

Security, Auditing, and E-signature (SAE) Administrator Console v3

USER GUIDE

for use with Diomni™ Design and Analysis (RUO) Software 3

Publication Number MAN0030171

Revision A



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

Revision history: MAN0030171 A (English)

Revision	Date	Description
A	18 February 2025	New document for Security, Auditing, and E-signature (SAE) Administrator Console v3 with Diomni™ Design and Analysis (RUO) Software 3.

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

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

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

TRADEMARKS: All trademarks are the property of Thermo Fisher Scientific and its subsidiaries unless otherwise specified. Microsoft, Windows, Excel, and Microsoft Edge are trademarks of Microsoft Corporation. Google Chrome is a trademark of Google LLC. Core and Intel are trademarks of Intel Corporation. Mozilla and Firefox are trademarks of Mozilla Foundation in the U.S. and other countries. Avast is a trademark of Gen Digital Inc. McAfee is a trademark of McAfee, LLC.

©2025 Thermo Fisher Scientific Inc. All rights reserved.

Contents

■	CHAPTER 1	About the software	8
		Network and password security requirements	8
		Network configuration and security	8
		Password security	8
		Compatibility	8
		Overview of a security, auditing, and e-signature administrator console	9
		Components of the SAE functions	10
		Local web browser interface	10
		File and database locations	11
■	CHAPTER 2	Get started	12
		Workflow: Set up the security, auditing, and e-signature administrator console	12
		Sign in to the security, auditing, and e-signature administrator console	14
		Start the console (host computer)	14
		Start the console (client computer)	15
		Sign in with the launchpad	16
		Sign out of the console	17
		Optional tasks	17
		Set up SAE messaging notifications	17
		View the notifications	18
		Determine the signed-in user	19
		Display the software version	19
		View the terms of use (EULA)	19
		Select the language	20
■	CHAPTER 3	Functions of the security, auditing, and e-signature administrator console	21
		Overview of security settings for data files	21
		Overview of security settings for projects	22
		Actions that are audited	23
		Objects that are audited	24

Functions that can be signed	24
Default permissions for the Diomni™ Design and Analysis (RUO) Software 3	25
Sample permissions	27
Project permissions	27
File server management permissions	27
■ CHAPTER 4 Perform tasks in Diomni™ Design and Analysis (RUO) Software 3	28
Specify audit reason	28
View audit records	28
Export audit records	29
Sign data in the software	29
View e-signatures in the software	30
Generate an e-signature history report	30
Generate an e-signature report	31
■ CHAPTER 5 Manage application profiles	32
Overview of application profiles	32
Install the application profiles	32
View the installed application profiles	33
Application profile versions	33
Update an application profile	34
■ CHAPTER 6 Manage SAE user accounts and roles	35
Change your SAE user account password (in Diomni™ Design and Analysis (RUO) Software 3)	35
Change your SAE user account password (in the security, auditing, and e-signature administrator console)	36
Create a user account	36
Edit an SAE user account	37
Inactivate an SAE user account	37
Activate a suspended or inactive SAE user account	38
Reset an SAE user account password	38
Manage roles	38
Create a role	39
Edit a role	39
Delete a role	40
View or print a user report	40
View or print a role report	41

■	CHAPTER 7	Manage the system security function	42
		Overview of the system security settings	42
		Functions that are controlled in the console	42
		Configure account setup and security policies	42
■	CHAPTER 8	Manage the audit function	45
		Audit function	45
		Enable or disable the audit function	45
		Select items to audit and set the Audit Mode	46
		Manage the audit reasons	46
		Edit audit reasons	46
		Delete audit reasons	46
		Add audit reasons	46
		View audit logs (audit history)	47
		View the System Configuration audit log	47
		View the Action Records audit log	47
		Actions that are audited in the security, auditing, and e-signature administrator console	48
		Export the audit history or generate an audit history report	48
■	CHAPTER 9	Manage the e-signature function	49
		Overview of the e-signature settings	49
		How the e-signature function works in the application	49
		Parts of the e-Signature tab	50
		Enable or disable the e-signature function	50
		E-signature meanings and data signed for a meaning	50
		Actions that require an e-signature	51
		Number of e-signatures required for the selected action	52
		Workflow to set up the e-signature function	53
		Enable the e-signature function	53
		(Optional) Add an e-signature meaning	54
		Select the actions that require e-signature	54
		Specify the number of signatures required for each action	54
		Delete an e-signature meaning	55
		Disable the e-signature function	56
■	CHAPTER 10	View and report audit and e-signature records	57
		Types of audit and e-signature history records	57
		View the action records audit log	58
		View the System Configuration audit log	58

View the application objects audit log	59
View the e-signatures	59
View the instrument run records	60
Export active Action or System Configuration records	61
■ CHAPTER 11 Back up, archive, and restore SAE records and files	62
Archive and backup options and frequency	62
Set up automatic archive of audit records	63
Manually archive audit records	64
View archived audit records	64
Restore archived audit records	65
Back up the encryption key	65
Back up the SAE program folder	66
Export archived audit records	66
Restore exported archived audit records	67
Export system security, audit, and e-signature settings	67
Import user, system security, audit, and e-signature settings	68
Back up to reinstall due to LDAP organizational unit error	69
■ CHAPTER 12 Manage user repositories	70
User repository overview	70
Overview of LDAP repository synchronization	71
Configure user repositories	72
Configure user repositories for SAE or external account access	72
User repository settings	73
User or administrator sign-in with LDAP or federated user repositories	74
Perform a full manual synchronization	74
■ APPENDIX A Troubleshooting	75
■ APPENDIX B Install and manage the software	77
Overview of the installer	77
Compatibility	78
Overview of an upgrade to Security, Auditing, and E-signature (SAE) Administrator Console v3	78
Overview of a downgrade	78
Installation requirements	79
Time difference for server connection	79
Recommended computer specifications	79
Antivirus software requirements	80
Network options	80

Firewall ports that must be open	80
Third-party software	81
Install all components	81
Update administrator password	82
Initial user name and password	83
Start the software service	83
Install Security, Auditing, and E-signature (SAE) Administrator Console v3	83
Update the administrator password at first login	84
Create a shortcut for the security, auditing, and e-signature administrator console .	85
Configure the SAE settings	85
Overview of the warning screens	85
Warning for the Google Chrome™ browser	86
Warning for the Mozilla™ Firefox™ browser	86
Warning for the Microsoft Edge™ browser	87
 ■ APPENDIX C Documentation and support	88
Customer and technical support	88
Limited product warranty	88



About the software

■ Network and password security requirements	8
■ Compatibility	8
■ Overview of a security, auditing, and e-signature administrator console	9

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.

Compatibility

Software	Security, auditing, and e-signature administrator console	Application profile ^[1]
Diomni™ Design and Analysis (RUO) Software v3.0	Security, Auditing, and E-signature (SAE) Administrator Console v3.0	Design And Analysis Server (1.0.<...>)

^[1] <...> represents the third digit of the application profile version.

Overview of a security, auditing, and e-signature administrator console

A security, auditing, and e-signature administrator console is the tool that you use to configure the security, audit, and e-signature functions in Diomni™ Design and Analysis (RUO) Software 3 (on-premise configuration). The console can be configured to meet specific requirements for security, audit, and e-signature functions.

The on-premise configuration of Diomni™ Design and Analysis (RUO) Software 3 can be used only with SAE functions. The SAE functions cannot be disabled for Diomni™ Design and Analysis (RUO) Software 3.

The desktop configuration of Diomni™ Design and Analysis (RUO) Software 3 is not compatible with a security, auditing, and e-signature administrator console.

- An instance of the console can be used for multiple instruments and software programs, including Diomni™ Design and Analysis (RUO) Software 3.
- If separate instances of a console are used for different applications, the records from the console are available separately. The records must be accessed individually from each instance of the console.
- The application profile for Diomni™ Design and Analysis (RUO) Software 3 must be installed in the console to access Diomni™ Design and Analysis (RUO) Software 3.
- Multiple application profiles can be installed. They can be installed in any order.
- The console can be installed on the same computer as Diomni™ Design and Analysis (RUO) Software 3 (*recommended*) or separate computers.
- A computer can have only one instance of a console. Multiple instances cannot be installed on the same computer.
- The computer that is running the console for an instrument does not need to be colocated with the instrument.

IMPORTANT! The installer for Diomni™ Design and Analysis (RUO) Software 3 includes Security, Auditing, and E-signature (SAE) Administrator Console v3. Depending on the options that are selected during the installation process, the installer can upgrade a previous version of the security, auditing, and e-signature administrator console. Ensure that all instruments and software that are connected to the instance of the console are compatible with Security, Auditing, and E-signature (SAE) Administrator Console v3.

The security, auditing, and e-signature administrator console 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 user accounts and permissions.
Auditing	Tracks actions performed by users and changes to the SAE settings. Some actions are audited silently. You can perform the following tasks: <ul style="list-style-type: none"> • Specify the audit mode. • Generate reports for audited user actions and SAE setting changes. • Generate reports for software actions.
Electronic signature (e-signature)	Determines if users are required to fulfill signature requirements before performing specific functions. You can perform the following tasks: <ul style="list-style-type: none"> • Configure e-signature so that a user can start a run only if the associated data are signed. • Configure the e-signature so that a user can export data or a report 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.

Components of the SAE functions

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

- Security, auditing, and e-signature administrator console—The tool that is used by the administrator to configure the settings.
It runs in the background and stores the following information:
 - SAE settings
 - User accounts
 - Roles and associated permissions
 - Audit records
 - E-signature records
- SAE screens—Screens that are displayed in an application (sign in, audit, and e-signature) that require user input.

Note: Diomni™ Design and Analysis (RUO) Software 3 can be used only with SAE functions.

Local web browser interface

A web browser is typically used to view information on the internet.

The security, auditing, and e-signature administrator console runs in a web browser interface, even though it is installed locally on a computer.

The address bar of the browser displays **localhost**. This indicates that the security, auditing, and e-signature administrator console is installed on the computer.

The console can be accessed on a different computer that is on the same network as the computer that the console is installed on. The IP address is displayed in the address bar of the browser.

File and database locations

The files for the security, auditing, and e-signature administrator console are installed in <...>:\Program Files (x86)\Applied Biosystems\SAE Admin Console, where <...> is the installation directory.

Records are managed by a relational database management system (RDBMS) in the software.

Database files are stored in <...>:\Program Files (x86)\Applied Biosystems\SAE Admin Console\SAEDB\seg0. The database folder is created when the first record is saved. Records for all applications are stored in the same database.

Records that are archived manually or with the automated archive function are stored in <...>:\Program Files (x86)\Applied Biosystems\SAE Admin Console\automated-archivals. The archive folder is created when the first automated archive occurs. Date- and time-stamped folders are created for each archive.

IMPORTANT! Do not move or edit files in this directory. For information on backing up and archiving the files and database, see Chapter 11, “Back up, archive, and restore SAE records and files”.

- Workflow: Set up the security, auditing, and e-signature administrator console 12
- Sign in to the security, auditing, and e-signature administrator console 14
- Sign out of the console 17
- Optional tasks 17

Workflow: Set up the security, auditing, and e-signature administrator console

Set up the security, auditing, and e-signature administrator console

Start the security, auditing, and e-signature administrator console

- Start the console (host computer) (page 14)
- Start the console (client computer) (page 15)
- Sign in with the launchpad (page 16)

Install the application profiles (page 32)

The installer for Diomni™ Design and Analysis (RUO) Software 3 includes the application profile. For more information, see “Overview of the installer” on page 77.

Configure the settings in the console

Manage user accounts

See Chapter 6, “Manage SAE user accounts and roles”.

Manage the system security function (page 42)

AND

Configure account setup and security policies (page 42)

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

Manage the audit function (page 45)

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

Manage the e-signature function (page 49)

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

View and report audit and e-signature records (page 57)

Perform the procedures in this chapter as needed.

Back up, archive, and restore SAE records and files (page 62)

Perform the procedures in this chapter as needed.

Sign in to the security, auditing, and e-signature administrator console

Start the console (host computer)

This section covers starting the console when it is installed on the computer that is in use (host computer). To start the console on a separate computer (client computer), see “Start the console (client computer)” on page 15.

1. In the Windows™ desktop, click **Start ▶ SAE Admin**.

The console is opened in a browser. A warning screen might be displayed. For more information, see “Overview of the warning screens” on page 85.

2. Enter your SAE account username and password, then click **Sign in**.

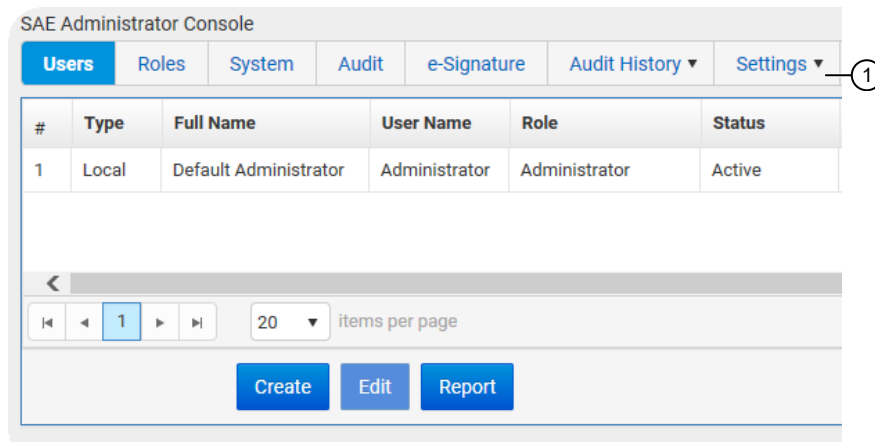
If messaging notifications are enabled (see “Set up SAE messaging notifications” on page 17), the **Event Notifications** dialog box is displayed.

3. You can do either of the following in the **Event Notifications** dialog box.

- Select the checkboxes for the events, then click **Acknowledge** to remove the selected events from the list.
- Click **Close** to close the dialog box and retain the events in the list.

If the notifications are retained, they are displayed the next time a user logs in to the console. They can also be viewed from the main screen (see “View the notifications” on page 18).

The console main screen is displayed with the URL specified as `local host` in the browser. Click the navigation tabs to display different screens in the software.



① Navigation tabs

The signed-in user is automatically signed out after 30 minutes of inactivity. This logout time is not configurable.

Start the console (client computer)

This section covers starting the console when it is installed on a different computer (client computer). To start the console on the same computer (host computer), see “Start the console (host computer)” on page 14.

In order to access the console from a client computer, the client computer must be on the same network as the host computer.

Depending on the way that the network is configured, the IP address might change. This affects the connection to console from a separate computer.

A DHCP network connection with a reserved IP address is recommended. A static IP address can also be used. For more information, see “Network options” on page 80.

Contact your IT department to configure your network.

1. Open a browser, then enter the IP address of the host computer followed by the port in the URL bar.

An example of an IP address format is 11.111.11.1

The port is 8443

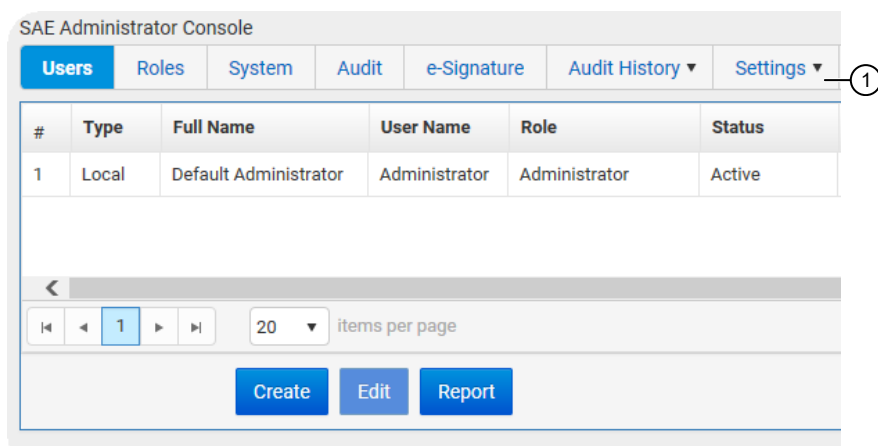
Example: `https://<...>:8443`, where <...> is the IP address of the server.

The console is opened in a browser. A warning screen might be displayed. For more information, see “Overview of the warning screens” on page 85.

2. Enter your SAE account username and password, then click **Sign in**.
If messaging notifications are enabled (see “Set up SAE messaging notifications” on page 17), the **Event Notifications** dialog box is displayed.
3. You can do either of the following in the **Event Notifications** dialog box.
 - Select the checkboxes for the events, then click **Acknowledge** to remove the selected events from the list.
 - Click **Close** to close the dialog box and retain the events in the list.

If the notifications are retained, they are displayed the next time a user logs in to the console. They can also be viewed from the main screen (see “View the notifications” on page 18).

The console main screen is displayed with the URL specified as the IP address and the port in the browser. Click the navigation tabs to display different screens in the software.



① Navigation tabs

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

Sign in with the launchpad

A launchpad is available to provide access to different applications, including the console.

The applications operate separately. Data from one application are not available in other applications.

Only one instance of Security, Auditing, and E-signature (SAE) Administrator Console v3 is available with the launchpad. The launchpad provides access to applications that are connected to the single instance of Security, Auditing, and E-signature (SAE) Administrator Console v3.

The applications must be an on-premise configuration, they must be on the same network, and they must be connected to the same instance of the console.

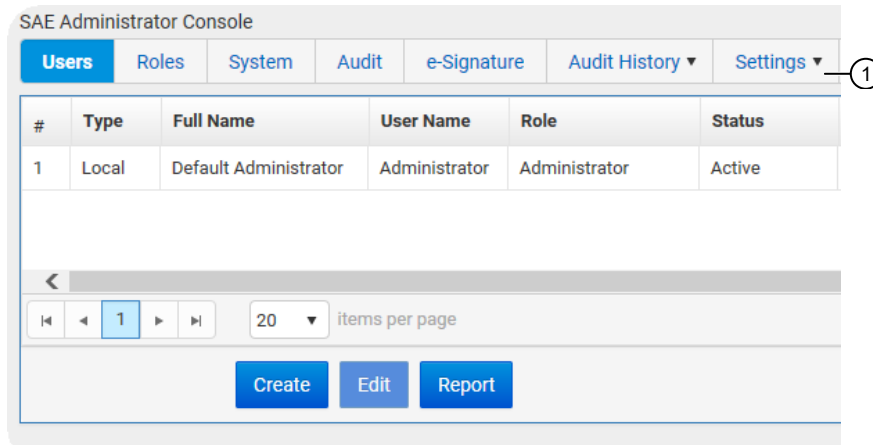
Only applications that were active in the last 60 minutes are displayed in the launchpad.

You must be signed in to a different application, for example, the on-premise configuration of Diomni™ Design and Analysis (RUO) Software 3.

1. In the software that you are signed in to, click  **(Launchpad)** ▶ **SAE**.
The sign-in screen is displayed in a new tab of the browser.
2. Enter your SAE account username and password, then click **Sign in**.
If messaging notifications are enabled (see “Set up SAE messaging notifications” on page 17), the **Event Notifications** dialog box is displayed.
3. You can do either of the following in the **Event Notifications** dialog box.
 - Select the checkboxes for the events, then click **Acknowledge** to remove the selected events from the list.
 - Click **Close** to close the dialog box and retain the events in the list.

If the notifications are retained, they are displayed the next time a user logs in to the console. They can also be viewed from the main screen (see “View the notifications” on page 18).

The console main screen is displayed with the URL specified as the IP address and the port in the browser. Click the navigation tabs to display different screens in the software.



① Navigation tabs

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

Sign out of the console

In the top-right corner of the screen, click ▾ ► **Sign Out**

Optional tasks

Set up SAE messaging notifications

You can specify when and how to be notified when specified events occur in the security, auditing, and e-signature administrator console. The following options are available for notifications:

- In the **Event Notification** dialog box that is displayed when you sign in to the security, auditing, and e-signature administrator console
- By email message

Note: The messaging email is not connected to your Thermofisher.com account.

IMPORTANT! You must configure the simple mail transfer protocol (SMTP) server to send email notifications (see “Configure the SMTP server for email notifications” on page 18). If the SMTP server is not configured, email notifications are not sent, even if email addresses are added.

1. In the main screen, click **Settings ▶ Notifications**.
2. In the **Edit Notification Settings** dialog box, select the events of interest in the **Notify at Administrator Sign In** column.
 - **Security enabled**
 - **Security disabled**
 - **User did not enter correct password**
 - **User account suspended**
 - **User session timeout**
 - **Role deleted**
3. Select the events of interest in the **Notify by Email** column, then enter an email address or multiple email addresses.
Up to five email addresses can be entered. Separate the email addresses with a comma.
4. Click **Save**, then click **Close**.

Configure the SMTP server for email notifications

Configure the SMTP server so that the console can send email notifications.

1. In the main screen, click **Settings ▶ Email Server**.
2. In the **SMTP Configuration** dialog box, enter the following:
 - **SMTP host, SMTP port, and SMTP sender**

Note: Select **Authentication required** if the SMTP server requires authentication.

- **User Name and Password**

Note: Select **Use SSL** if the SMTP server requires an encrypted channel connection.

3. Click **Save**.

View the notifications

Once the notifications have been acknowledged at sign-in or from the main screen, they are no longer available to view.

If there are notifications available to view, the number of notifications is displayed beside the signed-in user.

1. In the top-right corner of the screen, click the number that is displayed beside the signed-in user.
No number is displayed if there are no notifications.

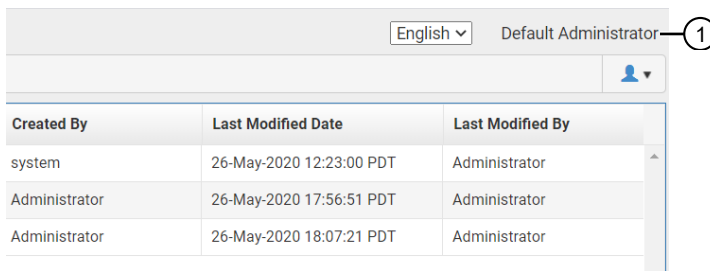
The **Event Notifications** dialog box is displayed.

2. Perform one of the following steps.

Option	Description
Click Close .	The notifications are retained. They are displayed at the next sign-in. They can also continue to be accessed after sign-in.
Select one or all of the notifications, then click Acknowledge .	The notifications are cleared. They are not displayed at the next sign-in. They cannot be accessed after sign-in.

Determine the signed-in user

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



① Signed-in user

Display the software version

1. In the main screen, click **Settings ▶ About**.

The **About** dialog box is displayed with the following information:

- Software version
- Build label
- Date

2. Click **Close**.

View the terms of use (EULA)

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

1. In the main screen, click **Settings ▶ About**.

2. In the dialog box, click **Terms of Use**.

The EULA is opened as a PDF in a new tab of the browser.

3. In the dialog box, click **Close**.

Select the language

Multiple languages are available for the user interface of the security, auditing, and e-signature administrator console.

To select a language, click the language at the bottom of the **Sign in** screen.

Alternatively, in the main screen menu bar, click the language in the language drop-down list.

Select the language.

- Before you sign in, click the name of the desired language.
The available languages are displayed below the **Sign in** button.
- After you sign in, select the name of the desired language from the dropdown list of languages.
The dropdown list of languages is displayed at the top-right corner of any screen in the console.



Functions of the security, auditing, and e-signature administrator console

■ Overview of security settings for data files	21
■ Overview of security settings for projects	22
■ Actions that are audited	23
■ Objects that are audited	24
■ Functions that can be signed	24
■ Default permissions for the Diomni™ Design and Analysis (RUO) Software 3	25

This chapter covers functions of the security, auditing, and e-signature administrator console that are specific to Diomni™ Design and Analysis (RUO) Software 3.

For actions that are audited in the security, auditing, and e-signature administrator console, see “Actions that are audited in the security, auditing, and e-signature administrator console” on page 48.

For functions that are controlled in the security, auditing, and e-signature administrator console, see “Functions that are controlled in the console” on page 42.

Overview of security settings for data files

The on-premise configuration is the only configuration of the software that is compatible with the Security, Auditing, and E-signature Administrator Console.

Depending on the settings in the security, auditing, and e-signature administrator console, data files with security settings and data files without security settings can be opened in the on-premise configuration.

See “Configure account setup and security policies” on page 42.

A data file without security settings is opened as a read-only version of the file in the on-premise configuration. Changes can be made to the original data file without security settings in order to view and analyze the data. The changes cannot be saved to the original data file. The edited data file must be saved as a copy.

When the copy of the data file is created in the on-premise configuration, an audit record begins.

A data file with security settings can be opened and edited in the on-premise configuration. The audit record is continued.

A data file with security settings can be opened in a configuration of the software that is not compatible with Security, Auditing, and E-signature Administrator Console. When the data file is opened in a configuration of the software without security settings, the audit record is stopped and the security settings for the data file are disabled.

Overview of security settings for projects

The on-premise configuration is the only configuration of the software that is compatible with the Security, Auditing, and E-signature Administrator Console.

When a project is created in the on-premise configuration, the project has security settings and the audit record begins when the project is created.

If a project is created in a configuration of the software that is not compatible with the Security, Auditing, and E-signature Administrator Console, the project does not have security settings and no audit record is created.

Depending on the settings in the security, auditing, and e-signature administrator console, data files with security settings and data files without security settings can be added to a project. Adding data files to a project does not affect the original data file and does not affect the security settings for the original data file.

See “Configure account setup and security policies” on page 42.

The audit record for a project does not affect the individual data files. When a data file is added to the project, the original data file is not edited. The software extracts the information that is required for the project from the data file without editing the original data file.

A project without security settings is opened as a read-only version of the file in the on-premise configuration. Changes can be made to the original project without security settings in order to view and analyze the data. The changes cannot be saved to the original project. The project must be saved as a copy.

When the copy of the project is created in the on-premise configuration, an audit record begins.

A project with security settings can be opened and edited in the on-premise configuration. The audit record is continued.

A project with security settings can be opened in a configuration of the software that is not compatible with Security, Auditing, and E-signature Administrator Console. When the project is opened in a configuration of the software without security settings, the audit record is stopped and the security settings for the project are disabled.

Actions that are audited

The following actions are audited. Auditing of these actions cannot be disabled. The audit records are viewed in the security, auditing, and e-signature administrator console (see “View the Action Records audit log” on page 47).

Audit records are time-stamped. Audit records cannot be overwritten.

Actions in the security, auditing, and e-signature administrator console are also audited. For more information see, “Actions that are audited in the security, auditing, and e-signature administrator console” on page 48.

- Adding or removing an instrument
- Editing the plate setup for a pre-run file
- Saving a pre-run file
- Editing the plate setup for a post-run file
- Saving a post-run file
- Sending a run to the run queue
- Generating a run report
- Generating an audit report for a run
- Exporting the run results
- Saving a project
- Exporting the project results
- Exporting the project results files (CSV files)
- Importing run files to a project
- Deleting run files from a project
- Editing the project settings
- Editing the plate setup in a project
- Editing the analysis settings of a project (after changes are saved)
- Uploading a file
- Deleting a file
- Sharing a file
- Downloading a file

Objects that are audited

Certain objects are audited. This depends on how the SAE administrator has configured the audit settings.

The audit mode can be set. The user can be required to select a reason. See “Select items to audit and set the Audit Mode” on page 46.

A reason can be added, deleted, or edited. See “Manage the audit reasons” on page 46.

Note: Template and data files are checksum protected. Checksum protection helps ensure that files are not edited outside of the system.

The plate the an audited object for Diomni™ Design and Analysis (RUO) Software 3.

Each time one of the following items is changed, it can be audited, depending on the audit function setup:

- Plate layout
- Analysis settings
- Run method
- Samples
- Assays

The following reasons are available:

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

Functions that can be signed

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

Each action that requires an e-signature is associated with an e-signature meaning and the data that are signed.

E-signature meaning	Data signed
Reviewed and approved template	<ul style="list-style-type: none">• Plate setup• Run method
Reviewed and approved plate results	<ul style="list-style-type: none">• Analysis results• Analysis setting

For detailed descriptions, see Chapter 9, “Manage the e-signature function”.

Default permissions for the Diomni™ Design and Analysis (RUO) Software 3

Function	Role		
	Administrator	Scientist	Technician
Instrument management			
Add instrument	Yes	Yes	No
Delete instrument	Yes	Yes	No
Export instrument	Yes	Yes	No
Template management			
Install template	Yes	Yes	No
Remove template	Yes	Yes	No
Setup			
Create a plate file	Yes	Yes	Yes
Edit run method	Yes	Yes	No
Edit analysis settings	Yes	Yes	Yes
Add, edit, or delete targets or assays	Yes	Yes	No
Assign targets or assays	Yes	Yes	No
Add, edit, or delete samples	Yes	Yes	Yes
Assign samples ^[1]	Yes	Yes	Yes
Add, edit, or delete reagents	Yes	Yes	Yes
Assign reagents	Yes	Yes	Yes
Add, edit, or delete custom dyes	Yes	Yes	No
Assign an analysis module	Yes	Yes	Yes
Edit passive reference	Yes	Yes	No
Project template management			
Install project template	Yes	Yes	No
Remove project template	Yes	Yes	No
Project^[2]			
Create project	Yes	Yes	Yes

(continued)

Function	Role		
	Administrator	Scientist	Technician
Edit project setting	Yes	Yes	No
Edit analysis setting	Yes	Yes	Yes
Assign analysis module	Yes	Yes	Yes
Add or delete run files	Yes	Yes	Yes
Add, edit, or delete targets or assays	Yes	Yes	No
Assign targets or assays	Yes	Yes	No
Add, edit, or delete samples	Yes	Yes	Yes
Assign samples	Yes	Yes	Yes
Add, edit, or delete reagents	Yes	Yes	Yes
Assign reagents	Yes	Yes	Yes
Add, edit, or delete custom dyes	Yes	Yes	No
Edit passive reference	Yes	Yes	No
Security configuration			
Log into timed-out user sessions	Yes	Yes	No
Perform e-signing	Yes	Yes	No
User preferences			
Edit preferences	Yes	No	No
File save destination			
Edit export destination	Yes	No	No
Edit RDML export destination	Yes	No	No
Edit report destination	Yes	No	No
File server management^[3]			
Create new folder	Yes	Yes	Yes
Move file or folder	Yes	Yes	Yes
Rename folder	Yes	Yes	Yes
Delete folder	Yes	Yes	Yes
Share or unshare folder	Yes	Yes	Yes

(continued)

Function	Role		
	Administrator	Scientist	Technician
Upload file	Yes	Yes	Yes
Open or read file	Yes	Yes	Yes
Edit file	Yes	Yes	Yes
Delete file	Yes	Yes	No
Rename file	Yes	Yes	No
Download file	Yes	Yes	No

[1] See “Sample permissions” on page 27.

[2] See “Project permissions” on page 27.

[3] See “File server management permissions” on page 27.

Sample permissions

A user has permission to assign a sample if they have permission to define, edit, or delete a sample. This applies even if the **Assign Sample** checkbox is not selected in the Security, Auditing, and E-signature (SAE) Administrator Console.

Project permissions

The Technician role can add targets and assays to a data file that is being added to a project if there are targets and assays in the data file that are not defined in the project. The Technician must have the **Add/Delete Run Files** permission in order to perform this action.

If a role has the permission of **Create Project**, the permission of **Add/Delete Run Files** must also be provided.

File server management permissions

The file server management permissions apply to all of the files within the application, including personal files and files that have been shared.

If you do not own a file, you cannot move, edit, delete, or rename the file.

You cannot upload a file to another user's personal file space. You cannot create a folder in another user's personal file space.

You cannot view and access the personal files or folders for another user unless these were specifically shared with you.



Perform tasks in Diomni™ Design and Analysis (RUO) Software 3

The following tasks are performed in Diomni™ Design and Analysis (RUO) Software 3.


Specify audit reason

Depending on the way that your SAE administrator configures audit settings in the SAE Administrator Console, the **Enter Audit Reason** screen might be displayed when you make changes to a plate file or a data file in Diomni™ Design and Analysis (RUO) Software 3.

Select a reason from the dropdown list, or add a custom reason.

Note: **Custom Reason** is not displayed if audit settings are configured to require users to select a reason.

View audit records

1. In an open run file or project file, select the **Data Audit** tab.
 - The **Audit Summary** pane contains a list of all the audit records created each time the plate file or data file was saved.
 - The **Change Records** pane displays all events in a selected audit record.
2. (Optional) Enter a date range to filter the displayed records.
3. (Optional) Click  to search the audit records.
4. Select an audit record in the **Audit Summary** pane to view audit record details in the **Change Records** pane.

Export audit records

The location to save the file is defined in the export settings.

For users with the permission of **Edit Report Destination**, the location can be selected for a file download. For users with the permission of **Edit Report Destination**, the location cannot be selected.

1. In an open run file or project file, select the **Data Audit** tab.
2. In the upper-right corner of the **Data Audit** tab, click **⋮ (More Options) ▶ Generate Full Audit Report**.
The data must be analyzed in order to generate the audit report. The **Generate Full Audit Report** button is inactive if the data are not analyzed.
3. In the **Export Audit Report** dialog box, edit the file name, if necessary.
The **File Name** field is populated with a default file name.
4. Click one of the following options.
 - Click **Download**, then select a destination for the file download. The **Download** button and the ability to edit the file location are available for users with the permission to define the report destination.
 - Click **Save**. The **Save** button is available for users who do not have the permission to define the report destination. The file location cannot be edited by users who do not have the permission to define the report destination.

The exported PDF file contains the information displayed in the **Audit Summary** and **Change Records** panes of the **Data Audit** tab.

Sign data in the software

An e-signature is permanent. The file maintains the complete e-signature history even when newer e-signatures are provided.

1. Save any new changes to an open file.
2. Click **Actions**, then select **Sign Data**.
3. Select an option from the dropdown list to indicate the meaning of the e-signature.
 - Reviewed and Approved Template (includes plate setup and run method)
 - Reviewed and Approved Plate Results
4. Enter your user name and password.
5. (Optional) To preview the e-signature report for the plate file or data file, click **Preview**.
To generate an e-signature report for the plate file or data file, see “Generate an e-signature report” on page 31.
6. Click **Sign**.

A record of the e-signature is available in the **e-Signature** tab (see “View e-signatures in the software” on page 30).

View e-signatures in the software

1. In an open run file or project file, select the **e-Signature** tab.
All of the e-signatures for the file display in the table. The table cannot be modified.
2. Review all of the e-signatures for the file in the table. The **Status** column indicates if the e-signature is **Current** or **Obsolete**.

Column	Description
Date	Indicates the date and time that the e-signature was added to the plate file or data file
User Name	Indicates the user name of the person that added the e-signature to the plate file or data file
User Role	Indicates the role assigned to the user in the SAE Administrator Console
Meaning	Indicates the meaning of the e-signature: <ul style="list-style-type: none"> • Reviewed and Approved Template • Reviewed and Approved Plate Results
Status	Indicates whether the e-signature is Current or Obsolete

Generate an e-signature history report

The location to save the file is defined in the export settings.

For users with the permission of **Edit Report Destination**, the location can be selected for a file download. For users with the permission of **Edit Report Destination**, the location cannot be selected.

The e-signature history report contains all of the e-signatures that were obtained for a meaning. To generate a report of only the most recent e-signatures, see “Generate an e-signature report” on page 31.

1. In an open run file or project file, in the **e-Signature** tab, select an e-signature record from the list.
2. In the upper-right corner of the **e-Signature** tab, click **⋮ (More Options) ▶ Generate e-Signature History Report**.
3. In the **Export e-Signature History Report** dialog box, edit the file name, if necessary.
The **File Name** field is populated with a default file name.

4. Click one of the following options.

- Click **Download**, then select a destination for the file download. The **Download** button and the ability to edit the file location are available for users with the permission to define the report destination.
- Click **Save**. The **Save** button is available for users who do not have the permission to define the report destination. The file location cannot be edited by users who do not have the permission to define the report destination.

Generate an e-signature report

The location to save the file is defined in the export settings.

For users with the permission of **Edit Report Destination**, the location can be selected for a file download. For users with the permission of **Edit Report Destination**, the location cannot be selected.

The e-signature report contains the most recent e-signatures that were obtained for a meaning. To generate a report of the e-signature history, see “Generate an e-signature history report” on page 30.

1. In an open run file or project file, in the **e-Signature** tab, select an e-signature record from the list.
2. In the upper-right corner of the **e-Signature** tab, click ... **(More Options)** ▶ **Generate e-Signature Report**.
3. In the **Export e-Signature Report** dialog box, edit the file name, if necessary.
The **File Name** field is populated with a default file name.
4. Click one of the following options.
 - Click **Download**, then select a destination for the file download. The **Download** button and the ability to edit the file location are available for users with the permission to define the report destination.
 - Click **Save**. The **Save** button is available for users who do not have the permission to define the report destination. The file location cannot be edited by users who do not have the permission to define the report destination.



Manage application profiles

■ Overview of application profiles	32
■ Install the application profiles	32
■ View the installed application profiles	33
■ Application profile versions	33
■ Update an application profile	34

Overview of application profiles

An application profile contains default settings for an application. The default settings include the roles and the permissions for each role.

Before you can use the console with an application, you must install a profile for the application. Each application has its own application profile, or its own set of application profiles.

You can install multiple application profiles in order to support the use of the console with multiple applications.

The application profiles for some applications are included in the installer for the application. For more information, see “Overview of the installer” on page 77.

An application profile cannot be uninstalled. An application profile can be updated by installing a new version.

IMPORTANT! When an application profile is upgraded, all the roles receive the permission for the new functions in the application profile. For example, if only the administrator receives permission for a function in a new installation, all of the roles receive the permission for a function in an upgrade.

Install the application profiles

For information about the versions of the application profiles, see “Application profile versions” on page 33.

1. In the main screen, click **Settings ▶ Manage Application Profiles**.
2. Click **Install Application Profile**.
3. In the **Install Application Profile** dialog box, click **Choose File**.
4. Select the application profile.
The application profile is a DAT file.

5. Click **Verify Data File**.
6. Review the information in the **Install Application Profile** dialog box, then select the **Install new application** checkbox.
7. Click **Install**.
The **Install Application Profile** dialog box displays the message **Application profile has been successfully installed**.
8. Click **Close**.

The application name and settings are added to the console.

If there is a workflow associated with the application profile, the workflow is available when a role is created (see “Create a role” on page 39).

View the installed application profiles

Click **Settings ► Manage Application Profiles**.

The installed application profiles are displayed. The following information is displayed for each application profile:

- Application name
- Description
- Number of functions
- Version of the application profile
- Date that the application profile was installed
- User who installed the application profile

Application profile versions

The console requires an application profile to be installed for each application.

Each application profile has a version.

IMPORTANT! The following information is provided as an example.

Application profiles have the following naming convention:

`<Application name> (<Application profile version number>).dat`

The file format for an application profile is DAT.

The following file name is an example of the application profile for Diomni™ Design and Analysis (RUO) Software 3. It is version 1.0.0.

`Design and Analysis Server (1.0.0).dat`

Update an application profile

IMPORTANT! Ensure that the new version of the application profile is compatible with your version of the application and your version of the console before updating it.

When an application profile is upgraded, all of the roles receive the permission for the new functions in the application profile. For example, if only the administrator receives permission for a function in a new installation, all of the roles receive the permission for a function in an upgrade.

For information about the versions of the application profiles, see “Application profile versions” on page 33.

1. In the main screen, click **Settings ▶ Manage Application Profiles**.
2. Click **Install Application Profile**.
3. In the **Install Application Profile** dialog box, click **Choose File**.
4. Select the application profile.
The application profile is a DAT file.
5. Click **Verify Data File**.
6. Review the information in the **Install Application Profile** dialog box, then select the **Install new application** checkbox.
7. Click **Install**.
8. Select **Verify Data File ▶ Install new application ▶ Install**.

The information about the updated application profile is displayed in the list of application profiles.

- Number of functions
- Version
- Date installed
- Installed by

The previous version of the application profile is not displayed. The new application profile is differentiated based on the version that is displayed.



Manage SAE user accounts and roles


■ Change your SAE user account password (in Diomni™ Design and Analysis (RUO) Software 3)	35
■ Change your SAE user account password (in the security, auditing, and e-signature administrator console)	36
■ Create a user account	36
■ Edit an SAE user account	37
■ Inactivate an SAE user account	37
■ Activate a suspended or inactive SAE user account	38
■ Reset an SAE user account password	38
■ Manage roles	38
■ View or print a user report	40
■ View or print a role report	41

Change your SAE user account password (in Diomni™ Design and Analysis (RUO) Software 3)

An administrator can reset a password for a user with another role in the security, auditing, and e-signature administrator console (see “Reset an SAE user account password” on page 38).


The password is updated for all of the applications that are connected to the instance of the security, auditing, and e-signature administrator console.

Note: External user accounts (External/Federated LDAP repository accounts) cannot change their password in the software.

1. In the upper-right corner of the Diomni™ Design and Analysis (RUO) Software 3 menu bar, click  **(Profile) ▶ Change password**.
The **Change password** dialog box is displayed.
2. In the **Change password** dialog box, enter the old password in the **Old Password** field.
3. Enter the new password in the **New Password** field and the **Confirm Password** field.
4. Click **Change**.

Change your SAE user account password (in the security, auditing, and e-signature administrator console)

To change a password to log in to an application for a user, see “Reset an SAE user account password” on page 38.

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**.

Create a user account

One thousand (1,000) user accounts are permitted.

A user account cannot be deleted after it is created. A user account can be inactivated. Inactivated user accounts are included in the maximum number of 1,000 user accounts.

Note: For information on advanced configuration options for user repositories, see “Configure user repositories” on page 72.

1. In the main screen, click the **Users** tab.
2. Click **Create**.
3. In the **Create User Account** dialog box, enter the following information:
 - User name
 - Password
 - First name
 - Middle initial (MI; optional)
 - Last name
 - Phone number (optional)
 - Email address (optional)
 - Comments (optional)

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

The phone number and email address are for information only.

Note:

- First name, MI (middle initial), and last name are used to create the **User Full Name**. This is displayed as the name of the signed-in user.
 - You cannot change the user name after you save the user account.
-

4. Select **User must set new password at next sign in** to require the user to specify a new 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.

5. Select the **Role** for the user account.
 - Each role grants specific permissions to the user.
 - The **No Privileges Role** is for internal use by the console. Do not assign this role to a user account.
 - For the default roles that are provided with the application, see “Default permissions for the Diomni™ Design and Analysis (RUO) Software 3” on page 25.
6. In the **Status** drop-down list, leave the status set to **Active**.
7. Click **Save**.

Edit an SAE user account

1. In the main screen, click the **Users** tab.
2. Select a user account, then click **Edit**.
3. Edit the settings as desired.

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

4. Click **Save**.

Inactivate an SAE user account

Inactivated user accounts are included in the maximum number of 1,000 user accounts.

1. In the main screen, click the **Users** tab.
2. Select a user account, then click **Edit**.
3. In the **Edit User Account** dialog box, change the status in the **Status** drop-down list to **Inactive**.

Note: The status of **Suspended** is an option in the **Status** drop-down list. This status is used by the software if the user has reached the number of sign-in attempts defined in the account lockout policy. For more information, see “Configure account setup and security policies” on page 42.

4. Click **Save**.

Activate a suspended or inactive SAE user account

An inactive or suspended SAE user account can be activated.

An SAE user account is set to be inactive by an administrator.

The suspended status is used by the software if the user has reached the number of sign-in attempts defined in the account lockout policy. For more information, see “Configure account setup and security policies” on page 42.

1. In the main screen, click the **Users** tab.
2. Select a user account, then click **Edit**.
3. In the **Edit User Account** dialog box, change the status in the **Status** drop-down list to **Active**.
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 11, “Back up, archive, and restore SAE records and files”.

1. In the main screen, click the **Users** tab.
2. Select the affected user account, then click **Edit**.
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 a list of permissions, see “Default permissions for the Diomni™ Design and Analysis (RUO) Software 3” on page 25.

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

Create a role

1. Select the **Roles** tab.
2. Click **Create**.
3. In the **Create Role** dialog box, enter a name for the role in the **Name** field.
4. *(Optional)* Enter a description in the **Description** field.
5. Select the checkbox associated with the workflow in the **Workflow** field.
The checkboxes that are available in the **Workflow** field depend on the application profiles that are installed. For example, the **IVD** checkbox is not displayed if there are no corresponding application profiles displayed.
The checkboxes filter the list of permissions based on the application profile.
6. Select permissions for the role.
 - The permissions that are available depend on the workflow that was selected.
 - The permissions are organized by the application. Select the checkbox next to the application to select all of the permissions for the application.
 - Select the checkbox next to the category to select all permissions in a category.
 - Expand the category to select individual permissions within the category.
7. Click **Save**.

New roles are available for selection when you create or edit a user account, and when you specify e-signature settings.

Edit a role

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

Note: You cannot edit the Administrator role or No Privileges role.

3. *(Optional)* Select the checkbox associated with the workflow in the **Workflow** field.
The checkboxes that are available in the **Workflow** field depend on the application profiles that are installed. For example, the **IVD** checkbox is not displayed if there are no corresponding application profiles displayed.
The checkboxes filter the list of permissions based on the application profile.
4. Edit the settings as needed, then click **Save**.

Delete a role

Default roles and custom roles can both be deleted.

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

1. In the main screen, click the **Roles** tab.
2. Select a role, then click **Delete**.
3. In the **Role Deletion** dialog box, click **Delete** to confirm deletion of the role.

View or print a user report

The user report is a PDF. The report contains the following information:

- User type
For more information about the user type, see “User repository overview” on page 70.
 - Full name
 - User name
 - Role
 - Status
 - Password pre-expired
If the user must set a new password the next time they sign in to an application, this value is set to **Yes** (see “Create a user account” on page 36).
 - Date created
 - Created by
 - Date last modified
 - Last modified by
 - Email
 - Phone
 - Password last modified
 - Comments
1. In the main screen, click the **Users** tab.
 2. Click **Report**.
The user report downloads to the default location set in the web browser.
 3. Access the report, save, then print the report.
 4. Close the report.

View or print a role report

The role report is a PDF. The report contains the following information:

- Role
- Workflow
- Description
- Number of privileges
- Number of users associated with the role
- Date created
- Created by
- Date last modified
- Last modified by

1. In the main screen, click the **Roles** tab.
2. Click **Report**.
The 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.



Manage the system security function

Overview of the system security settings

The **System** tab contains the settings for the following items:

- User name and password restrictions that apply when you create user accounts
- Lockout settings (how the software responds when a user tries to sign in multiple times with an incorrect password)
- Other settings such as automatic screen locking and report size

Functions that are controlled in the console

The following functions are controlled in the console:

- Configure security and auditing
- View action records
- View system configuration records
- View application object records
- View instrument run records

For a list of functions that are controlled in the software, see “Default permissions for the Diomni™ Design and Analysis (RUO) Software 3” on page 25.

Configure account setup and security policies

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 main screen, click the **System** tab.
2. In the **User Name Settings** pane, specify the minimum and maximum character length.

3. In the **Password Policy** pane, specify the password requirements.

The following items are specified:

- Minimum and maximum length
- Password reuse
- Complexity
- Minimum and maximum age
- Expiry reminder and length of time before the expiry that the reminder is sent
- User name check (cannot use a variation of the user name as the password)
- Check of compromised phrases

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 field and Account lockout duration field	If a user attempts to sign in with an incorrect user name or password more than the number of times set for the threshold, the user is locked out for the time specified.
Sign in attempts counter reset radio button and Reset failure sign in counter after field	<p>If the counter reset is enabled, the counter for the number of failed sign-in resets to 0 after the time specified.</p> <p>This setting applies before an account lockout occurs.</p> <p>For example, the threshold is set to 5 sign-in attempts and the counter reset is set to 15 minutes. If the user attempts to sign in with an incorrect user name or password 4 times, then waits for the specified time (15 minutes in this example), the number of failed sign-ins is reset to 0. The account lockout does not occur.</p>

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

Settings	Description when enabled
Automatic screen locking radio button and Inactivity duration field	The screen is locked if there is no activity for the time specified. A user must enter their user name and password to unlock the screen.
Client offline sign in radio button and Offline sign in threshold field	When the SAE server is offline, users can sign in and use an application for the time specified.
Report page size radio button	The report page size is A4 or letter.
Automatic inactive client removal radio buttons and Remove inactive client after field	If no users have signed in to the application after the defined number of days, an administrator must re-authenticate a secure connection with the application.
Open file from non-SAE system radio buttons	Diomni™ Design and Analysis (RUO) Software 3 allows users to access data files that were generated from a system without SAE functions, for example the desktop configuration. The application also allows users to open an item with an invalid audit trail. For more information, see “Overview of security settings for data files” on page 21 and “Overview of security settings for projects” on page 22.

6. Click **Apply Settings**.

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



Manage the audit function

■ Audit function	45
■ Enable or disable the audit function	45
■ Select items to audit and set the Audit Mode	46
■ Manage the audit reasons	46
■ View audit logs (audit history)	47

Audit function

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

- If audits are included for your application (see “Enable or disable the audit function” on page 45).
- The audit mode (see “Select items to audit and set the Audit Mode” on page 46).
- The audit reason settings when the audit mode is set to **Optional** or **Required**. See the following sections:
 - “Edit audit reasons” on page 46
 - “Delete audit reasons” on page 46
 - “Add audit reasons” on page 46

Audit records are time-stamped. Audit records cannot be overwritten.

Enable or disable the audit function

Auditing of objects can be enabled and disabled. Auditing of actions is always performed and cannot be disabled.

For a description of objects and actions, see “Objects that are audited” on page 24 and “Actions that are audited” on page 23.

1. In the main screen, click the **Audit** tab.
2. In the **Audit Settings** pane, select or deselect the **Include** checkbox for your application, if available.

Select items to audit and set the Audit Mode

1. In the main screen, click the **Audit** tab.
2. Select the **Audit Mode** for each application.

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 continue without entering a reason.
Required	The event is audited, a reason prompt is displayed, and the user must specify a reason.

3. Click **Apply Settings**.

Manage the audit reasons

If multiple applications are connected to the same instance of the security, auditing, and e-signature administrator console, the reason is added, edited, or deleted for all of the applications.

Edit audit reasons

1. In the main screen, click the **Audit** tab.
2. In the **Audit Reason Settings** pane, click **Edit** for the reason to be edited.
The **Edit Audit Reason** dialog box is displayed.
3. Edit the **Reason for change** field, then click **Save**.

Delete audit reasons

1. In the main screen, click the **Audit** tab.
2. In the **Audit Reason Settings** pane, click **Delete** for the reason to be deleted.
The **Delete Audit Reason** dialog box is displayed.
3. Click **Delete** to confirm.

Add audit reasons

1. In the main screen, click the **Audit** tab.
2. Under the **Audit Reason Settings** pane, click **New reason**.
The **Add New Audit Reason** dialog box is displayed.
3. Enter a reason in the **Reason for change** field, then click **Save**.

The new reason is displayed in the **Audit Reason Settings** pane.

View audit logs (audit history)

View the System Configuration audit log

The **System Configuration** audit history contains the audit records for actions performed in the security, auditing, and e-signature administrator console.

1. In the main screen, click **Audit History** ▶ **System Configuration**.
A log of the system security, audit, and e-signature configuration records is displayed.
2. *(Optional)* Click the column header to sort by the parameter.
3. *(Optional)* Check the **Enable System Configuration Records Filtering** checkbox to filter the records.
4. *(Optional)* Filter by one or more of the parameters, then click **Search**.
 - **Date Range**
 - **Action**
 - **Record Name**
 - **User Account**
 - **Record Type**

View the Action Records audit log

All items in the action records log are audited silently.

1. In the main screen, click **Audit History** ▶ **Action Records**.
A log of the audited events is displayed.
2. *(Optional)* Click the column header to sort by the parameter.
3. *(Optional)* Check the **Enable Action Records Filtering** checkbox to filter the records.
4. *(Optional)* Filter by one or more of the parameters, then click **Search**.
 - **Date Range**
 - **Application**
 - **Instrument**
 - **User Account**
 - **Action**

Note: The **Action** parameter is available when an **Application** is selected.

Actions that are audited in the security, auditing, and e-signature administrator console

For a list of actions that are audited for the application, see “Actions that are audited” on page 23.

Audit records are time-stamped. Audit records cannot be overwritten.

- Sign in to or out of the security, auditing, and e-signature administrator console
- Import or export an SAE configuration
- Install an application profile
- Archive, purge, or restore audit records
- Manual synchronization with LDAP Directory
- Failure to sign in

Export the audit history or generate an audit history report

Open the system configuration audit log or the action records audit log. Filter if required.

See “View the System Configuration audit log” on page 47 or “View the Action Records audit log” on page 47.

- Click **Export**.
A TXT file is downloaded.
- Click **Report**.
A PDF file is downloaded.



Manage the e-signature function

■ Overview of the e-signature settings	49
■ How the e-signature function works in the application	49
■ Parts of the e-Signature tab	50
■ Workflow to set up the e-signature function	53
■ Enable the e-signature function	53
■ (Optional) Add an e-signature meaning	54
■ Select the actions that require e-signature	54
■ Specify the number of signatures required for each action	54
■ Delete an e-signature meaning	55
■ Disable the e-signature function	56

Overview of the e-signature settings

Use the **e-Signature** tab to control the following items:

- Actions that require an e-signature check
- Number of e-signatures required for each action
- List of reasons that are available to users when they sign objects in the application

By default, the e-signature function is enabled. No actions are selected and no e-signatures are required.

E-signatures are enabled and disabled for all of the applications that are connected to the instance of the security, auditing, and e-signature administrator console.

How the e-signature function works in the application

When the e-signature function is enabled and configured in the security, auditing, and e-signature administrator console, the following steps occur in the application:

- A user with e-signature permission signs in to the application.
- The user performs an action that is configured to require an e-signature.
The user can also proactively provide an e-signature before the action is performed.
- The software checks the e-signatures associated with the action.
- If an e-signature is required and it has not yet been signed, or does not have the required number of e-signatures, the user is prompted to sign the required object before the action can continue.

- The user selects an e-signature meaning, then enters user name and password.
- When the e-signature requirements are met for the action, the action continues. The e-signature or the e-signatures are current.
- If the item that was signed is changed, the e-signature becomes obsolete. A new e-signature is required.

Parts of the e-Signature tab

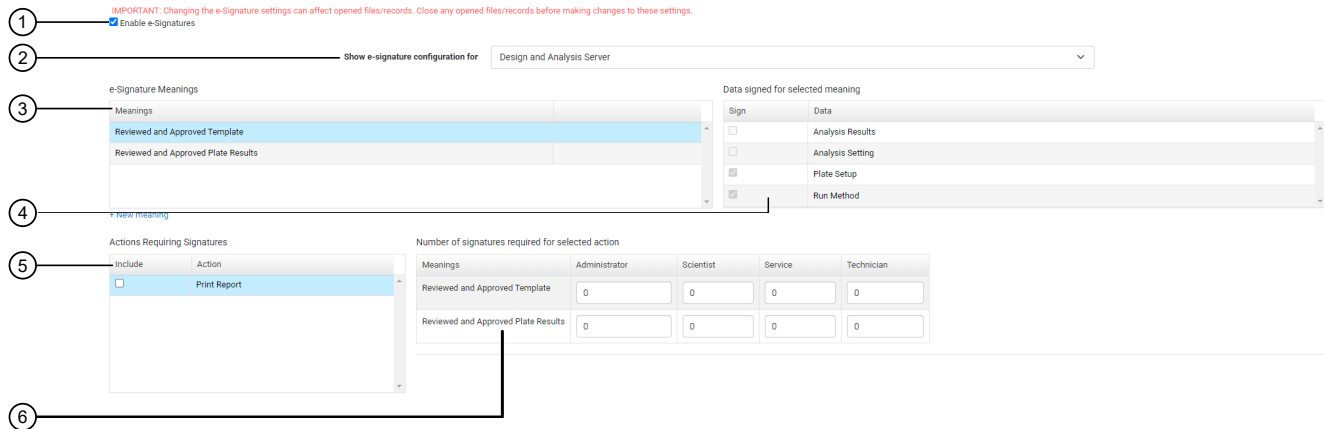


Figure 1 Parts of the e-Signature tab

- ① Enable/disable the e-signature function
- ② The application that the e-signature is being configured for (dropdown list)
- ③ E-signature meanings that can be applied when the object is signed
- ④ Objects that can be signed (**Data signed for selected meaning**)
- ⑤ Actions that require an e-signature
- ⑥ Number of e-signatures required for each action

Enable or disable the e-signature function

This section of the screen allows you to enable or disable the e-signature function. Enabling or disabling the e-signature function applies to all of the applications that are connected to the instance of the console.

See Figure 1 on page 50.

E-signature meanings and data signed for a meaning

Note: Ensure that the application that you would like to view and edit is selected in the **Show e-signature configuration for** drop-down list. The values can be different for each application.

See “Enable or disable the e-signature function” on page 50.

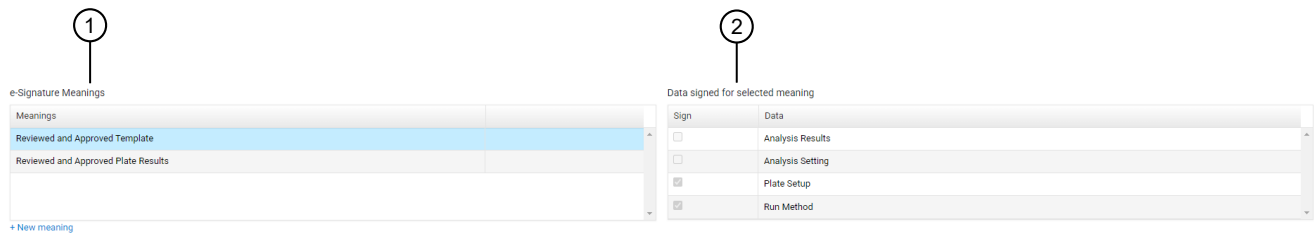


Figure 2 E-signature meanings and data signed for a meaning

- ① E-signature meanings
- ② Data signed for a selected meaning

This section of the screen displays the e-signature meanings and the data that are signed for a selected meaning. Each meaning is linked to specific data that are signed.

The e-signature meaning is the value that the user selects when providing an e-signature in the application.

The data signed indicates the items that are associated with an e-signature.

Click a specific e-signature meaning to see the data that are signed for the e-signature meaning. The e-signature meaning is highlighted in blue. The title above the list of data that are signed is updated to display the selected e-signature meaning.

The default e-signature meanings cannot be edited. The data signed associated with each default e-signature meaning cannot be edited.

E-signature meanings can be added. The data signed can be selected for a new e-signature meaning. Items cannot be added to the list of data that are signed. For more information, see “(Optional) Add an e-signature meaning” on page 54.

Note: For the default meanings that are provided with the application profile, the **Sign** checkboxes on the right of the screen are read-only. Select a default meaning on the left of the screen to see which object is linked to the selected meaning.

Actions that require an e-signature

This section of the screen allows you to select one or more actions that require e-signatures.

For the actions that can be selected for each application profile, see “Functions that can be signed” on page 24.

Note: The order of the actions in the **Actions Requiring Signatures** list is not sequential.

The figure below is an example. It shows the actions that can be selected to require e-signatures.

Actions Requiring Signatures

Include	Action
<input type="checkbox"/>	Print Report

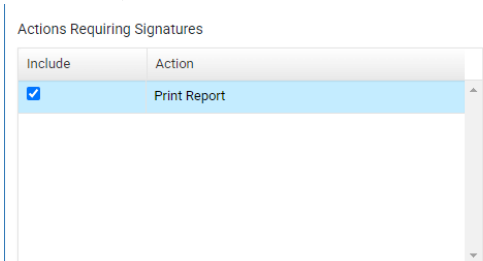
Figure 3 Actions that require e-signatures

Number of e-signatures required for the selected action

This section of the screen allows you to specify the number of e-signatures required from each role and for each meaning for each selected action.

The number of e-signatures applies to the action that is highlighted in blue. The title above the number of e-signatures is updated to display the selected action.

①



②

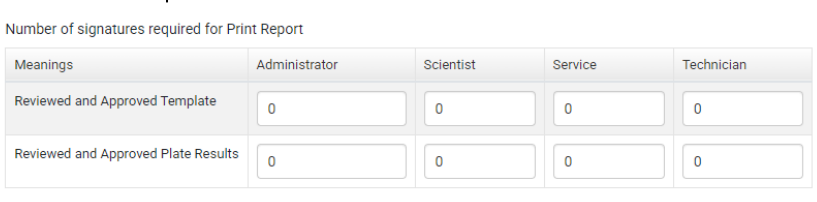


Figure 4 Number of e-signatures required for the selected action

- ① Actions that require e-signatures
- ② Number of signatures from each role and for each meaning for the selected action

The left side of the screen lists the actions that can be selected. You cannot add actions to this list.

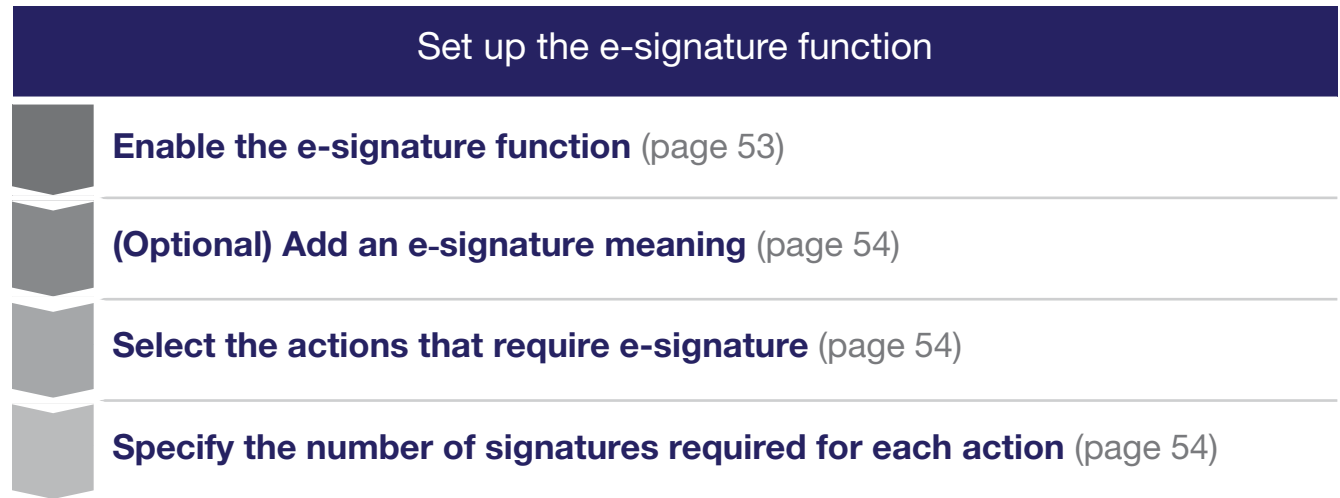
The right side of the screen lists the following information:

- All of the meanings from **e-Signature Meanings** (see “E-signature meanings and data signed for a meaning” on page 50). You can add to this list indirectly by adding to the list of meanings (see “(Optional) Add an e-signature meaning” on page 54).
- All of the roles that are defined in the console.

IMPORTANT! Roles are listed regardless of whether they have the e-signature permission enabled. Before specifying a number of signatures for a role, ensure that the role has the e-signature permission enabled.

Workflow to set up the e-signature function

To enable e-signature functions in an application, you must perform three of the four steps in the following workflow diagram. You can optionally perform one of the steps.



Enable 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.

Enabling the e-signature function applies to all of the applications that are connected to the instance of the security, auditing, and e-signature administrator console.

1. In the main screen, click the **e-Signature** tab.
2. Select or deselect the **Enable e-Signatures** checkbox.
3. Click **Apply Settings**.

(Optional) Add an e-signature meaning

For a description of the e-signature meanings and data that are signed, see “E-signature meanings and data signed for a meaning” on page 50.

Note: The default e-signature meanings for an application cannot be edited. The links to the data that are signed for the default e-signature meanings cannot be edited.

Perform this procedure to add custom e-signature meanings that are available in the application.

Enable the e-signature function (Enable the e-signature function (page 53)).

1. In the **e-Signature Meanings** pane, click **New meaning**.
2. In the **Create New Meaning** dialog box, enter a name in the **New e-signature meaning** field, then click **Save**.
The new meaning is listed in the **e-Signature Meanings** pane.
3. Select the new meaning.
The selected meaning is highlighted in blue.
4. In the **Data signed for <...>** pane, where <...> is the meaning, select the items to be associated with the meaning.
5. (Optional) Click **Apply Settings** if no other edits are made.

Select the actions that require an e-signature (see Select the actions that require e-signature (page 54)).

Select the actions that require e-signature

Enable e-signatures (see “Enable the e-signature function” on page 53).

1. In the **Actions Requiring Signatures** pane, select each action that requires an e-signature.
2. In the **Number of signatures required for selected action** pane, enter the number of e-signatures that are required from each SAE role before the associated action can be performed.
3. Click **Apply Settings**.

Specify the number of signatures required for each action

1. In the **Actions Requiring Signatures** pane, select an action that requires an e-signature.
When an action is selected for signatures in the left pane, it is highlighted in blue and the name of the action is displayed above the signature table.

Actions Requiring Signatures		Number of signatures required for Print Report				
Include	Action	Meanings	Administrator	Scientist	Service	Technician
<input checked="" type="checkbox"/>	Print Report	Reviewed and Approved Template	0	0	0	0
		Reviewed and Approved Plate Results	0	0	0	0

- For each selected action, enter the number of e-signatures that are required from each role and for each meaning before the associated action can be performed.

If you specify signatures for an action that is not enabled for e-signature (the checkbox is not enabled), the action does not require an e-signature.

IMPORTANT! Roles are listed regardless of whether they have the e-signature permission enabled. Before specifying a number of signatures for a role, ensure that the role has the e-signature permission enabled.

- Click **Apply Settings**.

Delete an e-signature meaning

Default e-signature meanings for the application cannot be deleted. Only e-signature meanings that were added can be deleted.

- In the main screen, select the **E-signature** tab.
- In the **e-signature Meanings** pane, click **Delete** for the e-signature meaning.
The **Delete** button is only displayed for the e-signature meanings that can be deleted. The default e-signature meanings for an application cannot be deleted.

e-Signature Meanings	
Meanings	
Reviewed and Approved Template	
Reviewed and Approved Plate Results	
New Meaning Example	Delete

① E-signature meaning that was added, can be deleted

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

Disable the e-signature function

If the e-signature function is disabled, it is disabled for all of the applications that are connected to the instance of the console.

1. In the main screen, select the **E-signature** tab.
2. Deselect the **Enable e-signatures** checkbox.
3. Click **Apply Settings**.

View and report audit and e-signature records

■ Types of audit and e-signature history records	57
■ View the action records audit log	58
■ View the System Configuration audit log	58
■ View the application objects audit log	59
■ View the e-signatures	59
■ View the instrument run records	60
■ Export active Action or System Configuration records	61

Types of audit and e-signature history records

The following records are available. Only roles with the appropriate permissions can view the records.

Record type	Description	Contents
Action records	Actions that are set to be audited	Audit records
System configuration	Changes that are made to security, audit, and e-signature settings	Audit records
Application object records	Objects that are set to be audited	Audit and e-signature records
Instrument run records	A summary of the run, objects that have been audited, actions that have been audited, data audits (Information about changes made during a run), and run completion information	Audit records

View the action records audit log

All items in the action records log are audited silently.

For a list of auditable actions in the console, see “Actions that are audited in the security, auditing, and e-signature administrator console” on page 48.

For a list of auditable actions in a specific application, see “Actions that are audited” on page 23.

1. In the main screen, click **Audit History** ▶ **Action Records**.
2. At the top left of the screen, select the **Enable Action Records Filtering** checkbox.
3. Use one or more of the following filtering tools.
 - **Date Range**
 - **Application** drop-down list
 - **Instrument** drop-down list
 - **User Account** drop-down list

The **Action** field cannot be edited.

4. Click **Search**.
The actions that meet the criteria set in step 3 are displayed.
5. (Optional) Click **Report** to create a PDF output of the action records.

View the System Configuration audit log

The **System Configuration** audit history contains the audit records for actions performed in the console.

1. In the main screen, click **Audit History** ▶ **System Configuration**.
2. At the top left of the screen, select the **Enable System Configuration Records Filtering** checkbox.
3. Use one or more of the following filtering tools.
 - **Date Range**
 - **Action** drop-down list
 - **Record Name**
 - **User Account** drop-down list
 - **Record Type** drop-down list
4. Click **Search**.
The actions that meet the criteria set in step 3 are displayed.
5. (Optional) Click **Report** to create a PDF output of the system configuration records.

View the application objects audit log

For a list of objects that can be audited for your application, see “Actions that are audited” on page 23. The auditing of objects for the application must be set up. See Chapter 8, “Manage the audit function”.

1. In the main screen, click **Audit History** ▶ **Application Object Records**.
2. At the top left of the screen, select the **Enable Application Objects Records Filtering** checkbox.
3. Use one or more of the following filtering tools.
 - **Last modified from**
 - **Application** drop-down list
 - **Last modified by**
 - **Instrument** drop-down list
 - **Object name**
 - **Data audit record name**
 - **Old or new value**
4. Click **Search**.

The actions that meet the criteria set in the filtering tools are displayed.
5. In the application objects table, select the record you want to view.

The record that is selected is highlighted in blue.
6. Select the **Data Audits** tab.
7. (Optional) Click **Report** to create a PDF output of the application objects.

View the e-signatures

For a list of items that require an e-signature, see “Functions that can be signed” on page 24.

1. In the main screen, click **Audit History** ▶ **Application Object Records**.
2. At the top left of the screen, select the **Enable Application Objects Records Filtering** checkbox.
3. Use one or more of the following filtering tools.
 - **Last modified from**
 - **Application** drop-down list
 - **Last modified by**
 - **Instrument** drop-down list
 - **Object name**
 - **Data audit record name**
 - **Old or new value**

4. Click **Search**.
The actions that meet the criteria set in step 3 are displayed.
5. In the application objects table, select the record you want to view.
The record that is selected is highlighted in blue.
6. Select the **e-Signature Records** tab, then select the e-signature record that you want to view from the list of available records.
The **e-Signature Record Details** dialog box opens.
7. (Optional) To create a PDF output of **Data Audit and e-Signature** history, click **Report**.
8. (Optional) Click **Report** to create a PDF output of the e-signature record.

View the instrument run records

1. In the main screen, click **Audit History ▶ Instrument Run Records**.
2. At the top left of the screen, select the **Enable Instrument Run Records Filtering** checkbox.
3. Use one or more of the following filtering tools.
 - **Run date from**
 - **Instrument** drop-down list
 - **File name**
 - **Started by** drop-down list
 - **Run name**
4. Click **Search**.
The instrument runs that meet the criteria set in step 3 are displayed.
5. In the instrument run records table, select the record you want to view.
The record that is selected is highlighted in blue.

6. Select one of the following tabs:

Tab	Displays the following information
Run Summary	<ul style="list-style-type: none"> 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)

7. (Optional) Click **Report** to create a PDF output of the instrument run records.

Export active Action or System Configuration records

The **Action** or **System Configuration** tabs provide an export function that allows you to export records in TXT format. The TXT files can be viewed in another program such as Microsoft™ Excel™.

The exported file for the action records is `action-records.txt`.

The exported file for the system configuration records is `audit-records.txt`.

IMPORTANT! Exported **Action** or **System Configuration** records cannot be imported back into the **Audit History** tab. To export records that can be restored into the **Audit History** tab, see Chapter 11, “Back up, archive, and restore SAE records and files”.

1. In the main screen, select one of the following options.

- Audit History ▶ Action Records**
- Audit History ▶ System Configuration**

2. (Optional) Use the filtering tools.

When the records are filtered, only the filtered records are exported in the TXT file.

For more information about the filtering tools, see “View the action records audit log” on page 58 and “View the System Configuration audit log” on page 58.

3. Click **Export**.



Back up, archive, and restore SAE records and files

■ Archive and backup options and frequency	62
■ Set up automatic archive of audit records	63
■ Manually archive audit records	64
■ View archived audit records	64
■ Restore archived audit records	65
■ Back up the encryption key	65
■ Back up the SAE program folder	66
■ Export archived audit records	66
■ Restore exported archived audit records	67
■ Export system security, audit, and e-signature settings	67
■ Import user, system security, audit, and e-signature settings	68
■ Back up to reinstall due to LDAP organizational unit error	69

Archive and backup options and frequency

Several options are available:

- Automatically archive records. SAE records are automatically removed from the database at the frequency you determine. SAE records can be viewed or restored in console.

Note: SAE records can be archived manually at any time.

- Export the settings for the console.
- Back up the entire SAE program folder with Windows™ Explorer.

Note: Records that are exported in the **Action** or **System Configuration** tabs cannot be restored. For information, see “Export active Action or System Configuration records” on page 61.

When to archive

The required frequency of archiving depends on your system configuration (such as the number of applications that use the SAE server, the configuration of the audit and e-signature functions). For the optimum performance of the SAE settings, the size of the database should not be large enough to affect SAE performance.

As a starting point, we suggest that you maintain a database size of <50 MB. If you notice a decrease in performance (for example, it takes a long time for the console to display records), consider maintaining a smaller database size.

A suggested approach for determining the required frequency is listed below.

- Configure the console to automatically archive.
- Check the size of the database monthly.
- If the database size is >50 MB after 3 months, increase the frequency of auto archiving.

Backing up the entire SAE program folder is optional. Perform the back up at a frequency determined by your laboratory and IT protocol.

Set up automatic archive of audit records

Automatically archiving audit records removes the records from the database and saves them in <...>:\Program Files (x86)\Applied Biosystems\SAE Admin Console\automated_archivals, where <...> is the installation drive.

Archived audit records can be viewed in the security, auditing, and e-signature administrator console.

1. In the main screen, click **Settings ▶ Auto Archive**.
2. In the **Auto Archival Settings** dialog box, select the **Enable Auto Archive** checkbox.,
3. Choose a setting in the **Archival mode** drop-down list.
 - **By number of records or retention period**
 - **By records retention period**
 - **By number of records**
4. Enter the number of records and the retention period.
The fields that are available depend on the setting that was selected in step 3.
5. Click **Save**.

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

Manually archive audit records

Manually archiving audit records removes the records from the database and saves them in <...>:\Program Files (x86)\Applied Biosystems\SAE Admin Console\automated_archivals, where <...> is the installation directory. They are saved in a folder named by the date and the time of the archival.

The audit records that are stored in the security, auditing, and e-signature administrator console are archived.

Some audit records are stored in the files in Diomni™ Design and Analysis (RUO) Software 3. These audit records are not included in a manual archive in the security, auditing, and e-signature administrator console.

1. In the main screen, click **Settings ▶ Archival History**.
2. Click **Ad-hoc Archival**.
3. In the **Archive Records** dialog box, enter a date range.
4. Click **Archive**.

The archive is listed when you click **Settings ▶ Archival History**. See “View archived audit records” on page 64.

View archived audit records

1. In the main screen, click **Settings ▶ Archival History**.
Each row represents an archive event. The **Run Duration** indicates how long the archival event took to complete.
2. Select a row, then select **View Archived Records** to display the records in the archive.
3. As needed, click the **Action Records** tab and the **System Configuration** tab.
The **Application Object Records** tab and the **Instrument Run Record** tab are visible. These items are not applicable for the Diomni™ Design and Analysis (RUO) Software 3.
4. Click the **Back to Archival History** to display the main archive record screen.

Restore archived audit records

Archived audit records are available in the security, auditing, and e-signature administrator console (see “View archived audit records” on page 64).

1. In the main screen, click **Settings ▶ Archival History**.
Each row represents an archive event. The **Run Duration** indicates how long the archival event took to complete.
2. Select a row, then click **Restore**.
3. In the **Restore Records** dialog box, click **Restore**.

The archival event remains listed after the audit records are restored. The audit records cannot be restored more than one time.

Back up the encryption key

The program data from Security, Auditing, and E-signature (SAE) Administrator Console v3 is encrypted. An encryption key is required to restore the data.

For Security, Auditing, and E-signature (SAE) Administrator Console v3 the encryption key is stored in the Credential Manager (Windows™).

We recommend backing up a copy of the encryption key, then saving it in a location where it can be accessed in the event that the computer on which Security, Auditing, and E-signature (SAE) Administrator Console v3 becomes inaccessible.

If the computer where the encryption key is stored is not accessible due to a failure, the data cannot be restored on another computer. In this scenario, the data are encrypted but the encryption key is not accessible.

The encryption key is the same for one instance of Security, Auditing, and E-signature (SAE) Administrator Console v3. The encryption key remains the same if the encryption key is downloaded more than one time. It is not necessary to back up the encryption key each time the data are backed up.

If you have multiple instances of Security, Auditing, and E-signature (SAE) Administrator Console v3 on separate computers, each instance requires its own encryption key.

The encryption key is in a TXT file format.

A user with an administrator account for the computer must back up the encryption key.


1. In the main screen, click **Settings ▶ Back Up Encryption Key**.
2. In the **Back Up Encryption Key** dialog box, click **Export**.
3. Save the encryption key that was downloaded to a location that is accessible if the host computer is no longer accessible.
The encryption key can be stored on a separate computer or a server.
The encryption key can be stored in the same location as the data that are backed up.

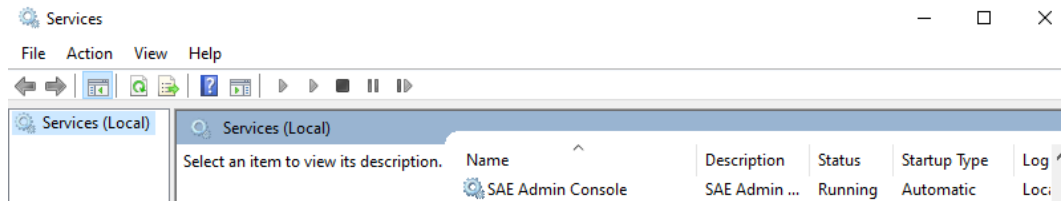
Back up the SAE program folder

IMPORTANT! For Security, Auditing, and E-signature (SAE) Administrator Console v3, back up the encryption key. The data are encrypted. If the encryption key is lost, the data that are backed up cannot be restored. See “Back up the encryption key” on page 65.

To obtain a complete copy of all SAE records and settings, you can back up the SAE program folder. Back up the entire program folder, not just the database folder, to help ensure compatibility between the SAE server software and the database files.

IMPORTANT! If the backed up files require re-installation or installation on another computer, contact Technical Support.

1. Instruct all users to sign out of the applications and the security, auditing, and e-signature administrator console.
2. Close the security, auditing, and e-signature administrator console.
3. Stop the SAE server.
 - a. In the Windows™ desktop, click , type **services**, then open the **Services** application.



- b. Scroll down to **SAE Admin Console**, right-click it, then click **Stop**.
4. Copy the <...>:\Program Files (x86)\Applied Biosystems\SAE Admin Console, where <...> is the installation directory, to a back up location.
5. Repeat step 3, then click **Start** to start the SAE server.
6. Start the security, auditing, and e-signature administrator console.

Export archived audit records

1. In the main screen, click **Settings ▶ Archival History**.
Each row represents an archive event. The **Run Duration** column indicates how long each archival event took to complete.
2. Select a row, then select **Export** to export a records compressed folder (ZIP folder) that contains the records in the archive.

The exported archived audit records can be imported (see “Restore exported archived audit records” on page 67).

Restore exported archived audit records

Exported archived audit records are stored in a compressed folder (ZIP folder). See “Export archived audit records” on page 66.

1. In the main screen, click **Settings** ▶ **Archival History**.
2. Click **Restore (upload)**.
3. In the **Restore Records** dialog box, click **Choose File**, then navigate to the folder that contains a compressed folder (ZIP folder) with the archived audit records.
4. Click **Restore**.
The **Restore Records** dialog box displays the number of records that were restored.

Export system security, audit, and e-signature settings

Use the export functions to transfer settings from one instance of the console to another instance.

Setting up a password for the file is required for Security, Auditing, and E-signature (SAE) Administrator Console v3.

1. In the main screen, click **Settings** ▶ **Export Configuration**.
2. In the **Export Configuration** dialog box, select an export option.

Setting	Items exported
All	All settings and user accounts
Custom, Users & roles	<ul style="list-style-type: none">• Active user accounts• Roles and their associated permissions
Custom, System & roles	<ul style="list-style-type: none">• Settings• Roles and their associated permissions

3. In the **File password** field, enter a password.
The password is created for the file. The password is required when the file is imported. The password must contain 6 characters. There are no complexity requirements for the password.
4. Click **Export**.
5. Click **Configuration file**.
The DAT file is downloaded.

6. (Optional) Click **Recovery key**.

A TXT file is downloaded. The content of the TXT file can be copied into the console when the file is imported. The recovery key is an alternative to the password if the password is forgotten or lost.

7. Click **Close**.

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

Settings that were exported from one instance of the console can be imported into another instance.

Settings that were exported from Security, Auditing, and E-signature (SAE) Administrator Console v3.0 and later require a password or recovery key to import into the console.

For information about the items that can be exported for import, see “Export system security, audit, and e-signature settings” on page 67.

Export the settings (“Export system security, audit, and e-signature settings” on page 67).

1. In the main screen, click **Settings ▶ Import Configuration**.
2. In the **Import Configuration** dialog box, click **Choose File**, then navigate to the file that contains the settings to import.

The settings are in a DAT file.

3. Select an import option.

Setting	Items exported
All	All settings and user accounts
Custom, Users & roles	<ul style="list-style-type: none"> • Active user accounts • Roles and their associated permissions
Custom, System & roles	<ul style="list-style-type: none"> • Settings • Roles and their associated permissions

The software imports the items that are in the DAT file. If **All** is selected for import but only **Users & roles** or **System & roles** were exported, the software imports the items that are available in the DAT file.

4. In the **File password** field, enter the password that was set for the file when the file was exported.
5. (Optional) Click **Use recovery key**.
The recovery key can be used if the password is lost or forgotten. The option to generate a recovery key was provided when the file was exported.
6. (For a recovery key) Copy the information from the TXT file, then paste the text into the **Recovery key** field.

7. If imported user accounts exist in the console, click **Skip** or **Overwrite** for each user account, then click **Confirm and Import**.
The **Import Configuration** dialog box displays a confirmation message. The number of created accounts and updated accounts is displayed.
8. Click **Close**.

If there are any notifications, the **Event Notifications** dialog box is displayed. Perform one of the following actions:

- Click **Close**.
- Select one or all of the notifications, then click **Acknowledge**.

Back up to reinstall due to LDAP organizational unit error

The number of accounts in the console is limited to 1,000. The synchronization of an organizational unit should be set up so it includes only users that need to access the console.

If an error is made in the organizational unit that is synchronized to the console and the number of users is close to the limit or over the limit, the console can be uninstalled, then reinstalled.

Export or back up the following items before uninstalling and reinstalling the console:

- Export the settings and roles (see “Export system security, audit, and e-signature settings” on page 67)
- Archive the audit records (see “Manually archive audit records” on page 64)

IMPORTANT! When exporting the settings and roles, ensure that the user accounts are not exported.

Reinstall the console, then import the following items:

- Import the settings and roles (see “Import user, system security, audit, and e-signature settings” on page 68)
- Import the audit records (see “Restore exported archived audit records” on page 67)

Synchronize with the LDAP and manually add local users.

■ User repository overview	70
■ Overview of LDAP repository synchronization	71
■ Configure user repositories	72

User repository overview

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

The 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 console.
 - SAE user accounts are created in the 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 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 **Users** tab.
 - User authentication is based on the accounts that are listed in the **Users** tab and the external LDAP user repository.

The following settings from the **System** tab are not used for LDAP:

 - **User Name 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 console.
- All local user accounts except the default Administrator account are set to **Inactive** and cannot sign in to the application.
- Passwords cannot be changed in the console.
- Users remain in the console with the status of **Removed** if they are removed from the LDAP user repository.
- **Federated**—Allows internal (local) and external account sign-in to an application.
 - User accounts are created in the console or in an LDAP user management system.
 - User authentication is based on the respective internal or LDAP user repository.

Overview of LDAP repository synchronization

The console can be configured to synchronize with an LDAP repository.

The console allows a maximum of 1,000 accounts. The maximum number of accounts applies to all user repositories.

The limit of 1,000 users includes users with a status of **Removed**. The users who are not in the LDAP repository remain in the console with the status of **Removed**.

If the organization has more than 1,000 users, the organization must create a lower-level organizational unit with a group of users to access the console. The console cannot be synchronized with the main organizational unit due to the number of users being over the limit of 1,000.

If the limit of 1,000 users is reached, a change to the organizational unit that is synchronized does not reset the limit.

The console pulls users from only a single organizational unit.

The console can pull users from multiple organizational units that are nested within a single organizational unit. The synchronization must be set up for the single organizational unit that contains the multiple organizational units.

The console does not allow aliases or complex filtering.

The user accounts cannot be searched or filtered within the console.

The console can perform a partial synchronization. For example, if 900 LDAP repository accounts are synchronized and 200 LDAP repository accounts are added to the directory, 100 LDAP repository accounts are synchronized. The partial synchronization in this example reaches the maximum number of 1,000 LDAP accounts. A warning message is displayed to indicate the 100 of the 200 LDAP repository accounts were not able to be synchronized.

A full synchronization is performed when the LDAP repository is configured. Following the initial configuration, an automatic synchronization is performed every 15 minutes. Any changes to the LDAP repository are reflected in the console during the automatic synchronization. Changes include adding new users, updating the status of removed users, any updates to user accounts, for example, password changes.

When the user repository settings are updated to an external LDAP repository, all local users except for the default administrator are set to an inactive status. Local users cannot sign in to any applications.

The local users are not set to an active status if the user repository settings are updated to an internal user repository. The local users must be set to active status manually.

Ensure the following items for a successful connection to an LDAP repository:

- The user is present in the organizational unit.
- Access must be given to the full organizational unit structure if there are nested organizational units.

If the user is in the third level of an organizational unit, the full structure or the full path of the applicable level must be given, for example, Domain/Organizational Unit Level 1/Organizational Unit Level 2/Organizational Unit Level 3. If the user is in

the third level of an organizational unit, Organizational Unit Level 2/Level 3 or Organizational Unit Level 3 are not sufficient.

- Ensure that you are providing access to an organizational unit that has only users who need to access the console. This is due to the limit of 1,000 users.
- The host for the organizational unit is correct.
- The password for the host is correct.

After the LDAP repository is synchronized, a user can log in to the application with their user name and password that is defined in the LDAP repository. The role for the user is defined during the user account mapping when the console is set up to synchronize with the LDAP repository.

The role is the method that information is segmented between users in the application. More detailed segmentation cannot be performed.

If the console cannot connect to an LDAP repository, the message **Unable to connect to directory server** is displayed.

Configure user repositories

Configure user repositories for SAE or external account access

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

1. Click **Settings ▶ User repositories (advanced)**.
2. In the **User Repository Settings** dialog box, in the **Definition** tab, select a value from the **User repository definition** dropdown list.

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

3. If you selected **External LDAP User Repository** or **Federated Repositories**, click **Next**.
4. Enter the required information in the **LDAP Server Configuration** tab, then click **Next**.
See “User repository settings” on page 73.
5. Enter the required information in the **User Account Mapping** tab, then click **Next**.
See “User repository settings” on page 73.
 - 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 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. In the **Authentication Verification** tab, enter the user name and password for the LDAP server, then click **Test Authentication**.
7. Click **Test Connection**
8. Click **Apply Settings**.
9. If needed, edit the user accounts to assign roles.
See Chapter 6, “Manage SAE user accounts and roles”.

The SAE server 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.

User repository settings

Table 1 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	<p>LDAP server attributes required for access</p> <p>The base is the highest level of the organizational hierarchy that should be synchronized.</p> <p>The bind is the user name that is used to search and request authentication. The format is <code>firstname.lastname</code>.</p>
User Account Mapping	
Directory type	<p>LDAP server configuration</p> <p>Click Set Defaults after you select the Directory type to display typical default parameters for mapping to an LDAP system.</p>
User name	Parameter that maps to the user name in the LDAP system
Default role assignment	<p>The SAE role that will be assigned to all user accounts. You can change the role after the user accounts are imported into the console.</p> <p>The No Privileges Role is the default value.</p>
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 server 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 are created in the console.	<ul style="list-style-type: none"> 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 .	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> External account Internal (local) account (with local/ prefix) Example: local/User name 	<ul style="list-style-type: none"> 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

Perform a full manual synchronization

The console periodically synchronizes with the LDAP.

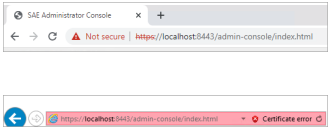
The **Manual Full Sync** is not available if the console is not set up with an external or federated user repository.

1. Select the **Users** tab.
2. Click **Manual Full Sync**.

The **Manual Full Sync** is disabled during the synchronization process.



Troubleshooting

Observation	Possible cause	Recommended action
<p>A security or warning message is displayed when you start the console</p> <p>Details: Examples of the messages you may see in a browser are shown below.</p> 	<p>The self-signed SSL certificate for the console URL cannot be verified by a certification authority.</p>	<p>See “Overview of the warning screens” on page 85.</p>
<p>The console automatically signs out after 30 minutes</p>	<p>The software is designed to automatically sign out after 30 minutes of inactivity. This lockout time is not configurable.</p>	<p>Sign in.</p>
<p>The application is not prompting for signatures</p>	<p>The user profile does not have the e-signature permission enabled.</p>	<p>Assign a role that has the e-signature permission enabled.</p> <p>Edit the role to allow e-signatures.</p> <ol style="list-style-type: none"> 1. In the main screen, click the Roles tab. 2. Select a role, then click Edit. 3. Click (expand) next to the application profile. 4. Click (expand) next to Security Configuration, then select the checkbox next to Perform E-Signing. 5. Click Save.
	<p>The e-signature function is not enabled for the application.</p>	<p>Enable the e-signature function for the application (“Enable the e-signature function” on page 53).</p>

Observation	Possible cause	Recommended action
The application is not prompting for signatures (continued)	All of the required settings that are required to enable e-signature function are not set.	<p>To enable the function, make all of the following settings (if all settings are not made, the function is not enabled):</p> <ul style="list-style-type: none"> • Select the Enable e-signatures checkbox. • Select an action. • Enter a number of signatures required for a meaning. <p>See “Workflow to set up the e-signature function” on page 53.</p>
An expected permission is not listed for an application when you create a role	A newer version of the application profile may be required.	Check the version of the application profile (Settings ▶ Manage Application Profiles), then contact Technical Support.
Default audit settings are not displayed for an application profile	In the Audit tab, the list in the Audit Settings pane contains additional rows that are not visible.	Scroll down to see settings for additional application profiles.
The expected audit records are not listed in the audit history screens	The records have been archived.	Select Settings ▶ Archival History to view archived records.



Install and manage the software

■ Overview of the installer	77
■ Compatibility	78
■ Overview of an upgrade to Security, Auditing, and E-signature (SAE) Administrator Console v3	78
■ Overview of a downgrade	78
■ Installation requirements	79
■ Install all components	81
■ Install Security, Auditing, and E-signature (SAE) Administrator Console v3	83
■ Configure the SAE settings	85
■ Overview of the warning screens	85

Overview of the installer

An installer is available that installs Diomni™ Design and Analysis (RUO) Software 3, Security, Auditing, and E-signature (SAE) Administrator Console v3, and the application profile.

The application profile is required in order to sign in to Diomni™ Design and Analysis (RUO) Software 3.

Different options for installation are available. The options depend on the following items:

- If the components are installed on the same computer or separate computers
- If the security, auditing, and e-signature administrator console has been installed
- If the application profile has been installed

Installing the Security, Auditing, and E-signature (SAE) Administrator Console v3 is not required during the installation process. An existing instance of a security, auditing, and e-signature administrator console on a different computer can be used. The instance must be compatible with Diomni™ Design and Analysis (RUO) Software 3.

Only one instance of a security, auditing, and e-signature administrator console can be installed on a computer.

IMPORTANT! If an earlier version of the security, auditing, and e-signature administrator console is detected on the computer, the installer can upgrade to Security, Auditing, and E-signature (SAE) Administrator Console v3 during the installation.

If you have other applications that must use the earlier version of the security, auditing, and e-signature administrator console, installing Security, Auditing, and E-signature (SAE) Administrator Console v3 can affect the connection to the other applications.

Compatibility

Software	Security, auditing, and e-signature administrator console	Application profile ^[1]
Diomni™ Design and Analysis (RUO) Software v3.0	Security, Auditing, and E-signature (SAE) Administrator Console v3.0	Design And Analysis Server (1.0.<...>)

[1] <...> represents the third digit of the application profile version.

Overview of an upgrade to Security, Auditing, and E-signature (SAE) Administrator Console v3

An earlier version of the console can be upgraded to Security, Auditing, and E-signature (SAE) Administrator Console v3. The upgrade is performed when you install Security, Auditing, and E-signature (SAE) Administrator Console v3 on a computer that has an earlier version of the console installed.

The upgrade can be performed by installing Security, Auditing, and E-signature (SAE) Administrator Console v3 on its own. The upgrade can be performed by using an installer for an application where the installer also includes Security, Auditing, and E-signature (SAE) Administrator Console v3.

All of the items are retained in an upgrade. This includes application profiles, roles, accounts, permissions, audit settings, e-signature settings, and all records.

Only one instance of a console can be installed on a computer, even if the instances of the console are different versions.

If you upgrade to Security, Auditing, and E-signature (SAE) Administrator Console v3, applications that are compatible with this version of the console can connect to it without needing to upgrade the application.

IMPORTANT! Ensure that all of your applications to connected to earlier versions of the console are compatible with Security, Auditing, and E-signature (SAE) Administrator Console v3 before upgrading.

Overview of a downgrade

A downgrade to an earlier version of a security, auditing, and e-signature administrator console is not supported.

Installation requirements

The security, auditing, and e-signature administrator console can be installed on a computer purchased from Thermo Fisher Scientific or a customer-supplied computer.

IMPORTANT! Antivirus software must be installed on the computer. See “Antivirus software requirements” on page 80.

If a customer-supplied computer is used, there are recommended computer specifications (see “Recommended computer specifications” on page 79).

Only one instance of a security, auditing, and e-signature administrator console can be installed on a computer. This applies to different versions of a security, auditing, and e-signature administrator console. This also applies to a security, auditing, and e-signature administrator console that is installed with the application, for example, the security, auditing, and e-signature administrator console that is installed with QuantStudio™ Design and Analysis Desktop Software v1.

Multiple applications can connect to the single instance of the console.

If the console is installed on a different computer than the instrument or software, a static IP address is recommended.

Note: An application software can be installed on the same computer as the console or a different computer than the console.

Time difference for server connection

If the console is installed on a separate computer from the application, the time difference between the application and the separate computer with the console must be less than 5 minutes to establish the connection. If the time difference is more than 5 minutes, the application displays an error message.

Recommended computer specifications

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

- Operating system—Windows™ 10 (64-bit) or Windows™ 11
- Intel™ Core™ processor or compatible
- Memory—16 GB RAM minimum
- Hard drive—500 GB minimum free space
- Monitor—1280 × 1024 resolution or higher
- One open Ethernet port for connecting directly to the application (instrument or software)
- Microsoft™ Excel™ software
- Browser options
 - Google Chrome™ v40 or later (recommended)
 - Mozilla™ Firefox™ v40 or later
 - Microsoft Edge™

Note: The installation is not stopped if the computer does not meet the recommended specifications. The specifications are recommendations and not requirements.

Antivirus software requirements

The optional computer that is available from Thermo Fisher Scientific does not include antivirus software because customer preferences and network requirements vary. You are responsible for installing antivirus software of your choice to protect the computer against viruses.

The following antivirus software applications have been tested for use with an optional computer:

- Microsoft™ Defender
- Avast™ Free Antivirus
- McAfee™ Total Protection

Network options

Contact your IT department to set up an appropriate network connection.

There are two network connection options:

- DHCP-assigned IP address (dynamic host configuration protocol)
- Static IP address

If a DHCP is used, a DHCP reservation is recommended. A DHCP reservation is also recommended instead of a static IP address.

A DHCP reservation prevents the DHCP server from assigning a different IP address to the system.

If a DHCP reservation is not used, it is possible that the IP address changes after a certain period. This results in a loss of connection between the security, auditing, and e-signature administrator console and the connected applications.

If the IP address changes after a certain period, it also affects users connecting to the security, auditing, and e-signature administrator console from separate computers on the network.

Firewall ports that must be open

Port 8443 must be open for the operating system on the computer that is running the console.

- Instrument-to-console server connection
- Computer-to-console server connection, if the application is software and the software is installed on a different computer than the console

Firewall ports

To open a port for Microsoft™ Defender, add inbound rules for the port, and apply to all profiles.

To open a port for Norton Internet Security™, use the **Settings** menu to open the port.

No action is required to open a port for Symantec™ Endpoint Protection.

Third-party software

Before installing third-party software on the computer running the product software, confirm that the third-party software will not have either/or of the following effects on the computer:

- Restrict Ethernet communication.
- Interfere with instrument or computer operation.

Install all components

Use this workflow to install all components.

- Diomni™ Design and Analysis (RUO) Software 3
- Security, Auditing, and E-signature (SAE) Administrator Console v3
- Application profile

If Security, Auditing, and E-signature (SAE) Administrator Console v3 is detected on the computer, it is not installed during the installation.

If an earlier version of the security, auditing, and e-signature administrator console is detected, the option to upgrade to Security, Auditing, and E-signature (SAE) Administrator Console v3 during the installation.

If the security, auditing, and e-signature administrator console is upgraded from an earlier version, the data are retained and migrated to Security, Auditing, and E-signature (SAE) Administrator Console v3.

IMPORTANT! If you have other applications that must use the earlier version of the security, auditing, and e-signature administrator console, installing Security, Auditing, and E-signature (SAE) Administrator Console v3 can affect the connection to the other applications.

1. Log in to the computer with a Windows™ Administrator account.
2. Download the compressed folder (ZIP format).
3. Extract the files from the compressed folder.
4. Double-click the Diomni™ Design and Analysis (RUO) Software 3 EXE file.
5. In the **Design and Analysis 3 Server Setup** dialog box, select the **Install SAE Administrator Console v3 on local machine** radio button.
6. Click **Next**, then follow the instructions in the installer.
The components are installed.
7. Accept the terms of the *License Agreement*.
8. Click **Finish**.

9. (Optional) Select the **Run Design and Analysis Server** checkbox.

The checkbox is selected by default.

10. Click **Finish**.

Start the service (see “Start the software service” on page 83). The software service is started during the installation procedure by default. If the **Run Design and Analysis Server** checkbox was deselected during the installation procedure, the software service must be started.

Sign in to Diomni™ Design and Analysis (RUO) Software 3 and change the password (see “Update administrator password” on page 82).

Set up the export settings.

Update administrator password

This procedure applies when Security, Auditing, and E-signature (SAE) Administrator Console v3 was installed at the same time as Diomni™ Design and Analysis (RUO) Software 3 and on the same computer as Diomni™ Design and Analysis (RUO) Software 3.

Updating the administrator password and enabling security is required when Security, Auditing, and E-signature (SAE) Administrator Console v3 is installed.

1. Log in to Diomni™ Design and Analysis (RUO) Software 3 with the initial administrator user name and password.
See “Initial user name and password” on page 83.
2. In the **Change Password** dialog box, enter the initial password in the **Old password** field.
3. Enter the new password in the **New password** field, then enter it again in the **Confirm password** field.

IMPORTANT! The administrator password cannot be recovered after it has been reset. The software must be uninstalled, then reinstalled.

4. Click **OK**.

The password must meet the policy for passwords. If an error message is displayed, enter a different password.

The following default password policies apply the first time the administrator logs in to Security, Auditing, and E-signature (SAE) Administrator Console v3.

- A minimum length of 12 characters
- A maximum length of 64 characters
- At least 2 letters, including at least 1 uppercase letter and at least 1 lowercase letter
- At least 1 number
- At least 1 special character

Initial user name and password

IMPORTANT! The password must be changed at the first login.

The administrator password cannot be recovered after it has been reset. The software must be uninstalled, then reinstalled. All of the information, including application profiles, permissions, SAE accounts, audit records, and e-signatures are lost when the software is uninstalled.

- Initial user name: **Administrator**
- Initial password: **Administrator**

Start the software service

1. In the Windows™ system tray, right click the icon for Diomni™ Design and Analysis (RUO) Software 3.
2. Click **Start Service**.
Service started successfully is displayed in a dialog box.
The icon is blue in the Windows™ system tray
3. Click **OK** to close the dialog box.

The software can be accessed from a different computer via a web browser.

Install Security, Auditing, and E-signature (SAE) Administrator Console v3

Security, Auditing, and E-signature (SAE) Administrator Console v3 can be installed separately.

1. Log in to the computer with a Windows™ Administrator account.
2. Download the EXE file.
3. Double-click the EXE file.
4. Click **Install**.
5. Accept the terms of the *License Agreement*.
6. Click **Finish**.

Update the administrator password (see “Update the administrator password at first login” on page 84).


Install the application profile (see Chapter 5, “Manage application profiles”).

Update the administrator password at first login

Log in to the Security, Auditing, and E-signature (SAE) Administrator Console v3 with the initial administrator user name and password at the first login (see “Initial user name and password” on page 83). You are prompted to change the password.

If Security, Auditing, and E-signature (SAE) Administrator Console v3 and Diomni™ Design and Analysis (RUO) Software 3 are installed at the same time, you can log in to Diomni™ Design and Analysis (RUO) Software 3 to update the administrator password.

IMPORTANT! The administrator password cannot be recovered after it has been reset. The software must be uninstalled, then reinstalled.

1. Click  **(Windows Start Menu) ▶ Applied Biosystems ▶ SAE Admin** to open the console.
You can create a shortcut for the console on the desktop, then access it directly from the desktop. See “Create a shortcut for the security, auditing, and e-signature administrator console” on page 85.

Note: Security, Auditing, and E-signature (SAE) Administrator Console v3 console runs in a browser. For more information, see the documentation for Security, Auditing, and E-signature (SAE) Administrator Console v3.



The **Change Password** dialog box is displayed.

2. In the **Change Password** dialog box, enter the initial password.
See “Initial user name and password” on page 83.
3. Enter the new password in the **New password** field, then enter it again in the **Confirm password** field.
4. Click **Update**.
The password must meet the policy for passwords. If an error message is displayed, enter a different password.
The following default password policies apply the first time the administrator logs in to Security, Auditing, and E-signature (SAE) Administrator Console v3.
 - A minimum length of 12 characters
 - A maximum length of 64 characters
 - At least 2 letters, including at least 1 uppercase letter and at least 1 lowercase letter
 - At least 1 number
 - At least 1 special character

Create a shortcut for the security, auditing, and e-signature administrator console

Creating a shortcut is optional. A shortcut enables the software to be launched directly.

If a shortcut is not created, the software can be launched from the Windows™ start menu.

1. Navigate to <...>\Users\Public\Public Desktop, where <...> is the installation drive.
2. Copy  **SAE Admin**.
3. Paste  **SAE Admin** to the appropriate location.

The icon is available and it can be double-clicked to launch the software.

Configure the SAE settings

1. In the Windows™ system tray, right click the icon for Diomni™ Design and Analysis (RUO) Software 3.
2. Click **SAE Setting**.
3. In the **SAE Setting** dialog box, enter the
4. In the **SAE Setting** dialog box, enter the applicable value in the **SAE Host IP** field.
 - If Security, Auditing, and E-signature (SAE) Administrator Console v3 is installed on the same computer, enter *localhost*.
 - If Security, Auditing, and E-signature (SAE) Administrator Console v3 is installed on a separate computer, enter the IP address of the computer.

The **Host port** field is populated with **8443**. This is the required port. Do not edit this value.

IMPORTANT! If the instance of the security, auditing, and e-signature administrator console is changed, the accounts are changed and the audit trail is affected.

5. Click **Test connection**.
6. Click **Save & close**.

Overview of the warning screens

If a security or warning screen is displayed when you start the security, auditing, and e-signature administrator console, you can bypass the security or warning screen.

See the following sections for more information:

- “Warning for the Google Chrome™ browser” on page 86
- “Warning for the Mozilla™ Firefox™ browser” on page 86
- “Warning for the Microsoft Edge™ browser” on page 87

After you bypass the security or warning screen, the browser might still indicate that the connection is not secure, or that there is a certificate error. It is safe to use the security, auditing, and e-signature administrator console when a security or warning screen is displayed, because the default communication between the client (security, auditing, and e-signature administrator console) and server (SAE server) is encrypted.

The security, auditing, and e-signature administrator console runs locally on your computer, even though it is displayed in a web browser format. Google Chrome™ is the recommended web browser. Mozilla™ Firefox™ or Microsoft Edge™ can be used.

When you start the security, auditing, and e-signature administrator console, it opens the URL for the SAE server in your default browser.

Note: When any browser accesses a URL that uses the HTTPS protocol, the browser attempts to check the web server certificate with a Certificate Authority (CA). Several well-known and trusted authorities exist, from which a website/URL owner can purchase a certificate that uniquely identifies the URL and verifies its authenticity.

The web server certificate that is provided for the SAE server URL is self-signed (meaning it is not purchased from a CA). Because it cannot be verified by a CA, a security or warning screen is displayed.

If your organization has an internal CA, your IT representative might be able to generate and install a self-signed certificate for the SAE server URL. The certificate is then verified with your internal CA, and the security or warning screen is not displayed when you start the security, auditing, and e-signature administrator console.

Adding the URL as a trusted site does not eliminate the security or warning screen.

Warning for the Google Chrome™ browser

Launch the security, auditing, and e-signature administrator console.

The "**Your connection is not private**" warning message is displayed.

Click **ADVANCED ▶ Proceed to <domain name> (unsafe)** to proceed.

The security, auditing, and e-signature administrator console is launched with **Not Secure** displayed in the URL bar. The user can log in.

If the self-signed SSL certificate is installed in the Google Chrome™ browser, the warning message is not displayed (for the localhost domain only). With a self-signed SSL, the warning message is displayed if the security, auditing, and e-signature administrator console is accessed from a separate computer.

Warning for the Mozilla™ Firefox™ browser

Launch the security, auditing, and e-signature administrator console.

The "**Warning: Potential Security Risk Ahead**" warning message is displayed.

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

The security, auditing, and e-signature administrator console is launched with **Not Secure** displayed in the URL bar. The user can log in.

If the self-signed SSL certificate is installed in the Mozilla™ Firefox™ browser, the warning message is not displayed (for the localhost domain only). With a self-signed SSL, the warning message is displayed if the security, auditing, and e-signature administrator console is accessed from a separate computer.

Warning for the Microsoft Edge™ browser

Launch the security, auditing, and e-signature administrator console.

The "**Your connection isn't private**" warning message is displayed.

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

The security, auditing, and e-signature administrator console is launched with **Not Secure** displayed in the URL bar. The user can log in.

If the self-signed SSL certificate is installed in the Microsoft Edge™ browser, the warning message is not displayed (for the localhost domain only). With a self-signed SSL, the warning message is displayed if the security, auditing, and e-signature administrator console is accessed from a separate computer.



Documentation and support

Customer and technical support

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

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

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

Limited product warranty

Life Technologies Corporation and its affiliates warrant their products as set forth in the Life Technologies' General Terms and Conditions of Sale at www.thermofisher.com/us/en/home/global/terms-and-conditions.html. If you have questions, contact Life Technologies at www.thermofisher.com/support.

