



thermo scientific

Thermo Scientific

SciVault 2

User Guide

M023 SciVault 2 UG

Revision A February 2025

ThermoFisher
SCIENTIFIC

© 2024 Thermo Fisher Scientific Inc. All rights reserved.

Wi-Fi is either a trademark or a registered trademark of Wi-Fi Alliance in the United States and/or other countries. Bluetooth is either a trademark or a registered trademark of Bluetooth Special Interest Group. Windows is either a trademark or a registered trademark of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of Thermo Fisher Scientific Inc. and its subsidiaries.

For U.S. Technical Support, please contact:

Thermo Fisher Scientific
3411 Silverside Road
Tatnall Building, Suite 100
Wilmington, DE 19810 U.S.A.

Telephone: 302 479 7707
Toll Free: 1 877 724 7690 (U.S. & Canada only)
E-mail: nanodrop@thermofisher.com

For International Support, please contact:

[http://www.thermofisher.com/
NanoDropSupport](http://www.thermofisher.com/NanoDropSupport)

Contact your local distributor. For contact information go to:

[http://www.thermofisher.com/
NanoDropDistributors](http://www.thermofisher.com/NanoDropDistributors)

Thermo Fisher Scientific Inc. provides this document to its customers with a product purchase to use in the product operation. This document is copyright protected and any reproduction of the whole or any part of this document is strictly prohibited, except with the written authorization of Thermo Fisher Scientific Inc.

The contents of this document are subject to change without notice. All technical information in this document is for reference purposes only. System configurations and specifications in this document supersede all previous information received by the purchaser.

Thermo Fisher Scientific Inc. makes no representations that this document is complete, accurate or error-free and assumes no responsibility and will not be liable for any errors, omissions, damage or loss that might result from any use of this document, even if the information in the document is followed properly.

This document is not part of any sales contract between Thermo Fisher Scientific Inc. and a purchaser. This document shall in no way govern or modify any Terms and Conditions of Sale, which Terms and Conditions of Sale shall govern all conflicting information between the two documents.

For Research Use Only. This instrument or accessory is not a medical device and is not intended to be used for the prevention, diagnosis, treatment or cure of disease.



WARNING Avoid an explosion or fire hazard. This instrument or accessory is not designed for use in an explosive atmosphere.

Contents

Chapter 1	Getting Started with SciVault 2 Software	5
	SciVault 2 Configuration Options	6
	Installation Overview	9
	Installation Roles and Responsibilities	16
	Default Authorization Roles	17
	Cybersecurity Recommended Assignments	18
	SciVault 2 installed on a PC/Server	18
	SciVault 2 activated on the local instrument	19
	Important Terms	19
	Supporting Documents	20
Chapter 2	Introduction	23
	Activating, Installing, or Updating Software	23
	Activate SciVault 2 Software	24
	Install SciVault 2 Software	24
	Update Your Instrument Applications	24
	Changing the SciVault 2 Server Location	25
	View Profile Settings	26
	Logout of User Profile	26
	View Profile	26
	Resetting the SuperAdmin Password	27
Chapter 3	SciVault 2 Overview	29
	The Role of the IT Administrator	29
	The Role of the Security Administrator	30
	Windows Local User Groups and Rights	31
	Windows User Profiles	32
	Other Security Features	32
	Audit Logging	32
Chapter 4	User Management Feature	33
	About the Display	33
	Role Management	34
	User Management	35

Chapter 5	User Privileges Feature	39
	About the Display	39
	Controlling Access to the User Privileges Feature	40
	Specify Access Rights for Protected Features	41
	Add an Application	42
	Remove an Application	43
	Export Application Settings	44
	Setting Security Features for Monitored Applications	44
	Control Access to Application Features	45
	Set System Policies for SciVault 2 Software Applications	46
	Set System Policies for a Policy Group	47
	Create a Policy Group, Delete a Group or Edit a Group's Name	48
	LIMS API Integration	51
	Assign Signature Meanings to SciVault 2 Software Applications	52
	About Digital Signatures	53
	View or Change Signature Meaning Assignments	53
	Default Signature Meanings for All Applications	54
	Edit Signature Meanings	56
	Saving Your Privileges Settings	57
Chapter 6	Audit Logs Feature	59
	Audit Logging	59
	Install the Audit Logs	61
	Set Up the Audit Logs	61
	Open the Audit Logs	62
	Work with the Audit Logs	62
	Event Information	63
	Create, Sign and Print Reports	65
	Set User Preferences	67
Chapter 7	System Settings	69
	Connecting Instrument To Your Domain	69
	Database Configuration	71
	Database Network Export Setup	73
	Network Paths	73
	General System Settings	75
	Set Language	75
Chapter 8	Help	77
	About	77
	Documentation	78

Getting Started with SciVault 2 Software

The Thermo Scientific™ SciVault™ 2 software allows you to manage User Accounts, User Privileges, and view Audit Logs for your Thermo Scientific™ instrument. The SciVault 2 software works in conjunction with your network's or computer's operating system and your Thermo Scientific instrument applications to provide a secure environment that will help you support the requirements of 21 CFR Part 11. The SciVault 2 software uses a proprietary event viewer to log application events and changes to acquired spectral data and associated files. When an instrument application configured with the SciVault 2 software is running, it is in constant communication with the SciVault 2 software in order to enforce the defined security policies.

IMPORTANT

- You must have an IT Administrator present during the Thermo Scientific software installation!
- If you plan on installing SciVault 2 on a computer, be prepared to provide an administrative login and password for each instrument computer.
- Instrument computer 52311 port is available for LAN access to perform the installation.

Contents

- [SciVault 2 Configuration Options](#)
- [Installation Overview](#)
- [Installation Roles and Responsibilities](#)
- [Default Authorization Roles](#)
- [Cybersecurity Recommended Assignments](#)
- [Important Terms](#)
- [Supporting Documents](#)

SciVault 2 Configuration Options

The following is an overview of the steps required to install and configure the SciVault 2 software for one or more Thermo Scientific instruments installed at the customer site.

The term SciVault 2 Software Server is used to indicate the computer or Thermo Scientific instrument used for user management, access control, policy management, and audit logs.

Local Server with Single Computer

Install SciVault 2 software and instrument software on one computer which will act as the SciVault 2 Software Server. The computer should be connected directly to the instrument via a USB or Ethernet cable. With this configuration, each Thermo Scientific instrument will have its own policy settings and audit log. In this configuration, the user accounts managed within the User Management application are pulled from the available local and/or domain Windows accounts.

Note Local Server configurations through PC control require an administrative login and password for each instrument computer. With these configurations:

- SciVault 2 software settings must be applied individually for each Thermo Scientific instrument.
- Each instrument will have a separate audit log.

Figure 1. Example of the SciVault 2 local server with single computer configuration



Stand-alone configurations are intended for small laboratories with no network facilities. If you run User Privileges on a stand-alone system, pay special attention to the following points:

- Each stand-alone computer must have a unique name
- Each user must have a unique Windows local or domain user account

- Users other than an IT administrator or Security Administrator must not have access to the local administrator account
- Users must not be able to change the date and time on the computer

Local Server with Single Instrument

Activate SciVault 2 software on the local instrument which will act as the SciVault 2 Software Server. With this configuration, each Thermo Scientific instrument will have it's own policy settings and audit log. In this configuration, user accounts can be created and managed within the User Management application or Windows domain accounts can be pulled after connection to an LDAP server.

Note With this configuration:

- SciVault 2 software settings must be applied individually for each Thermo Scientific instrument.
- Each instrument will have a separate audit log.

Figure 2. Example of the SciVault 2 local server with single instrument configuration



Instrument Control + SciVault 2

Stand-alone configurations are intended for small laboratories with no network facilities. If you run User Privileges on a stand-alone system, pay special attention to the following points:

- For each stand-alone instrument, a password will be required to setup the SuperAdmin user account
- Each user must either have a unique user account created within the User Management feature or a unique Windows domain user account (LDAP settings must be configured)
- Users other than an IT administrator or Security Administrator must not have access to the local Windows administrator account or the SuperAdmin user account
- Users must not be able to change the date and time on the local system clock

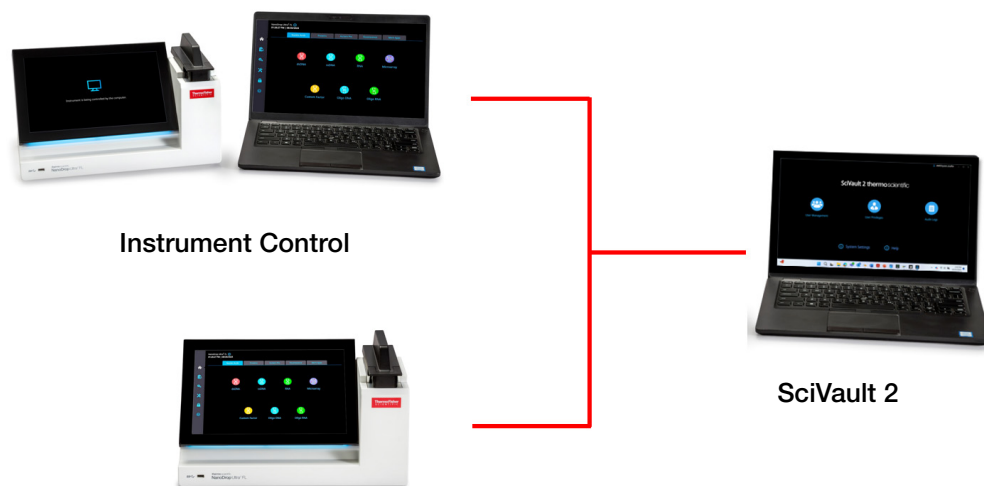
Remote Server

Install SciVault 2 software on a computer or server to act as the SciVault 2 Software Server. Then from either a computer running the instrument control software or directly from an instrument itself, establish connection to the SciVault 2 Software Server. With this configuration, the SciVault 2 software is installed on a networked computer/server which is then used to remotely manage networked instruments and computers on the same domain in multiple areas.

IMPORTANT

- Thermo Scientific instruments intended for central SciVault 2 software control must be connected to the same network domain and the SciVault 2 software should be installed on that domain. With these configurations, security settings are applied globally for all connected instruments and all instruments send events to the same Thermo Scientific audit log.
- Remote installations require an administrative login and password for the network domain.
- A network server running the Windows Server operating system (version 2012, rev2) is preferred over one running the Professional version of Windows operating system software.

Figure 3. Example of the SciVault 2 remote server configuration



Note Instruments that include touchscreens capable of local control cannot act as the SciVault 2 Software Server in a remote server configuration.

Installation Overview

The following is an overview of the steps required to install and configure the SciVault 2 software for one or more Thermo Scientific instruments installed at the customer site.

For the Local Server with Single Instrument Configuration

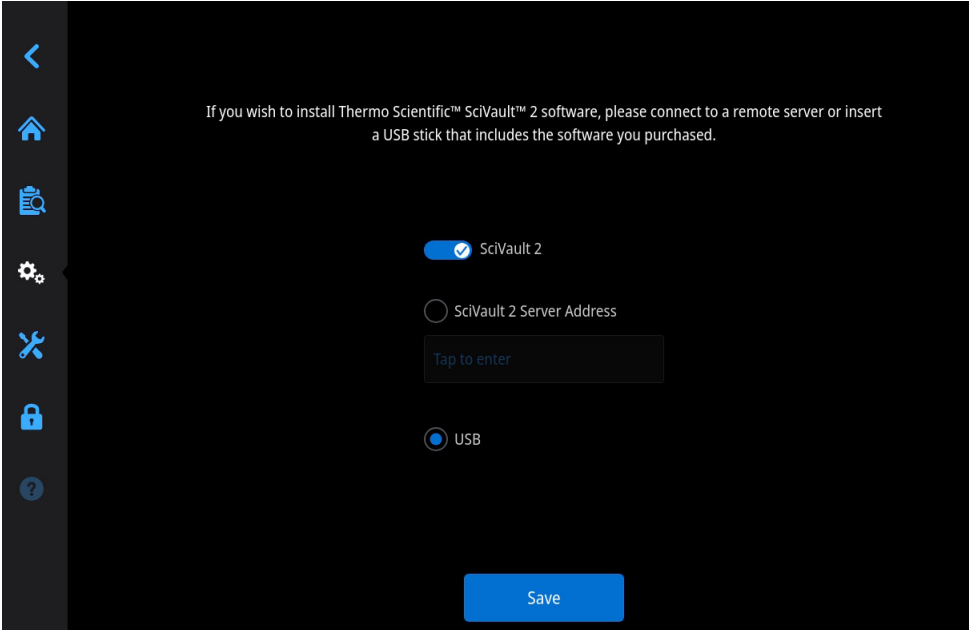
When using the "local server" configuration without a connected computer, the first step is to activate the SciVault 2 software components on the Thermo Scientific instrument. Follow the steps below.

Table 1. SciVault 2 software activation overview for the Thermo Scientific instrument without a connected PC.


Step	Person	Task
1	IT Administrator	Ensure computer LDAP port is available if Windows domain users will be used. LDAP settings within the SciVault 2 System Settings must also be configured for this purpose.

1 Getting Started with SciVault 2 Software

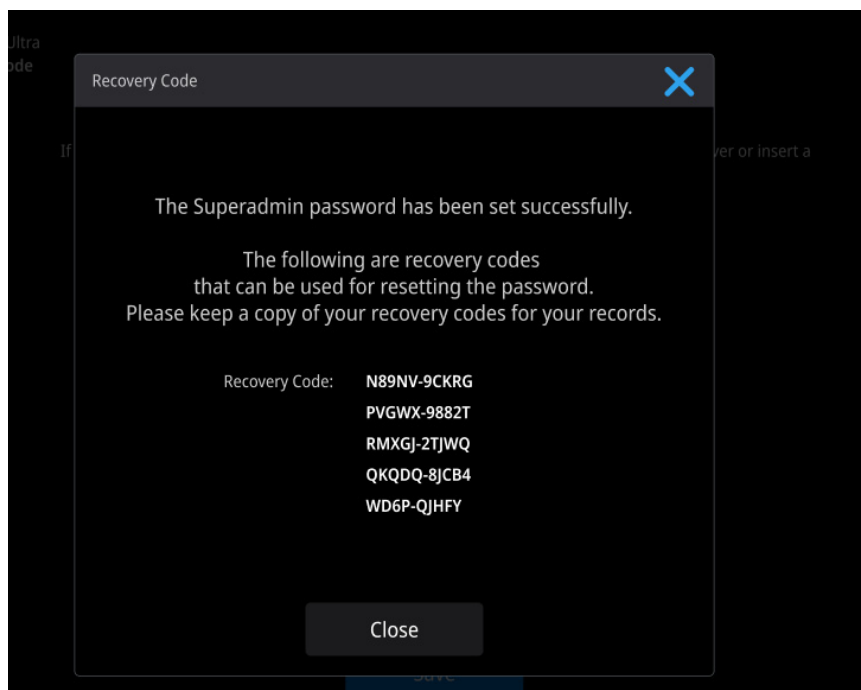
Installation Overview

Step	Person	Task
2	TFS Service Representative or Instrument Owner	

Complete the SciVault 2 software installation on the Thermo Scientific instrument:

- Insert the USB drive containing the SciVault 2 activation key which comes with the purchase of the SciVault 2 software.
- From the home screen, tap the settings icon  from the left panel.
- Tap **SciVault 2 Mode** to open the activation screen.
- Tap the toggle next to SciVault 2 to show more options, the toggle should be blue with a checkmark after enabled.
- Tap the bubble next to USB and select **Save**.
- Set the password for the SuperAdmin account in each field by tapping on each to present a keyboard. Tap **Done** to close the keyboard. Please store this password in a secure location.
- Tap **Save**.

Step	Person	Task
------	--------	------



- h. The Recovery Code window will display, it is **extremely important** that you record the Recovery Code in a safe location. This code will be the only way to reset the SuperAdmin password. Tap **Close**. The instrument will now restart.

3	TFS Service Representative or Instrument Owner	<p>Complete the configuration of local SciVault 2 Software Server</p> <ul style="list-style-type: none"> • Launch the Thermo Scientific instrument, enable SciVault 2 software features by logging in.
---	--	---

For the Local Server with Single Computer Configuration

When using the "local server" configuration with a connected computer, the first step is to install SciVault 2 software components on the computer connected to the Thermo Scientific instrument. Follow the steps below:

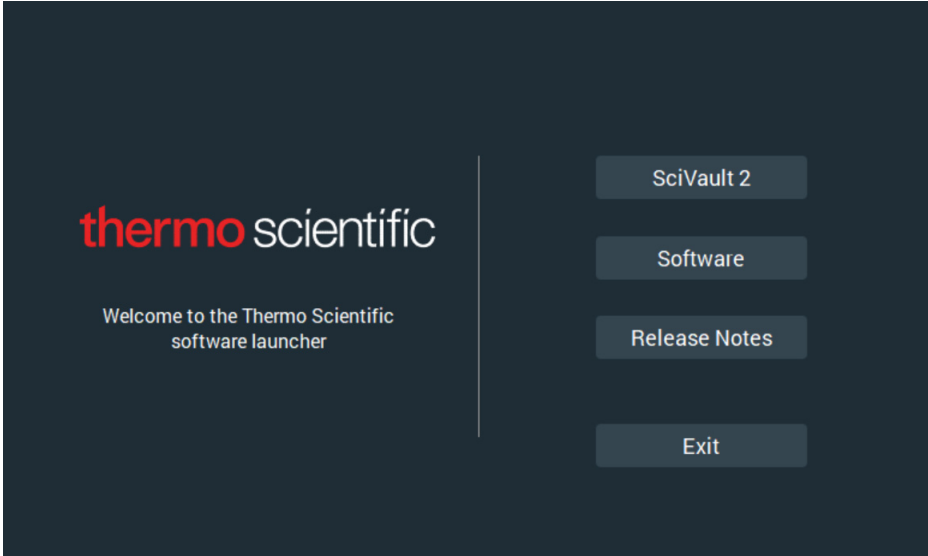
Note You must be an administrator with password login credentials on the computer attached to this Thermo Scientific instrument in order to install the SciVault 2 software


Table 2. SciVault 2 software installation and activation overview for the Thermo Scientific instrument with a connected PC.

Step	Person	Task
1	IT Administrator	Ensure computer 52311 port is available for LAN access to perform the installations.

1 Getting Started with SciVault 2 Software

Installation Overview

Step	Person	Task
2	TFS Service Representative or Instrument Operator	
		<p>Complete the SciVault 2 software installation on the single computer attached to the Thermo Scientific instrument:</p> <ol style="list-style-type: none">Insert the installation media and right-click run as administrator the Start.exe application to start the SciVault 2 software and instrument control software installation launcher screenClick SciVault 2 software on Thermo Scientific software launcherAccept the terms and click Next to install the SciVault 2 softwareFollow the instructions in the wizard and click NextClick Next to start the installationChoose OK to complete the SciVault 2 software installation
3	TFS Service Representative or Instrument Operator	<p>Complete the Thermo Scientific instrument control software installation on the single computer attached to the Thermo Scientific instrument:</p> <ol style="list-style-type: none">Click Software on Thermo Scientific software launcherAccept the terms and click Next to install the softwareFollow the instructions in the wizard and click NextClick Next to start the installationChoose OK to complete the Thermo Scientific installation

Step	Person	Task
<p>Note In the event that the Thermo Scientific instrument is disconnected from the computer, the instrument will no longer be 21 CFR Part 11 compliant. To mitigate this situation, you may follow the steps outlined in Table 1 step 2 of the For the Local Server with Single Instrument Configuration section. This will allow you to control the instrument from the connected PC while ensuring the local touchscreen is locked regardless of connection.</p>		
4	TFS Service Representative or Instrument Operator	<p>Complete the configuration of local SciVault 2 software server</p> <ol style="list-style-type: none"> a. Launch the Thermo Scientific software, enable SciVault 2 software features by logging in. b. In the event that you attempt to open the Thermo Scientific software on the connected computer, and it does not prompt you for a password follow the steps below: <ol style="list-style-type: none"> i. Open SciVault 2. ii. Select Help at the bottom of the home screen. iii. Select Copy next to the SciVault 2 Server Address. iv. Open the Thermo Scientific Instrument Software. v. From the home screen, select the settings icon  from the left panel. vi. Select SciVault 2 Mode. vii. Toggle the SciVault 2 slider on and paste the SciVault 2 Server Address into the field. viii. Select Save.

For the Remote Server

When using the "remote server" configuration, the first step is to install the SciVault 2 software components on the computer that will serve as the SciVault 2 Software Server. Follow the steps below.

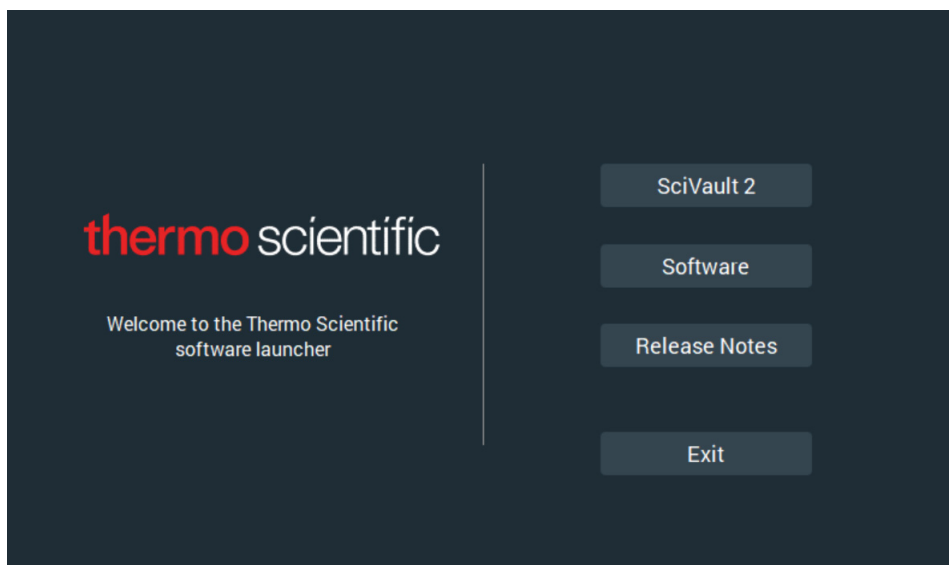
Note You must be an administrator with password login credentials on the computer acting as the SciVault 2 Software Server in order to install the SciVault 2 software.

1 Getting Started with SciVault 2 Software Installation Overview

Table 3. Overview of SciVault 2 software installation on the computer or server to be used as the SciVault 2 Software Server.



Step	Person	Task
1	IT Administrator	Ensure computer 52311 port is available for LAN access to any computer that will be connected to an instrument. Ensure computer LDAP port is available.

2 TFS Service Representative



Complete the SciVault 2 software installation on the computer or server managing the SciVault 2 software settings:

- Insert the installation media and right-click run as administrator the **Start.exe** application to start the SciVault 2 software and instrument control software installation launcher screen.
- Click **SciVault 2** on Thermo Scientific software launcher.
- Accept the terms and click **Next** to install the SciVault 2 software.
- Follow the instructions in the wizard and click **Next**.
- Click **Next** to start the installation.
- Choose **OK** to complete the SciVault 2 software installation.

Step	Person	Task
3	TFS Service Representative	<p>Complete the Thermo Scientific instrument control software installation on a computer attached to a Thermo Scientific instrument:</p> <ol style="list-style-type: none"> Insert the installation media and right-click run as administrator the Start.exe application to start the software installation launcher screen. Click Software on the Thermo Scientific software launcher. Accept the terms and click Next to install the software. Follow the instructions in the wizard and click Next. Click Next to start the installation. Choose OK to complete the Thermo Scientific installation.
4	TFS Service Representative	<p>Establish connection between the SciVault 2 Software Server and a networked computer attached to a Thermo Scientific instrument:</p> <ol style="list-style-type: none"> Launch and login to the SciVault 2 software, navigate to the Help > About tab and copy the SciVault 2 software server address. Launch the Thermo Scientific software, from the home screen, select the settings icon . Select SciVault 2 Mode. Tap the toggle next to SciVault 2, the toggle should be blue with a checkmark after enabled. Type in the SciVault 2 Server Address found within the SciVault 2 software Help screen and select Save. <p>Establish connection between the SciVault 2 Software Server and a networked Thermo Scientific instrument:</p> <ol style="list-style-type: none"> Insert the USB drive containing the SciVault 2 activation key which comes with the purchase of the SciVault 2 software. From the instrument home screen, tap the settings icon  from the left panel. Tap SciVault 2 Mode to open the activation screen. Tap the toggle next to SciVault 2 to show more options, the toggle should be blue with a checkmark after enabled. Tap the bubble next to SciVault 2 Server Address. Tap the box below SciVault 2 Server Address, a keyboard will be displayed. Type in the SciVault 2 Server Address found within the SciVault 2 software Help screen and tap Done. Tap Save. The instrument will now restart.

For all installation configurations (local server and remote server), perform these steps to complete the installation:

- TFS service representative: If SciVault 2 software was installed on a computer, perform installation qualification (IQ) to verify the installation and configuration of the system.
- Security administrator (or IT administrator): In the **User Management** feature, use the **Roles** tab to determine the authorization roles that will be available for users. In the **Users** tab, assign local (Windows or Instrument) or domain (Windows) users to one of the available roles. In the **User Privileges** feature, review the access rights, policy permissions and signature meanings for the SciVault 2 software authorization roles and the Thermo Scientific instrument applications that will be controlled by the **User Privileges** feature. Reset access rights, policy permissions and signature meanings as needed to ensure compliance for your facility.

Note

- Each computer that will control this SciVault 2 software installation must reside on the same (or a trusted) network domain as the "main" Thermo Scientific instrument computer.
- You must be an administrator with password logon credentials on the computer attached to each Thermo Scientific instrument in order to install the SciVault 2 software.

Installation Roles and Responsibilities

The SciVault 2 software installation requires a coordinated effort between the person performing the installation (normally a Thermo Scientific service representative) and the administrators at the installation site (one or more for the instrument and one from the company's IT department). In this documentation set, we use the following terms to designate these roles.

Table 4. Roles and responsibilities to perform SciVault 2 software installation

Role	Responsibilities
System Owner	A user (most likely a scientist or lab manager) is responsible for the use and management of the Thermo Scientific instrument and its associated computer (if used) at the customer site.

Table 4. Roles and responsibilities to perform SciVault 2 software installation

Role	Responsibilities
Security Administrators	One or more individual users (or a group of users) are responsible for administration of the roles and users available within the User Management feature along with administration of system policies and access control of the applications managed by the User Privileges feature. These users should have full control access to the User Management and User Privileges features. See “The Role of the Security Administrator” on page 30 for details.
Instrument Operators	One or more individual users (or a group of users) are responsible for running Thermo Scientific instruments at the customer site. These users typically have no access to the User Privileges feature and limited access to specific features in the software applications used to run the instrument.
TFS Service Representative	A certified service representative from Thermo Fisher Scientific is responsible for installing and servicing the Thermo Scientific instruments and for installing software and configuring the instruments.
IT Administrator	<p>Information Technology administrator at the customer site. This person must be available during the SciVault 2 software installation.</p> <p>IT administrator tasks:</p> <ul style="list-style-type: none"> • Create any required user accounts and authorization groups for the SciVault 2 software. • Configuration and setup of the LDAP settings if domain Windows accounts will be used. • Install any required Remote Server Installation. <p>See “The Role of the IT Administrator” on page 29 for details.</p>

Default Authorization Roles

The SciVault 2 software automatically uses three default authorization groups with recommended compliance assignments, such as to allow or deny access to the User Privileges feature, or to require the use of electronic signatures and/or comments. The default group names represent the three main types of users of the SciVault 2 software (that is, administrators of the User Privileges feature

(Administrators), instrument operators with elevated privileges (Power User), and instrument operators with basic privileges (Users)). Accounts for individual users or Windows domain groups (SciVault 2 through PC only) can then be assigned to one of these roles or a new role can be created and assigned.

Table 5. Default user roles for SciVault 2 software

Authorization Group	Description
Administrator	Role that has full control access to all the options of the User Privileges feature, including system configuration. These users will be responsible for administration of security settings for all applications managed by User Privileges feature.
Power User	Role that has no access to the User Privileges feature and elevated access to the applications that are controlled by the User Privileges feature.
User	Role that has no access to the User Privileges feature, and limited access to the applications that are controlled by the User Privileges feature.

Note

- The default groups are intended to save your time in setting system policies for each instrument application. The access rights and policy settings for the default groups are based on typical use. You can easily change the default rights and settings to customize User Privileges for your needs.
- You can utilize the default roles or replace them with additional roles that are more meaningful to your organization. For more information, see [“To add a Role to the User Management Feature”](#) on [page 34](#) in this document.

Cybersecurity Recommended Assignments

To comply with cybersecurity best practices, it is strongly advised to adhere to the following recommendations.

SciVault 2 installed on a PC/Server

Windows Group Configuration

- By default, Windows has two built-in user groups, administrators and users.

- ONLY adding IT/Security Administrators and System Owners to the Administrators Windows group on the PC.
- All other users should be added to the Users Windows group. This means that these users should ONLY log in to Windows as standard users.
- Alternative user management tools with strict access control at the Windows system level, are also acceptable.

Instrument Role Configuration

- ONLY the IT/Security Administrators and System Owners be assigned to the Administrator and Power Users role.
- All other users should ONLY be assigned the User role.
- For small lab environments, ONLY using the Administrator and User roles should be sufficient.

SciVault 2 activated on the local instrument

Instrument Role Configuration

- ONLY the IT/Security Administrators and System Owners be assigned to the Administrator and Power Users role.
- All other users should ONLY be assigned the User role.
- For small lab environments, ONLY using the Administrator and User roles should be sufficient.

Important Terms

These terms are used in the SciVault 2 software installation wizard and throughout the documentation set.

Table 6. Terms used in the SciVault 2 software installation wizard and documentation set

Term	Meaning
instrument	Thermo Scientific instrument and any accessories it came with.
instrument applications	Thermo Scientific software applications are used to run the Thermo Scientific instrument and accessories and for data analysis.
PC control	The Thermo Scientific instrument application is managed on a PC that is connected to the instrument.

Table 6. Terms used in the SciVault 2 software installation wizard and documentation set, continued

Term	Meaning
Local control	The Thermo Scientific instrument application is managed locally on the instrument through a touchscreen.
Security settings	Access control, system policy and signature meaning requirements for each SciVault 2 software application covering such things as access to menu commands and requiring electronic signatures. Settings for all SciVault 2 software applications can be configured in the Thermo Scientific User Privileges feature and are described in the SciVault 2 software setup guide for each application.
SciVault 2 installation wizard	Thermo Scientific application walks the operator (typically a Thermo Scientific service representative) through the SciVault 2 software installation, starting and ending on the computer attached to the Thermo Scientific instrument.
Installation Qualification (IQ)	Verifies the proper installation of the SciVault 2 software on a PC by running the Thermo Software IQ.
Operational Qualification (OQ)	Verifies that the SciVault 2 software has been installed correctly and will operate smoothly with the Thermo Scientific instrument software. Can help confirm that User Privileges are working correctly and that logged events are being shown in the Audit Log feature.
Thermo Software IQ	<p>Thermo Scientific software application can be used to verify that the correct software files were installed on the computer connected to the Thermo Scientific instrument and that the files have not been changed, deleted or overwritten since they were installed.</p> <p>The Thermo Software IQ program is installed with all Thermo Scientific instrument applications run on a PC.</p>

Supporting Documents

The following documents are included with this software installation package. PDF versions are provided in the documentation set, which is on separate media from the software.

Table 7. SciVault software documentation set of main components

Document Name	Description
SciVault 2 Software User Guide	Describes the components and underlying concepts of the SciVault 2 and explains how to use the User Management, User Privileges, and Audit Logs features application.
SciVault 2 OQ	Document containing instructions on how to perform the OQ of the SciVault 2 software. Results of the OQ are to be recorded on this document along with the operator signature.

This page is intentionally blank.

Introduction

This document explains how to use Thermo Scientific™ SciVault 2 software, which can be used to run one or more Thermo Scientific instrument(s) with change event logging and secure data storage. The SciVault 2 software can function either independently or in conjunction with your network's or computer's operating system and your Thermo Scientific instrument applications to provide a secure environment that will help you support the requirements of 21 CFR Part 11.

The SciVault 2 software uses an Application Programming Interface (API) to provide an audit trail of activities with your Thermo Scientific instruments. The API records User Management and instrument application operations, or "events" in a secure database.

When an instrument application configured with data security is running, it is in constant communication with the SciVault 2 software in order to enforce the defined security settings. In addition, spectral data and associated files can be saved only to a secure location that prevents users from deleting, renaming or modifying data while using a non-Thermo Scientific application such as Microsoft® Windows® Explorer.

Manual Conventions

NOTICE Follow instructions with this label to avoid damaging the system hardware or losing data.

Note Contains helpful supplementary information.

Tip Provides helpful information that can make a task easier.

Activating, Installing, or Updating Software

The Thermo Scientific SciVault 2 software comes preinstalled on compatible instruments that can be controlled by a touchscreen. Although installed, the software will still need to be activated with an activation key before it is functional on the instrument. When installing the software on a computer, the software installation package will include both the instrument application as well as the SciVault 2

2 Introduction

Activate SciVault 2 Software

software and when installed in the correct order SciVault 2 will activate automatically. After the initial SciVault 2 software installation, you can update your instrument software and update or move other SciVault 2 software components without losing your security configuration settings. See below for details.

Activate SciVault 2 Software

Instructions to activate the SciVault 2 software can be found in [Getting Started with SciVault 2 Software](#). A SuperAdmin user account will be created after activation has been completed which will automatically be added to the Administrator role.

Install SciVault 2 Software

Instructions on installing the SciVault 2 software can be found in [Getting Started with SciVault 2 Software](#). The windows user that completes the installation of the software will automatically be added to the Administrator role.

Note You must be an administrator on the computer to install or update the Security Suite software.

After you have installed the SciVault 2 software, you can use the Thermo Software IQ software to perform installation qualification (IQ) if desired. To start the software, launch the Thermo Software IQ program from the list of Thermo Scientific applications installed on your computer.

Update Your Instrument Applications

When SciVault 2 is installed on a PC

If you are installing a new version of SciVault 2 on a PC, insert the installation media on the instrument or instrument computer and follow the on-screen instructions to perform the installation. All the previous User Privileges configuration settings (for example, Access Control, System Policies and Signature Meanings) for the new versions of instrument software will be the same as they were in the previous version.

If you are installing a new version of instrument software that has new features controlled by the User Privileges feature, use **Add Application** on the User Privileges screen to add the new .XML files after you install the new version. If you are using a translated version of User Privileges feature, add the file that is appropriate for your language. The .XML files are in the root of the instrument software installation media. See [“Add an Application”](#) on [page 42](#) for more information.

Access control items for new features will be set to their default settings for the default roles (Administrators, Power Users, and Users) in the User Privileges feature.

When SciVault 2 is installed on the Thermo Scientific instrument

SciVault 2 will update automatically any time the local control instrument software is updated. Please see your instrument model's specific user guide for more details. All of the User Privileges configuration settings (for example, Access Control, System Policies and Signature Meanings) for the new versions of instrument software will be the same as they were in the previous version.

If you are installing a new version of instrument software that has new features controlled by the User Privileges feature, use **Add Application** on the User Privileges screen to add the new .XML files after you install the new version. If you are using a translated version of User Privileges feature, add the file that is appropriate for your language. The .XML files are in the root of the instrument software installation media. See [“Add an Application”](#) on [page 42](#) for more information.

Access control items for new features will be set to their default settings for the default roles (Administrators, Power Users, and Users) in User Privileges feature.

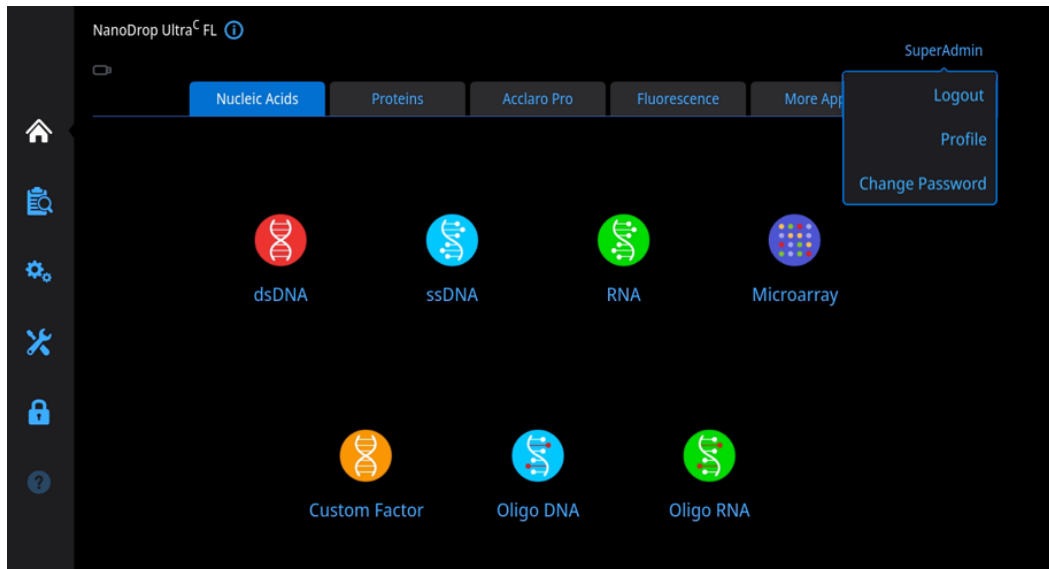
Changing the SciVault 2 Server Location

If you need to reinstall the SciVault 2 software on a different network computer or server that has a different computer or server name, use the SciVault 2 software installation media and follow the steps 1-2 outlined in the [Installation Overview](#) section under [Table 3](#). See [Chapter 5, “User Privileges Feature”](#) for more information on exporting User Privilege settings and adding them back into the SciVault 2 software.

After you have verified that the required Remote Server Installation have been installed in the new location(s), open the SciVault 2 software and copy the new SciVault 2 software Server Address from Help/About screen. Then run the application software on each instrument or instrument computer and update (paste) the new SciVault 2 software Server Address in the **Settings**. After being updated and clicking **Save** button to re-open the application software, it will update to the new SciVault 2 software server.

View Profile Settings

The SciVault 2 user profile settings can be view from most screens by selecting the Username in the top right of the screen.

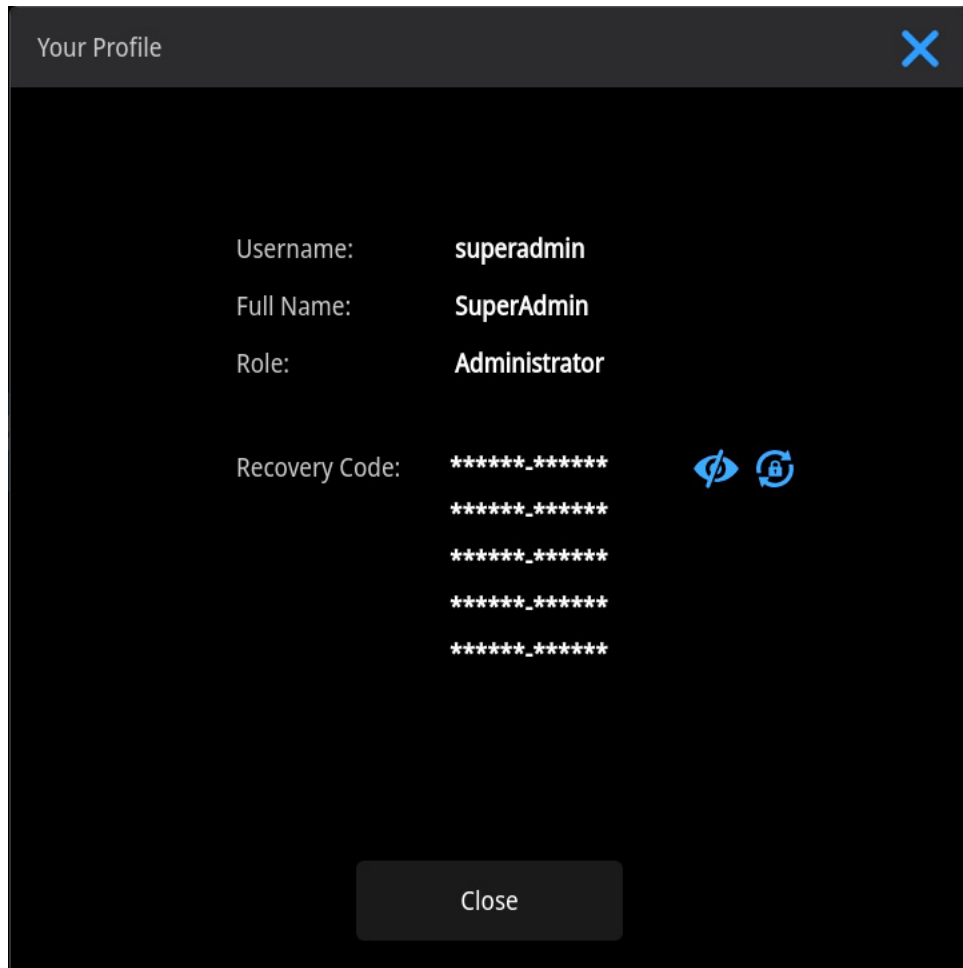


Logout of User Profile

Select **Logout** to logout of the current user profile. The initial login screen will then be displayed.

View Profile

To view profile information pertaining to the current user, select **Profile**. Information displayed will include Username, Full Name, Role, and Recovery Code (Applicable to SuperAdmin account).



To Show the Recovery Code

Select , then enter the SuperAdmin password and select **OK**.

To Reset the Recovery Code

Select , then select **Confirm** to confirm. A new set of recovery codes will be displayed.

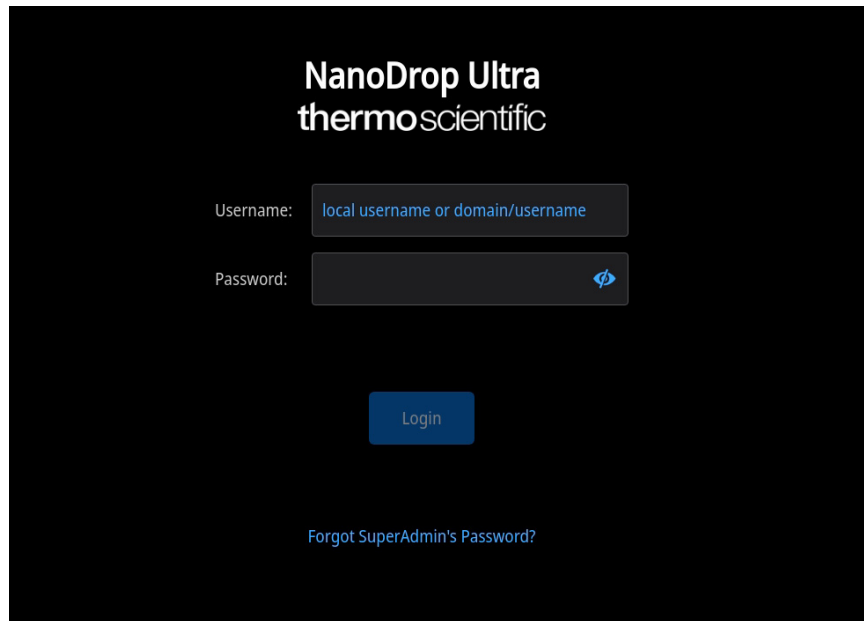
Resetting the SuperAdmin Password

In the event that the SuperAdmin user has forgotten their password, follow the steps below to reset the password.

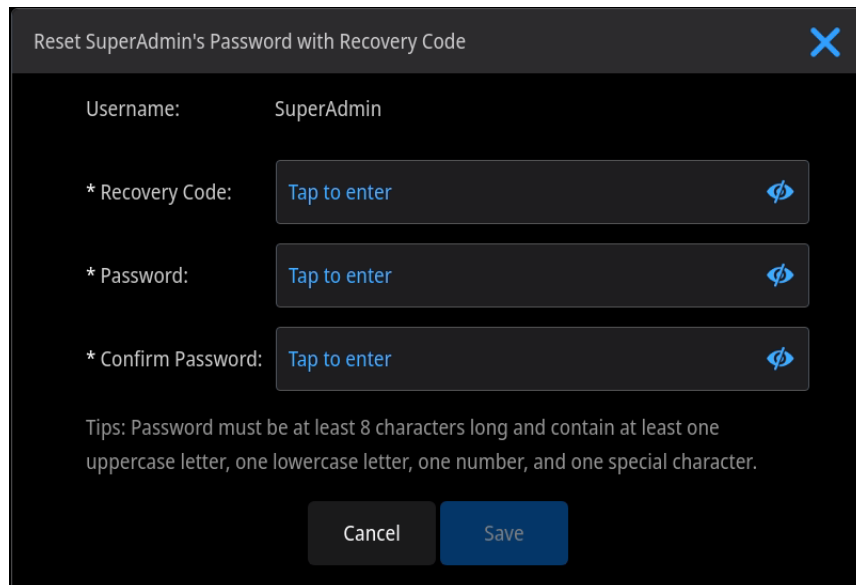
2 Introduction

Resetting the SuperAdmin Password

1. From the initial login screen, select "**Forgot SuperAdmin's Password?**", then select **Confirm**.



2. Enter a Recovery code, a list of Recovery codes was provided when the SuperAdmin account was first created.
3. Next enter the desired password into the New password and Confirm password fields and select **Save**.



4. The password will now be reset for the SuperAdmin user.

SciVault 2 Overview

The SciVault 2 software comprises three applications that work independently or in conjunction with your computer's operating system or network to provide a secure environment that supports the requirements of 21 CFR Part 11.

- **User Management feature** lets users (typically people designated as a Security Administrator) define roles and users within the software.
- **User Privileges feature** lets users (typically people designated as a Security Administrator) define security settings for access control, auditing of electronic records and control of electronic signatures. When the SciVault 2 software is installed with a remote server configuration, this allows the User Privileges feature to provide centralized administration for all user accounts on the network. The security settings defined using this software are stored on the network server or computer in a secure file where they are then queried by the SciVault 2 software applications.
- **Audit Logs feature** lets you view logged security events and create reports of logged events.

The Role of the IT Administrator

An Information Technology (IT) administrator is a person who belongs to the network Administrators group and can create new users and groups on the network. This is essential if a remote server installation is performed.

Only a user who is a member of the Windows Administrators group can perform installation and initial configuration of the SciVault 2 software for the computer on which the software was installed.

Before the SciVault 2 software installation is performed, the IT administrator should complete the following tasks:

- Review the operating system configuration and make any changes required to ensure compatibility with the requirements of 21 CFR Part 11.
- Create any additional local or domain users or groups (if necessary).

3 SciVault 2 Overview

The Role of the Security Administrator

- Create additional authorization roles (if necessary). Additional authorization roles can be created for additional flexibility if the user is not satisfied with the default roles.
- Add local or domain users to the Administrator role (if desired). This will grant those users the right to open and manage the User Privileges feature.
- Add local or domain users to the Power User role (if desired).
- Add local or domain users to the User role (if desired). Adding users to this role will grant those users basic privileges within the User Privileges feature.
- For remote server installation configurations, all users or user groups must be on the network domain. For local server installation configurations, the users can be a local or domain Windows account or created locally on the instrument itself. Adding users to this role will grant those users elevated privileges within the User Privileges feature.
- Setup of the LDAP settings within System Settings, if domain Windows accounts will be used in a Local Server with Single Instrument Configuration.

After the installation and initial setup, the IT administrator may need to:

- Add new users to the system.
- Make any changes that are needed to the composition of user groups.

The Role of the Security Administrator

The Security Administrator may or may not be the same person as the IT administrator, depending on which computer or instrument the User Privileges feature is enabled and Thermo Scientific SciVault 2 Service are installed on and the policies of the network on which User Privileges is running (if applicable).

Before the IT administrator has carried out the tasks listed in the preceding section, the Security Administrator needs to:

- Create the lists of users and roles permitted to perform each of the protected functions of the instrument applications that are controlled by the User Privileges feature.
- Review the User Privileges system policies and disable (deny or remove) any policies that are not required for certain roles.
- Set up the list of signature meanings that can be attached to electronic signatures and specify which role can use those meanings.

After the initial setup, the Security Administrator will need to perform the following maintenance tasks:

- Make changes to the rights of roles permitted to perform each of the protected functions of the instrument applications.
- Make any changes that are needed to the list of signature meanings.

If the Security Administrator is not the same person as the IT Administrator, the Security Administrator may not be able to:

- Add new Windows users to the system.

This feature is performed by the IT administrator.

Windows Local User Groups and Rights

The IT Administrator can set up Windows local or global user groups to manage users more efficiently. A Windows local group is a group of users associated with a particular Windows computer. A Windows global group is a group of users associated with a network domain, which can include more than one Windows computer. Local groups can contain global groups from a network domain. Rights and permissions can be assigned to a local group, and users or global groups can be added and deleted from the local group.

Windows local and global groups can be set up in the Microsoft Management Console by using New Group in the Action menu in the Local Users and Groups in Computer Management in Windows software. Rights and privileges can then be assigned or unassigned to those groups by using the Windows Local Security Policy.

Some of the rights that can be assigned or removed include:

- The right to access the workstation from a network. This right must be granted to every user of the instrument applications.
- The right to change the system date and time.
- The right to log on to the system locally.
- The right to shut down the system.
- The right to take ownership of files or other objects.

Note When SciVault 2 is installed on a computer or server, restricting the right to change the system date and time is an important security feature. If this right is removed from a user group, the users in that group cannot collect data under a falsified date and time.

Note Windows groups cannot be added into the User Management feature of the SciVault 2 software.

Windows User Profiles

The IT administrator can assign users mandatory profiles that control the users' desktop settings and prohibit users from permanently changing their desktop settings. The administrator can assign profiles by using Local Users and Groups in Computer Management in Windows software.

Other Security Features

If the workstation will be connected to a network with Windows Server, or if Windows Server client-based administration tools are installed on the workstation, the IT administrator can take the following additional security features into consideration:



- Allowing users to have access to the network or workstation only during specified hours.
- Restricting users from logging on or allowing users to log on to specific workstations on a network.
- Specifying user account expiration dates.

These security features can only be changed by users who are network administrators. If you want these settings changed, you may need to ask your network administrator to make the changes.

Audit Logging

The SciVault 2 software generates an audit trail of activities with your Thermo Scientific instruments. It records User Management changes, User Privileges changes, and instrument application operations, or "events" in a secure database. Use the Audit Logs to view logged security events and create reports of specific event types or time frames or from specific users. For more information, see ["Audit Logs Feature"](#) on [page 59](#).

User Management Feature

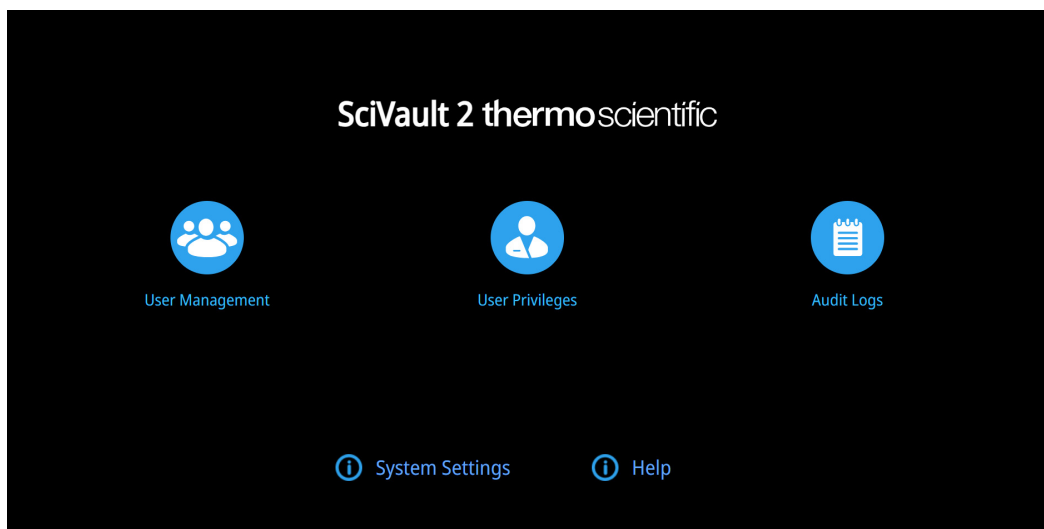
The SciVault 2 software can be directly accessed within the instrument software by selecting  on the home screen. When using a connected PC, the SciVault 2 software can also be accessed directly by double-clicking the SciVault 2 software shortcut on the Windows desktop: .

The User Management feature contains two different options: Users and Roles.

The next section explains the features contained in the SciVault 2 software main window.

About the Display

When you start SciVault software, the home screen appears.



Click the **User Management** icon to display the User Management window. The User Management window will contain two tabs, a tab specific to role management and a tab specific to user management.

Role Management

The SciVault 2 software automatically uses three default authorization groups with recommended compliance assignments. These default authorization groups cannot be deleted or edited. Additional information about the default roles can be found in [Chapter 1, “Getting Started with SciVault 2 Software.”](#)


Figure 4. Roles tab

Role Name	Created By	Creation Time	Description
Administrator	System	8/21/2024 11:29:18 AM	Predefined role for managing and controlling everything.
Power User	System	8/21/2024 11:29:19 AM	Predefined role as power user.
User	System	8/21/2024 11:29:19 AM	Predefined role as normal user.
TEST	SuperAdmin	8/22/2024 14:21:03 PM	

To add a Role to the User Management Feature


1. After navigating to the **Roles** tab within the User Management feature, select Add Role.
2. Select the box next to **Role Name** and enter a unique Role Name which must be greater than two characters.
3. A description of the role may be entered into the box next to **Description**, but this is not required.
4. Select **Save**. The user logged in during the creation of the role along with the date and time will be recorded.

To edit a Role within the User Management Feature

1. After navigating to the **Roles** tab within the **User Management** feature, select  located on the right of the screen of any of the non-default roles.
2. Select the box next to **Role Name** to edit the unique Role Name which must be greater than two characters.
3. Select the box next to **Description** to edit the Description of the role.

4. Select **Save**.

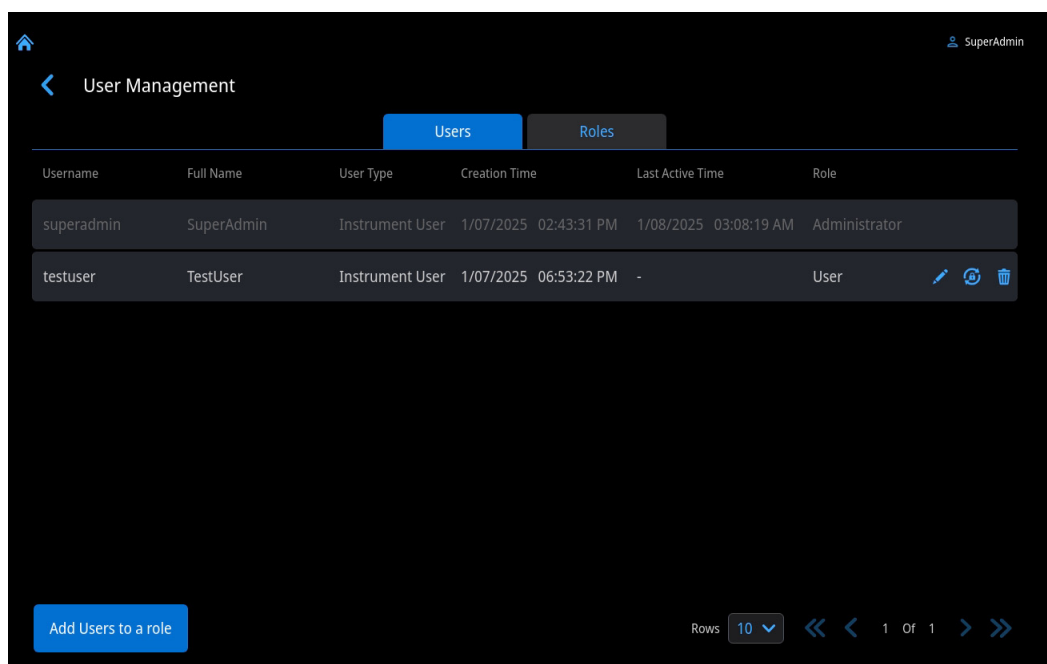
To delete a Role within the User Management Feature

1. After navigating to the **Roles** tab within the User Management feature, select  located on the right of the screen of any of the non-default roles.
2. Select **Confirm** to permanently delete the role.

User Management

At the conclusion of activating or installing SciVault 2 software there will be one default user appearing within the Users tab of the User Management feature. If the SciVault 2 software was activated on a Thermo Scientific instrument, the default user will be the SuperAdmin account created during the activation period. If the SciVault 2 software was installed on a computer or server, the default user will be the Windows account logged in at the time of installation. These default users cannot be deleted or edited and have been assigned to the Administrator role.

Figure 5. Users tab



To add a Local User to the User Management Feature (SciVault 2 Installed on Thermo Scientific Instrument)

A Local User in this scenario will be a user account created on the instrument itself as opposed to a previously created Windows user account.

1. After navigating to the Users tab within the User Management feature, select **Add Users to a role**.

2. Select the **Local User** option at the top.
3. Type in a unique Username for the user by selecting the box next to **Username**. Capitalized letters or special characters cannot be used in the username.
4. Type in the full name for the user by selecting the box next to **Full Name**. This is a descriptive, readable name associated with the user account and typically includes the users first and last name.
5. Assign the user to a role by selecting one of the available role options from the dropdown menu next to **Role**.
6. Select **Save**. The date and time the user was created will be recorded.

To add a Windows Domain User to the User Management Feature (SciVault 2 Installed on Thermo Scientific Instrument)

Note Before following the steps below, please see [Chapter 7, “System Settings,”](#) for more information on connecting your Thermo Scientific instrument to your domain.

1. After navigating to the **Users** tab within the **User Management** feature, select **Add Users to a role**.
2. Select the **Domain User** option at the top.
3. Type in the email or user ID of a Windows domain user by selecting the box next to **Username**.
4. Assign the user to a role by selecting one of the available role options from the dropdown menu next to **Role**.
5. Select **Save**. The date and time the user was created will be recorded.


To add a Windows Local or Domain User to the User Management Feature (SciVault 2 Installed on Windows Computer or Server)

A Local User in this scenario will be a previously created Windows user account on the local computer.


1. After navigating to the **Users** tab within the **User Management** feature, select Add Users to a role.
2. Within the box next to **Username**, type in an email or user ID of a Windows domain user or the name of a Windows local user. When typing in a local Windows user account type in ".\" directly in front of the name. When entering a Windows domain user account, the domain name must be entered first followed by the User ID (i.e. AMER\user.name).
3. Assign the user to a role by selecting one of the available role options from the dropdown menu next to **Role**.

4. Select **Save**. The date and time the user was created in the software will be recorded.


To edit a Role assigned to a User within the User Management Feature

1. After navigating to the **Users** tab within the **User Management** feature, select  located on the right of the screen of any of the non-default users.
2. Reassign the user to a different role by selecting one of the available role options from the dropdown menu next to **Role**.
3. Select **Save**.

To delete a User within the User Management Feature

1. After navigating to the **Users** tab within the **User Management** feature, select  located on the right of the screen of any of the non-default users.
2. Select **Confirm** to permanently delete the user from the software.



To reset the password of a Local User within the User Management Feature (SciVault 2 Installed on Thermo Scientific Instrument)

1. After navigating to the **Users** tab within the **User Management** feature, select  located on the right of the screen of any of the non-default users.
2. Select **Confirm** to reset the password for the selected user.
3. A window will appear with a new temporary password for the user, copy this password and select **OK**. After entering the temporary password at their next login attempt, the user will be instructed to create a new password.

4 User Management Feature

This page is intentionally blank.

User Privileges Feature

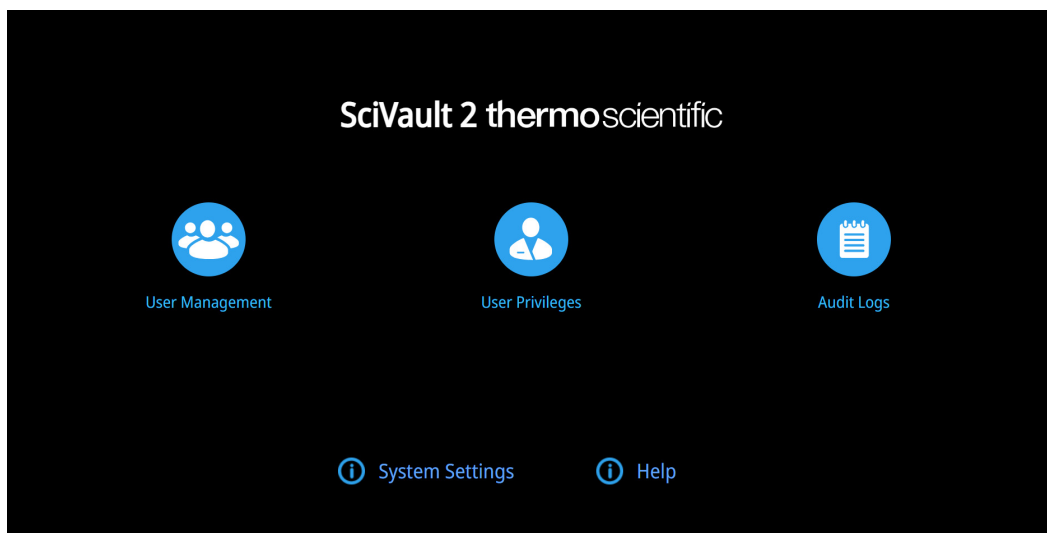
The SciVault 2 software can be directly accessed within the instrument software by selecting  on the home screen. When using a connected PC, the SciVault 2 software can also be accessed directly by double-clicking the SciVault 2 software shortcut on the Windows desktop .

The User Privileges feature contains three different options: Access Control, System Policies, and Signature Meanings.

The next section explains the features contained in the SciVault 2 software main window.

About the Display

When you start SciVault 2 software, the home screen appears.

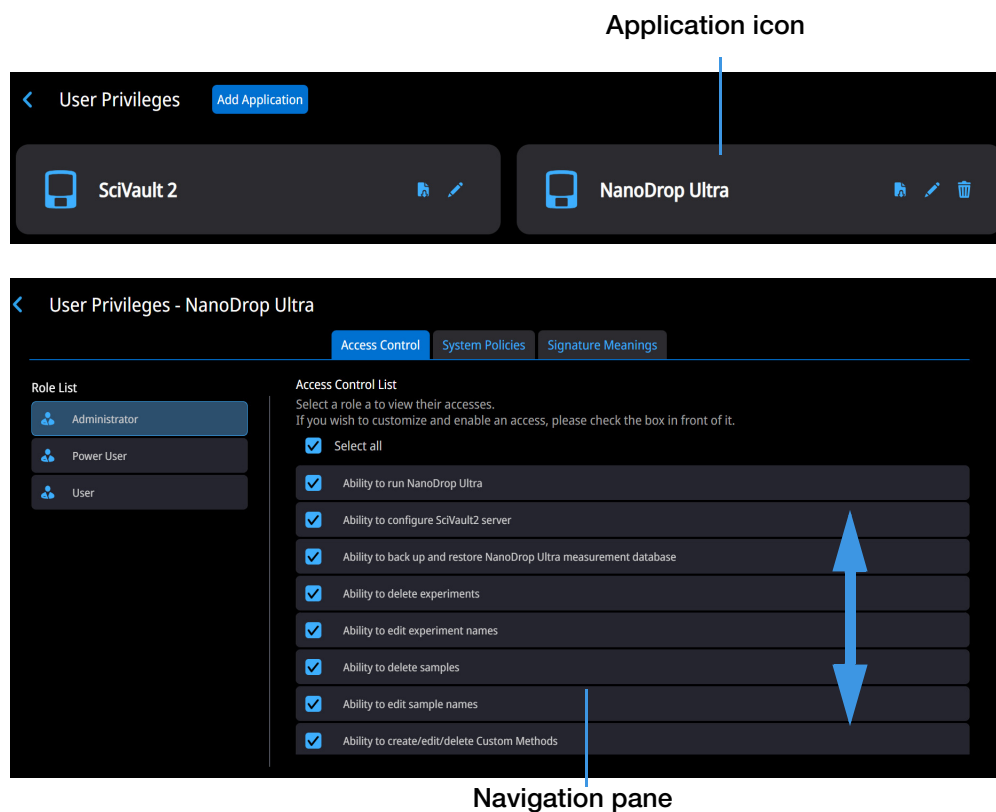


Click the **User Privileges** icon to display the User Privileges window. The User Privileges window will contain multiple modules, each module will contain Access Control, System Policies, and Signature Meanings specific to that application. Here is an example of the window showing security settings for an added application:

5 User Privileges Feature

Controlling Access to the User Privileges Feature

Figure 6. User Privileges for the NanoDrop Ultra instrument

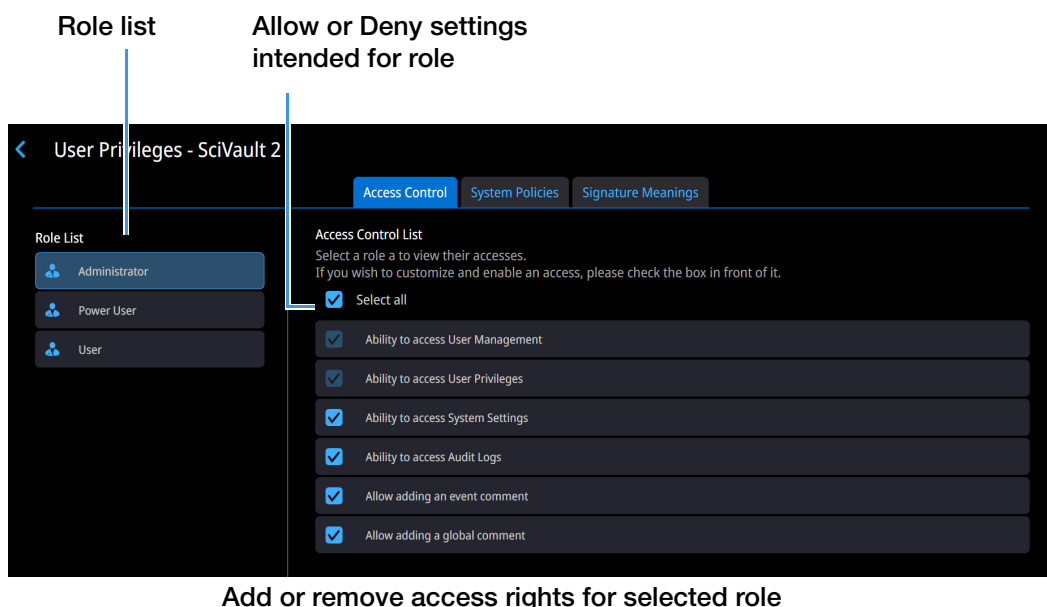


The navigation pane allows you to set security features for the highlighted role in the left panel.

Controlling Access to the User Privileges Feature

Setting up security for your system must include controlling who can run the User Privileges feature. Within the User Privileges - SciVault 2 screen, the Access Control tab is displayed. The Ability to access User Privileges is one of the options within the Access Control List, the Access Control List includes other settings relative to granting or denying access to certain features within that module. Here is an example:

Figure 7. Specify who can start the User Privileges Feature



The left pane contains the Role List, which can be used to specify which role can access (start) the User Privileges feature and edit the security settings for that module. The Ability to access User Privileges and Ability to access User Management are default privileges of the Administrator role and cannot be removed.

Specify Access Rights for Protected Features

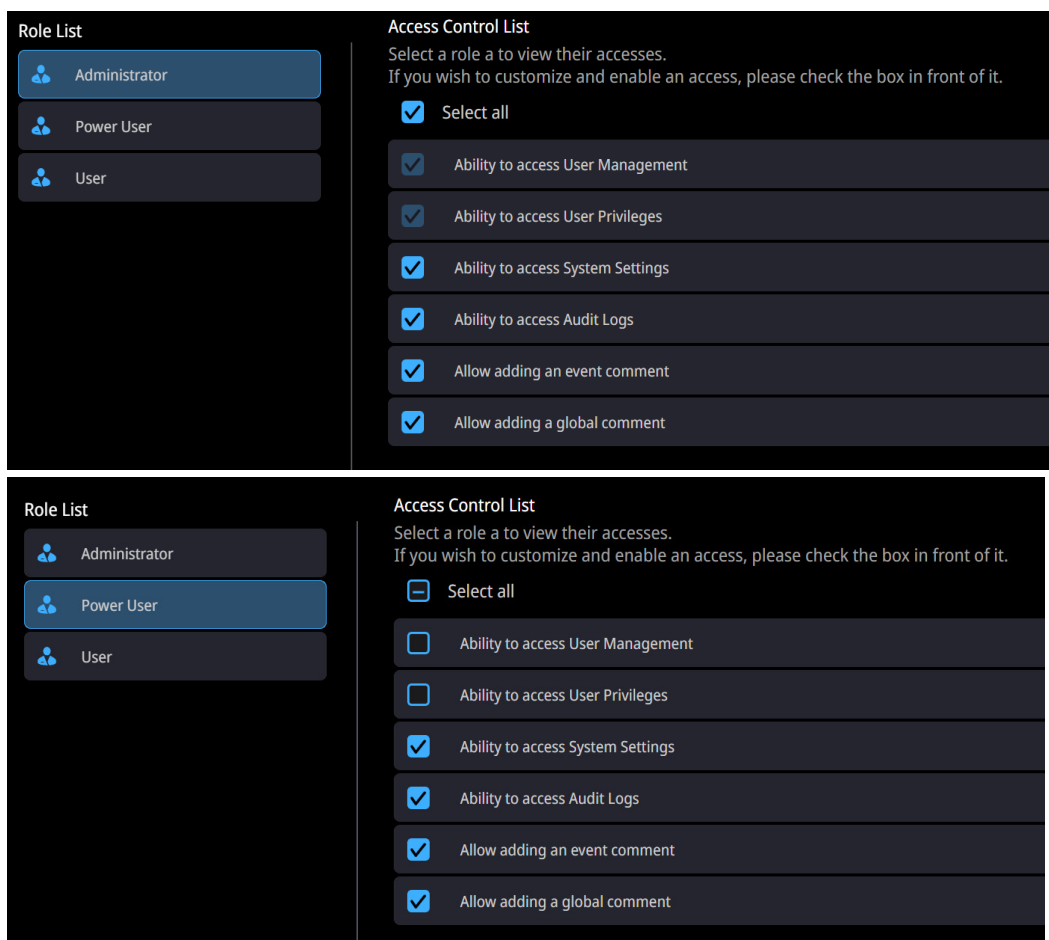
The roles defined within the User Management feature will appear in the Role List. Access to each feature is defined by the role that is selected. If a user or group name was not added to a role, that user or group is denied the right to access the feature.

Note If a user or group without access attempts to start the User Privileges Feature, User Privileges icon is disabled.

To allow a role access to the feature, click the box next to that feature, a checkmark will indicate access has been granted. If the box does not contain a checkmark, the access has been denied. (The default access rights for each of the default roles differ) Here is an example:

5 User Privileges Feature

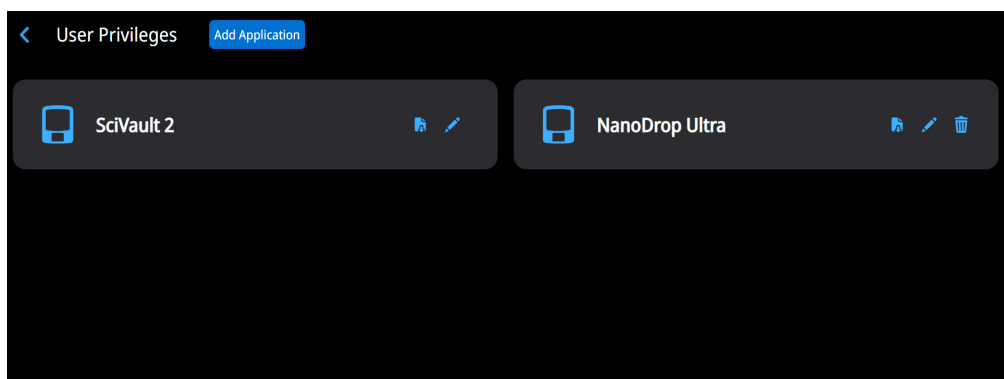
Add an Application



To deny a role access to a feature, deselect the box adjacent that feature to remove the checkmark.

Add an Application

When the SciVault 2 software is first installed, the XML files for all the included applications are added to the User Privileges feature automatically. When you run the User Privileges feature, icons for folders for each application will be available in the navigation pane. Here are some examples:



You can then set access rights, system policies, and signature meanings for those application.

If you have just installed a new version of an application that has new features controlled by User Privileges feature, use Add Application button to add the new version's .XML file to the User Privileges feature. This merges the new features into the security settings file and preserves all of your existing settings.

To add an application to the User Privileges Feature

1. Choose **Add Application** in User Privileges page.
2. Locate and select the application (.XML) file you want to open.

Typically, the application (.XML) file is in the root directory of the application installation media.

Note Some .XML files are available in different languages. The language is indicated by its standard Windows abbreviation included in the file name. Use these language versions of the .XML files if you want the Access Control and System Policies settings displayed in a language other than English. If the English .XML file has been loaded, you can switch to a different language by loading a different .XML file. All of the text will be changed to the selected language, but the settings made in English will be retained.


3. Choose **Open**.

The application appears as a badge in User Privileges page. See [“Setting Security Features for Monitored Applications”](#) on [page 44](#) for instructions for setting security features for the new application.

Remove an Application

Use the Delete button to remove an application in User Privileges Feature.

To remove an application from the User Privileges Feature

1. From the User Privileges screen, select the Delete button  to the right of the intended application.


A confirmation message is displayed.

2. Select **Confirm** to remove the application.

Export Application Settings

Use the Export button to export current User Privileges settings. Follow the steps outlines in the [Add an Application](#) section to add these settings to a SciVault 2 software located in a different location.

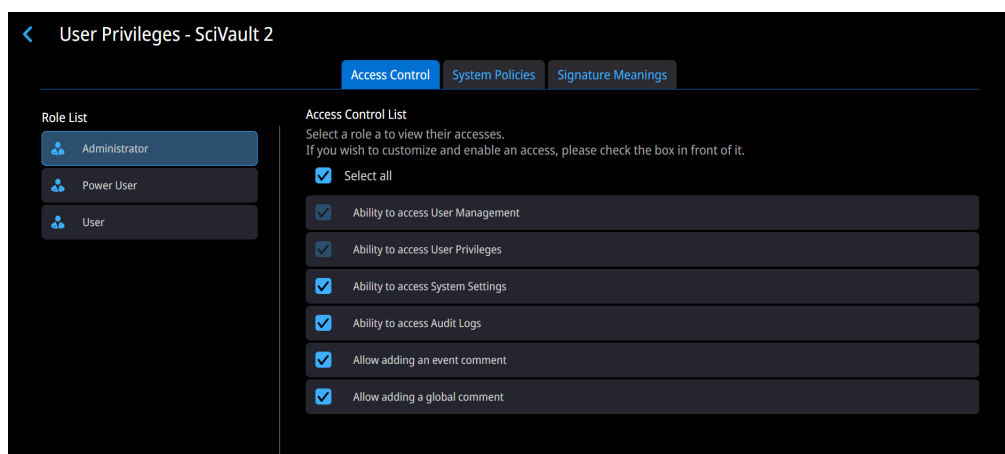
To export application settings from the User Privileges Feature

1. From the User Privileges screen, select the Export button  to the right of the intended application.
2. Use the dropdown menu to select the preferred destination to save to.
3. Select **Confirm** to export the .XML file to the designated location.

Setting Security Features for Monitored Applications

When you open the icon for a monitored application in User Privileges feature, three kinds of security features for the application become available on the banner: Access Control, System Policies and Signature Meanings. Here is an example:

Security features for the application



- Using **Access Control**, you can set the rights of individual roles to use the protected features of the application. See [“Control Access to Application Features”](#) on [page 45](#) for more information.
- With **System Policies** you can set policies covering such things as preventing the exportation or importation of data files and when electronic signatures are required. See [“Set System Policies for SciVault 2 Software Applications”](#) on [page 46](#) for details.
- The **Signature Meanings** tab feature lets you specify the meanings (reasons) that will be available for electronic signatures for each role. See [“Assign Signature Meanings to SciVault 2 Software Applications”](#) on [page 52](#).

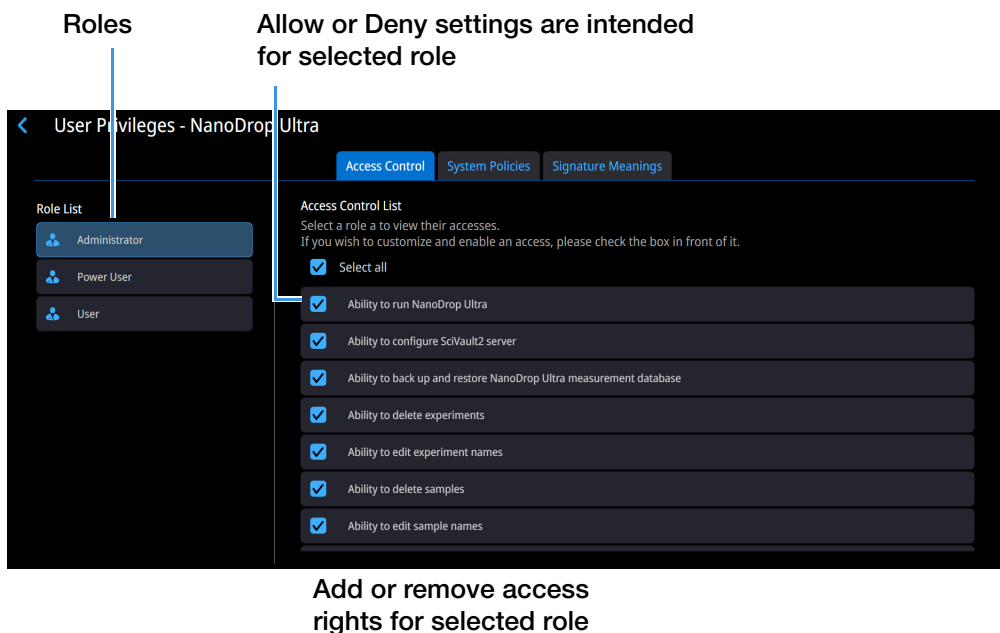
Note When using a network, changes to the access rights, system policies, or signature meanings on the central computer where the User Privileges Feature is installed are immediately used by all of the SciVault 2 software and computers on the network.

Control Access to Application Features

Use **Access Control** to set the rights of individual roles to use the protected features of an application that has been added to the User Privileges feature. A feature in the application will be available only if the logged-in user has the right to use it.

Within the Access Control category for the application, all protected features for that application will appear in the left panel. Each item represents a protected feature or group of features in the application; that is, operations for which access control is available. Here is an example showing a selected item that represents the Ability to restrict who can run the NanoDrop Ultra software:

Figure 8. Specify who can access the features of your SciVault 2 software applications



First highlight one of the roles in the left pane then select any of the available Access Control options to grant or deny access to the selected role. For details, see [“Specify Access Rights for Protected Features”](#) on page 41 and [“User Management Feature”](#) on page 33.

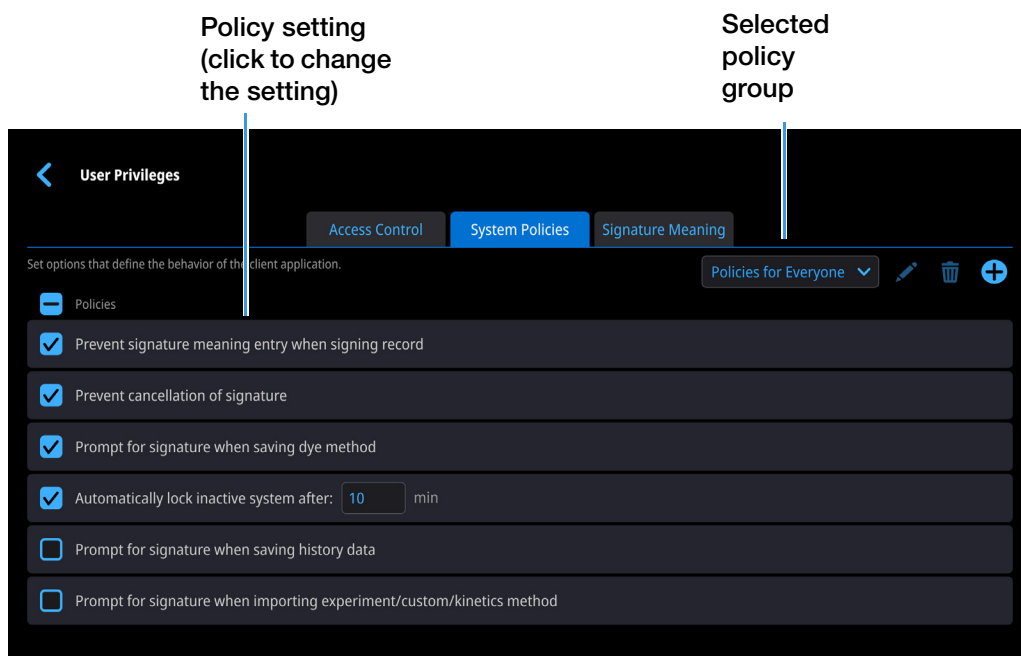
The options provided depend on the application you are setting up. See the SciVault 2 OQ document for your application for more specific information about controlling access to its protected features.

Set System Policies for SciVault 2 Software Applications

Use System Policies to set policies covering such things as preventing import of data files and requiring electronic signatures. By default, all the system policies for an application are configured to provide the most restrictive and controlled environment.

Within the System Policies tab, a list of policies will appear. Each row in the list represents a system policy. Here is an example of a selected system policy for a SciVault 2 software application:

Figure 9. Specify the system policy settings for each policy group



You can use the tools within this tab to create policy groups and then define policy settings for each policy group. A policy group is a group of users for whom you can set system policies. One policy group, Policies For Everyone, is present for every system policy. Its purpose is to provide policy settings for users whom you have not yet assigned to a group. All users are automatically members of this group. You cannot delete this policy group, change its name, delete users from it or add users to it. If a user is a member of another group, that group's policy settings for the user are used instead of the settings of the Policies For Everyone group.

The available policies depend on the application you are setting up. Use the check box that appears to the left of each policy to specify whether that policy will be in effect for the selected policy group. Some policy settings may not allow you to use the check box, instead it will let you specify a system attribute (i.e. Directory for AutoExport). See the SciVault 2 OQ document that came with your instrument software application for specific instructions for setting its system policies.

Set System Policies for a Policy Group

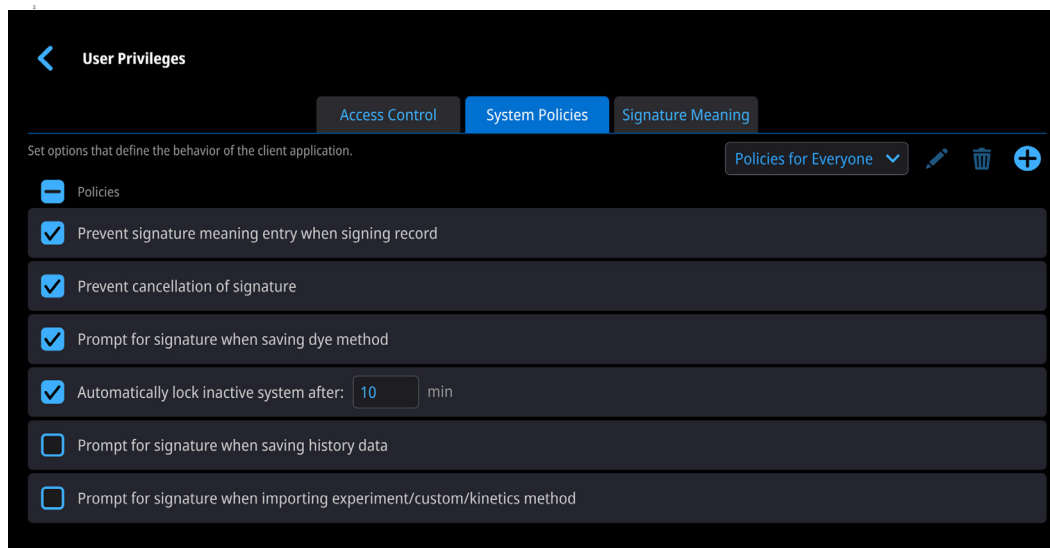
When you select a policy group in the Policy Groups box, that group's settings for the selectable policies appear on the screen (a check mark appears or does not appear in the check box to the left of each policy name). This lets you see all the group's selectable settings at a glance. Once you have selected a policy group, follow these steps to set policies for the group.

5 User Privileges Feature

Create a Policy Group, Delete a Group or Edit a Group's Name

To set system policies for a policy group

1. Select the System Policies tab, then select the desired policy group in the Policy Groups box.
2. Select or deselect the check box associated with each policy depending on your preferred settings. Here is an example of a policy that is selected (required) for the default policy group:





4. Continue selecting and setting the remaining system policies for the selected policy group until all policies have been set or reviewed.

Create a Policy Group, Delete a Group or Edit a Group's Name

You can create a new system policy group, delete a policy group, or edit a policy group's name and/or members in the User Privileges feature. If you create a new policy group, you can set policies individually for that policy group. User accounts can then be assigned to the policy group. User accounts should be members of no more than one policy group.

To create a policy group

1. In the User Privileges feature, open the application you want to create a policy group for by selecting .
2. Select the System Policies tab in the navigation pane within the selected application.
3. Select  to the right of the trash bin icon, enter a name for the new policy group (for example, Policy Group 1), confirm the name by selecting it in the box below the dropdown menu. When operating the software directly on an

instrument with a touchscreen, a keyboard will appear, select **Done** to close the keyboard.

4. Add all applicable users to the policy group by entering in their username or email address, then select **Save**.

When SciVault 2 is on a computer, enter the username of a Windows domain account (networked computer) or the username of a Windows local account.

Note When typing in a local Windows user account, type "." directly in front of the name. When entering a Windows domain user account, the domain name must be entered first followed by the User ID (i.e. AMER\user.name).

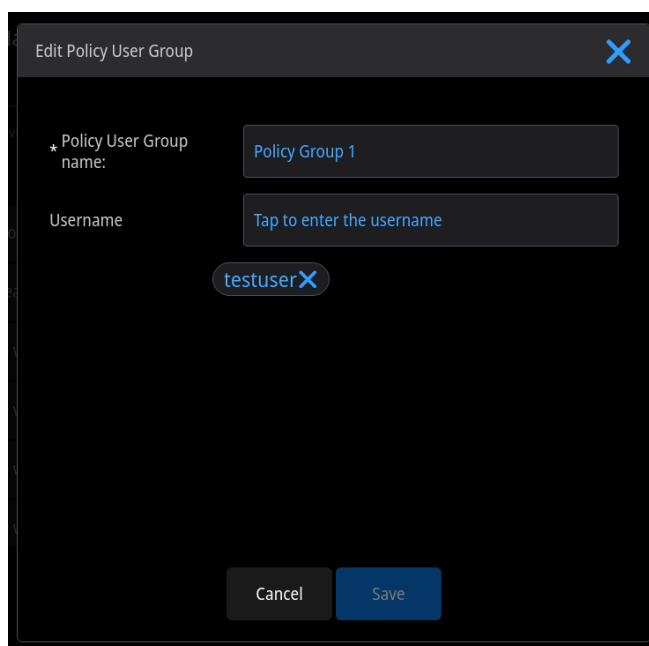
When SciVault 2 is on the instrument, enter the username of a Windows domain account (networked instrument with LDAP configured) or the username of a local instrument account.

The screenshot shows a dark-themed dialog box titled "Add a New Policy User Group" with a close button (X) in the top right corner. The dialog contains two input fields: "Policy User Group name" with the text "Policy Group 1" and "Username" with the text "Tap to enter the username". Below the "Username" field is a suggestion bubble containing "testuser" and a close button (X). At the bottom are "Cancel" and "Save" buttons.

5 User Privileges Feature


Create a Policy Group, Delete a Group or Edit a Group's Name

- The new group appears in the Policy Groups list, with a name that includes the descriptive name you entered. Here is an example:



The screenshot shows a dark-themed dialog box titled "Edit Policy User Group" with a close button (X) in the top right corner. The dialog contains two input fields: "Policy User Group name:" with the text "Policy Group 1" and "Username" with the text "testuser". Below the "testuser" text is a small blue "X" icon. At the bottom of the dialog are two buttons: "Cancel" and "Save".

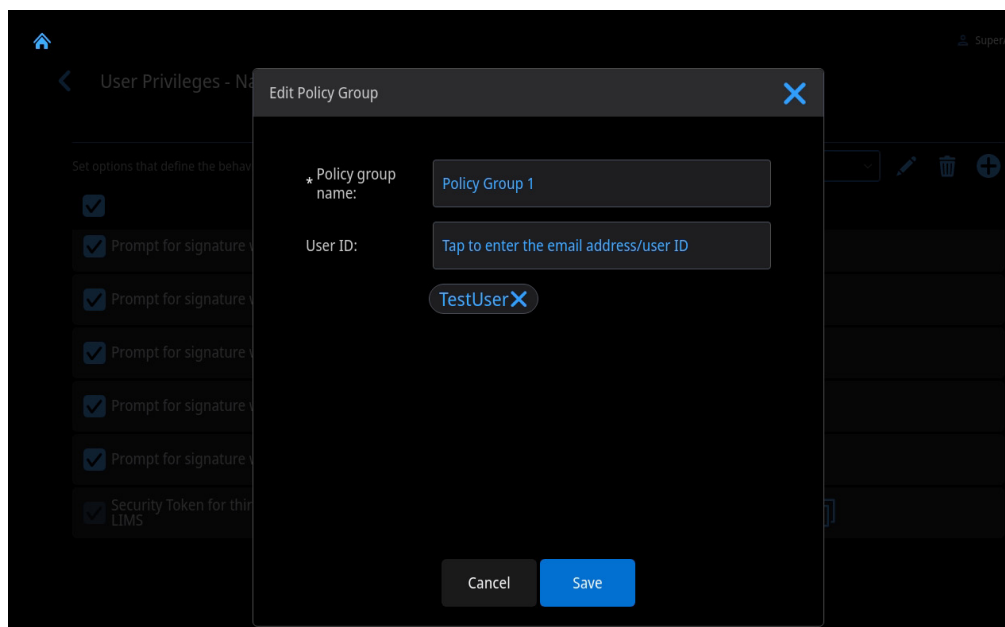
To delete a policy group

- Select a group (other than the Global Policies for Everyone Group) in the **Policy Groups** box.
- Select  to the right of the Policy Groups box, then select **Confirm**.
The group is removed from the list.


To edit a policy group

- Select a group (other than the Global Policies for Everyone Group) in the Policy Groups box.
- Select  to the right of the **Policy Groups** box.

The Edit Policy Group box is displayed. Here is an example:



3. If desired, edit the description for the group or add additional users to the group.

Users that have already been added to the policy group can be removed by selecting  to the right of their username.


4. Select **Save**.

The edited group name appears in the Policy Groups box.

LIMS API Integration

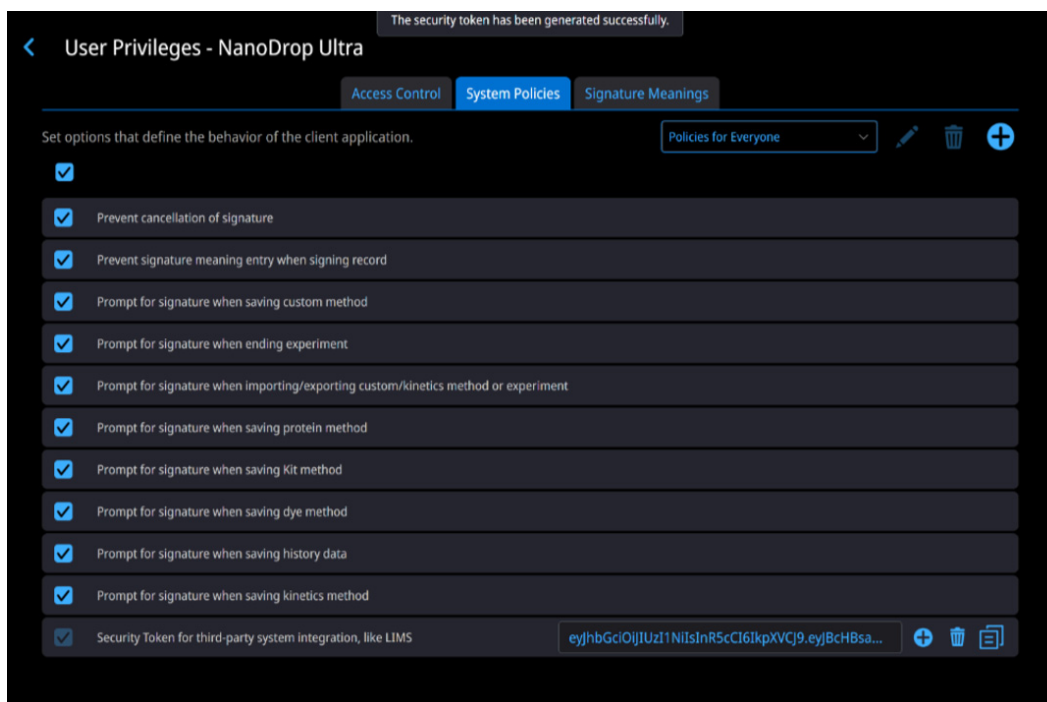
Some instrument applications like NanoDrop Ultra provide a System Policy that enables seamless integration with your Laboratory Information Management System (LIMS). The REST API allows for efficient data exchange, including the submission, retrieval, and updating of data between the instrument and your LIMS.


Set up LIMS API Integration

1. Within the User Privileges screen, select the **System Policies** tab.
2. Scroll to find the "Security Token for third-party system integration, like LIMS" policy. This policy can generate a Token for third-party LIMS authorization.
3. Click  to generate a unique Token.

5 User Privileges Feature

Assign Signature Meanings to SciVault 2 Software Applications



4. When accessing SciVault 2 directly from an instrument, click the Export icon and select the location to export a Token to. This can then be transferred to the LIMS system for authorizing REST API.
5. When accessing SciVault 2 from a PC, click the Copy icon  to copy a Token to the LIMS system for authorizing REST API.

For more information on how to utilize the REST API, please refer to the NanoDrop Ultra API Reference Manual.

Assign Signature Meanings to SciVault 2 Software Applications

The Signature Meanings tab of the User Privileges feature lets you specify the meanings (reasons) that will be available for electronic signatures of any available role. For example, you could set the Signature Meanings features so that only a particular role—for instance, the Power User—is allowed to sign a file with the "Approval" meaning. See [“About Digital Signatures”](#) on [page 53](#) for a general discussion of digital signatures.

Each application has its own list of available signature meanings. You can edit or delete these meanings and add new meanings. You can also specify which roles can use which meanings.


Note Some applications include a system policy that specifies whether users can enter custom signature meanings depending on the role they have been assigned. See the "Prevent signature meaning entry when signing file" system policy for your application for more information.

About Digital Signatures

Several of the system policies for the SciVault 2 software applications cover the use of digital signatures for protecting various kinds of files, such as those containing spectra (.spa and .jdx files), experiments (.exp), configurations (.con) or macros (.mac). The visible portion of a digital signature consists of a username, a date and a stated reason for signing (the "meaning" of the signature). See ["Edit Signature Meanings"](#) on [page 56](#) for information on specifying the meanings that will be available for electronic signatures supplied by users of Thermo Scientific applications. A digital signature also contains encrypted information that lets you detect whether the experiment has changed since it was signed.

A user can digitally sign an experiment in many of the applications or verify that an experiment has been digitally signed.

When saving an experiment, the user can specify that a digital signature should be required when the experiment is saved. A user may be prompted to sign the experiment depending on the system policies selected by the user privileges.

When a user opens a stored spectrum, digital signature information appears when selecting  and then selecting **Signature Logs**. If the experiment has not been signed, "Signature: Not Signed" appears. If the file has been signed, the username of the person who signed it appears, along with the date and time of the signature and the meaning of the signature; for example, "Signature: SuperAdmin, 02-21-2024 12:02:37 (GMT-06:00), Authorship." (The "GMT-06:00" indicates the location relative to Greenwich Mean Time).

Multiple signatures are allowed and listed if the experiment's contents have not been changed. If the experiment is changed, the signature or signatures are invalid, and the file needs to be signed again.

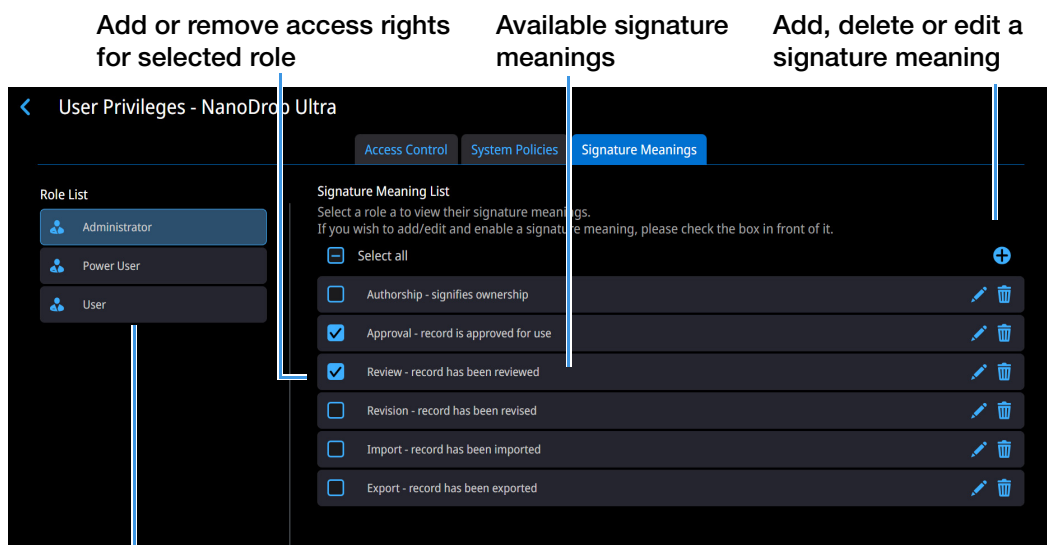
View or Change Signature Meaning Assignments

To see the current signature meaning assignments, click the Signature Meanings category for the application. The Signature Meanings features appear in the right pane. Here is an example:

5 User Privileges Feature

Assign Signature Meanings to SciVault 2 Software Applications

Figure 10. Specify who can access the signature meanings for your applications



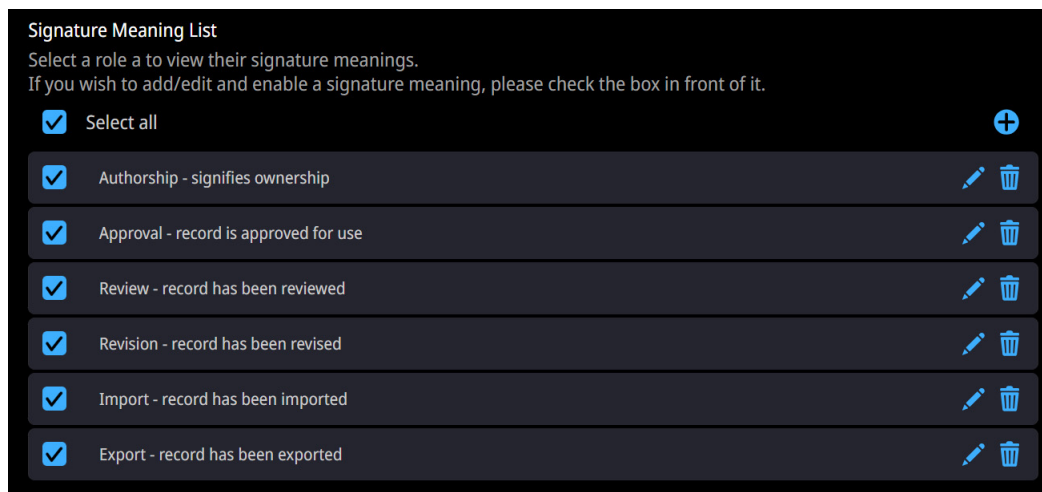
Allow or Deny settings are intended for roles

First highlight one of the roles in the left pane then select any of the available Signature Meanings options to grant or deny use to the selected role. For details, see [“Specify Access Rights for Protected Features”](#) on page 41 and [“User Management Feature”](#) on page 33.

Default Signature Meanings for All Applications

This section explains the default signature meanings for the SciVault 2 software applications and their permissions for the roles created by the SciVault 2 software (Administrator, Power User, and User). You can keep the current (recommended) settings and roles or change them as needed to ensure compliance with the security requirements at your installation site.

The following signature meanings are included in the default list of available signature meanings for all Thermo Scientific applications:



This list appears when you click the Signature Meanings tab for any application in the banner the first time you use the User Privileges Feature. If you have made changes to the list of signature meanings, the available meanings in your software may be different. See [“View or Change Signature Meaning Assignments”](#) on [page 53](#) for more information to specify which users can select each meaning when signing a file.

The default signature meanings are intended to be used as explained below.

- **Authorship.** Indicates that the user signing the experiment is the person who created it. For example, a chemist saving a spectrum could select this signature meaning to show who collected the spectrum.
- **Approval.** Indicates that the user signing the file has approved it for use. For example, a lab supervisor saving an experiment could select this signature meaning to approve the experiment for use by technicians.
- **Review.** Indicates that the user signing the experiment has reviewed it. For example, a lab supervisor saving a spectrum processed by a technician could select this signature meaning to show that the spectrum has been reviewed by the appropriate person.
- **Revision.** Indicates that the user signing the experiment has changed it. For example, a technician saving a processed spectrum could select this signature meaning to show who changed the spectral data.
- **Import.** Indicates that the user signing the experiment has imported it. For example, a lab supervisor importing an experiment created by a technician. Only select this signature meaning to import the experiment.

5 User Privileges Feature

Assign Signature Meanings to SciVault 2 Software Applications

- **Export.** Indicates that the user signing the experiment has exported it. For example, a lab supervisor exporting an experiment created by a technician. Only select this signature meaning to export the experiment.


The table below shows the default Signature Meaning access rights settings for the default roles created by the SciVault 2 software.

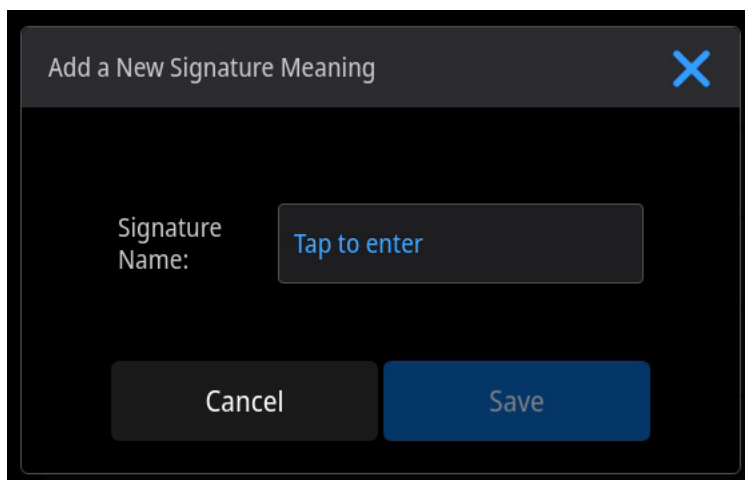
Table 8. Default signature meaning groups and settings for all SciVault 2 software applications

Signature Meaning	Description	Default Access
Authorship	Signifies ownership	Administrator, Power User, User
Approval	Record is approved for use	Administrator
Review	Record has been reviewed	Administrator, Power User
Revision	Record has been revised	Administrator, Power User
Import	Record has been imported	Administrator, Power User
Export	Record has been exported	Administrator, Power User


Edit Signature Meanings


Follow the instructions below to change the list of available signature meanings.

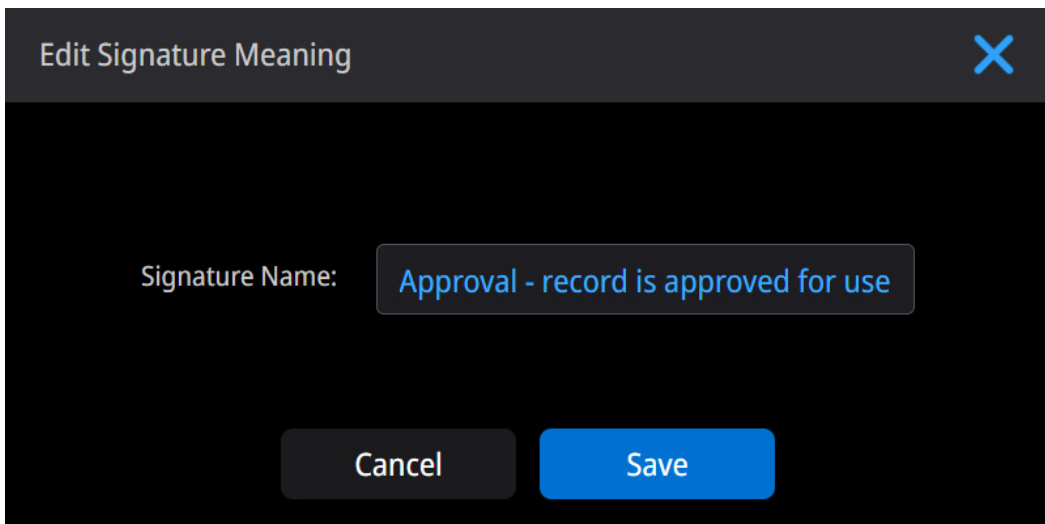
To add a new signature meaning to the list of available meanings, select . The Add a New Signature Meaning box is displayed. Here is an example:



Type the desired text in the box and choose **Save**. The text you entered appears in the list of available signature meanings. You can then specify which roles can select this signature meaning when signing a file.

To delete a signature meaning from the list of available meanings, select  to the right of the Signature Meaning and select **Confirm**. The meaning will no longer be available to any users when they sign files.

To edit a signature meaning from the list of available meanings, select  to the right of the Signature Meaning. The **Edit Signature Meaning** box is displayed. Here is an example:



Edit the text in the box as desired and choose **Save**. The edited text appears in the list of available signature meanings.

Saving Your Privileges Settings

Any new User Privileges settings you have specified for the SciVault 2 software and instrument software applications will automatically save in real time. Your new settings must be saved for them to be in effect when users start the applications.

The new settings will not take effect until the user logs out and back into the software.

Note Every change you make to the privileges settings is recorded in the audit log when you save your settings.

This page is intentionally blank.

Audit Logs Feature

The SciVault 2 software generates an audit trail of activities with your Thermo Scientific™ instruments and software. It records User Management changes, User Privileges changes, and instrument application operations. These records are stored as "events" in a secure database. Use the Audit Logs to view logged security events and create reports of specific event types or time frames or from specific users.

Thermo Scientific Audit Logs- Writes logged events to the log database

Contents

- [Audit Logging](#)
- [Install the Audit Logs](#)
- [Set Up the Audit Logs](#)
- [Open the Audit Logs](#)
- [Work with the Audit Logs](#)
- [Event Information](#)
- [Create, Sign and Print Reports](#)
- [Set User Preferences](#)

Audit Logging

Every logged event includes fields containing some or all the kinds of information listed below. By recording this information, the SciVault 2 software helps you support the audit trail requirements of 21 CFR Part 11. The following information is captured for logged events:

- The event triggers
- The date and time when the event occurred
- The name of the instrument application that was being used when the event occurred

- The type of event that occurred and a detailed description
- The significance of the event
- The Thermo Scientific™ SciVault™ 2 username or Microsoft® Windows® full username and ID of the person who was logged in when the event occurred
- The identification of the instrument (serial number) or computer (name) that was being used when the event occurred

Once the SciVault 2 software is installed/activated and one or more instrument applications have been installed and added to the User Privileges feature, the audit logs on SciVault 2 Software Server automatically begin recording significant operations performed with the applications on any computers on the network where the applications are installed. Changes you make to the security settings in the User Privileges feature are recorded in the audit log when they are saved. For more information, see “[User Privileges Feature](#)” on [page 39](#).

IMPORTANT The SciVault 2 software allows all operations to be logged, both within and outside of all applications that are run on the system. Thus, it logs any attempt to modify any records on the system, even if an application is not running.

There can be many sources of logged events:

SciVault 2 — Tracks changes to the SciVault 2's software security settings.

Thermo Scientific instrument applications — Tracks activity in the instrument applications while the instrument applications are running.

Events that are logged for the above include the following (grouped by source):

SciVault 2

- User created
- User change
- User deleted
- Role created
- Role change
- Role deleted
- Access control change
- System policy group created
- System policy group change

- System policy group deleted
- System policy change
- Signature meaning created
- Signature meaning change
- Signature meaning deleted

Thermo Scientific instrument application(s)

- Log on
- Log off
- Sample collection started
- Experiment created
- Experiment modified
- Experiment deleted
- Experiment signed
- Instrument disconnected

Note Other specific events may be included for the Thermo Scientific instrument applications you use.

Install the Audit Logs

The Audit Logs is a feature of the Thermo Scientific™ SciVault 2™. It is installed automatically in addition to the User Management and User Privileges features.



Set Up the Audit Logs

Like other applications managed by the User Privileges feature, the Audit Logs has associated security policies (i.e., access control, system policies and signature meanings) that can be configured to ensure compliance with the security requirements at your installation site. The default settings and roles provide the most restricted environment. You can keep the current (recommended) settings and the roles or change them as needed. For more information, see the [User Management Feature](#) and [User Privileges Feature](#) chapters in this document.

6 Audit Logs Feature

Open the Audit Logs

Open the Audit Logs

The SciVault 2 software can be directly accessed within the instrument software by selecting  on the home screen. When using a connected PC, the SciVault 2 software can also be assessed directly by double-clicking the SciVault 2 software shortcut on the Windows desktop .

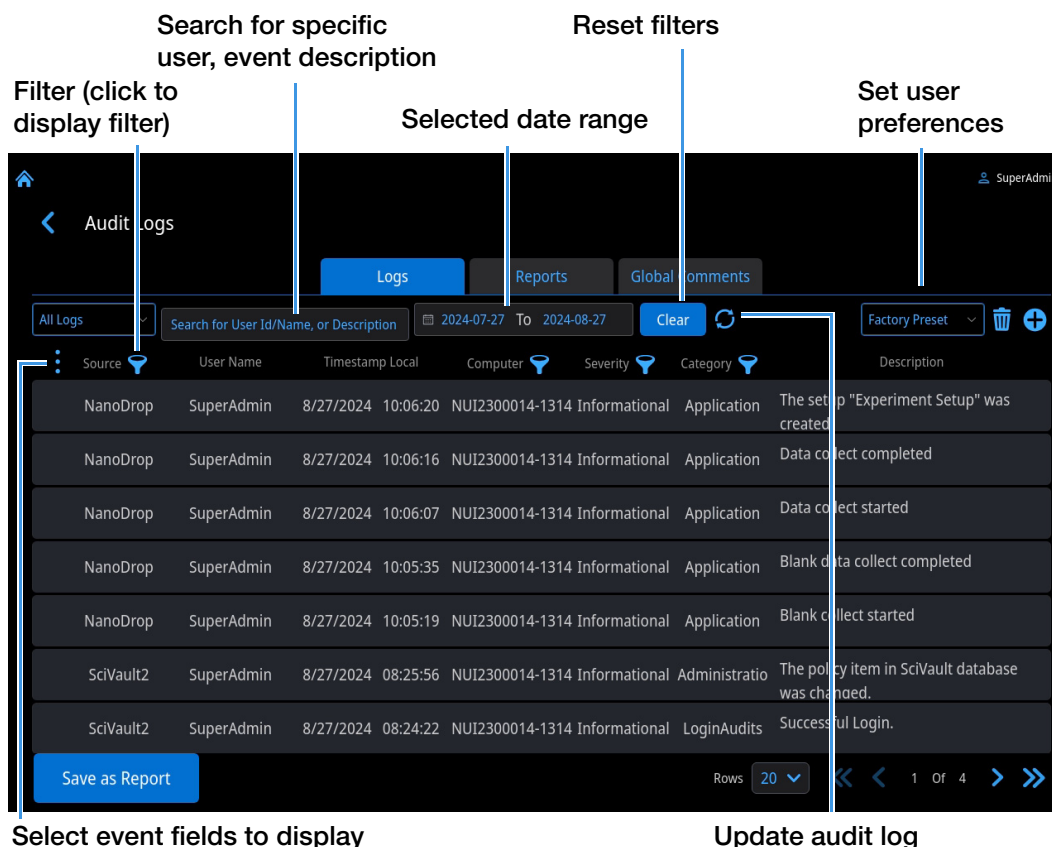
Once opened, the Audit Logs feature will appear as one of three options.

The Audit Logs feature contains three different options: Logs, Reports, and Global Comments.

The next section explains the features contained in the SciVault 2 software main window.

Work with the Audit Logs

The Audit Logs main window contains a log of tracked events. Here is an example:



Search for specific user, event description

Reset filters

Filter (click to display filter)

Selected date range

Set user preferences


Source	User Name	Timestamp	Local	Computer	Severity	Category	Description
NanoDrop	SuperAdmin	8/27/2024	10:06:20	NUI2300014-1314	Informational	Application	The setup "Experiment Setup" was created
NanoDrop	SuperAdmin	8/27/2024	10:06:16	NUI2300014-1314	Informational	Application	Data collect completed
NanoDrop	SuperAdmin	8/27/2024	10:06:07	NUI2300014-1314	Informational	Application	Data collect started
NanoDrop	SuperAdmin	8/27/2024	10:05:35	NUI2300014-1314	Informational	Application	Blank data collect completed
NanoDrop	SuperAdmin	8/27/2024	10:05:19	NUI2300014-1314	Informational	Application	Blank collect started
SciVault2	SuperAdmin	8/27/2024	08:25:56	NUI2300014-1314	Informational	Administratio	The policy item in SciVault database was changed.
SciVault2	SuperAdmin	8/27/2024	08:24:22	NUI2300014-1314	Informational	LoginAudits	Successful Login.

Select event fields to display

Update audit log

You can scroll through the list or use these tools to quickly locate specific events:

- **To sort events** according to Source, select from the drop-down menu to the left of the search window.

- **To filter events** based on Source, Username, Full Name, Severity or Category, click the associated filter  button.
- **To reset all filters** to their default settings (to show all events), click **Clear** button.
- **To search for events that contain a key word or event from a particular user**, enter the key word or username in the Description search box.
- **To search for events created on a specific day or within a given time frame**, specify the day or time frame.

Note The Date Range search is based on the Timestamp Local field.

- **To display all the available information about an event**, double tap or tap and hold the event (row) in the log. The Details window will appear for that event. If the event was the signing of a file, the signature meaning appears in the Description.
- **To configure the fields in the audit logs**, click the three-dot (More) button to the left of the table column headers. Select (or deselect) the fields to display (or hide).
- **To update the audit log to display events that were added after you started the Audit Logs application**, click the **Refresh** icon.
- **To add a comment to an event, double tap or press and hold the event to open the Details window**, select **Add Comments**, type the comment and click the **Add** button.
- **To add a global comment to the audit log, such as an audit date**, select the **Global Comments** tab, then select **Add Comments**. Then type the comment and select the **Add** button.

Event Information

The table below lists and describes the categories of information available for logged events.

Table 9. Information available for each logged event

Field	Description
Source	Action that triggered the event. The following sources are available: <ul style="list-style-type: none">• SciVault 2• Application Names
Username	Full instrument or Windows username for the logged in user
Full Name	Full descriptive, readable instrument or Windows name associated with the logged in user
Computer Name	Full instrument hostname or Windows computer name on which the event occurred
Severity	Significance of the event to the security of the system. The following Severity ratings are possible: <ul style="list-style-type: none">• Informational• Error• Warning• Critical
Timestamp Local	Date and time when the event occurred translated to the local date and time on instrument or computer depending on where the instrument software is installed
Timestamp UTC	Date and time when the event occurred based on the Coordinated Universal Time (UTC) time clock
Timestamp at Origin	Date and time when the event occurred on the instrument or computer in which it occurred
Category	Type of event that occurred. The following event types are possible: <ul style="list-style-type: none">• Administration• Login Audits• Signature• Data Change• File Change• Application• Configuration• Analyze Data

Table 9. Information available for each logged event

Field	Description
Description	Detailed description of the event type. Here are some examples: <ul style="list-style-type: none"> • Successful logon • The user successfully exited or logged off the application
Event ID	Unique identification number for the event
Event Name	Name for the event

Note The information in each of these fields is generated automatically.

Create, Sign and Print Reports


You can easily configure the audit log to show specific event types or time frames or events from specific users, and then save, sign, and print the list as a report.

To create a report

1. Click the three-dot button to the left of the column headers to select (or deselect) the fields to display (or hide) for this report.
2. To filter events for this report based on Source, Computer, Username, Severity or Category, click the associated filter  button. Select (or deselect) items to display (or hide) and exit filter.
3. To save the report, click **Save as Report** at the bottom left, in the Save as Report box, enter custom report name then select **Next**. Enter password and choose the reason, then click **Confirm**.

Note Audit log reports are automatically saved in HTML format (.html filename extension) in the audit log database.

To sign a saved report

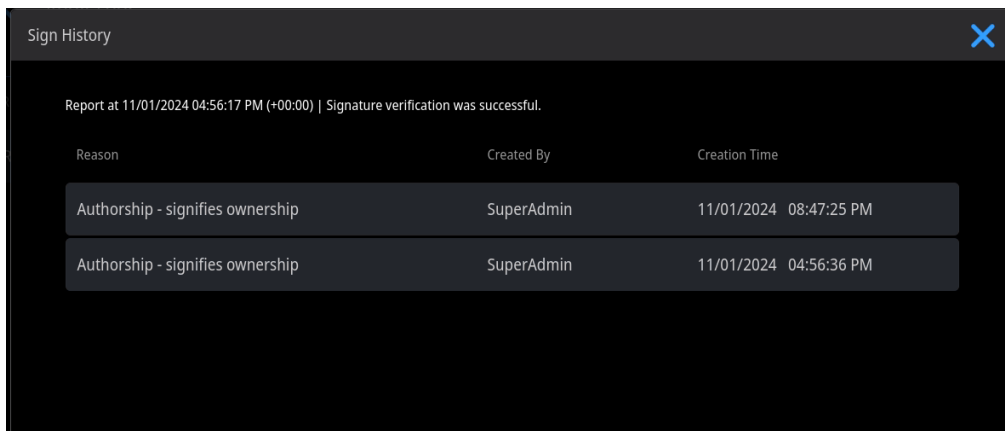
1. Select the **Reports** tab, then select  to the right of the saved report to sign.
2. In the Sign Report box, enter your password (if the instrument is being operated by a touchscreen, a keyboard will appear when selecting the box next to Password, select **Done** to close the keyboard) and choose the reason, then click the **Confirm** button.


A message indicates the report was successfully signed.

To verify a signed report


1. Select the **Reports** tab, then select  to the right of the saved report to view all signatures that have been applied to the report.

The Sign History box shows the signature status, report name, signer, signature time/date and signature reason. Here is an example:



2. Select  at the top right of the window to close the message box.

To print to .PDF a saved report

1. Select the **Reports** tab, then select  to the right of the saved report to print and select an export location for the .PDF file of the report.
2. Select **Confirm**.

Here is an example:

Audit Event Report

Report at 08/27/2024 11:06:03 AM (-04:00)

Source	User Name	Timestamp Local	Computer	Severity	Category
SciVault2	AMER\justin.shaffer	08/27/2024 07:06:00 AM	TF-607869955880	Informational	Administration
Description: The policy item in SciVault database was changed. Application: NanoDrop Ultra. Policy item: Ability to delete samples. Was unassigned from role: Administrator.					
SciVault2	AMER\justin.shaffer	08/27/2024 07:05:57 AM	TF-607869955880	Informational	Administration
Description: The policy item in SciVault database was changed. Application: NanoDrop Ultra. Policy item: DeleteExperiment. Was assigned to role: Administrator.					
SciVault2	AMER\justin.shaffer	08/27/2024 06:34:02 AM	TF-607869955880	Informational	LoginAudits
Description: Successful Login.					
SciVault2	AMER\justin.shaffer	08/27/2024 06:34:02 AM	TF-607869955880	Informational	LoginAudits
Description: Successful Login.					

Signature:	Title:
Date:	Comments:



This file was digitally signed by AMER\justin.shaffer on 08/27/2024 11:06:47 AM.
Reason: Approval - the record is approved for use

Set User Preferences


You can set up the audit logs to display specific columns and use filters to eliminate certain types of events and then save your display settings. You can easily select your preferences from a drop-down list or set them as the default preferences.

The software automatically loads the "Factory Preset" user preferences after startup unless you select another set of preferences as the default. The Factory Presets user preferences cannot be overwritten.

To create a set of user preferences

1. Within the Logs tab, select  to the left of the column headers and select the fields to display (or hide) in the report.
2. To filter events for these user preferences based on Source, Username, Computer, Severity or Category, click the associated filter  button, select (or deselect) items to display (or hide).



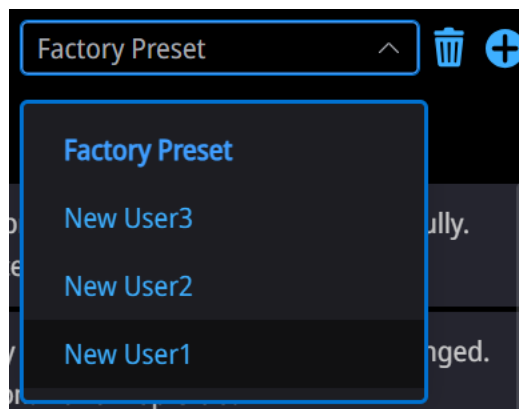
4. Select  beside the preference box, enter a name for these user preferences (for example, New User1), confirm the name by selecting it in the box below the dropdown menu, and then select (or deselect) **Set as Default** option. After that, select the **Confirm** button.

The name of the new set of user preferences appears in the Preferences box above the audit log and becomes the selected user preferences.



To select a set of user preferences

- Click the down arrow in the Preferences box and select a set of user preferences.



The user preferences name appears in the Preferences box and the list of displayed events updates.

To refresh user preferences

- If changes are made to one of the filter settings and you would like to return to the default settings for that preference, select the down arrow in the Preferences box and select a set the user preferences to refresh.

To delete a set of user preferences


1. Click the down arrow in the Preferences box and select a set of user preferences to delete.



3. Select the trash bin to the right of the preference box and then select **Confirm**.

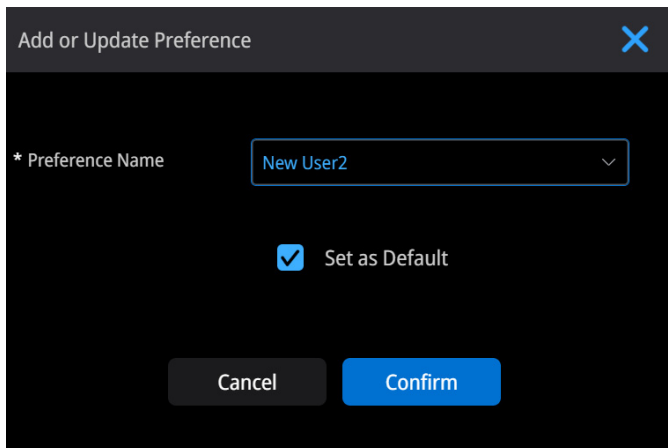
That set of user preferences no longer appears in the drop-down list and the default set of user preferences becomes the selected preferences.

To specify the default user preferences

1. Select  to the right of the reference box and select a set of user preferences to use as the default. You can add a new preference option or choose one of the existing options from the down-down.



3. In the Add or Update Preference box, select **Set As Default** and select **Confirm**.



The next time you start the Audit Logs, the software will load these user preferences.

System Settings

From the home screen of the SciVault 2 software, select System Settings. The System Settings are split into three separate tabs: LDAP, Database, and System.

Connecting Instrument To Your Domain

To integrate your instrument with a networked domain (allows the use of domain Windows accounts) using LDAP (Lightweight Directory Access Protocol), follow these steps to ensure a secure and efficient connection:

1. At a minimum fill out all required (*) fields within the tab.
 - a ***LDAP Server**
 - Resolvable hostname or address of the Active Directory server. Example: amer.thermo.com
 - b ***LDAP Port**

7 System Settings

Connecting Instrument To Your Domain

- The Port used by Active Directory, refers to the following:
 - Regular LDAP (no SSL) . By default, it's 389
 - Encrypted LDAP (SSL). By default, it's 636

c *Bind User

- LDAP user that has permission to read all LDAP objects and attributes that exist in the LDAP base DN. Example: firstname.lastname

d *Bind Password

- Password of the LDAP Bind User.

e *Base DN

- The domain's Distinguished Name. Make sure to use the DN of the desired Domain DN root.

Example: "OU=Users,OU=CN Shanghai (CNSHO),OU=thermoUsers,DC=apac,DC=thermo,DC=com",

f *User Filter

- The criteria which you want to apply on that particular domain controller in the search filter text field.

Example: "(&(objectClass=user)((sAMAccountName={0})(mail={0})))"

The example indicates that the user wants to search a specific user (not a computer or other objects) whose sAMAccountName or mail match the search text.

g Name Attribute

- LDAP Attribute for user logon name, typically, it's sAMAccountName.

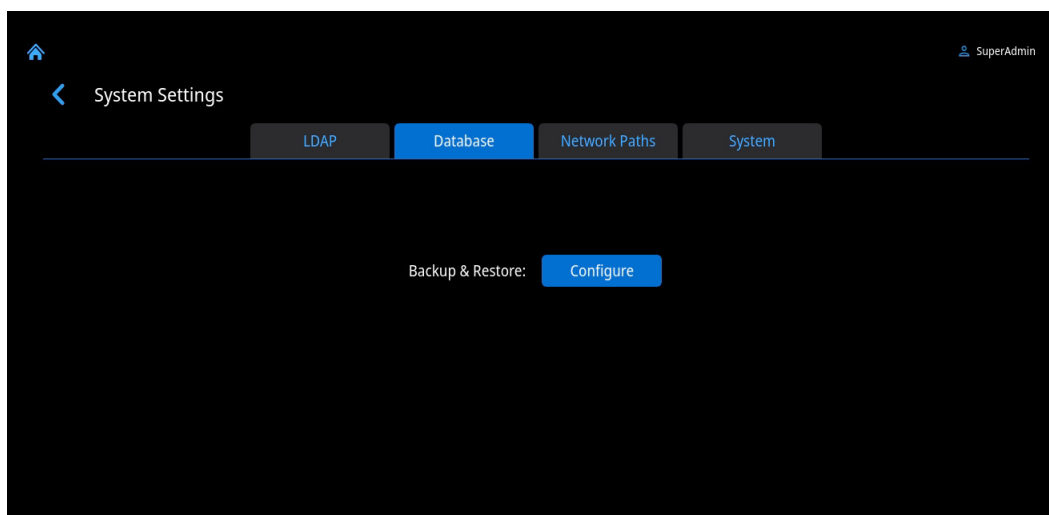
h Email Attribute

- LDAP Attribute for user's email address, normally, it's mail.

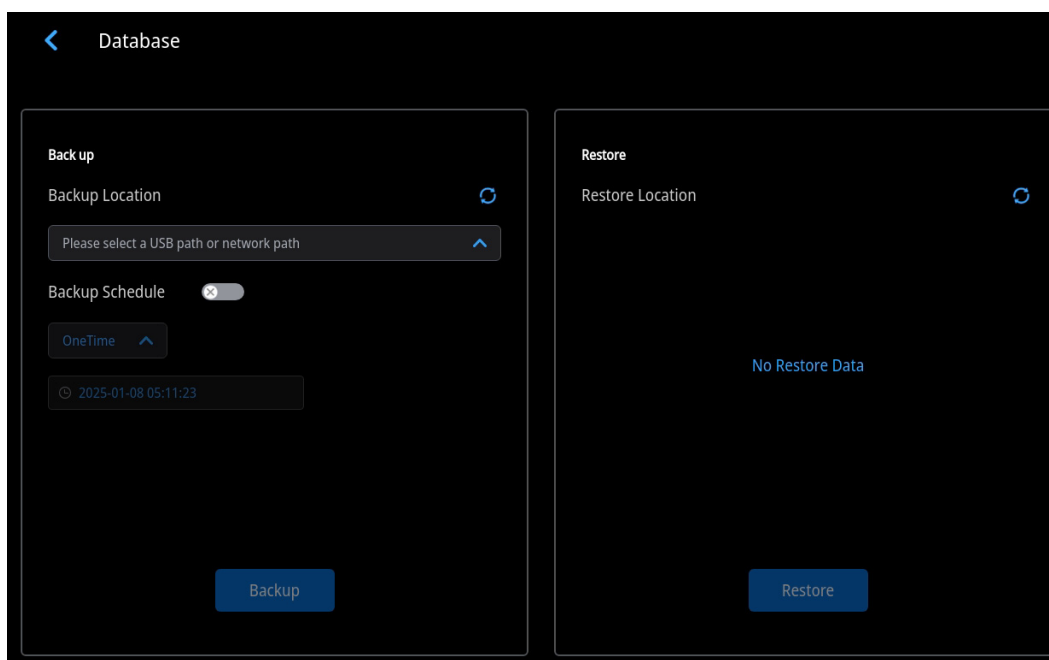
2. Select **Server Test** to test for a successful connection to the domain.
3. Select **Save** to save the LDAP settings.

Database Configuration

Within the **Database** tab, you can Backup & Restore the Audit Log database to a specified location of your choosing. The Selected database folder location is displayed.



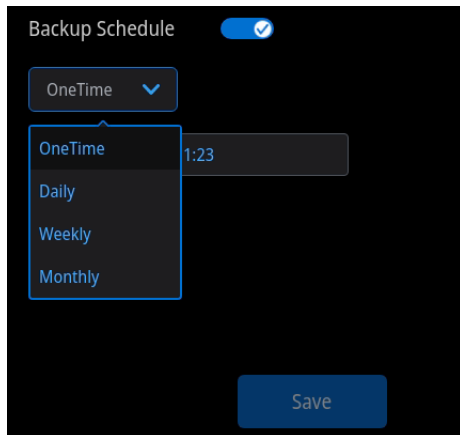
Select **Configure**, within the Database tab, use the drop-down menu under **Backup Location** to select a backup location.



7 System Settings

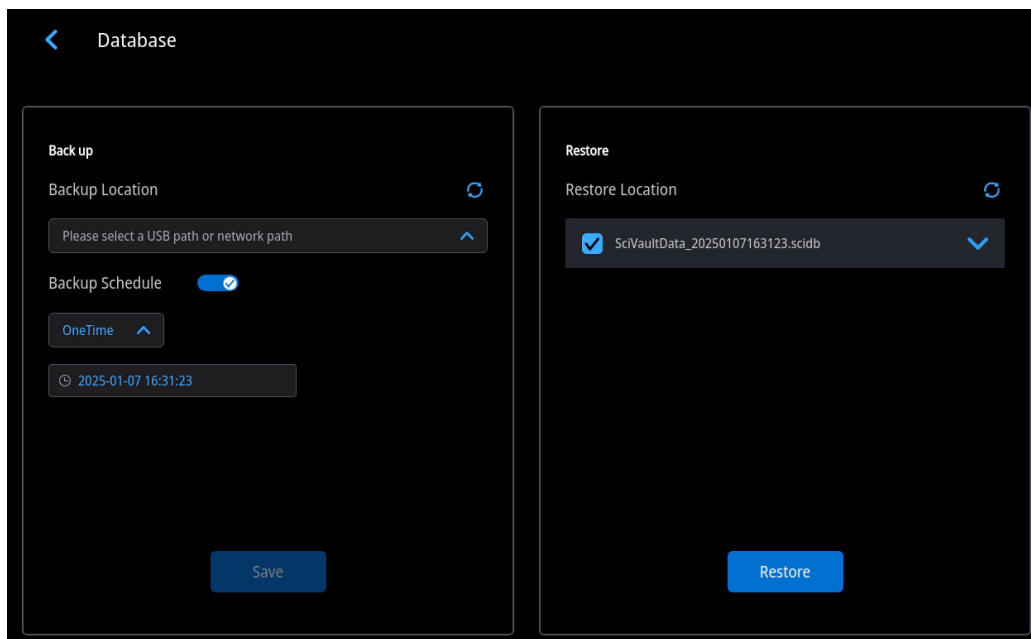
Database Configuration

To enable the backup to occur, select the **Backup Schedule** toggle to move it to the enabled position. You can configure a database backup as a one-time event, or as a periodic scheduled backup. Specify the date and time of a one-time backup, or select the period of the backup.



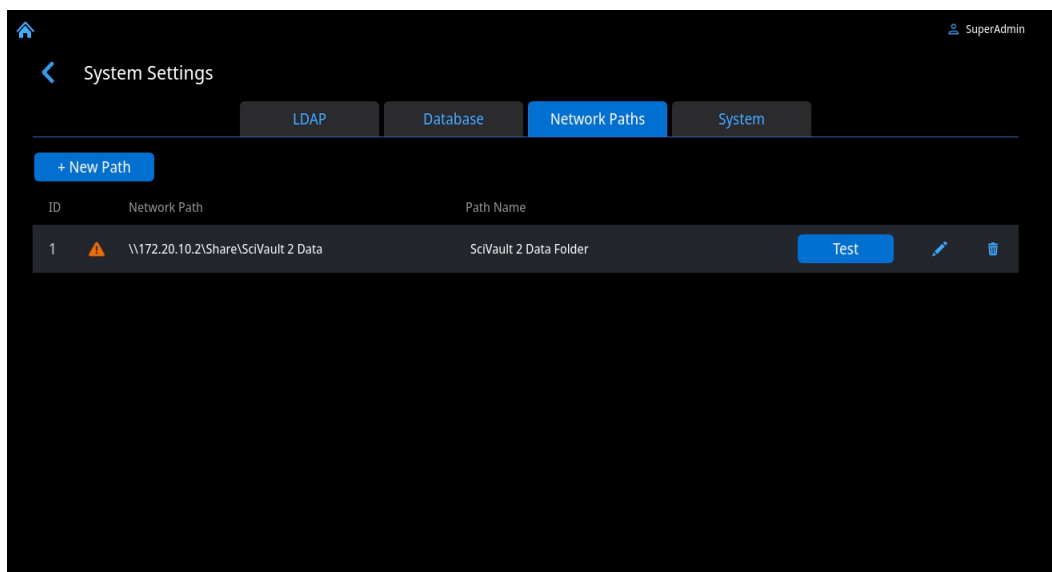
Select **Save** to save the database to the backup location.

To restore data from a previous backup event, select from one of the available backup files listed under the **Restore Location**.



Select **Restore** to restore the database to a previously saved state. After the restore is complete, select **Reboot** to restart the instrument.

Database Network Export Setup



Network Paths

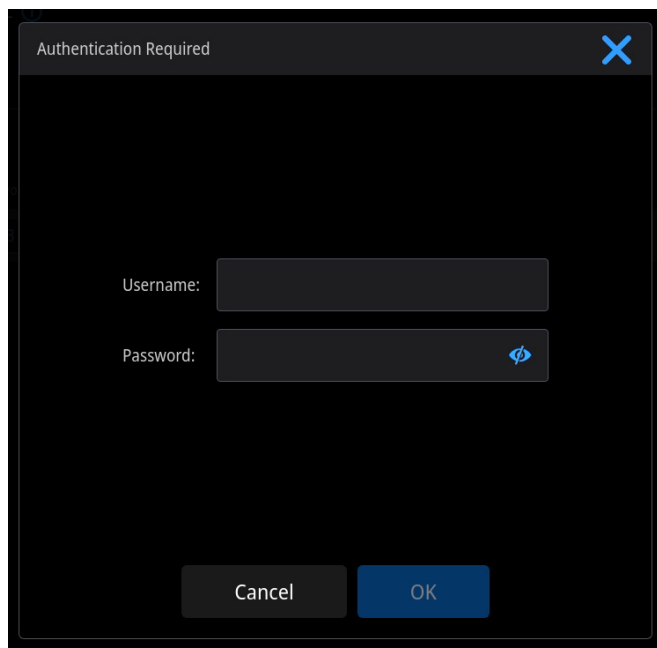
Use this tab to specify one or more network paths for exporting acquired data when the instrument is connected to a network (connection can be wired or wireless). Network paths defined here will appear in the USB/Network path drop-down menu when using the Backup & Restore SciVault 2 database tool.

Add Network path

1. Select **+ New Path** to add a new entry box for a network path. Each entry will have a unique ID.
2. Enter the Network Path in the following format: \\IP Address of Server\Name of share drive\Name of folder on share drive. (from local control, tap field to display keyboard, tap **Done** key to close keyboard).
3. Enter a unique Path Name which will appear in the USB/Network path drop-down menu when exporting data.



Test Network path

1. After all information has been input, select **Test** to confirm connection and access to the network location.
2. Enter a Username and Password for the network you are trying to connect to and select **OK**.



The image shows a dark-themed dialog box titled "Authentication Required". It features a close button (X) in the top right corner. Below the title, there are two input fields: "Username:" and "Password:". The "Password:" field has a blue eye icon to its right, indicating a password toggle. At the bottom of the dialog, there are two buttons: "Cancel" and "OK".

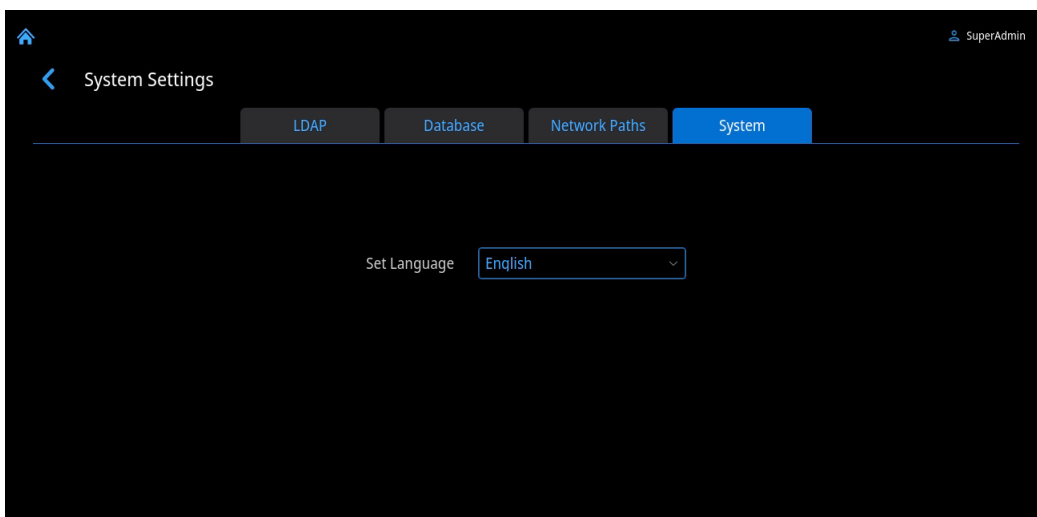
Edit or Delete Network path

- The Network Path and Path Name can be edited at any time by selecting the edit icon  to the right of the row and making any necessary changes, when finished select **Test** to reconfirm connection.
- Select  to the right of the row containing the Network Path to delete it, select **Confirm** to confirm deletion.

General System Settings

Set Language

Within the **System** tab, use the dropdown menu next to Set Language to determine the language settings for the SciVault 2 software.



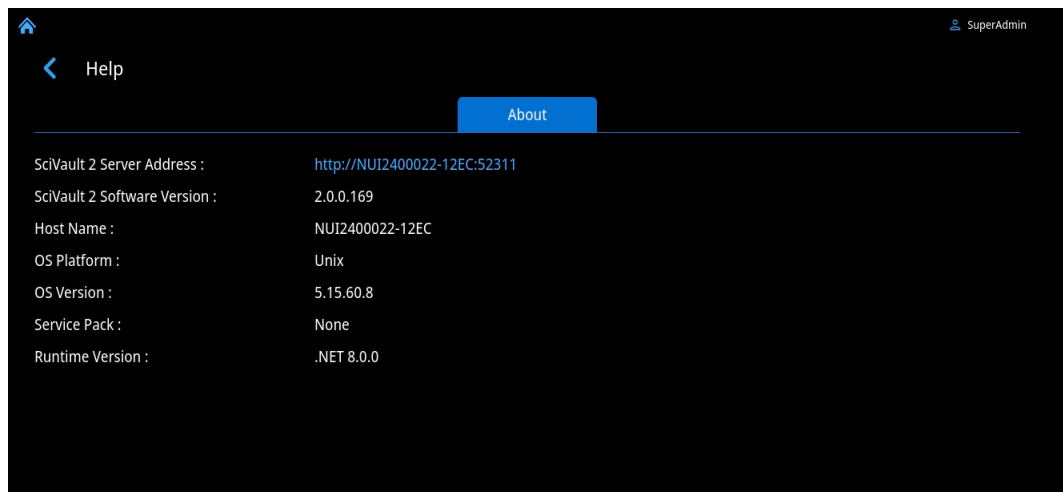
This page is intentionally blank.

Help

From the home screen of the SciVault 2 software, select **Help**. The Help section is split into two separate tabs: About and Documentation.

About

Access the **About** tab within Help to view/copy the SciVault 2 Server Address and to view the SciVault 2 Software Version, the name of the instrument or computer that SciVault 2 is installed on, and additional information pertaining to the software version.



Documentation

Access the Documentation tab within Help to launch the user guide or other relevant documents.

