



thermo scientific

Thermo Scientific Security Suite

Security Suite

User Guide

269-340000 Revision C • March 2020

ThermoFisher
SCIENTIFIC

© 2003–2020 Thermo Fisher Scientific Inc. All rights reserved.

Microsoft and Windows are either trademarks or registered trademarks 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 technical support, please contact: www.thermofisher.com

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	Introduction and Overview	3
Chapter 2	Install and Set Up Security Suite	4
	Local and Global User Groups and Rights.	4
	User Profiles	5
	Other Security Features	5
	Installation Options.	5
	Single Computer Installation.	6
	Distributed Installation	6
	Before Installation	6
	Create a Custom Database for OMNIC Paradigm Data (Optional)	7
	Create a Custom Database for the Audit Log (Optional)	8
	Create Network Authorization Groups (Optional)	9
	Install Security Suite Software	9
	Single Computer Installation	9
	Distributed Installation	10
	Update Instrument Application Software	11
Chapter 3	Set System Policies and Control Access to Application Features	13
	Navigate Security Administration Software	14
	Specify Access Rights for Protected Features	16
	Control Access to Application Features	16
	Add or Remove a User or Group for Access Control	18
	Grant or Deny Users Access to All Protected Features of an Application.	20
	Remove a User's Access Designation for all Protected Features of an Application.	20
	Replace a Group Name for All Protected Features of an Application	21
	Set System Policies for Security Suite Applications	23
	Set System Policies for a Policy Group	25
	Create, Edit, or Delete a Policy Group	25
	Add or Remove Users from a Policy Group	28

	Assign Signature Meanings to Security Suite Applications	29
	Default Signature Meanings	30
	View or Change Assignments of Signature Meanings	31
	Edit Signature Meanings	32
	Add an Application	33
	Remove an Application	33
	Set up Automatic Screen Lock	34
	Save Your Security Settings	35
	Print Security Settings	35
	Preview the Security Settings	35
	Set Print Options	36
	Print the Security Settings	36
Chapter 4	View and Manage the Audit Log	37
	About Audit Logs	38
	Reconfigure the Audit Log Database	40
	View the Audit Log	41
	Event Information	42
	Create, Sign, and Print Reports	43
	Set Audit Manager User Preferences	46
Chapter 5	Default Settings and Policies	48
	Default Access Control	48
	Security Administration	48
	Audit Manager	49
	OMNIC Paradigm Software	49
	Default System Policies	51
	Security Administration	52
	Audit Manager	52
	OMNIC Paradigm Software	52

Introduction and Overview

Thermo Scientific™ Security Suite software includes a suite of software applications designed to ensure the security and integrity of your spectral data and to provide a secure environment to help you meet the requirements of 21 CFR Part 11.

The Security Suite uses an event logging service to provide an audit trail of activities with your Thermo Scientific instruments. The service records Security Administration 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 Security Suite software in order to enforce the defined security settings.

The Security Suite includes four primary components:

- **Security Administration software** lets users, typically people designated as Security Administrator, define security settings for access control, auditing of electronic records, and control of electronic signatures. Typically, this software is installed on a network server or computer 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 Security Suite applications.
- **Audit Manager software** is used to view logged security events and to create reports of logged events. A copy of the Audit Manager is automatically installed on the same computer as the Security Administration software. The audit manager software can be installed on other systems on the network that have access to the audit manager database.
- **Thermo Scientific Security Service** runs as a service under the Windows operating system software and provides information for the security settings defined within the Security Administration program. The Security Service can service multiple simultaneous Thermo Scientific instrument applications running on different computers on the network.
- **Thermo Scientific Audit Log Service** writes logged events to the audit log database.

Install and Set Up Security Suite

Thermo Scientific Security Suite software can be installed on a single computer or on a distributed network. The distributed network allows you to manage the security of many instruments and store your data and audit log in a single, secure location.

Contents

- [Local and Global User Groups and Rights](#)
- [Installation Options](#)
- [Before Installation](#)
- [Install Security Suite Software](#)
- [Switch From a Single to a Distributed Installation](#)
- [Update Instrument Application Software](#)

Local and Global User Groups and Rights

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.

The IT Administrator can set up local or global user groups to manage users more efficiently. A local group is a group of users associated with a particular workstation. A global group is a group of users associated with a network domain, which can include more than one workstation. 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.

Local and global groups can be set up in User Manager 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 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.

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.

However, 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.

Installation Options

Install Security Suite software on a single computer or distributed on a network.

Single Computer Installation

With a single computer installation, each Thermo Scientific instrument will have all of the Security Suite components installed.

Note Single computer installations require an administrative login and password for each instrument computer. With a single computer installation,

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

Distributed Installation

With a distributed installation, multiple instrument computers are controlled by Security Administration software from a separate network location. The audit log database and storage database can be in the same or a separate shared network location.

Note

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

Before Installation

Before you install Security Suite software, you may need to carry out the following administrative tasks:

- (Optional) Create a custom database for OMNIC Paradigm data
- (Optional) Create a custom database for the audit log
- (Optional) Create network authorization groups
- (Required) Create a service account

Create a Custom Database for OMNIC Paradigm Data (Optional)

OMNIC Paradigm uses a secure database for storing spectra data, settings, and other data. Create a custom database if the default database (MariaDB) is unsuitable for your installation site.

If you set up a custom database, you will need the following information while you install Security Suite software.

Database name: _____
(for example, ParadigmData)

Database engine: Maria DB SQL Server Oracle Amazon Aurora
(Select one)

The following table lists supported database engines:

Database Engine	Supported Versions
Maria DB	<ul style="list-style-type: none"> • 10.3 • 10.2 • 10.1 • 10.0
SQL Server	<ul style="list-style-type: none"> • 2017 • 2016 • 2014 • 2012
Oracle	<ul style="list-style-type: none"> • 18c • 12c Release 2 • 12c Release 1 • 11g Release 2
Amazon Aurora	<ul style="list-style-type: none"> • MySQL 5.7 compatible • MySQL 5.6 compatible

Database version: _____

Database server name or URL: _____

Database port: _____

Use default port

Create a Custom Database for the Audit Log (Optional)

If you are using the default database (SQLite) on a single computer installation, you do not need to create a custom database.

Create a custom database for your audit log to meet your installation site's needs.

If you are setting up a custom database, you will need the following information while you install Security Suite software.

Database name: _____

(for example, Audit Log Database)

Database engine: SQL Server Oracle MariaDB SQLite
(Select one) (SQLite is appropriate for single computer installations only)

Note

- If using the SQLite database engine (appropriate for Single Computer configurations only), the Security Suite creates the Audit Log database automatically and sets appropriate access rights for the Audit Log Service account you specify. No other database information is required.

The following table lists database engines that are supported by the Thermo Scientific Audit Log Service.

Database Engine	Supported Versions
Maria DB	<ul style="list-style-type: none">• 10.2• 10.1• 10.0
SQL Server	<ul style="list-style-type: none">• 2016• 2014• 2012
Oracle	<ul style="list-style-type: none">• 12c Release 2• 12c Release 1• 11g Release 2

Database server name or URL: _____
(not required for SQLite)

Database port: _____
(not required for SQLite)

Create Network Authorization Groups (Optional)

Create network authorization groups, if desired, that will be used for security administration and secure instrument operation and then add user accounts to those groups. (If using the default Windows user groups (not recommended), then just add user accounts to those groups.)

Note

- For all distributed installation configurations, both authorization groups must be on the network domain. For single computer configurations, the authorization groups can be on the local computer. The default authorization groups (Administrators and Users) are on the local computer.
- Each group must include at least one user.

Security Administrators group name:

(will have Full Control access to Security Administration software)

Instrument Operators group name:

(will have limited access to Thermo Scientific instrument applications)

Install Security Suite Software

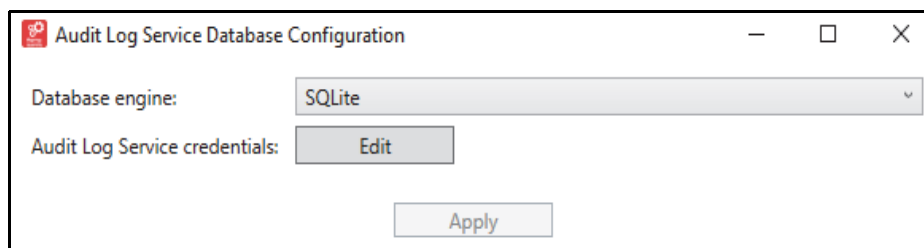
Installing Security Suite software requires you to run the Setup.exe file, specify a database for the audit log, and configure the security server in OMNIC Paradigm software.

Single Computer Installation

To install Security Suite in a single computer, run the installer and specify the appropriate security settings on each device.

❖ To install Security Suite software on a single computer

1. Insert the installation media and run start.exe. Follow the on-screen prompts.
2. When prompted, specify a database engine for Security Suite Audit Manager. SQLite is the default database engine.
 - a. To use the default, click Edit to enter Audit Log Service credentials, and then click Apply.



- b. Enter your username and password.
 - c. Click Apply.
 - d. When the dialog displays “Status: Succeeded” close the dialog to finish installation. Security Administration software opens automatically.
3. **Security administrator** (or IT administrator): In Security Administration software, review the access rights, policy permissions, and signature meanings for the Security Suite authorization groups and software. Reset access rights, policy permissions, and signature meanings as needed to ensure compliance for your facility. For details on settings and managing security settings, see Set System Polices and Control Access to Application Features.

Distributed Installation

When installing Security Suite software in a distributed configuration, the Security Administration and Audit Manager software are installed in a network location and a Security Client is installed on each instrument computer or workstation.

Before completing a distributed installation, create a service account. The service account should be a Windows domain user account to be used for the audit manager service. This account must have read and write access to the server and to any client devices.

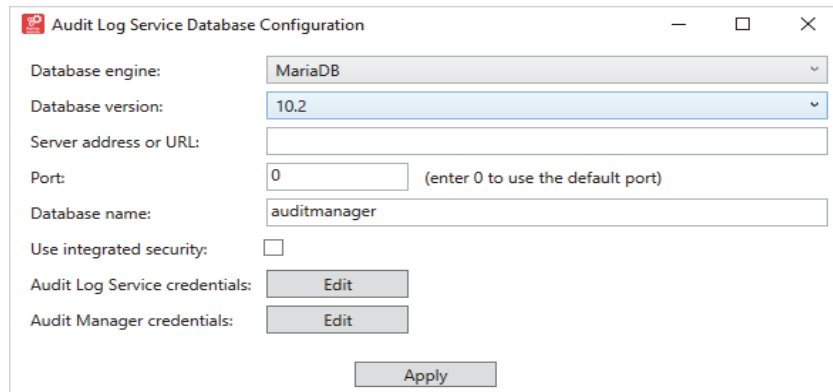
❖ To install Security Suite software in a distributed configuration

1. Install Security Server software.

The security server is the computer you will be using to manager security settings.

- a. Using the security server, insert the installation media.
- b. In the installation media files, open **DVD1** and run **Start.exe** and follow the on-screen prompts. DVD1 is used to install the security server software and DVD2 is used to install the security client on your Nicolet Summit spectrometer.
- c. When you are prompted to enter Audit Log Service Database Configuration information, select a database engine from the list and enter the details for the database you are using.

Note You cannot use the default SQLite database option with a distributed installation. You must edit the database settings to use a shared database on your network.



- i. Disable **Use Integrated Security**.
- ii. Click **Edit** to enter credentials for the Audit Log Service and Audit Manager service.
- iii. Click **Apply**.
- iv. When the dialog displays "Status: Succeeded" close the dialog to finish installation.

3. Install Security Client software.

The client refers to the Nicolet Summit Spectrometer that will have security settings enforced.

- a. On the client device, insert the installation media and open **DVD2**.
 - b. Run **Start.exe** and follow the on-screen prompts.
 - c. When installation is complete, open **OMNIC Paradigm software**.
 - d. Navigate to **Configure > Security Server**.
 - e. Enter the address or hostname of the security server and click OK. OMNIC Paradigm software will restart and will require a password.
4. **Security administrator** (or IT administrator): In Security Administration software, review the access rights, policy permissions, and signature meanings for the Security Suite authorization groups and software. Reset access rights, policy permissions, and signature meanings as needed to ensure compliance for your facility. For details on settings and managing security settings, see Set System Polices and Control Access to Application Features.

Update Instrument Application Software

If you update or install a new version of OMNIC Paradigm software, you may have to update your security settings in the Security Administration software.

See the release notes for the new version of OMNIC Paradigm for information on whether you need to update any Security Administration settings.

Set System Policies and Control Access to Application Features

Use Security Administration software to define security settings for access to application features, set system and application policies, and control electronic signatures.

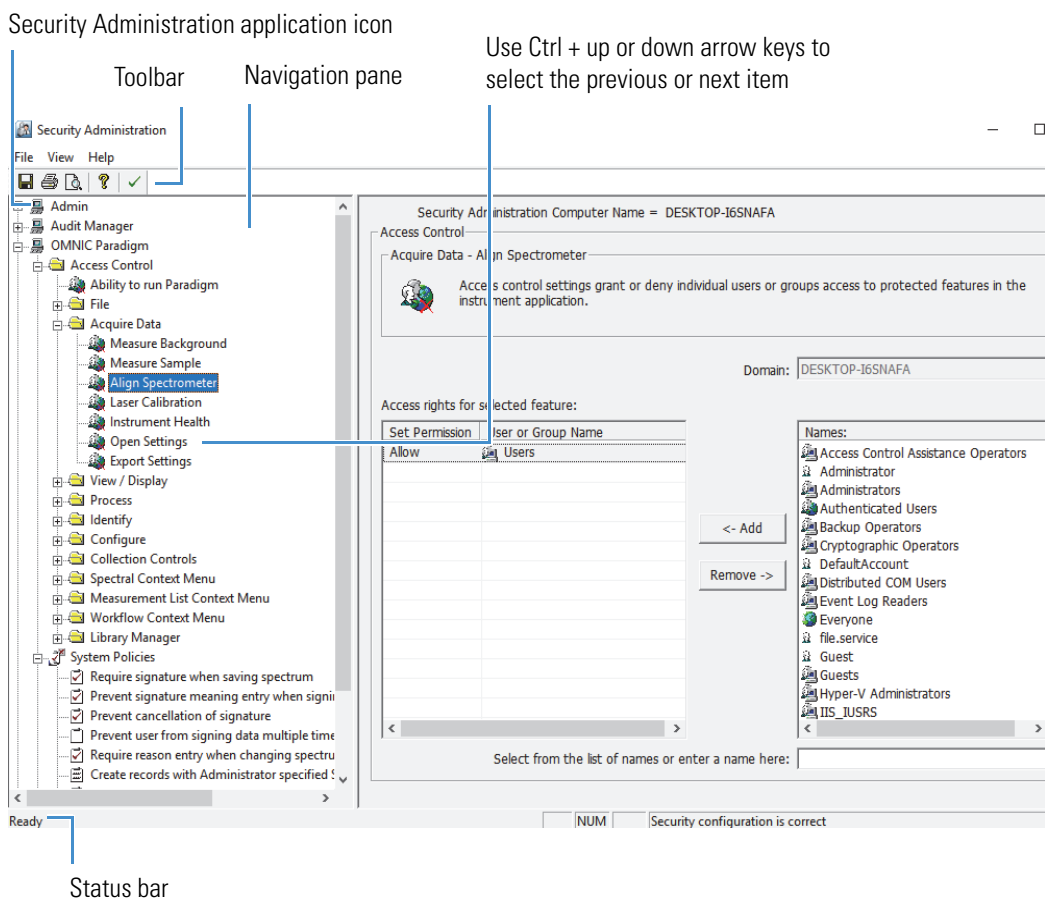
Contents

- [Navigate Security Administration Software](#)
- [Specify Access Rights for Protected Features](#)
- [Set System Policies for Security Suite Applications](#)
- [Assign Signature Meanings to Security Suite Applications](#)
- [Add an Application](#)
- [Remove an Application](#)
- [Set up Automatic Screen Lock](#)
- [Save Your Security Settings](#)
- [Print Security Settings](#)

Navigate Security Administration Software

When you start Security Administration software, the Security Administration window appears. Here is an example of the window showing security settings for an added application:

Figure 1. Security Administration main window








The navigation pane has a “tree” structure that is initially displayed with its sub-levels collapsed. Clicking the plus sign to the left of an icon or folder in the tree expands it to display more icons or folders in the tree. Clicking some icons in the tree displays features in the right pane, allowing you to set security features for Security Administration or another Security Suite application.

Display the Toolbar

Use Toolbar in the View menu to display or remove a toolbar containing buttons for choosing some commonly used menu commands. See the illustration in the preceding section for the location of the toolbar.

Toolbar options are described briefly below:

Table 1. Security Administration toolbar buttons

Toolbar button	Description
	Saves your security settings.
	Allows you to select a printer and print the security settings.
	Displays a preview of the security settings for review or printing.
	Opens the Help system for Security Administration software.
	Shows the current status of the Thermo Scientific Audit Log Service for the Security Suite software. A green check mark indicates the Audit Log service is installed and running correctly. A red “X” indicates the service is either not installed or not set up correctly.

Display the Status Bar

Use Status Bar in the View menu to display or remove a status bar showing status information such as the status of underlying Security Suite services. The status bar appears below the navigation pane.

Use the Keyboard to Select Items in the Navigation Pane

If you have selected a security feature for an application in the navigation pane (for example, a system policy), you can use **Select Previous** or **Select Next** in the View menu to select the previous item in the tree (if there is one) or hold down the Ctrl key and press the up or down arrow key.

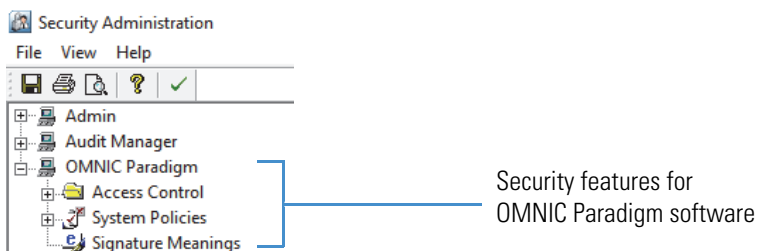
These keyboard shortcuts are useful when you are setting several access control features or system policies in sequence. You can quickly select the next (or previous) item in the tree using the keyboard with one hand and change the settings for that item using the mouse with your other hand.

3 Set System Policies and Control Access to Application Features

Specify Access Rights for Protected Features

Specify Access Rights for Protected Features

When you open the icon for a monitored application in the navigation pane of Security Administration software, three kinds of security features for the application become available in the navigation pane: Access Control, System Policies and Signature Meanings. Here is an example:



- Using **Access Control**, you can set the rights of individual users or groups of users to use the protected features of the application. See “Controlling Access to Application Features” for more information.
- With **System Policies** you can set policies covering such things as preventing the overwriting of files and requiring electronic signatures. See “Set System Policies for Security Suite Applications” for details.
- The **Signature Meanings** features let you specify the meanings that will be available for electronic signatures supplied by users of the system. See “Assign Signature Meanings to Security Suite Applications” for more information.

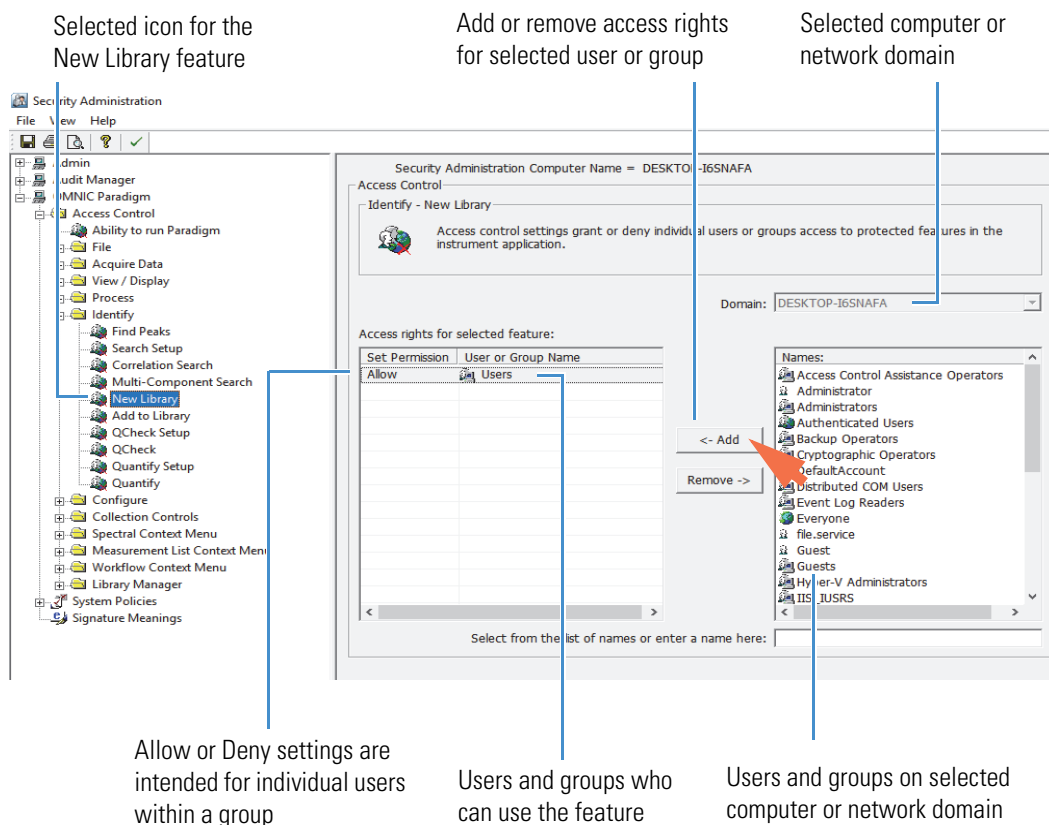
After you use these features to set security features for the Security Suite applications, choose **File > Save Settings** to save your security settings.

Note When using a network, changes to the access rights, system policies, or signature meanings on the central computer where the Security Administration program is installed are immediately used by all of the Security Suite applications and computers on the network.

Control Access to Application Features

Use **Access Control** to set the rights of individual users or groups of users to use the protected features of an application that has been added to the Security Administration program. A feature in the application will be available only if the logged-in user has the right to use it.

When you open the Access Control folder for the application by clicking its plus sign, a tree of folders and other items appears. Each item in the tree represents a protected feature or group of features in the application; that is, operations for which access control is available. If there is a plus sign to the left of a folder, the folder represents a group of features such as a menu of commands. When you open one of these folders by clicking its plus sign, a tree of icons appears. Here is an example showing a selected icon that represents the Delete Annotation command in a menu:

Figure 2. Specify who can access the features of your Security Suite applications

You can use the tools in the right pane to specify which users or groups can access the selected feature. For details, see “Specify Access Rights for Protected Features” and “Add or Remove a User or Group for Access Control” in this document. The tools provided depend on the application you are setting up.

Note You can use Add To All Access Control Items in the File menu to quickly grant or deny a user access to all the features of an application whose access is controlled by Security Administration software. See “Grant or Deny Users Access to All Protected Features of an Application” in this document for details.

Similarly, you can use Remove From All Access Control Items in the File menu to remove the grant or deny designation for a user from all the features of an application whose access is controlled by Security Administration software. See “Remove a User’s Access Designation for all Protected Features of an Application” for details.

3 Set System Policies and Control Access to Application Features

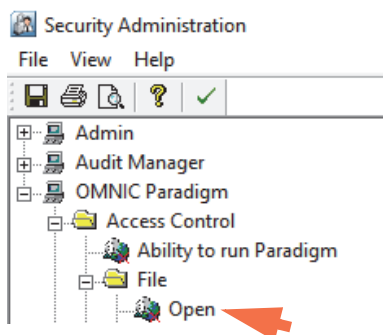
Specify Access Rights for Protected Features

Add or Remove a User or Group for Access Control

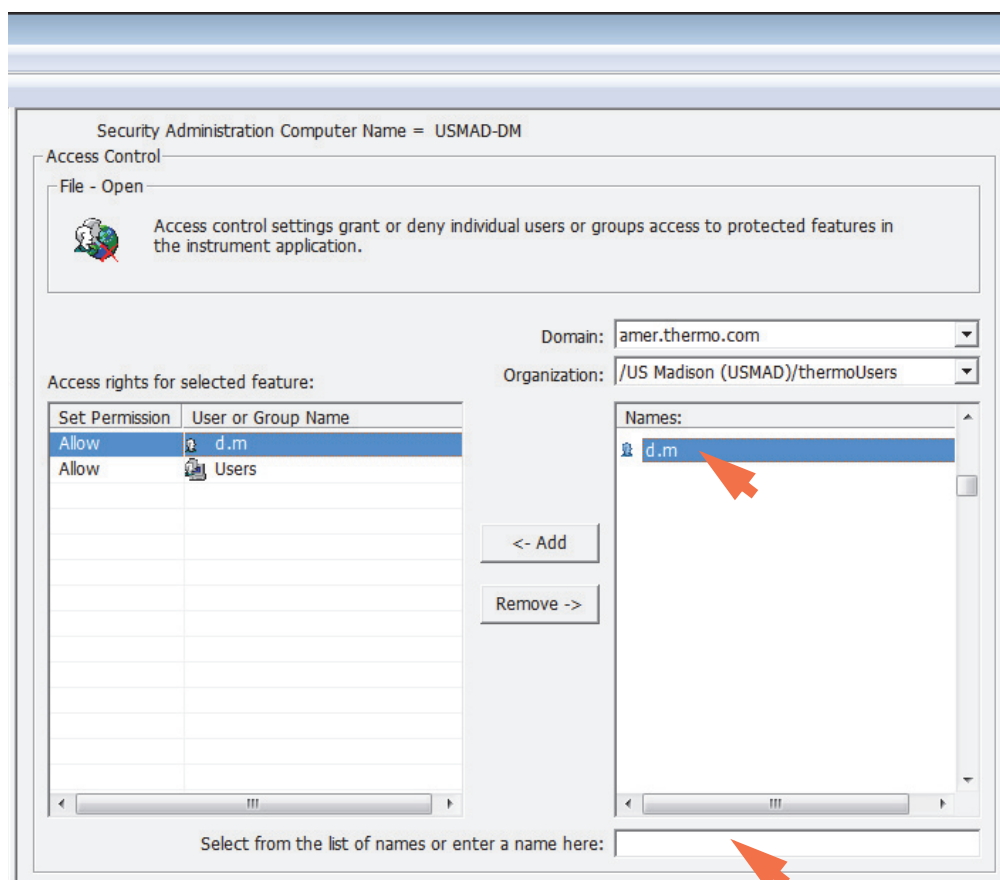
Use the tools in the right pane of the Security Administration main window to specify access for a user or group not listed in the Access Rights box for the Security Administration program for a feature or signature meaning in a Security Suite application.

❖ To add a user or group for access control

1. Select a feature under Access Control in the Security Administration navigation (left) pane. Here is an example:



2. Select the user or group you want to specify access for in the Names box on the right side of the right pane, or type it in the text box below the list.



If you type the name, use the following syntax:

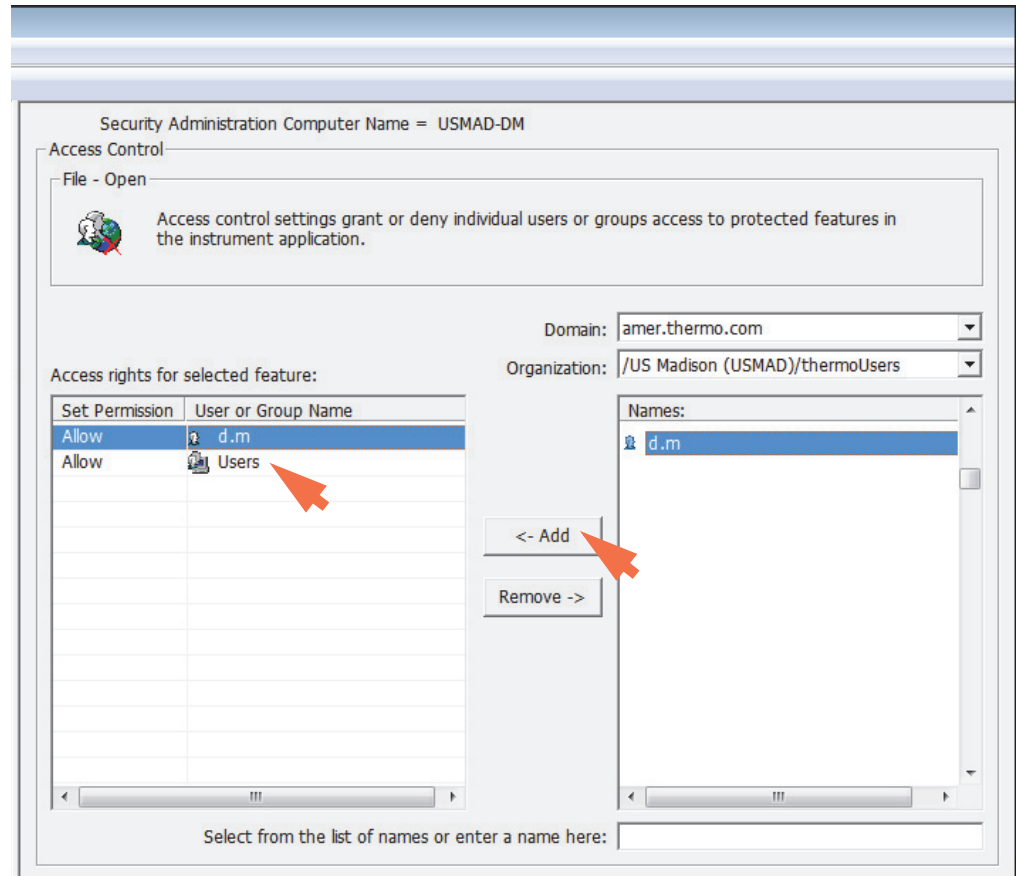
<domainname>\<accountname>

where “domainname” is the name of the domain location of the user or group, and “accountname” is the account name of the user or group.

Note Selecting a network or the local computer from the Domain box lists the users and groups on that network or computer in the Names box. If the selected Domain supports Active Directory, another list box appears that lets you choose an Organization. When you choose an Organization, it lists only the user and groups in that organization rather than all the users and groups on the domain.

3. Choose **Add**.

The user or group name is added to the Access Rights For Selected Feature box. The default access rights setting is “Allow.” You can then change the access specification by clicking the Allow cell and selecting Deny in the resulting list box.



To remove a user or group from the Access Rights box, select it and choose **Remove**.

This removes that user’s or group’s right for the selected feature. (There is an exception to this: If a removed user is a member of a group that has the right to start the software, the user will have that right.)

3 Set System Policies and Control Access to Application Features

Specify Access Rights for Protected Features

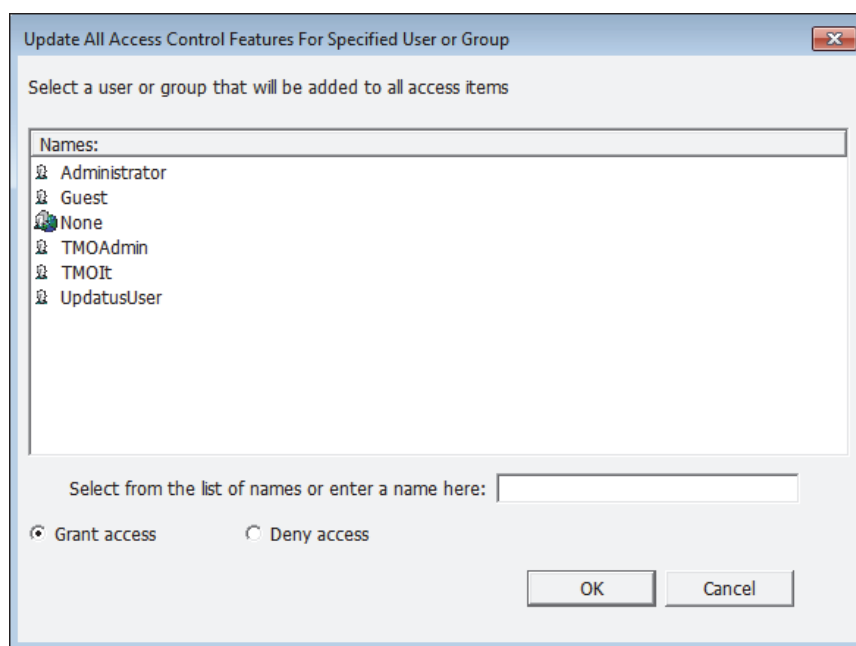
Grant or Deny Users Access to All Protected Features of an Application

Use Add To All Access Control Items in the File menu to quickly grant or deny a user or user group access to all of the protected features of an application. This has the same effect as granting or denying the user or user group access to all of the features individually.

❖ To grant or deny users access to all of an application's protected features

1. Select the application for which you want to grant or deny access by clicking its icon in the navigation pane.
2. Choose **File** (menu) > **Add To All Access Control Items**.

A box lists the available users and groups. Here is an example:



3. Specify the user or user group to whom you want to grant or deny access.
To do this, select an item in the list box or type a name in the text box.
4. Specify whether to grant or deny access by selecting **Grant Access** or **Deny Access**.
5. Choose **OK**.

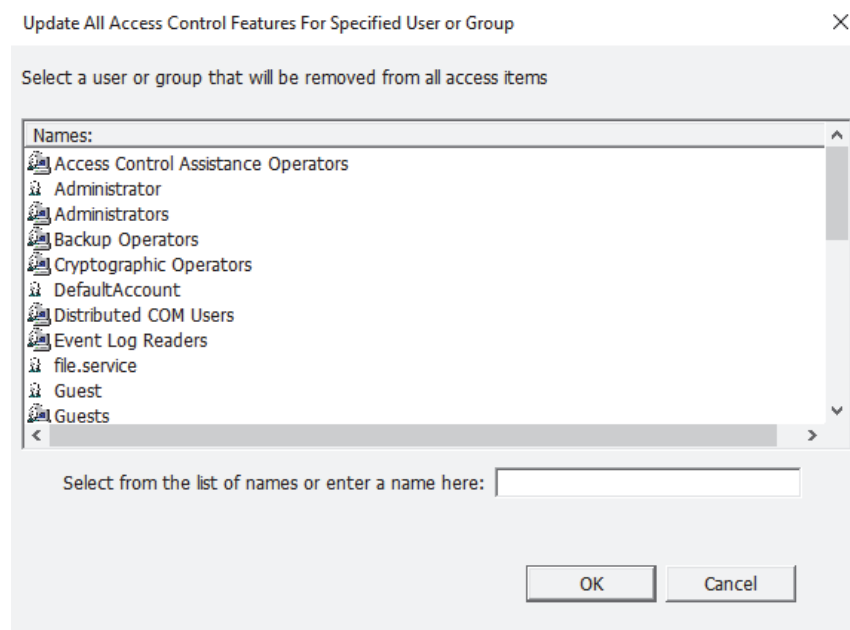
Remove a User's Access Designation for all Protected Features of an Application

Use Remove From All Access Control Items in the File menu to quickly remove a user's or user group's grant or deny designation for all of the protected features of an application. This has the same effect as removing the designation for all of the features individually.

❖ **To remove a user's access designation for all of an application's protected features**

1. Select the application for which you want to remove the user's access designation by clicking its icon in the navigation pane.
2. Choose **File** (menu) > **Remove From All Access Control Items**.

A box lists the available users and groups. Here is an example:



3. Specify the user or user group to whom you want to deny access.
To do this, select an item in the list box or type a name in the text box.
4. Choose **OK**.

Replace a Group Name for All Protected Features of an Application

The Security Suite's default user group names (Administrators and Users) are based on default authorization groups for administrators and users in Windows software. The default group names represent the two main groups of people who typically use the Security Suite software (that is, administrators of Security Administration software (Administrators) and instrument operators (Users)). The "Administrators" group has access to all of the capabilities of Security Administration software, including system configuration. The "Users" group has no access to the Security Administration program and limited access to the instrument applications that are controlled by Security Administration software (i.e., only those features needed to operate the instrument with secure data storage).

You can reassign the default group names in Security Administration software with group names that are more meaningful to your organization without affecting their current access control settings.

3 Set System Policies and Control Access to Application Features

Specify Access Rights for Protected Features

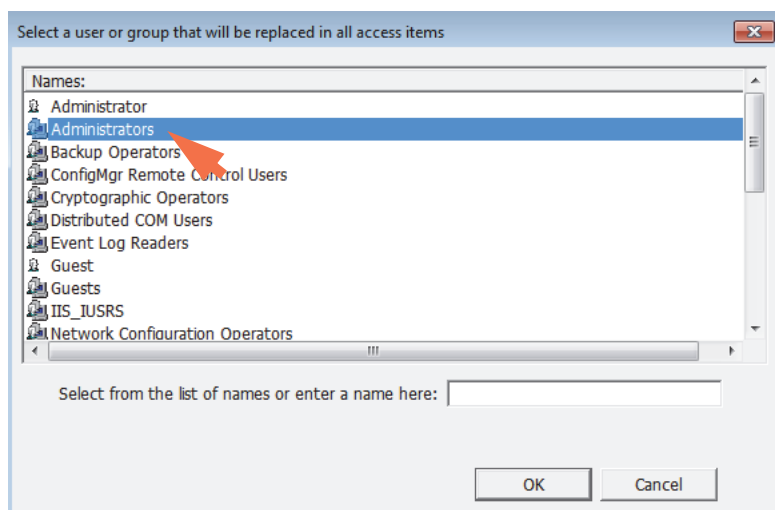
Note Before a new user group will be available in Security Administration software, you (or the IT administrator at your installation site) must create the new user group in Windows administration. See your on-site IT administrator for more information.

❖ To replace a Security Suite user group name

1. In Security Administration software, choose **File** (menu) > **Replace User/Group in All Access Control Items**.

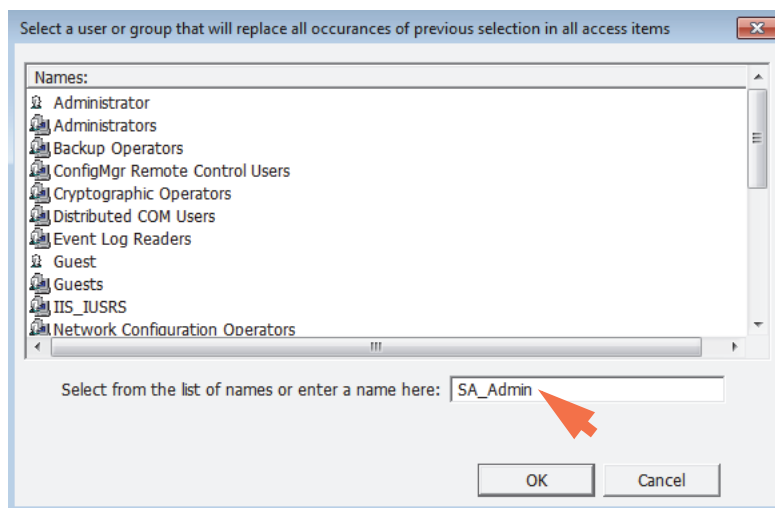
A message box lists the names of the user accounts and groups that are available for this computer.

2. Select the user group you want to reassign (for example, Administrators) and choose **OK**.



Another message box lists the names of the user accounts and groups that are available for this computer.

3. Find the new user group name you want to assign (for example, SA_Admin) or type its name in the entry box and choose **OK**.



Note

- If the new group name does not appear in this list, ask your IT administrator to create the new group in Windows administration.
- The replacement user group will have the same access control settings as the user group it replaced.
- Network user groups are used only for access control settings in Security Administration software. Therefore, this replacement does not affect System Policies and Signature Meanings, which are discussed later in this document.

Set System Policies for Security Suite Applications

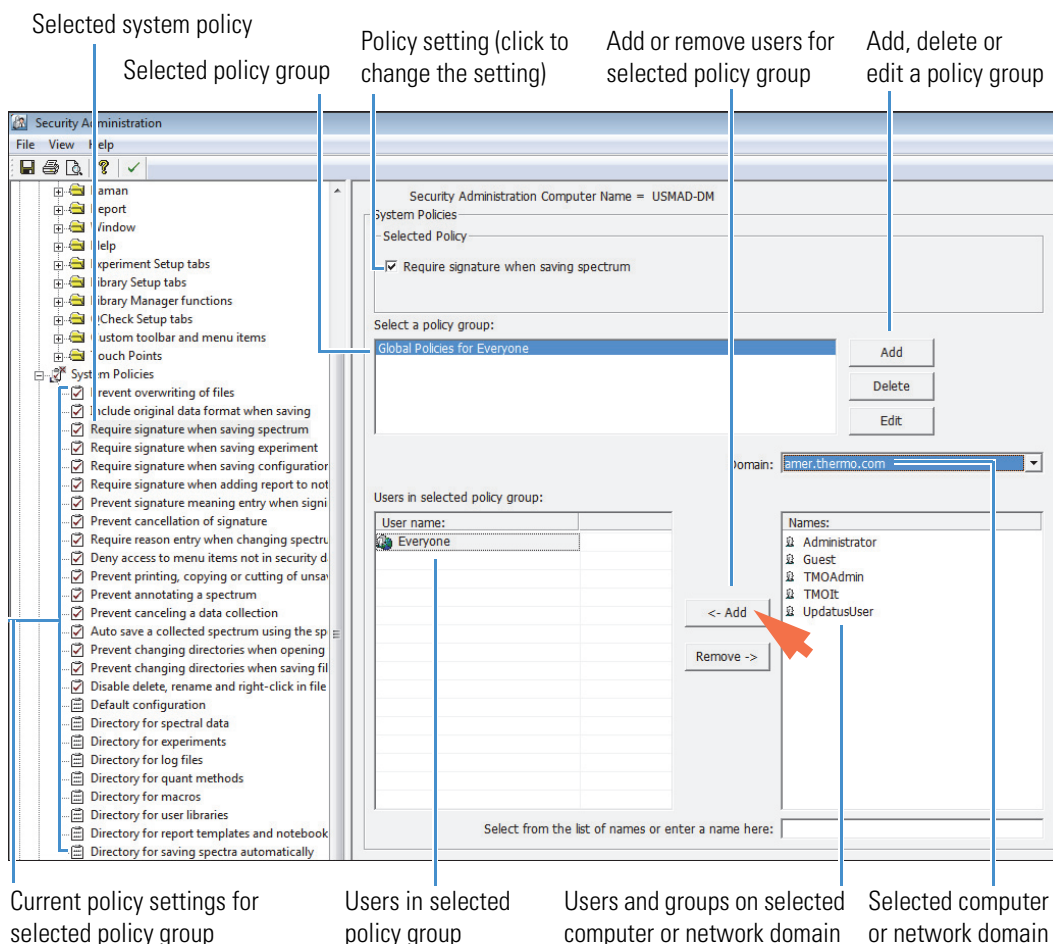
Use System Policies to set policies covering such things as preventing the overwriting of files and requiring electronic signatures. By default, all of the system policies for an application are configured to provide the most restrictive and controlled environment.

When you open the System Policies item in the navigation pane by clicking its plus sign, a tree of icons appears. Each icon in the tree represents a system policy or, if there is a plus sign to the left of the icon, a group of related policies; click the plus sign to reveal the individual policies. Here is an example of a selected system policy for a Security Suite application:

3 Set System Policies and Control Access to Application Features

Set System Policies for Security Suite Applications

Figure 3. Specify the system policy settings for each policy group



You can use the tools in the right pane 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, Global 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 the 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 Global Policies For Everyone group.

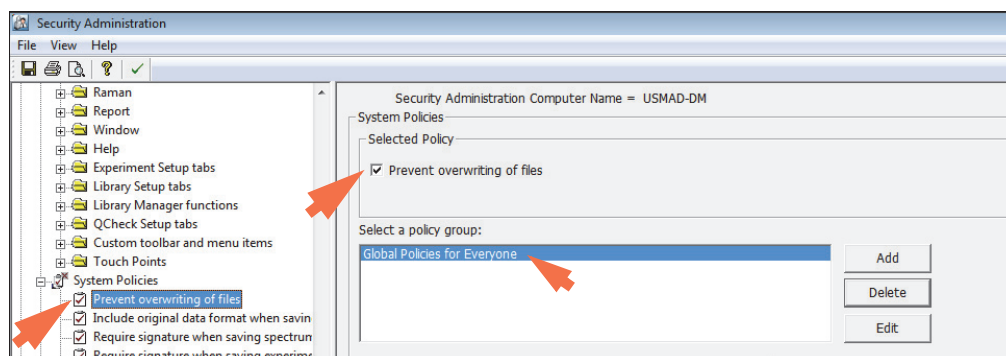
The available policies depend on the application you are setting up. If a check box appears to the left of a policy in the navigation pane, you can specify whether it is selected or not selected for the selected policy group. If no check box appears to the left of a policy (for example, Default Configuration), it lets you specify a system attribute, such as a default configuration or default directory, for policy groups. See the Security Setup Guide that came with your Security Suite 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 in the tree in the navigation pane (a check mark appears or does not appear in the check box to the left of each policy name). This lets you see all of the group's selectable settings at a glance. In addition, the members of the selected group are listed in alphabetical order in the Users In Selected Policy Group box. Once you have selected a policy group, follow these steps to set policies for the group.

❖ To set system policies for a policy group

1. Select the first policy under System Policies in the left pane of Security Administration software.
2. Select the policy group in the Select a Policy Group box in the right pane.
3. Select or deselect the check box associated with that policy in the right pane. Here is an example of a policy that is selected (required) for the default policy group:



4. Select the next policy in the left pane and select or deselect its check box on the right pane.
5. Continue selecting and setting the remaining system policies for the selected policy group until all policies have been set or reviewed.
6. Choose **File** (menu) > **Save Settings** to save your security settings.

Create, Edit, or Delete a Policy Group

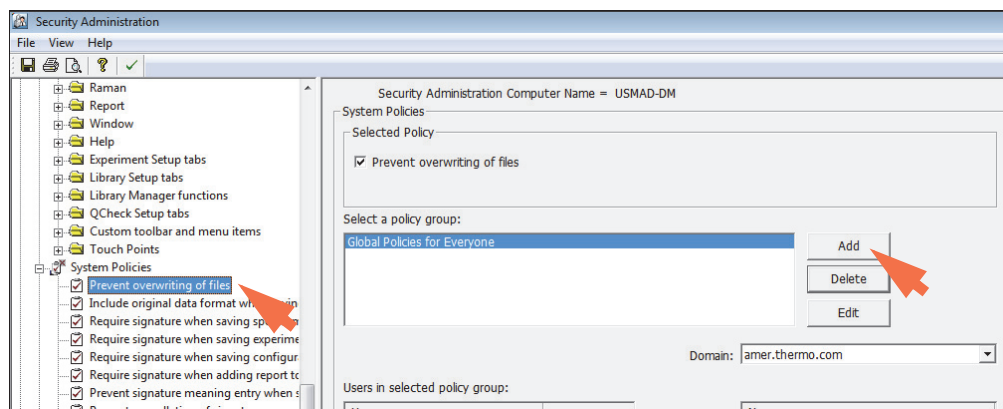
You can create a new system policy group in Security Administration software, delete a policy group or edit a policy group's name. If you create new policy group, you can set policies individually for that policy group. User accounts can then be assigned to the policy group. User accounts should be members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

3 Set System Policies and Control Access to Application Features

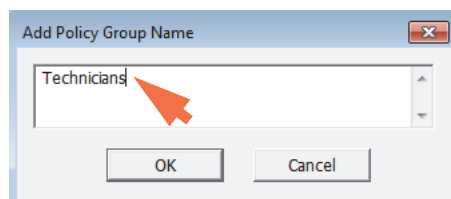
Set System Policies for Security Suite Applications

❖ To create a policy group

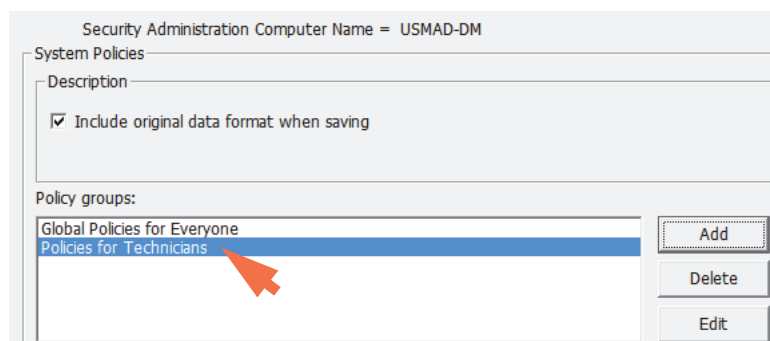
1. In Security Administration software, open the icon for the application you want to create a policy group for in the navigation (left) pane.
2. Open the System Policies group for the selected application in the navigation pane and select any system policy.
3. In the right pane, click the **Add** button under Policy Groups.



4. In the Add Policy Group Name box, enter a descriptive name for the system policy user group you want to create and choose **OK**.



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



You can then add users to the group by using the Add button to the right of the Access Rights box, as explained later in this section.

❖ To delete a policy group

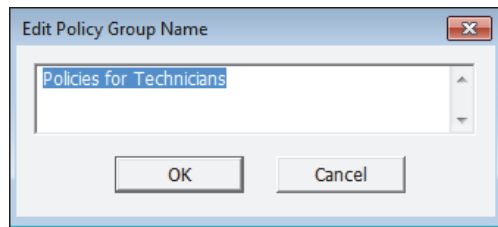
1. Select a group (other than the Global Policies For Everyone Group) in the Policy Groups box.
2. Click **Delete**.

The group is removed from the list.

❖ To edit the name of a policy group

1. Select a group (other than the Global Policies For Everyone Group) in the Policy Groups box.
2. Click **Edit**.

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



3. Type a new description for the group and choose **OK**.

The edited group name appears in the Policy Groups box.

3 Set System Policies and Control Access to Application Features

Set System Policies for Security Suite Applications

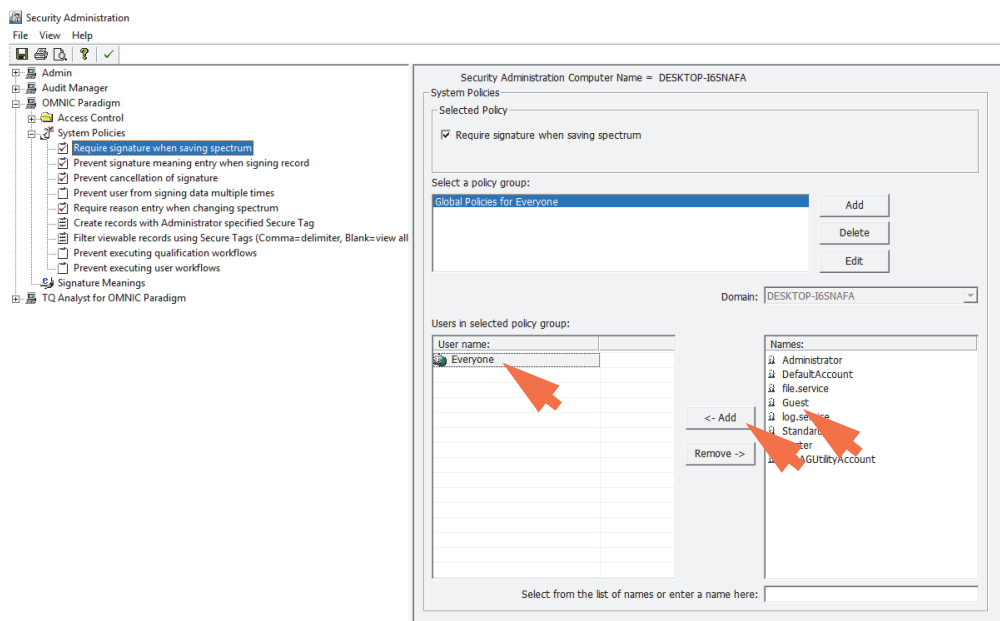
Add or Remove Users from a Policy Group

You can add users to the selected policy group or remove them from the group.

❖ To add a user to a policy group

1. Select the user name in the Names box, or type the name in the text box below the list.
2. Choose **Add**.

The user name appears in the “Users in this policy group” box as shown below.



If you type the name, use the following syntax:

<domainname>\<accountname>

where “domainname” is the name of the domain location of the user or group, and “accountname” is the account name of the user or group.

If the user is in a different organization on a different domain, use the Domain and Organization list boxes to select the desired location.

❖ To remove a user from a policy group

1. Select the user in the Policy Group Members box.
2. Choose **Remove**.

Assign Signature Meanings to Security Suite Applications

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 a Security Suite application. For example, you could set the Signature Meanings features so that only a particular user—for instance, the lab manager—is allowed to sign a file with the “Approval” meaning. See “About Digital Signatures” in the next section 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 users or groups can use particular meanings.

Note Some applications include a system policy that specifies whether users can enter custom signature meanings. See the “Prevent signature meaning entry when signing file” system policy in the security setup guide for your application for more information.

About Digital Signatures

The visible portion of a digital signature consists of a user name, a date and a stated reason for signing (the “meaning” of the signature). See “Edit Signature Meanings” 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 record has changed since it was signed.

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

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

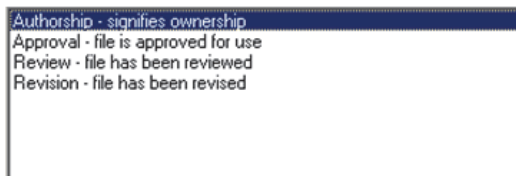
When a user opens a stored spectrum, digital signature information can be found in the History or in the Spectrum Information under the Security tab. To view history, select a spectrum, then select the clock icon above the results pane. To view the spectrum information, select the ‘I’ button next to a spectrum. If the record has not been signed, “Signature: Not Signed” appears. If the record has been signed, the name 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: Smith, John, 02-21-2017 12:02:37 (GMT-06:00), Authorship.” (The “GMT-06:00” indicates the location relative to Greenwich Mean Time.

Multiple signatures are allowed only if the record’s contents have not been changed. If the record is changed, the signature or signatures are invalid, and the record needs to be signed again.

Default Signature Meanings

This section explains the default signature meanings for the Security Suite applications and their permissions for the user groups created by the Security Suite software (Administrators and Users). You can keep the current (recommended) settings and user groups 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 icon for any application 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 “View or Change Signature Meaning Assignments” in the previous section for general instructions for changing the available meanings or to specify which users can select each meaning when signing a file.

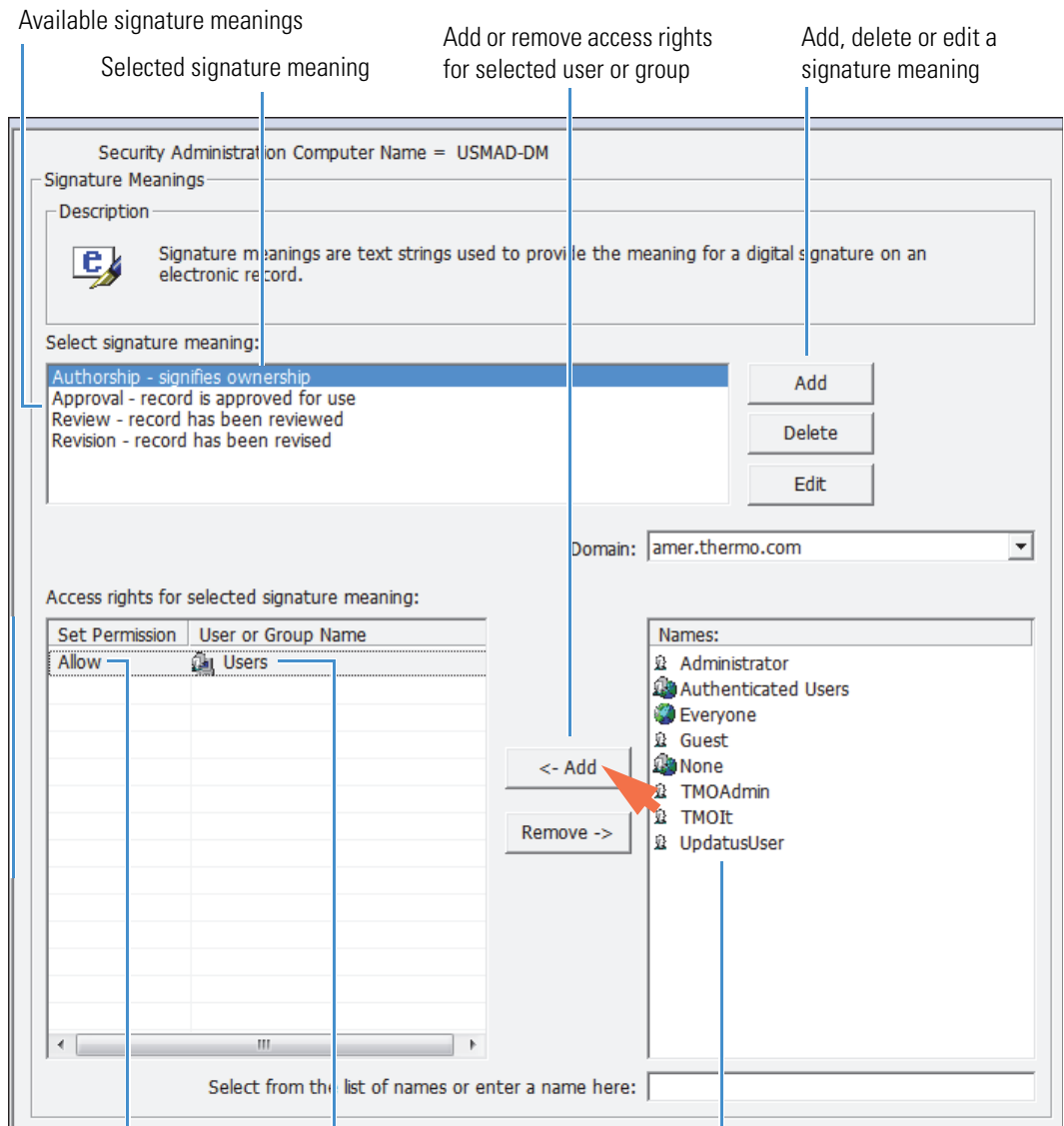
The default signature meanings are intended to be used as explained below.

- **Authorship.** Indicates that the user signing the file 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 file 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 file has changed it. For example, a technician saving a processed spectrum could select this signature meaning to show who changed the spectral data.

View or Change Assignments of Signature Meanings

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

Figure 4. Specify who can access the signature meanings for your applications



Allow or Deny settings are intended for individual users within a group

Users and groups who can use the signature meaning

Users and groups on selected computer or network domain

You can use the tools in the right pane to specify which users or groups can access the selected signature meaning when signing a file. For details, see “Specify Access Rights for Protected Features” and “Add or Remove a User or Group for Access Control” in this document.

When you are finished, choose **File** (menu) > **Save Settings** to save your security settings.

3 Set System Policies and Control Access to Application Features

Assign Signature Meanings to Security Suite Applications

The table below shows the default Signature Meaning access rights settings for the user roles created by the Security Suite software (Administrators and Users).

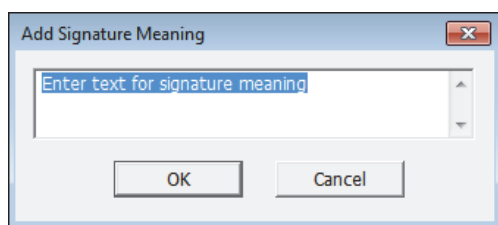
Table 2. Default signature meaning groups and settings for all Security Suite applications

Signature Meaning	Description	Default Access
Authorship	Signifies ownership	Users
Approval	File is approved for use	Administrators
Review	File has been reviewed	Administrators
Revision	File has been revised	Users

Edit Signature Meanings

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

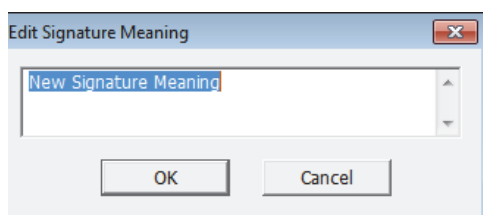
To add a new signature meaning to the list of available meanings, choose Add. The Add Signature Meaning box is displayed. Here is an example:



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

To delete a signature meaning from the list of available meanings, select the meaning by clicking it and choose Delete. The meaning will no longer be available to users when they sign files.

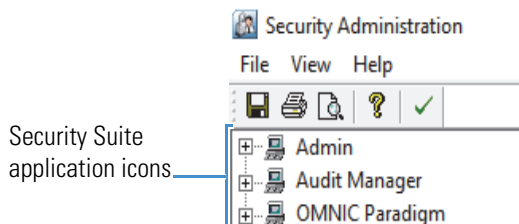
To edit a signature meaning in the list of available meanings, select the meaning by clicking it and then choose Edit. The Signature Meaning box is displayed. Here is an example:



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

Add an Application

When the Security Suite is first installed, the XML files for all the included applications are added to the Security Administration program automatically. When you run the Security Administration program, 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 Security Administration software, use Add Application in the File menu to add the new version's .XML file to the Security Administration software. This merges the new features into the security settings file and preserves all of your existing settings.

❖ To add an application to the Security Administration program

1. Choose **File** (menu) > **Add Application**.

The Open box is displayed.

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.

3. Choose **Open**.

The application appears as an icon in the tree in the navigation pane. See “Setting Security Features for Monitored Applications” for instructions for setting security features for the new application.

Remove an Application

Use Remove Application in the File menu to remove an application from the navigation pane of Security Administration software.

❖ To remove an application from the Security Administration program

1. Select the application's icon in the navigation pane of Security Administration software.
2. Choose **File** (menu) > **Remove Application**.

A message is displayed.

3 Set System Policies and Control Access to Application Features

Set up Automatic Screen Lock

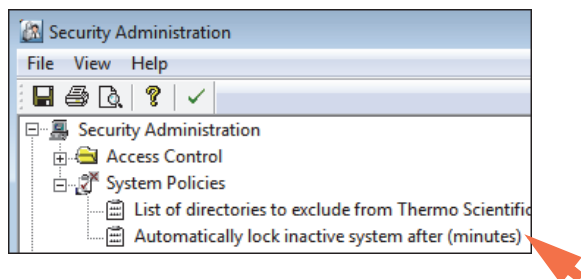
3. Choose **Yes** to remove the application.

Set up Automatic Screen Lock

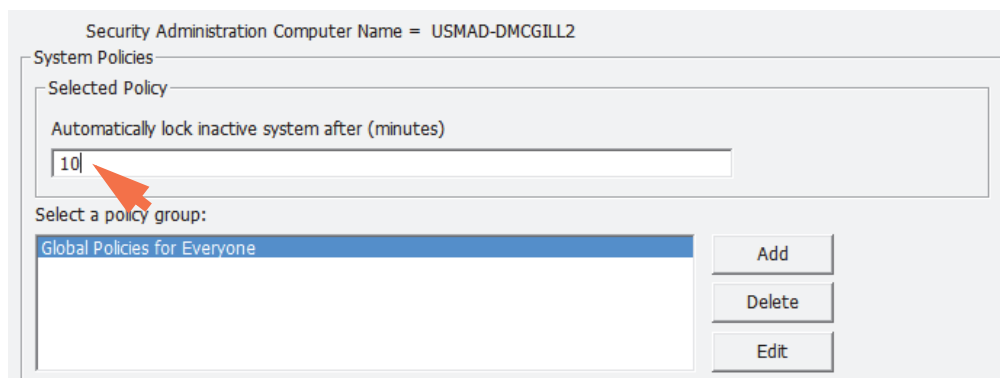
You can set up all Security Suite applications to automatically lock the computer screen after the system has been inactive for a specified length of time.

❖ To set up automatic screen lock for all Security Suite applications

1. In the Security Administration main window, open the Admin group at the top of the navigation (left) pane.
2. In the Admin group, open the System Policies group and select the “Automatically lock inactive system after (minutes)” feature.



3. In the right pane, specify the number of minutes of inactivity after which the system will be automatically locked.



4. Use the Select A Policy Group box to select the users or groups that will be affected, or leave the default group (Global Policies for Everyone) selected to apply the policy to everyone.

Note You can also create user groups for specific system policies or add Windows user groups or individuals from a selected computer or domain. See “Set System Policies for Security Suite Applications” in this document for details.

5. Choose **File** (menu) > **Save Settings**.

Save Your Security Settings

Use Save Settings in the File menu to save the security settings you have specified for the Security Suite applications. Your new settings must be saved in order for them to be in effect when users start the applications.

After you save your settings, you can view or print them. See “Printing the Security Settings” for more information.

Note If you have inadvertently removed your own access rights to run Security Administration software, a message informs you. Close the message, use the Administer Security Database item in the Access Control folder under the Admin icon to restore your access rights (see “Controlling access to Security Administration”) and then save your changes. Only another user with rights to use Security Administration can remove your rights to run the program. This prevents a sole administrator from being locked out of the program accidentally.

If a Security Suite application was running while you used the Security Administration program to change its security settings, the new settings will not take effect until the application is exited and restarted.

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

Print Security Settings

The File menu contains three commands that let you preview the security settings before printing them, set options that affect printing, and print the list of the settings. Printing lets you keep a hard-copy record of your most recently saved settings.

Preview the Security Settings

Use Print Preview in the File menu to view your security settings before printing them.

Note Only settings that you have saved will appear. See “Saving Your Security Settings” for more information.

❖ To preview the security settings

1. Choose **File** (menu) > **Print Preview**.

A window is displayed showing the first page or first two pages of the security settings. (The number of pages displayed depends on whether one or two pages were displayed when you last finished using Print Preview.)

3 Set System Policies and Control Access to Application Features

Print Security Settings

Note The security settings may not display correctly if no printer driver is installed on the computer. If this happens, install an appropriate printer driver.

While you are viewing the security settings, you can switch between displaying one page at a time and two pages by using the **Two Page** and **One Page** buttons.

At the top of the first page is a list showing who last saved security settings, the network domain to which that person belongs, and the date and time the settings were saved. Following the list are the current security settings.

You can enlarge the text on the page to make it easier to read by clicking the **Zoom In** button. Only one page is displayed at a time when you zoom in. To zoom out in order to see more of a page, click the **Zoom Out** button. The buttons are available only when the limit of the size adjustment has not been reached.

You can also click a page to zoom in. When the page is enlarged as much as possible, clicking it again zooms the view all the way out.

To see the next (or previous) page (or pages), click the **Next Page** (or **Prev Page**) button.

If you want to print the security settings, click the **Print** button. Set the print options in the box that appears and choose OK. If you need help, see your Windows documentation.

2. When you are finished viewing the security settings, click the **Close** button.

Set Print Options

Choose **Print Setup** from the **File** menu to set options such as paper size and page orientation before printing the security settings.

Print the Security Settings

Choose **Print** from the **File** menu to print the security settings.

View and Manage the Audit Log

The Security Suite generates an audit trail of activities with your Thermo Scientific™ instruments and software. It records Security Administration and instrument application operations, or “events” in a secure database. Use the Audit Manager to view logged security events and create reports of specific event types or time frames or from specific users.

The Audit Manager adds the following service to the Security Suite:

Thermo Scientific Audit Log Service — Writes logged events to the audit log database

Contents

- [About Audit Logs](#)
- [Reconfigure the Audit Log Database](#)
- [View the Audit Log](#)
- [Create, Sign, and Print Reports](#)
- [Set Audit Manager User Preferences](#)

About Audit Logs

The OMNIC Paradigm application automatically tracks changes to spectral data in the Audit Manager log and with the spectral data record in the database.

When the Security Suite is installed, the instrument operator has no control over this logging process, and the audit trail cannot be modified. This provides a secure spectral-data-change audit trail that is automatically stored with the spectral data and in the Audit Manager database. The spectra data history can be viewed and printed from the OMNIC Paradigm software, or pasted into other word processing or graphical programs.

Spectral processing information that is logged automatically includes the following:

- Date and time of collection (In local time or UTC)
- Operator name
- Data collection parameters
- Spectrometer information
- Spectral processing history
- Digital signature information
- Spectral quality check results
- Collection errors
- Collection and processing details

For each modification of the data the following items are logged:

- Operation performed
- Operator name
- Date and time the modification occurred (UTC)

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

- The event trigger
- The date and time 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, including current and previous settings
- The severity of the event
- The Microsoft® Windows® full user name and ID of the person who was logged in when the event occurred
- The identification of the computer that was being used when the event occurred
- The computer name

Once the Security Suite applications and one or more instrument applications have been installed and added to the Security Administration program, the audit log on the computer where Security Administration software is installed automatically begins recording significant operations performed with the applications on any computers on the network where the applications are installed. Changes you make to security settings in Security Administration software are recorded in the log when you save the changes.

IMPORTANT The Security Suite allows all file 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:

Admin — Tracks changes to the Security Administration software settings.

Thermo Scientific Security Service — Tracks activity of and changes to Thermo Scientific Security Service.

Thermo Scientific Audit Manager — Tracks activity with the Audit Manager application and changes to its associated reports.

Thermo Scientific Audit Log Service — Writes logged events to the audit log database.

Thermo Scientific instrument applications — Tracks activity in the instrument applications such as OMNIC Paradigm software and changes to files while the instrument applications are running.

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

Thermo Scientific Security Service

- Service started
- Security settings file opened
- Service could not start
- Service stopped

Admin

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

Thermo Scientific Audit Manager

Log on succeeded
Log on failed
Log off succeeded
Windows event import succeeded
Windows event import failed

Thermo Scientific Audit Log Service

Service started
Service stopped

Thermo Scientific OMNIC Paradigm software(s)

Log on to OMNIC Paradigm
Log off OMNIC Paradigm
Log on to OMNIC Paradigm failed
Start data collection
End data collection
Record created
Record signed
Record signing failed
Record modified
Record deleted
Fail to verify files signature (file tampering)
Library created
Library spectrum added
Library spectrum deleted
Library deleted
Text fields of a library spectrum edited

Reconfigure the Audit Log Database

We provide a utility program to help you reconfigure the Audit Log database in case you change the database engine type or its release version to other properties. The utility program is located in the following directory:

C:\Program Files (x86)\Thermo Scientific\Audit Log Service\Configuration Utility.exe

Run the utility and enter your new database information to reconfigure the Audit Log database.

View the Audit Log

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

Update audit log Reset filters to show all Menus Filter (click to display filter options) Search for specific user, event description or date range Set user preferences Select event fields to display


Source	Severity	Timestamp Local -06:00	Category
Thermo Scientific Log Service	Warning	26-Oct-2017 09:39:23	File Change
Admin	Warning	30-Oct-2017 11:04:37	Login Audits
Thermo Scientific Log Service	Warning	01-Nov-2017 13:49:27	File Change
Thermo Scientific Log Service	Warning	01-Nov-2017 15:04:01	File Change
Thermo Scientific Log Service	Warning	01-Nov-2017 15:04:07	File Change
Thermo Scientific Log Service	Warning	01-Nov-2017 15:17:45	File Change
Admin	Warning	02-Nov-2017 09:51:59	Login Audits
Thermo Scientific Log Service	Warning	02-Nov-2017 11:25:17	File Change
Thermo Scientific Log Service	Warning	03-Nov-2017 12:58:03	File Change
Thermo Scientific Log Service	Warning	08-Nov-2017 11:21:03	File Change
Thermo Scientific Log Service	Warning	08-Nov-2017 11:21:10	File Change
Thermo Scientific Log Service	Warning	08-Nov-2017 11:21:22	File Change

Source: Thermo Scientific Log Service Category: File Change
 Severity: Warning Timestamp UTC: 26-Oct-2017 14:39:23
 Computer: USMAD-DMCGILL2.amer.thermo.com Timestamp Local: 26-Oct-2017 09:39:23 -05:00
 User ID: SYSTEM Timestamp at Origin: 26-Oct-2017 09:39:23 -05:00
 User Fullname:
 Unknown event ID
 Comments:
 Add Comment

From 20-Oct-2017 to 20-Nov-2017, total events: 124.
 Number of events after filtering: 24.

Selected date range Total events with filters applied Total events All available information for selected event Comment log for selected event

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

- To **sort** events according to Timestamp, Category, Source and so on, click the associated column heading.
- To **filter** events based on Source, Computer Name, Severity or Category, click the associated filter  button, select (or deselect) items to display (or hide) and click Done.
To **reset all filters** to their default settings (to show all events), click Clear Filters.
- To **search for events generated by a specific user**, enter the user name (or partial name) or the user ID in the User search box.
To **search for events that contain a key word**, enter the key word in the Description search box.

To **search for events created on a specific day or within a given time frame**, click the Date Range button, specify the day or time frame and click Done.

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

- To **display** all the available information about an event, select the event (row) in the log. The information is displayed in the pane at the bottom of the window. If the event was the signing of a file, the signature meaning appears in the information pane.

To see information about the **preceding** or **next** event in the list, click the up or down arrow key on the keyboard.

- To **configure the fields** in the audit log, click the Columns button, select (or deselect) the fields to display (or hide) and click Done.
- To **update the audit log** to display events that were added after you started the Audit Manager application, click the Refresh button.
- To **add a comment to an event**, select the event, click Add Comment, type the comment and click Done.

To **add a global comment** to the audit log, such as an audit date, open the Global Comments menu and choose Open. Then click Add Comment, type the comment and click Submit. When you are finished adding global comments, click Done.

Event Information

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

Table 3. 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"> • Admin • Thermo Scientific Security Service • Thermo Scientific Audit Manager • Thermo Scientific instrument applications, such as OMNIC Paradigm
User ID	Windows account name for the logged in user
User Name	Full Windows user name for the logged in user
Computer Name	Full Windows computer name for the computer on which the event occurred

Table 3. Information available for each logged event

Field	Description
Severity	Significance of the event to the security of the system. The following Severity ratings are possible: <ul style="list-style-type: none"> • Information • Error • Warning • Critical
Timestamp Local	Date and time the event occurred translated to the local date and time on this computer
Timestamp UTC	Date and time the event occurred based on the Coordinated Universal Time (UTC) time clock
Timestamp at Origin	Date and time the event occurred on the computer in which it occurred
Category	Type of event that occurred. The following event types are possible: <ul style="list-style-type: none"> • Server • Login Audits • File Change • Signature • Data Change • Application
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
Details	Additional information about the event, including measurement settings


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 **Columns** button and select (or deselect) the fields to display (or hide) for this report.

2. To filter events for this report based on Source, Computer Name, Severity or Category, click the associated filter  button, select (or deselect) items to display (or hide) and click **Done**.
3. To sort events for this report according to date, category, user and so on, click the associated column heading.
4. To save the report, click **Report** (menu) > **Save**.
5. In the Save Report box, enter a filename for the report and choose **Save**.

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

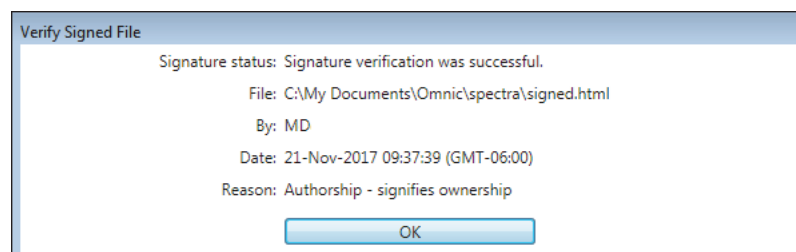
❖ To sign a saved report

1. Click **Report** (menu) > **Sign**.
2. In the Sign Report box, select a saved report to sign and choose **Open**.
3. In the Digital Signature box, enter your user name and password and choose **OK**.
A message indicates the report was successfully signed.
4. Choose **OK** to close the message box.

❖ To verify a signed report

1. Click **Report** (menu) > **Verify**.
2. In the Verify Report box, select a report to verify and choose **Open**.

The Verify Signed File box shows the signature status, filename, signature, signature date and signature reason. Here is an example:



3. Choose **OK** to close the message box.

❖ To print a saved report

1. Click **Report** (menu) > **Print**.
2. In the Print Report box, select a report to print and choose **Open**.

The report is displayed in HTML format along with the Print box. Here is an example:



The screenshot shows a window titled "Print report" containing an "Audit Event Report" for the period "13-Dec-2017T10:38:00-06:00". The report is presented as a table with the following data:

Source	Severity	Timestamp Local -06:00	Category
Thermo Scientific Audit Log Service	Information	12-Dec-2017T11:02:59	Server
Thermo Scientific Audit Log Service	Information	06-Dec-2017T15:10:16	Server
Thermo Scientific File Change Monitor Service	Warning	02-Dec-2017T17:33:26	File Change
Thermo Scientific File Change Monitor Service	Warning	02-Dec-2017T17:32:45	File Change
Thermo Scientific File Change Monitor Service	Information	01-Dec-2017T10:20:20	Server
Thermo Scientific File Change Monitor Service	Information	01-Dec-2017T10:20:19	Server
Thermo Scientific Audit Log Service	Information	01-Dec-2017T10:19:54	Server


3. Use the tools in the Print box to select a printer and print the report.
4. When you are finished, click the close button to close the report window.

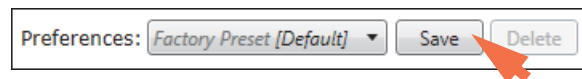
Set Audit Manager User Preferences

You can set up the audit log 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 Presets” 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. Click the **Columns** button and select the fields to display (or hide).
2. To filter events for these user preferences based on Source, Computer Name, Severity or Category, click the associated filter  button, select (or deselect) items to display (or hide) and click **Done**.
3. Click **Save**.



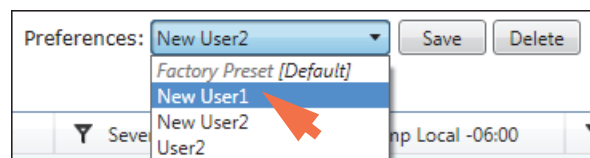
4. In the Save Preferences box, enter a name for these user preferences (for example, New User1) and choose **OK**.

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

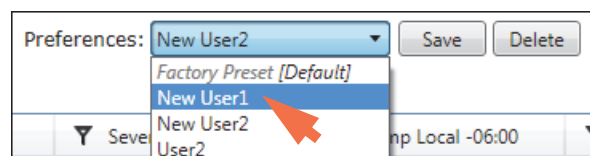
1. Click the down arrow in the Preferences box and select a set of user preferences.



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

❖ To update user preferences

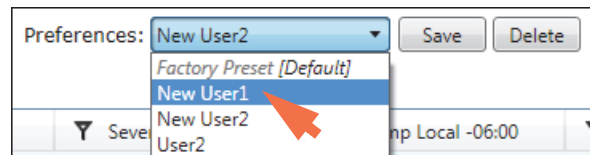
1. Click the down arrow in the Preferences box and select a set of user preferences to update.



2. Change any column or filter settings as needed.
3. Click **Save**.
4. In the Save Preferences box, choose **OK**.
5. Choose **Yes** to confirm.

❖ **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.

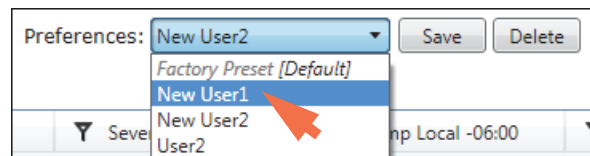


2. Click **Delete**.
3. Choose **OK** to confirm.

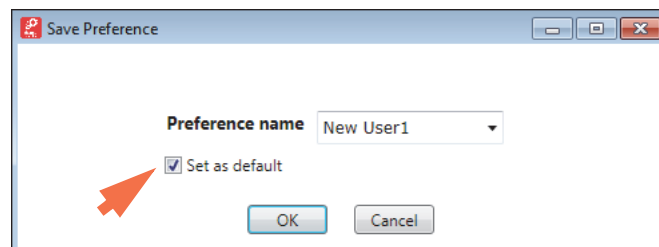
That set of user preferences no longer appears in the drop down list and the default set of user preferences becomes the selected preferences.

❖ **To specify the default user preferences**

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

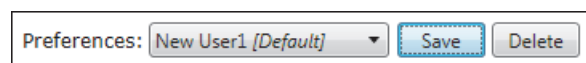


2. Click **Save**.
3. In the Save Preferences box, select **Set As Default** and choose **OK**.



4. Choose **Yes** to confirm.

The word “default” appears at the right of the user preferences name.



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

Default Settings and Policies

The following lists default settings for logged events as well as Access Control and System Policy settings in the Security Administration application.

For an overview and instructions on managing security settings and system policies, see [“Set System Policies and Control Access to Application Features.”](#)

Default Access Control

The Access Control features of the Security Administration program let you set the rights of individual users or groups of users to use the protected features of each application in your Security Suite (the features included in the security database). A protected feature will be available in the application only if the logged-in user has the right to use it. For example, if the user does not have the right to use a protected menu command, it will not appear in the menu.

The following sections list the default Access Control settings for Security Suite software and instrument applications for the Security Suite’s default user groups (Administrators and Users).

The default group names represent the two main groups of users who typically use the Security Suite software (that is, administrators of Security Administration software (Administrators) and instrument operators (Users)). The Administrators group has **full access** to all the features of the Security Administration program, including system configuration. The Users group has **no access** to the Security Administration program and **limited access** to the instrument applications that are controlled by Security Administration software (i.e., only those features needed to operate the instrument with secure data storage.) You can keep the current (recommended) settings and the default user groups, or change them as needed to ensure compliance with the security requirements at your installation site.

Security Administration

Select Admin from the navigation pane to view or edit settings for Security Administration software.

5 Default Settings and Policies

Default Access Control

Feature Controlled by Security Administration Software	Default Access
Administer security database	Administrators
Determines which users or groups can run the Security Administration software.	

Audit Manager

Control which users or groups have access to Audit Manager features.

Feature Controlled by Security Administration Software	Default Access
Ability to run Audit Manager	Users ^a Note: Access is denied for Guests.
Allow adding an event comment	Administrators
Allow adding a global comment	Administrators
Allow configuring database comment	Administrators

^a Default Users group also includes Administrators.

OMNIC Paradigm Software

Determine which users or groups have access to features in OMNIC Paradigm software.

Feature Controlled by Security Administration Software	Default Access
Ability to run Paradigm	Users ^a Note: Access is denied for Guests.
File Menu	
Open	Users
Export	Users
Create Report	Users
Open Workflow	Users
Create Workflow	Users
Export Workflow	Users
Reset Workflow Password	
Sign	Users
Acquire Data Menu	
Measure Background	Users
Measure Sample	Users
Align Spectrometer	Users
Laser Calibration	Users

Feature Controlled by Security Administration Software	Default Access
Instrument Health	Users
Open Settings	Users
Export Settings	Users
View / Display Menu	
Absorbance	Users
% Transmittance	Users
% Reflectance	Users
Log (1/R)	Users
Kubelka Munk	Users
Switch between Desktop and Touchscreen	Users
Process Menu	
Automatic Baseline Correction	Users
Spectral Math	Users
Noise	Users
Kramers-Kronig Correction	Users
Retrieve Interferograms	Users
Advanced ATR Correction	Users
Identify Menu	
Find Peaks	Users
Search Setup	Users
Correlation Search	Users
Multi-Component Search	Users
New Library	Users
Add to Library	Users
QCheck Setup	Users
QCheck	Users
Quantify Setup	Users
Quantify	Users
Configure Menu	
Connectivity	Administrators
Access the Simulator option in the Connectivity dialog	Users
Database	Administrators
Database Maintenance - Restore	Administrators
Database Maintenance - Backup	Administrators
Security Server	Administrators
Options	Users

5 Default Settings and Policies

Default Access Control

Feature Controlled by Security Administration Software	Default Access
Update	Administrators
Edit the paths libraries are read from	Administrators
Collection Controls	
Stop Background or Sample Measurement	Users
Restart Background or Sample Measurement	Users
Spectral Context Menu	
Peak Area	Users
Peak Height	Users
Peak Area Ratio	Users
Peak Height Ratio	Users
Export Background	Users
Show Spectrum Information	Users
Measurement List Context Menu	
Manage Tags	Users
Rename Measurement	Users
Delete Selected Measurements	Users
Workflows	
Execute Qualification Workflows	Users
Execute User Workflows	Users
Workflow Context Menu	
Edit	Users
Delete	Users
Duplicate	Users
Rename	Users
Library Manager	
Delete Spectra from Library	Users
Delete Library	Users
Extract Library Spectrum	Users
Print Listing	Users
Edit Fields	Users
Reports	
Access report options	Users
Create reports for Microsoft Word, Excel, and PowerPoint	Users
Options	
Configure automatic baseline correction	Users
Configure digits displayed in peak height/area	Users

^a Default Users group also includes Administrators.

Default System Policies

While you can use Access Control to determine which software features are available to users or groups, use System Policies to set options for additional application behaviors. For example, with system policies, you can set when signatures are required, lock the system automatically after a period of inactivity, and more.

Like Access Control settings, system policies can be set for specific users or groups or can be applied to everyone at the site.

Security Administration

Set system policies for Security Administration software. Policies for Security Administration software are listed in the left pane under Admin.

System Policy Controlled by Security Administration Software	Default Setting
Automatically lock inactive system after (minutes)	10 minutes

Audit Manager

Set system policies for Audit Manager software.

System Policy Controlled by Security Administration Software	Default Setting
Prevent signature meaning entry when signing file	True
Prevents users from entering a custom signature meaning when signing a file. When this policy is selected, only the standard signature meanings defined in Security Administration software are available for the affected users.	
Prevent cancellation of signature	True
Disables the Cancel button in the Sign File dialog box, which requires the user to sign the file in order to complete the previous operation.	

OMNIC Paradigm Software

Set system policies for OMNIC Paradigm software.

System Policy Controlled by Security Administration Software	Default Setting
Require signature when saving spectrum	True

5 Default Settings and Policies

Default System Policies

System Policy Controlled by Security Administration Software	Default Setting
Prevent signature meaning entry when signing record Prevents users from entering a custom signature meaning when signing a record. When this policy is selected, only the standard signature meanings defined in Security Administration software are available for the affected users.	True
Prevent cancellation of signature Disables the Cancel button in the Sign File dialog box, which requires the user to sign the file in order to complete the previous operation.	True
Prevent user from signing data multiple times When True, a user will be able to sign the data record only one time. That user may be able to review the data record later but will be prohibited from signing it after any other data changes or updates.	False
Require reason entry when changing spectrum using any of the Process menu commands listed below: <ul style="list-style-type: none">• Spectral Math• ATR Correction• Conversions• Automatic Baseline Correction• Find Peaks See the spectrum history to view any of these changes.	True
Create records with Administrator specified Secure Tag Automatically appends a secure tag to the data record when the data is acquired. Specify the tag to be added. Only a single tag can be added per user or group.	
Filter viewable records using Secure Tags (Comma=delimiter, Blank=view all) Filters data that can be viewed by the current user. Users will be able to view only data with the specified tags. If no tags are specified, the user will be able to view all data.	False
Require signature when creating report	False
Require reason entry when backing up or restoring the database	False