## **Installing Insight Pro with Security Suite**

# (Local Computer Installation)

## **Basic PC Prerequisites:**

- A computer supports to install 64-bit windows 10(Build 1607 or above) or Windows 11 operating systems.
- Windows 10/11 Enterprise and Windows 10/11 Professional are recommended Windows versions.
   Minimum hardware configuration:
  - Intel Core i5 (6 cores, 3.3 GHz)
  - 8 GB RAM with system managed memory enabled
  - 500 GB Hard Drive
- Minimum computer resolution display 1366 × 768.
- Current user has administrative privilege to install system and services. Please contact your IT administrator for helps if you don't have administrative privilege.

## Pre-installation Tasks:

The following tasks should be completed before installing the Insight Pro software on a single computer.

- Save your works and close all other running applications
- Uninstall any previous version of Insight software
- Create a dedicated windows local user account to run the Audit Log service (See Appendix A below for instructions to establish this account and setting it's policies. Once that has been created, return to the next step)

#### To proceed you will need the "log-in" credentials to that service account.

Installing any version of Insight Pro prior to version 1.8 will require internet access for the PC for the install. This can be disconnected after the installation if desired.

## Software Installation:

1) Logged in as a Local Admin, insert the DVD or USB drive and open to the root directory. Double click on Start to begin the installation.



2) An installation screen will be prompted as below. Click Install

	thern	nosci	entific	
	Thermo	o Scientific Ins	ight Pro	
Install		Release Notes		Browse
Exit				

3) When this second screen appears Click>Software

Note: Drivers will be installed with the software. The option in this screen is for installing/reinstalling drivers if needed at some point, but should not be needed for the initial software installation.

t	hermoscientific	
	Thermo Scientific Insight Pro	
Software	Drivers	CUE Tutorials
Exit		Back

4) A screen will appear with the License Agreement.

Accept the license and proceed

portant: ease read the following information carefully.	SCIENTIFI
You must accept the End-User Software License Agreement before you may the terms and conditions of the End-User Software License Agreement, you	install this product. If you do not accept should choose Cancel.
<b>Thermo Fish</b> S C I E N T I F	
THERMO FISHER SCIENTIN END-USER SOFTWARE LICE AGREEMENT	FIC INSE
Please read this document carefully. This End-User Softw "Agreement") is a legal contract between you (hereafter "Licensee") and Thermo Electron Scientific Instruments LLC By installing, breaking any seals of, and/or using the Therm constructions and microanalysis, instrumentation, software	rare License Agreement (the in this Agreement "you" or ; ("Thermo Fisher Scientific"). no Fisher Scientific molecular a and the publiched user
O I do not accept the terms in the license agreement.	

5) A screen will appear with Customer info. Enter User and Company names. Select Typical install as the Installation Option which will install all the components of the Suite.

ielect an installation option. Click Next.	SCIENTIFIC
Customer Information	
User name: Customer	
Company name: Thermo Fisher	
Installation Options	
O Custom - Lets you select products and set op	tions.

6) The next screen to appear allows for the choice of a Network installation of the Security Suite or Local PC installation. Choose Local PC Installation by clicking on the picture



7) When this below Data Storage Service Configuration screen appears enter the name of the Service account you set up previously. Type the account or Click Browse and locate the service account. Enter the Password twice. Click >Next

Note: For Insight Pro, entering the credentials here does not set anything up for Insight Pro. This Security Suite is used in a number of applications and most of those, use this Data Storage Servie configuration. However, you cannot proceed with this installation without populating these fields.

ecify the account in	ormation to use for secure data storage. Click Next.	SCIENTIFIC
Data Storage Servi Specify the account write access to all for Account name:	ce Credentials t name and password to use for secure data storage. This olders used for secure data storage.	account must have Browse
Password:		

#### 8) Click "Next >" button.



9) Wait for software installation to complete. When the Audit Log Service Database Configuration screen appears, Leave the Database dropdown as the default (SQLite) Click>Edit

Database engine:	SQLite		
Audit Log Service credentials:	Edit		
	1 <del>5</del>		

10) Click on Browse to select the Service account from the next screen.

	100000000000000000000000000000000000000	

11) Type the name of the service account in the "Enter the object name to select field", the click on check names. The field should then populate with the PC Name and service account name. Click>OK

elect this object type:		
User or Built-in security principal	Object Type	s.,
rom this location:		
DESKTOP-DS5JTVO	Locations.	
inter the object name to select ( <u>examples</u> ):		
	Check Nam	

12) Back at this screen, enter the password for that account twice, then Click>OK

Jsername:	OMCSVS	Browse
<sup>p</sup> assword:		
/erify password:		

13) Once back to this screen, clcik on Apply. You should see the word "Succeeded" appear indicating this was setup correctly.

Database engine:	SQLite		199
Audit Log Service credentials:	Edit		

14) You should see the word "Succeeded" appear indicating this was setup correctly. Click on the "X" upper right of this dialog box to close and the installation should indicate it is complete. This will take a few minutes to wrap up as the software finishes the setup

📔 Audit Log Service Database	Configuration		×
Database engine:	SQLite		Ŷ
Audit Log Service credentials:	Edit		
	Status: Succeeded		
	Apply		

15) When the software is finished setting up, Thermo Security Administration will automatically open and prompt for credentials. (current admin log in). Enter those and review the present settings. (The password cannot be blank / empty)

Note: By default, the Security Policies will all be in their selected state and access will be such that any authenticated user log in in will be able to run Insight Pro logging into it with their PC log in credentials. With respect to the Thermo Security Administrator program, by default anyone who is an Administrator on the PC will be able to log in an open that program

User name:	Administrator
Password:	alcalcalcalcalcalcalcalcalcalcalcalcalca

Once in Thermo Security Administrator Click File->Exit menu or Close button at the top right-hand corner of main window.

Note: This step is mandatory to run Insight Pro software with local security. Otherwise, you will see the message "<u>The security server has not been configured for this application</u>." when you try to log in Insight Pro software.

\*\* At this point, you should Restart the PC \*\*

16) To open Insight Pro, double click on the Thermo Insight Pro icon on the desktop



The following splash screen will appear. Enter the credentials for the currently logged on user. Remember: This Security Suite utilizes the name and password of the current user. If another user is presently logged in that wishes to use Insight Pro, the current user will need to log off and the next user log in and then they will then be able to use their credentials to log into the program.

TIP: Users should always be "Logging off / Signing out" when fishished with the PC or when another user needs to log on. Never use "Switch User" feature of Windows. This can result in multiple instances of these programs being open under different users resulting in performance issues.

×
Insight Pro
thermoscientific
Welcome
User Name <b>UV</b>
Password
Login

## **Appendix A:**

## **Service Account Setup**

Security Suite requires a service account to store audit trail information in a secure manner.

This account is setup just like any other user account in Computer Management or Local Users and Groups management console.

This account should:

- 1. Have password expiration disabled
- 2. Be granted the "Log on as a service" right
- 3. Be denied the "Log on locally" and "Log on through Remote Desktop Services" rights

These steps (account Creation & Configuring Log on Rights for the account) are detailed below

#### Account Creation

- 1. Open the Local Users and Groups management console:
  - a. Press 💐 + R
  - b. Type *lusrmgr.msc*

10	Type th	ne name of a prog	ram, folder, docun	nent, or Interne
	resourc	ce, and Windows	will open it for you	
Open:	lusrm	gr.msc		
	190000000	-		
		OK	Cancel	Browse

Local Users and Groups (Loca	Name	Actions
Crowns	齸 Users	Local Users and Groups (Local)

2. Single click on the Users folder

- 3. Click <u>Action (menu item)→New user...</u>
- 4. Set up the Secure Data Storage service account:
  - a. Enter the <u>User name</u> (e.g. audit.log.service, insightSVC, etc.)
  - b. Enter the **Password** and **Confirm password**
  - c. Uncheck User must change password at next logon

New User		?	×
User name:			
<u>F</u> ull name:			
Description:			
Password:			
Confirm password:			
User must change password at next	logon		
User cannot change password			
Password never expires			

#### d. Check Password never expires

New User				?	×
<u>U</u> ser name:	data	a.storage.servi	ce		
<u>Full name:</u>					
Description:					
Password:		•••••	•		
<u>C</u> onfirm passwo	rd:	•••••			
User <u>m</u> ust cl	hange p	password at ne	ext logon		
User cannot	chang	e password			
Password ne	ever exp	pires			
Account is d	lisa <u>b</u> led				
Help			Create	Clg	ose

- 5. Click Create
- 6. Click Close
- 7. Close the Local Users and Groups window

# Configure Log on Rights

1. Open the Local Group Policy Editor management console:

Image: Second	b.	Type <i>gpedit.msc</i>		
C. Click OK Local Group Policy Editor File Action View Help Computer Configure Software Settings Windows Settings Mundows Settings		Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.		
<ul> <li>c. Click OK</li> <li>Local Group Policy Editor</li> <li>Ele Action View Help</li> <li>Computer Policy</li> <li>Computer Policy</li> <li>Computer Configuration</li> <li>Software Settings</li> <li>Windows Setting</li> <li>Software Settings</li> <li>Windows Setting</li> <li>Administrative Te</li> </ul>		OK Cancel Browse		
<ul> <li>Computer Policy</li> <li>Computer Configura</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Software Settings</li> <li>Software Settings</li> <li>Software Settings</li> <li>Windows Setting</li> <li>Maministrative Te</li> </ul>	C. Local G <u>File</u> <u>A</u> ction	Click OK roup Policy Editor on <u>View H</u> elp	1 <u>1111</u>	- Contra
<ul> <li>Local Computer Policy</li> <li>Computer Policy</li> <li>Software Settings</li> <li>Administrative Te</li> <li>Software Settings</li> <li>Software Settings</li> <li>Windows Setting</li> <li>Administrative Te</li> </ul>	(= = ) [			
	> 2 5 > 2 1 > 2 1 = 2 1 = 2 1 = 2 1 = 2 1 = 2 1 =	Select an item to view its description. Name Windows Settings Vaministrative Te Configuration Software Settings Vindows Setting Administrative Te		
	<	Extended \Standard \		

2. Navigate to Computer Configuration → Windows Settings → Security Settings → Local Policies → User Rights

Local Group Policy Edito	Č-		×
File Action View Help			
🔶 🏟 🖄 📰 🗙 🗟	? 💵		
ocal Computer Policy Computer Configuratio Software Settings Windows Settings Signa Name Resolution	Policy Access Credential Manager as a trusted caller Access this computer from the network Act as part of the operating system Add workrations to domain	Security Setting Everyone,Administrators	Ŷ
<ul> <li>Scripts (Startup/:</li> <li>Epologed Printer</li> <li>Security Settings</li> <li>Account Poli</li> <li>Local Policie</li> <li>Audit Pol</li> <li>Local Policie</li> <li>User Righ</li> <li>User Righ</li> <li>Windows Det</li> <li>Network List</li> </ul>	Adjust memory quotas for a process     Adjust memory quotas for a process     Allow log on locally     Allow log on through Remote Desktop Services     Back up files and directories     Bypass traverse checking     Change the system time     Change the time zone     Create a pagefile     Create a token object	LOCAL SERVICE, NETWO Guest, Administrators, Us Administrators, Remote Administrators, Backup Everyone, LOCAL SERVIC LOCAL SERVICE, Admini LOCAL SERVICE, Admini Administrators	
<ul> <li>Network List</li> <li>Public Key P(</li> <li>Software Res</li> <li>Application (</li> <li>P Security P(</li> <li>Advanced At</li> <li>Policy-based Qo</li> <li>Administrative Temp</li> </ul>	Increate a token object         Create global objects         Create grownanent shared objects         Create symbolic links         Debug programs         Deny log on as a batch job         Deny log on as a service	LOCAL SERVICE,NETWO Administrators Administrators Guest	
< >	Deny log on locally	log.service,file.service,G	~

3. Select Log On As A Service and open its properties

Deny log on locally P	operties	?	×
Local Security Setting	Explain		
Deny log o	n locally		
Guest		 	
Add User or Gro	up		
		 1	

4. Click Add User or Group...

select osers of oloups		
Select this object type:		
Users or Built-in security principals		Object Types
rom this location:		
DESKTOP-QQFM1GP		Locations
Enter the object names to select (examples):		
		Check Names
	the second se	

5. Enter the account name(s) you created previously separated by a semicolon

	• • •	,	•
Select Users or Groups			
Select this object type:			
Users or Built-in security principals			Object Types
From this location:			
DESKTOP-QQFM1GP			Locations
Enter the object names to select (exa	imples):		
file.service;log.service			Check Names
			1.1
<u>A</u> dvanced		OK	Cancel
lick <b>OK</b>			
Deny log on locally Properties			? ×
Local Security Setting Fundain			
Deny log on locally			
file.service Guest			
log.service			
P.			
Add User or Group	Remove		
Provide statements and statem	CH CAPELON COLOR DE LA		
	OK	Connel	Aminto
	OK	Cancel	Apply

7. Click OK

6.

- 8. It is recommended that you Repeat Steps 2 through 7 for **Deny Log On Through Remote Desktop Services** and **Deny Log On Locally**
- 9. Close the Local Group Policy Editor window