# Diomni™ Design and Analysis (RUO) Software 3

On-premises configuration

Publication Number MAN0030170 Revision A

## Overview of installation

The software is installed on one computer that is the host computer. The software is accessed on a browser of the host computer or any other computer on the same network.

The software must be used with the Security, Auditing, and E-signature (SAE) Administrator Console v3.

The installer contains all of the components that are required. The components can be installed at the same time or the components can be installed separately.

Security, Auditing, and E-signature (SAE) Administrator Console v3 can be installed on the same computer as Diomni™ Design and Analysis (RUO) Software 3 or a separate computer from Diomni™ Design and Analysis (RUO) Software 3.

Files from QuantStudio™ Design and Analysis Software 2 or the desktop configuration of Diomni™ Design and Analysis (RUO) Software 3 must be imported into the on-premises configuration of Diomni™ Design and Analysis (RUO) Software 3. There is no process to transfer files during the installation of the on-premises configuration of Diomni™ Design and Analysis (RUO) Software 3.

### 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.

---

For more information about the different options for installation, see “Installation workflow options (local computer)” on page 4 and “Installation workflow options (separate computer)” on page 5.

# Compatibility

## Compatibility with the security, auditing, and e-signature administrator console

For information about compatibility between the software, the security, auditing, and e-signature administrator console, and the application profile, see *Diomni™ Design and Analysis (RUO) Software 3 (On-Premises) User Guide* (Pub. No. MAN1000091).

## Instruments compatible with plate files from Diomni™ Design and Analysis (RUO) Software 3

Plate files for the QuantStudio™ 7 Pro Real-Time PCR System can be created on the on-premises configuration of Diomni™ Design and Analysis (RUO) Software 3.

Plate files for the following instruments can be created on the desktop configuration or on the Thermo Fisher™ Connect Platform, then opened in the on-premises configuration:

- QuantStudio™ 7 Pro Real-Time PCR System
- QuantStudio™ 6 Pro Real-Time PCR System
- QuantStudio™ 12K Flex Real–Time PCR System (all block formats, except the OpenArray™ Plate format)
- QuantStudio™ 7 Flex Real-Time PCR System
- QuantStudio™ 6 Flex Real-Time PCR System
- QuantStudio™ 5 Real-Time PCR System
- QuantStudio™ 3 Real-Time PCR System
- QuantStudio™ 1 Real-Time PCR System
- QuantStudio™ 1 Plus Real-Time PCR System (available in China)

Pre-run files for the OpenArray™ Plate cannot be created in the Diomni™ Design and Analysis (RUO) Software 3.

## Compatible data files

The software is compatible with data files from the following real-time PCR instruments, if the plate file for the run was created with QuantStudio™ Design and Analysis Software 2 or Diomni™ Design and Analysis (RUO) Software 3:

- QuantStudio™ 7 Pro Real-Time PCR System (including TaqMan™ Array Card format)
- QuantStudio™ 6 Pro Real-Time PCR System
- QuantStudio™ 12K Flex Real–Time PCR System (including TaqMan™ Array Card format, but not including the OpenArray™ Plate format)
- QuantStudio™ 7 Flex Real-Time PCR System (including TaqMan™ Array Card format)
- QuantStudio™ 6 Flex Real-Time PCR System
- QuantStudio™ 5 Real-Time PCR System
- QuantStudio™ 3 Real-Time PCR System
- QuantStudio™ 1 Real-Time PCR System
- QuantStudio™ 1 Plus Real-Time PCR System (available in China)

Data files for the OpenArray™ Plate are in the legacy file format.

## Compatible data files (legacy file format)

If a data file is generated from a plate file that was created with legacy software or legacy instrument software, it must be saved as the updated file format.

For information about saving as the updated file format, see *Diomni™ Design and Analysis (RUO) Software 3 (On-Premises) User Guide* (Pub. No. MAN1000091).

Data files from the following instruments are compatible after they have been saved as the updated file format:

- QuantStudio™ 7 Flex Real-Time PCR System (including the TaqMan™ Array Card format)
- QuantStudio™ 6 Flex Real-Time PCR System
- QuantStudio™ 12K Flex Real–Time PCR System (including the TaqMan™ Array Card and the OpenArray™ Plate format)
- QuantStudio™ 5 Real-Time PCR System
- QuantStudio™ 3 Real-Time PCR System
- QuantStudio™ 1 Real-Time PCR System
- QuantStudio™ 1 Plus Real-Time PCR System (available in China)

# Installation workflow options (local computer)

The following information applies to installing all of the components on the same computer. For information about installing components on a separate computer, see “Installation workflow options (separate computer)” on page 5.

---

**IMPORTANT!** 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 is provided 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.

---

Not installing Security, Auditing, and E-signature (SAE) Administrator Console v3 allows you to connect Diomni™ Design and Analysis (RUO) Software 3 to an instance of the console on a separate computer.

Security, Auditing, and E-signature (SAE) Administrator Console v3 is not installed if the installer detects that it is already installed on the local computer.

The application profile is included in the installer. You can choose to install the application profile during the installation procedure.

The application profile is required to sign in to the software. The software cannot be used if the application profile is not installed.

The installer for Diomni™ Design and Analysis (RUO) Software 3 includes a script that automatically creates a firewall rule for TCP traffic on port `10443`. This rule allows inbound traffic for Diomni™ Design and Analysis (RUO) Software 3. This makes it possible for other computers on the same network to access the software without having to manually configure their own firewalls. The script is works with the default Windows™ firewall. The script might not be compatible with third-party firewalls.

## ① Install all components

### Use the installer to install all components

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

## ② Install Diomni™ Design and Analysis (RUO) Software 3 and the application profile

### Use the installer to install Diomni™ Design and Analysis (RUO) Software 3 and the application profile

The installer detects an instance of Security, Auditing, and E-signature (SAE) Administrator Console v3 on the computer. The console is not installed.

## ③ Install Diomni™ Design and Analysis (RUO) Software 3

### Use the installer to install Diomni™ Design and Analysis (RUO) Software 3

The installer detects instance of Security, Auditing, and E-signature (SAE) Administrator Console v3 on the computer. The console is not installed.

The installer detects that the application profile is available. The application profile is not installed.

# Installation workflow options (separate computer)

The following workflow options apply to using an instance of the security, auditing, and e-signature administrator console and the application profiles on a remote computer.

For information about installing all of the components on the same computer, see “Installation workflow options (local computer)” on page 4.

**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.

The installer does not upgrade the security, audit, and e-signature administrator console on a separate computer or does not install the console on a separate computer.

The installer does not install application profiles on a separate computer. Ensure that the application profile for Diomni™ Design and Analysis (RUO) Software 3 is installed.

The application profile must be installed in the security, auditing, and e-signature administrator console. See “Install the application profile” on page 14.

You must have the application profile installed in order to use Diomni™ Design and Analysis (RUO) Software 3.

The installer for Diomni™ Design and Analysis (RUO) Software 3 includes a script that automatically creates a firewall rule for TCP traffic on port `10443`. This rule allows inbound traffic for Diomni™ Design and Analysis (RUO) Software 3. This makes it possible for other computers on the same network to

access the software without having to manually configure their own firewalls. The script is works with the default Windows™ firewall. The script might not be compatible with third-party firewalls.

**1 Install the software**

**Use the installer to install Diomni™ Design and Analysis (RUO) Software 3**

**In the installer, select that you have an existing security, audit, and e-signature administrator console**

**Test the connection to the existing security, audit, and e-signature administrator console**

**Install the application profile**

The application profile is installed in the security, auditing, and e-signature administrator console.

# Prepare for the installation

## Required computer specifications

The following specifications are required for the computer that the Diomni™ Design and Analysis (RUO) Software 3 is installed on:

- Operating system—Windows™ 10 (64-bit) or Windows™ 11
- Memory—16 GB RAM
- Hard drive—40 GB storage capacity (500 GB storage capacity is recommended)
- System drive is `C:` drive

The required resolution of the monitor is 1920 × 1080 higher. This applies to the computer that is used as a client to access the software.

Open the Ethernet port in order to connect to the software via the network.

Ensure that port `10443` and port `8443` are open. For more information about these ports, see “Ports to open” on page 8. Contact your IT department for assistance in opening the ports.

The software can be used with the following browsers:

- Google Chrome™
- Microsoft Edge™
- Mozilla™ Firefox™

The software cannot be installed on a Mac™ computer. A Mac™ computer can be used as a client to access the software with the compatible browsers.

The desktop configuration of the software can be installed on the same computer as the host computer for the on-premises configuration. This configuration is not recommended. If both instances are installed on the same computer, the files are not accessible between the configurations. The files must be opened in the desktop configuration. The files must be uploaded to the on-premises configuration

## Installation recommendations for security, auditing, and e-signature administrator console

The security, auditing, and e-signature administrator console can be installed on the same computer as the Diomni™ Design and Analysis (RUO) Software 3 (*recommended*) or a different computer.

Ensure that the port `8443` is open. Contact your IT department for assistance in opening the port.

If the security, auditing, and e-signature administrator console is installed on a different computer from the Diomni™ Design and Analysis (RUO) Software 3, the IP address is used to establish a connection. To prevent the loss of the connection, see “Network options” on page 7.

See the Software Release Notes provided with the security, auditing, and e-signature administrator console for the minimum computer system specifications.

A warning screen might be displayed in the browser when the security, auditing, and e-signature administrator console is launched. The warning screen can be bypassed. For more information about the warning screens, see the documentation for the security, auditing, and e-signature administrator console.

The same instance of the security, auditing, and e-signature administrator console can be used for multiple applications.

Only one instance of a console can be installed on one computer. A computer is required for each instance of a console.

If separate instances of the security, auditing, and e-signature administrator console are used, the audit records are separate.

## 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 DCHP 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 software and the connected instruments. It also results in a loss of connection between the software and the security, auditing, and e-signature administrator console.

If the IP address changes after a certain period, it also affects users connecting to the software from separate computers on the network.

## Ports to open

Ports identify specific types of computer network traffic. In order for communication to occur, specific ports need to be open to allow the flow of traffic to and from the software.

Contact your IT department for assistance with opening the appropriate ports. Open the appropriate ports on the computer where the Diomni™ Design and Analysis (RUO) Software 3 is installed.

The installer for Diomni™ Design and Analysis (RUO) Software 3 includes a script that automatically creates a firewall rule for TCP traffic on port `10443`. This rule allows inbound traffic for Diomni™ Design and Analysis (RUO) Software 3. This makes it possible for other computers on the same network to access the software without having to manually configure their own firewalls. The script is works with the default Windows™ firewall. The script might not be compatible with third-party firewalls.

| Port | Type of connection |
|---|---|
| `8443` | Connect to the security, auditing, and e-signature administrator console. |
| `10443` | Connect to real-time PCR instruments and connect to the software from a browser on a separate computer. |

Other ports on the real-time PCR instruments might need to be opened for other connections. See the documentation for the instrument and contact your IT department for assistance in opening the appropriate ports.

Other ports on the real-time PCR instruments might need to be opened for other connections. See the documentation for the instrument and contact your IT department for assistance in opening the appropriate ports.

## Antivirus software

We recommend the use of antivirus software on the computers that are used to run the security, auditing, and e-signature administrator console and the Diomni™ Design and Analysis (RUO) Software 3.

Thermo Fisher Scientific has tested the following antivirus software with the security, auditing, and e-signature administrator console and the Diomni™ Design and Analysis (RUO) Software 3:

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

Antivirus software other than those listed has not been tested and is not supported. The impact of antivirus software other than those listed has not been established.

## Compatible USB drive formats

The system supports USB drives with formats: FAT, FAT32, and NTFS.

**IMPORTANT!** Do not use a USB drive with exFAT formatting. It may cause file corruption.

### USB drives

USB drives that are used with the instrument or the co-located computer must be kept virus-free and malware-free.

A regular scan of the USB drives with an antivirus software is recommended.

## Third-party software

We do not recommend installing any third-party software on the computer that is running the security, auditing, and e-signature administrator console or Diomni™ Design and Analysis (RUO) Software 3. The exception is antivirus software that we recommend (see “Antivirus software” on page 8).

## 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.

# Install the software

## 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.

---

If you have an instance of Security, Auditing, and E-signature (SAE) Administrator Console v3 on a separate computer, see “Install the software” on page 11.

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 15). 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 10).

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 11.
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***

## Install the components separately

### Install the software

Use this workflow if you have an instance of Security, Auditing, and E-signature (SAE) Administrator Console v3 on the same computer or a separate computer.

If you have an existing instance of a security, audit, and e-signature administrator console, ensure that it is compatible with Diomni™ Design and Analysis (RUO) Software 3.

The application profile is not installed if you use an instance of Security, Auditing, and E-signature (SAE) Administrator Console v3 on a separate computer. Ensure that the application profile is installed on the separate computer or the installation of Diomni™ Design and Analysis (RUO) Software 3 cannot proceed.

If you need to install all of the components, see “Install all components” on page 9.

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 **I have an existing SAE Administrator Console** radio button.

   The **Design and Analysis 3 Server Setup** dialog box is not displayed if the installer detects an instance of Security, Auditing, and E-signature (SAE) Administrator Console v3 on the same computer.
6. Click **Next**.

7. 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.

8. Click **Test connection** to confirm that the connection information is correct.

   The installer checks for the version of the console and that the application profile is installed. If the incorrect version of the console is installed on the remote computer or the application profile is not installed, the installation of Diomni™ Design and Analysis (RUO) Software 3 cannot proceed.

   To proceed by installing the security, auditing, and e-signature administrator console on the same computer, select the **Install SAE Administrator Console v3.0 on local machine** checkbox. For detailed instructions, see “Install all components” on page 9.

   Alternatively, upgrade the security, auditing, and e-signature administrator console on the separate computer, then return to this installation procedure. The installer cannot upgrade the security, auditing, and e-signature administrator console on a separate computer.

   If the application profile is not installed, it must be installed in order to proceed with the installation procedure. Install the application profile, then return to this installation procedure.

   If the correct versions of the console and the application profile are installed, the installation of Diomni™ Design and Analysis (RUO) Software 3 can proceed.

9. Select the **Install Design and Analysis Profile v<…>** checkbox, where <…> is the version of the application profile.

   The checkbox is displayed only if the correct version of the console is installed but the application profile is not installed.

   This is applicable only if the console is installed on the same computer. The installer cannot install items on a separate computer.

10. Accept the terms of the *License Agreement*.

11. Click **Next**.

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

    The checkbox is selected by default.

13. Click **Finish**.

Start the service (see “Start the software service” on page 15). 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.

Use the software with the accounts that were set up on the existing instance of the Security, Auditing, and E-signature (SAE) Administrator Console v3.

## 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 13).

Install the application profile (see "Install the application profile" on page 14).

## 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 11). 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 14.

   ---

   **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 11.

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.

## Install the application profile

An application profile contains default settings for an application. An application profile is in a DAT file format.

Before you can use a security, auditing, and e-signature administrator console for Diomni™ Design and Analysis (RUO) Software 3, you must install the application profile that corresponds to the software.

The software cannot be accessed if the corresponding application profile is not installed.

The application profile is installed in Security, Auditing, and E-signature (SAE) Administrator Console v3. The application profile cannot be installed in Diomni™ Design and Analysis (RUO) Software 3.

1. In the main screen of Security, Auditing, and E-signature (SAE) Administrator Console v3, click **Settings ▸ Manage Application Profiles**.
2. Click **Install Application Profile**, click **Choose File**, then navigate to the location that the DAT file is saved.
3. Select the DAT file for the application profile, then click **Verify Data File**.
4. Select the **Confirmation** checkbox, then click **Install**.

   If you are installing an application profile for the first time, **Install new application** is displayed next to the **Confirmation** checkbox.

If a previous version of the application profile was installed, **Upgrade profile** is displayed next to the **Confirmation** checkbox.

5. Close the dialog box after the application profile is successfully installed.

If you are connecting instruments to the same instance of the security, auditing, and e-signature administrator console, you must install the applications profiles for the instruments. There are different requirements for the console for each instrument.

An application profile cannot be uninstalled after it has been installed.

# Configure the server settings

The server settings are available on the host computer only (the computer on which the software is installed). The server settings cannot be accessed from a client computer.

The following items can be managed in the server settings:

- Start the software (see “Start the software service” on page 15)
- Stop the software (see “Stop the software service” on page 16)
- Configure the SAE settings (see “Configure the SAE settings” on page 16)
- Configure the location to save files
  See *Diomni™ Design and Analysis (RUO) Software 3 (On-Premises) User Guide* (Pub. No. MAN1000091).

## Overview of the Windows™ system tray

The server settings for Diomni™ Design and Analysis (RUO) Software 3 are accessed in the Windows™ system tray. The Windows™ system tray contains icons for some of the programs that run in the background.

The Windows™ system tray is accessed by clicking the ^ icon that is located at the bottom-right of the taskbar.

Right-click the Diomni™ Design and Analysis (RUO) Software 3 icon to access the server settings. The server settings are available on the host computer only (the computer on which the software is installed).

The icon is blue when the server is running (  ).

The icon is gray when the server is stopped (  ).

## 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.

## Stop the software service

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

The software cannot be accessed from a different computer via a web browser.

## 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 data backup

The data are located in `C:\ProgramData\Design and Analysis Server`.

Stop the software service before copying the folder, then start the software service (see “Stop the software service” on page 16 and “Start the software service” on page 15).

Copy the folder to a backup location to back up the data.

The folder `C:\ProgramData` is hidden by default. Viewing the hidden folders must be enabled in the Windows™ **File Explorer** program.

# Manage certificates

## Overview of certificates

When any browser accesses a URL that uses the HTTPS protocol, the browser attempts to check the web server certificate with a certificate authority.

Several well-known and trusted authorities exist, from which a website or URL owner can purchase a certificate that uniquely identifies the URL and verifies its authenticity.

By default, Diomni™ Design and Analysis (RUO) Software 3 and Security, Auditing, and E-signature (SAE) Administrator Console v3 use self-signed certificates to enable transport layer security (TLS) encryption for the connection between the browser and the software server. Data are encrypted in transit going to and coming from the software server and this facilitates secure communication.

The default web server certificate that is provided for the server URL is self-signed. It is not purchased from a certificate authority. Because it cannot be verified by a certificate authority, a security or warning screen is displayed. The security or warning screen can be bypassed. It is safe to use the software.

For more information about the warning screens, see “Warning messages” on page 17.

The following options are available:

- Continue to use the software with the warning message.
  It is safe to bypass the warning message and continue to use the software.
- Install a self-signed certificate on the browser.
  A self-signed certificate can be downloaded from the software, then installed in the browser that is being used to access the software.

## Warning messages

### Warning for the Google Chrome™ browser

Launch Diomni™ Design and Analysis (RUO) Software 3.

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

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

Diomni™ Design and Analysis (RUO) Software 3 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).

## Warning for the Microsoft Edge™ browser

Launch Diomni™ Design and Analysis (RUO) Software 3.

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

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

Diomni™ Design and Analysis (RUO) Software 3 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™, the warning message is not displayed (for the localhost domain only).

## Warning for the Mozilla™ Firefox™ browser

Launch Diomni™ Design and Analysis (RUO) Software 3.

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

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

Completing this step in the Mozilla™ Firefox™ browser adds a self-signed certificate to the security exceptions for the browser. Downloading a self-signed certificate, then installing a self-signed certificate is not required.

# Download and install a self-signed certificate

A self-signed certificate prevents the warning message from being displayed in one browser (the localhost domain only). To prevent the warning message from being displayed, the self-signed certificate must installed on the browser of each computer that is used to access the software.

## Download a self-signed certificate (Windows™ operating system or Mac™ operating system)

Download a self-signed certificate.

| Browser | Instructions[1] |
|---|---|
| Google Chrome™ browser | a. Launch the Google Chrome™ browser.<br>b. In the address bar, click **Not secure**.<br>c. In the dialog box, click **Certificate is not valid**.<br>d. In the **Certificate Viewer** dialog box, select the **Details** tab.<br>e. Click **Export**, then save the certificate. |
| Microsoft Edge™ browser | a. Launch the Microsoft Edge™ browser.<br>b. In the address bar, click **Not secure**.<br>c. In the dialog box, click **Your connection to this site isn't secure**.<br>d. In the dialog box, click the certificate icon.<br>e. In the **Certificate Viewer** dialog box, select the **Details** tab.<br>f. Click **Export**, then save the certificate. |
| Mozilla™ Firefox™ browser | • Launch the Mozilla™ Firefox™ browser.<br>• Click **Advanced**.<br>• Click **Accept the Risk and Continue**.<br>**Note:** Completing this step in the Mozilla™ Firefox™ browser adds a self-signed certificate to the security exceptions for the browser. Downloading and installing a self-signed certificate is not required. |

[1] The wording displayed in the browser can differ slightly from the wording that is listed here.

Proceed to “Install the self-signed certificate (Windows™ operating system)” on page 19.

## Install the self-signed certificate (Windows™ operating system)

To prevent the warning message from being displayed, the self-signed certificate must be installed on the browser of each computer that is used to access the software. The warning message is displayed on the browser of any computer where the self-signed certificate is not installed.

Installing a self-signed certificate is not required for Mozilla™ Firefox™. For more information, see “Warning for the Mozilla™ Firefox™ browser” on page 18.

Download a self-signed certificate.

| Browser | Instructions[1] |
|---|---|
| Google Chrome™ browser | a. Launch the Google Chrome™ browser.<br>b. Click ⋮ **(Customize and control) ▸ Settings ▸ Privacy and security ▸ Security ▸ Manage certificates**.<br>c. In the **Certificates** dialog box, select the **Trusted Root Certification Authorities** tab.<br>d. Click **Import**.<br>e. Follow the instructions in the wizard to import the certificate. |
| Microsoft Edge™ browser | a. Launch the Microsoft Edge™ browser.<br>b. Click ··· **(Settings and more) ▸ Settings ▸ Privacy, search, and services ▸ Manage certificates**.<br>c. In the **Certificates** dialog box, select the **Trusted Root Certification Authorities** tab.<br>d. Click **Import**.<br>e. Follow the instructions in the wizard to import the certificate. |

[1] The wording displayed in the browser can differ slightly from the wording that is listed here.

## Install the self-signed certificate (Mac™ operating system)

To prevent the warning message from being displayed, the self-signed certificate must be installed on the browser of each computer that is used to access the software. The warning message is displayed on the browser of any computer where the self-signed certificate is not installed.

Installing a self-signed certificate is not required for Mozilla™ Firefox™. For more information, see “Warning for the Mozilla™ Firefox™ browser” on page 18.

Download a self-signed certificate.

| Browser | Instructions[1] |
|---|---|
| Google Chrome™ browser | a. Navigate to the location where the downloaded self-signed certificate is stored, then keep the folder open.<br>b. Launch the Google Chrome™ browser.<br>c. Click ⋮ **(Customize and control) ▸ Settings ▸ Privacy and security ▸ Security ▸ Manage certificates ▸ Manage imported certificates from MacOS**.<br>d. In the **Keychain Access** dialog box, in the left pane, click **System**.<br>e. At the top of the dialog box, select the **Certificates** tab.<br>f. Copy the downloaded self-signed certificate, then paste the certificate into the **Keychain Access** dialog box.<br>A dialog box is displayed to enter your password.<br>g. Enter your password.<br>The password is for the system. It is not the password to sign in to the software.<br>h. Click **Modify Keychain**.<br>The certificate is displayed with the name `localhost`.<br>i. Double-click the certificate.<br>j. In the dialog box, expand the **Trust** pane.<br>k. In the **When using this certificate** dropdown list, click **Always Trust**. |
| Microsoft Edge™ browser | a. Navigate to the location where the downloaded self-signed certificate is stored, then keep the folder open.<br>b. Launch the Microsoft Edge™ browser.<br>c. Click ··· **(Settings and more) ▸ Settings ▸ Privacy, search, and services ▸ Manage certificates**.<br>d. In the **Keychain Access** dialog box, in the left pane, click **System**.<br>e. At the top of the dialog box, select the **Certificates** tab.<br>f. Copy the downloaded self-signed certificate, then paste the certificate into the **Keychain Access** dialog box.<br>A dialog box is displayed to enter your password.<br>g. Enter your password.<br>The password is for the system. It is not the password to sign in to the software.<br>h. Click **Modify Keychain**.<br>The certificate is displayed with the name `localhost`.<br>i. Double-click the certificate.<br>j. In the dialog box, expand the **Trust** pane.<br>k. In the **When using this certificate** dropdown list, click **Always Trust**. |

[1] The wording displayed in the browser can differ slightly from the wording that is listed here.

# 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**.

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.

**Revision history: MAN0030170 A (English)**

| Revision | Date | Description |
|---|---|---|
| A | 14 April 2025 | New document for Diomni™ Design and Analysis (RUO) Software v3.0 (on-premises configuration). |