the server when the computer is restarted.	Set a static IP address on the computer.
You have reached the maximum sign in attempts.	SAE user account is locked.	User can sign in as an administrator user into the SAE Administrator Console to unlock the account.
Account is disabled.	SAE user account is disabled.	User can sign in as an administrator user into the SAE Administrator Console to set the account back to active mode.

(continued)

Message	Possible cause	Action
Unable to sign in. Unknown failure.	Unknown reason, likely network issue or configuration.	Check on the network for both instrument and the SAE Administrator Console and ensure they are on the same network. Issuing a command ping to the instrument iIP address. If the network is fine, ensure the IP address and port number is correct from the instrument to the SAE Administrator Console. The IP address of the SAE Administrator Console may change if using DHCP. If the network settings is correct, sign in to ensure the SAE Administrator Console is running. If able to sign in but still not able to connect via the instrument, try with another instrument (if available) to determine if it is an instrument issue.
Unable to reach SEA server. Please check SAE server settings.	SAE administrator server console IP address or port number may be incorrect, or the SAE Administrator Console may not be running.	Check on the network for both instrument and the SAE Administrator Console and make sure they are on the same network. Issuing a command ping to the instrument IP address. If the network is fine, ensure the IP address and port number is correct from the instrument to the SAE Administrator Console. The IP address of the SAE Administrator Console may change if using DHCP. If the network settings is correct, sign in to ensure the SAE Administrator Console is running. If able to sign in but still not able to connect via the instrument, try with another instrument (if available) to determine if it is an instrument issue.
Enable security failed. Unsuccessful login.	Wrong username input.	Key in the correct username.
Enable security failed. The username or password is incorrect.	Wrong password input	Key in the correct password

(continued)

Message	Possible cause	Action
Unable to sign in. Unsuccessful login.	Wrong username input.	Key in the correct username.
Unable to sign in. The username or password is incorrect.	Wrong password input	Key in the correct password
Signing error. Unsuccessful login.	Wrong username input.	Key in the correct username.
Signing error. The username or password is incorrect.	Wrong password input	Key in the correct password
Enable security failed. Instrument time skewed.	The time difference on the instrument and the SAE Administrator Console is greater than 5 minutes.	Change the instrument time to match the SAE Administrator Console time.
Unable to reach the SAE server. Please check SAE server settings.	The account that is used to enable SAE from the instrument do not have the administrator rights.	Please use another SAE account with administrator rights.

Documentation and support

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**.

thermofisher.com/support | thermofisher.com/askaquestion

thermofisher.com

18 August 2023