Setting Up RESULT Software for Security Administration

Part of Thermo Fisher Scientific

Thermo SCIENTIFIC

The information in this publication is provided for reference only. All information contained in this publication is believed to be correct and complete. Thermo Fisher Scientific shall not be liable for errors contained herein nor for incidental or consequential damages in connection with the furnishing, performance or use of this material. All product specifications, as well as the information contained in this publication, are subject to change without notice.

This publication may contain or reference information and products protected by copyrights or patents and does not convey any license under our patent rights, nor the rights of others. We do not assume any liability arising out of any infringements of patents or other rights of third parties.

We make no warranty of any kind with regard to this material, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Customers are ultimately responsible for validation of their systems.

For Technical Support, please contact:
Thermo Fisher Scientific
5225 Verona Road
Madison, WI 53711-4495 U.S.A.
Telephone: 1 800 532 4752
E-mail: us.techsupport.analyze@thermofisher.com
World Wide Web: http://www.thermo.com/spectroscopy

For International Support, please contact:
Thermo Fisher Scientific
Telephone: +1 608 273 5017
E-mail: support.madison@thermofisher.com
World Wide Web: http://www.thermo.com/spectroscopy

269-238302, Rev A

Contents

This page intentionally left blank.

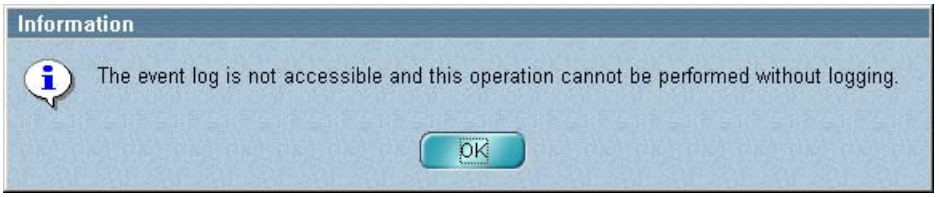
Introduction

This manual explains how to use the Thermo Scientific Security Administration software to set up special system policies and other security features for your RESULT Integration or RESULT Operation software. These features are used as an addition to the standard security features of RESULT software. Use this manual in conjunction with the *Security Administration User Guide*, which explains how to use the general features of your Security Administration software.

See the manual titled *Installing Your Software* for instructions for installing Security Administration software.

Security Administration software uses the Event Log service in Windows® to record client application operations, or "events," in a log that you can view with Event Viewer. See the "Event Logging" chapter in this manual and "Event logging" in the "Overview of Windows Administration" chapter of the *Security Administration User Guide* for details.

Note If you are using a networked computer and lose communication between it and the computer on which Thermo Security Service is running, an error message will appear when you attempt to save a file whose type is controlled by Security Administration software:



Choose OK and then restore communication by securing cables, etc. ▲

Manual conventions

This manual includes safety precautions and other important information presented in the following format:

Note Notes contain helpful supplementary information. ▲

Notice Follow instructions labeled "Notice" to avoid damaging the analyzer hardware or losing data. ▲

Questions or concerns

In case of emergency, follow the procedures established by your facility. If you have questions or concerns about safety or need assistance with operation, repairs or replacement parts, you can contact our sales or service representative in your area or use the information at the beginning of this document to contact us.

Event Logging

The Security Administration and RESULT software track changes to a variety of file types. These change events are automatically logged by the Windows Event Viewer once Security Administration and RESULT software have been installed. You can view these events by starting Event Viewer and clicking the Thermo Scientific icon in the navigation pane. The sources of events that are logged include the following:

Admin – Tracks changes to Security Administration software's security database.

Thermo Security Service – Tracks activity of and changes to Thermo Security Service.

Thermo Log Service – Tracks changes to files that are registered to RESULT software. This tracking occurs whether or not RESULT software is running. The types of files whose changes are tracked is determined by the extensions specified by the .xml file.

RESULT – Tracks activity in RESULT software and changes to files while RESULT software is running.

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

Admin
Access control item changed
Policy group added
Policy group changed
Signature reason added
Signature reason changed
Signature reason deleted

Thermo Security Service
Service started
Security database opened
Service could not start
Service stopped

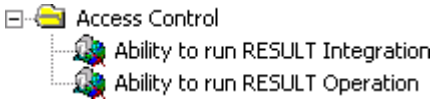
Thermo Log Service
File created
File modified
File deleted
File renamed

RESULT
File modified with comments
File created with comments
File modified
File created
General information
Verify signature failed
Sign file succeeded
Sign file failed

Note The specific file types that are audited by RESULT software and Thermo Log Service include files with the following extensions: .wfl, .qnt, .lbd, .lbt, .spa, .jdx, .spc, .csv, .srs, .sri and .cnc. ▲

Controlling Access to RESULT Software

The Access Control features of Security Administration software let you set the rights of individual users or groups of users to use RESULT Integration and RESULT Operation software. When you open the Access Control folder for RESULT software, the items shown below appear:



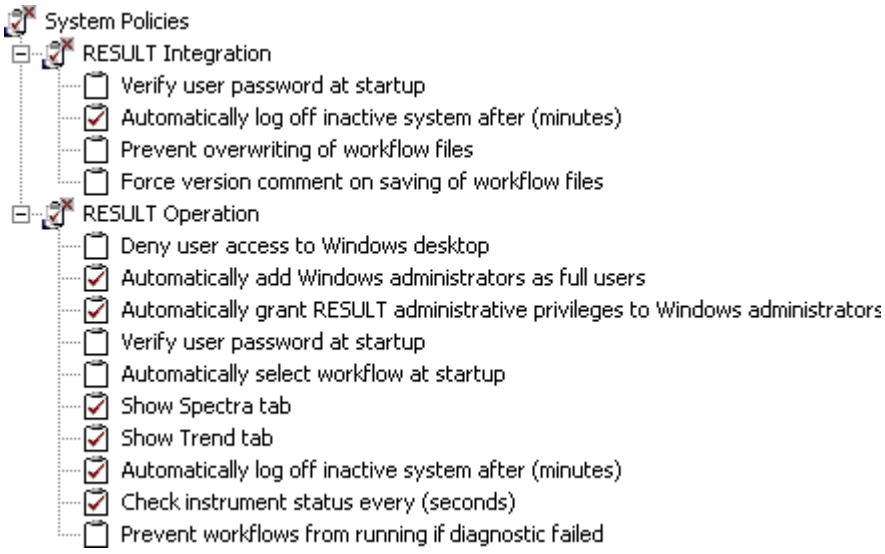
These items let you specify which users can run the RESULT applications. If a user has not been granted the ability to run an application, an error message appears when the user attempts to start it.

See "Controlling access to client application features" in the "Using Security Administration" chapter of the *Security Administration User Guide* for instructions for using the Access Control features.

When you are finished specifying access control, save your settings in the security database. See "Saving your security policy settings" in the "Using Security Administration" chapter of the *Security Administration User Guide* for details.

Setting System Policies for RESULT Software

The System Policies features of Security Administration software let you set many system policies controlling the use of RESULT Integration and RESULT Operation software. For example, you can prevent the overwriting of workflow files or require users to enter a comment when saving a workflow. The sections that follow explain how to set these policies.



Note Some system policies correspond to similarly named options in RESULT software; that is, they are designed to control the same aspect of software operation. In these cases, the system policy setting supersedes the RESULT option setting. The affected option appears in RESULT software but is unavailable. ▲

See "Setting system policies for the client application" in the "Using Security Administration" chapter of the *Security Administration User Guide* for instructions for using the System Policies features. The rest of this chapter provides information that is specific to setting system policies for RESULT software.

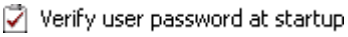
When you are finished setting the policies, save your settings in the security database. See “Saving your security policy settings” in the “Using Security Administration” chapter of the *Security Administration User Guide* for details.

RESULT Integration software policies

The next sections describe how to add security control of RESULT Integration software by setting system policies in Security Administration software. (Unlike RESULT Operation software, RESULT Integration software does not include standard security features for controlling the use of the software.)

Verifying the user’s password when RESULT software starts

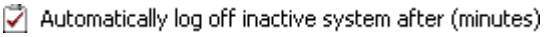
Select the Verify User Password At Startup policy to require that users in the specified policy groups enter the correct user password when RESULT Integration software starts.



Here is an example of a prompt requesting a password:

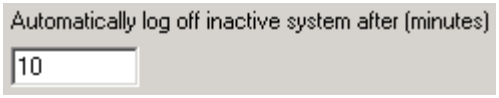
Automatically logging off an inactive system

Select the Automatically Log Off Inactive System After (Minutes) policy to automatically exit RESULT Integration software and log the current user off the system when it is inactive for a specified number of minutes.



This policy helps prevent unauthorized users from using the system when it is unattended. To resume working with RESULT Integration software, the authorized user must log on.

Type the desired whole number of minutes in the text box that appears when you select the policy.

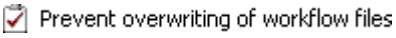


The setting will take effect after you save the security database and log off and a user in the specified policy group logs on.

If you enter zero, the policy will have no effect.

Preventing the overwriting of workflow files

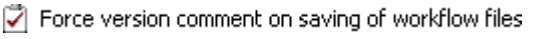
Select the Prevent Overwriting Of Workflow Files policy to prevent users in the specified policy groups from overwriting RESULT workflow files (.wfl extension) when saving them.



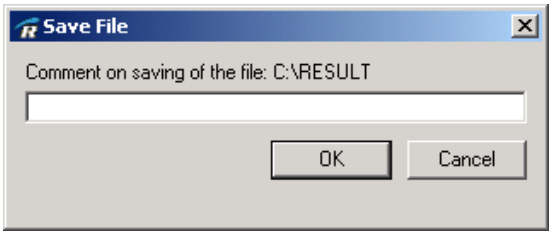
An error message appears when the user attempts to overwrite a workflow file.

Requiring a version comment when a workflow file is saved

Select the Force Version Comment On Saving Of Workflow Files policy to require users to enter a comment when saving workflow files (.wfl extension).



Here is an example of a prompt requesting a comment:

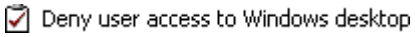


RESULT Operation software policies

The next sections describe the system policies for RESULT Operation software. These policies are used as an addition to the standard security features of RESULT Operation software.

Denying users access to the Windows desktop

Select the Deny User Access To Windows Desktop policy if you want users in the specified policy groups to be unable to view or access features of the Windows desktop. This prevents them from using shortcuts, browsing for files, accessing items in the Start menu, and using any other features of the Windows desktop.



If you select this policy, we recommend disabling the Verify User Password At Startup policy. See "Verifying the user's password when RESULT starts" for more information.

Automatically adding Windows administrators as full users

Select the Automatically Add Windows Administrators As Full Users policy if you want users with Windows administrative-level privileges to the workstation to be full users of RESULT Operation software.

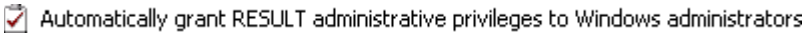
This policy adds these users to the RESULT Operation user list and ensures that they can always gain access to RESULT Operation software.

Notice If both this policy and the Automatically Grant RESULT Administrative Privileges To Windows Administrators policy (described in the next section) are disabled, you run the risk of not having any user able to access the administrative features of RESULT software. If this happens, select at least one of these policies. ▲

Note Disabling the two policies mentioned above does not automatically remove Windows administrators from the RESULT user list, nor does it un-assign the administrative-level privilege from users who have already been assigned that privilege. To remove users and privileges, a RESULT administrator must make these changes to each user through the Manage Users dialog box. See "Chapter 5 Managing Users" in the *RESULT User Guide* for more information. ▲

Automatically granting RESULT administrative privileges to Windows administrators

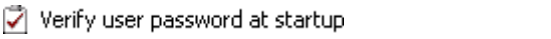
Select the Automatically Grant RESULT Administrative Privileges To Windows Administrators policy if you want to grant RESULT administrative privileges to all Windows administrators who are added to the RESULT user list.



Note See the preceding section for information about the effects of disabling this policy and the Automatically Add Windows Administrators As Full Users policy. ▲

Verifying the user's password when RESULT software starts

Select the Verify User Password At Startup policy to require that users in the specified policy groups enter the correct user password when RESULT Operation software starts. The software verifies that the user's logon name is on the RESULT user list and that the password matches the user's Windows password.

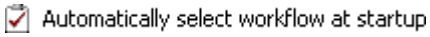


Here is an example of a prompt requesting a password:

If this policy is disabled, the software will verify only that the logged-on user is on the RESULT user list. Selecting this policy allows an extra level of security for RESULT Operation software. However, if your system is configured to start RESULT Operation software automatically or restart the system when a user logs off RESULT software, you may want to disable this policy to avoid the redundancy of requiring users to enter their Windows password twice when starting the system. We also recommend disabling this policy if the Deny User Access To Windows Desktop policy is selected (see "Denying users access to the Windows desktop").

Automatically selecting a workflow when RESULT software starts

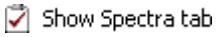
Select the Automatically Select Workflow At Startup policy if you want the Select Workflow dialog box to appear automatically when RESULT Operation software starts. The dialog box lets the user select an appropriate workflow.



If this policy is disabled, the user can load a workflow with the Select Workflow button on the RESULT Operation main window toolbar.

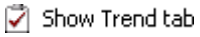
Displaying the Spectra tab

Select the Show Spectra Tab policy to display the Spectra tab in RESULT Operation software so that the user can view the spectral data as well as the report data (on the Report tab) during data collection. (When data collection is finished, the Report tab is displayed automatically.)



Displaying the Trend tab

Select the Show Trend Tab policy to display the Trend tab in RESULT Operation software.



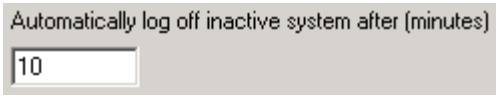
This tab lets the user view a series of data measured from one or more workflows over a period of time. See "Viewing trend data while running a workflow" in "Section 3 RESULT Operation Software" in the *RESULT User Guide* for more information.

Automatically logging off an inactive system

Select the Automatically Log Off Inactive System After (Minutes) policy to automatically exit RESULT Operation software and log the current user off the system when it is inactive for a specified number of minutes.

This policy helps prevent unauthorized users from using the system when it is unattended. To resume working with RESULT Operation software, the authorized user must log on.

Type the desired whole number of minutes in the text box that appears when you select the policy.

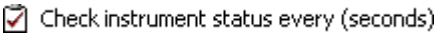


The setting will take effect after you save the security database and log off and a user in the specified policy group logs on.

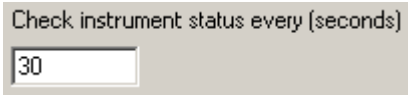
If you enter zero, the policy will have no effect.

Automatically checking the status of the analyzer

Select the Check Instrument Status Every (Seconds) policy to automatically check the operation status of the analyzer at a specified interval when it is used by a user in the specified policy groups. The status is displayed by the Instrument Status indicator in the RESULT Operation main window.



Specify the interval by typing the desired whole number of seconds in the text box that appears when you select the policy.

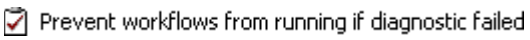


The setting will take effect after you save the security database and log off and a user in the specified policy group logs on.

If you enter zero, the policy will have no effect.

Preventing the running of workflows when the analyzer is not operating properly

Select the Prevent Workflows From Running If Diagnostic Failed policy to prevent users in the specified policy groups from running workflows when the analyzer has failed a diagnostic test. (The software automatically checks the operation of the analyzer to determine its status.)



Assigning Signature Meanings

The Signature Meanings features of Security Administration software let you specify the meanings that will be available for electronic signatures supplied by specified users of RESULT software. For example, you could set the Signature Meanings features so that only a particular user—for instance, a manager—is allowed to sign a file with the "Approval" meaning. The illustration below shows the available signature meanings for RESULT software:

This list appears when you click the Signature Meanings icon for RESULT software in the navigation pane the first time you use the Security Administration program. If you have made changes to the list of signature meanings, the available meanings in your software may be different. See "Assigning signature meanings" in the "Using Security Administration" chapter of the *Security Administration User Guide* for general instructions for using the Signature Meanings features to change the available meanings or to specify which users can select each meaning when signing a file.

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

"Authorship" indicates that the user signing the file is the person who created it.

"Approval" indicates that the user signing the file has reviewed it and approved it for use.

"Review" indicates that the user signing the file has reviewed it.

"Revision" indicates that the user signing the file has changed it.

Setting File Permissions

After you have set the security policies for your system, set file permissions to control which Windows file operations—such as overwriting a workflow file—can be performed by specified users.

The procedures in the next sections explain how to locate the features for setting file permissions in Windows software. It is your responsibility to set permissions as necessary to comply with 21 CFR Part 11 or other security requirements of your organization.

Setting file permissions in Windows

Follow these steps:

1. **Log onto the system as an administrator.**

2. **Navigate to the C:\RESULT Data\Archive folder.**

   If your local disk is designated by a letter other than "C," use the appropriate letter instead.

3. **Right-click the Archive folder and choose Properties from the shortcut menu.**

   The Properties dialog box appears.

Note The setting of the Read-only check box on the General tab does not necessarily reflect the file permission settings specified with the Security tab (see the next steps). ▲

4. **Click the Security tab.**

Note If you are using a stand-alone or workgroup computer, the Security tab may not appear in the dialog box. In this case follow these steps to display the Security tab:

In Windows XP:

a. Open the Windows Control Panel.
b. If you are not using category view, choose Switch To Category View.
c. Choose the Appearances And Themes category. The Appearances And Themes window appears.
d. Choose Folder Options in the right pane. The Folder Options dialog box appears.
e. On the View tab, uncheck Use Simple File Sharing (Recommended) in the Advanced Settings list.
f. Choose OK and then close the Appearances And Themes window. □

In Windows 7:

a. Open the Windows Control Panel.
c. Double-click Folder Options. The Folder Options dialog box appears.
d. On the View tab, uncheck Use Sharing Wizard (Recommended).
e. Click OK and then close the Control Panel window. ▲

5. **Click the Advanced button.**

   The Advanced Security Settings dialog box appears. It provides features for setting file permissions for users. Use the Help button (labeled "?") to view instructions for using features.

   You can see the current permissions for a user by using the Effective Permissions tab.

6. **Set the file permissions as desired and then choose OK.**

7. **Choose OK to close the Properties dialog box and then close My Computer.**

Index

T

V

W