



iCE 3000 Series AA Spectrometers

SOLAAR*security* Software Manual

Version 1.09

BRE0017280 Revision B September 2018

iCE 3000 Series AA Spectrometers

SOLAAR*security* Software Manual

Version 1.09

BRE0017280 Revision B September 2018

Legal Notices

© 2018 Thermo Fisher Scientific Inc. All rights reserved.

Published by:

Thermo Fisher Scientific (Bremen) GmbH, Hanna-Kunath-Str. 11, 28199 Bremen, Germany
Tel: +49(0)421 5493 0, Fax: +49(0)421 5493 396

Excel, Microsoft, and Windows are registered trademarks of Microsoft Corporation.

QR Code is a registered trademark of DENSO WAVE INCORPORATED in Japan and other countries.

All other trademarks are the property of Thermo Fisher Scientific Inc. and its subsidiaries.

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.

Release History: Revision A released August 2018.
Revision B released September 2018.

Software Version: SOLAAR*security* 1.09

For Research Use Only. Not for use in diagnostic procedures.

Contents

	Using this Manual	1
	About this Manual	1
	Who Uses this Guide	1
	Scope of this Guide	1
	Related Documentation	2
	Typographical Conventions	3
	Signal Words.....	3
	Data Input	3
	Topic Headings.....	4
	Contacting Us.....	5
Chapter 1	Introduction	1-1
	SOLAAR <i>security</i> Components.....	1-2
	Administrator and Server Applications	1-2
	Client Applications	1-2
Chapter 2	Pre-Installation and Installation	2-1
	System Overview.....	2-1
	The Single Domain Model.....	2-1
	The Multiple (Trusted) Domain Model.....	2-2
	Stand alone Configuration	2-3
	System Prerequisites	2-4
	Installation and Configuration Prerequisites.....	2-4
	Planning the Installation	2-6
	Scope	2-6
	Reviewing the Operating System Configuration.....	2-6
	User Accounts	2-7
	Group Membership	2-8
	User Rights Policy.....	2-8
	Account Policy	2-8
	Audit Policy	2-9
	File/Folder Access Control	2-9
	Domain Trust Relationships	2-9
	Event Log Configuration	2-9
	Special Considerations for Stand-alone Systems	2-10
	NTLM System	2-11
	SOLAAR <i>security</i> Pre-installation Report	2-12
	Installation	2-13
	Validation	2-13
	Regional Options - Time Settings	2-13
	File and Folder Protection.....	2-13

Initial Installation..... 2-15
 Updates, Repairs and Uninstalls..... 2-19

Chapter 3 SOLAARsecurity Client Software..... 3-1

Starting the Client Applications 3-1
 Working with Analysis Results Records..... 3-3
 Creating Analysis Results Records 3-3
 Viewing Analysis Results records 3-4
 Viewing an Analysis Results record Audit Trail 3-4
 Viewing Analysis Results record Signatures 3-5
 Signing an Analysis Results record..... 3-5
 Editing an Analysis Results record..... 3-6
 Printing Analysis Results records 3-7
 Exporting Analysis Results records 3-8
 Managing Analysis Results records 3-9
 Compressing and Repairing Results databases 3-10
 Copying Analysis Results records 3-11
 Deleting Analysis Results records 3-11
 Working with Method Records..... 3-13
 Creating Method records 3-14
 Viewing Method records 3-15
 Signing Method records 3-16
 Loading Method records 3-16
 Editing and Saving Method records 3-17
 Printing Method records 3-17
 Managing Method records 3-18
 Compressing and Repairing Methods databases 3-19
 Copying Method records 3-20
 Deleting Method records 3-20
 Working with PQ Tests Results Records..... 3-22
 Creating PQ Analysis Results records 3-22
 Viewing PQ Tests Results records 3-22
 Viewing a PQ Test Results record Audit Trail..... 3-23
 Viewing PQ Test Results record Signatures..... 3-23
 Signing a PQ Tests Result record 3-24
 Printing PQ Tests Result records 3-25
 Exporting PQ Tests Result records..... 3-27
 Managing PQ Tests Result records..... 3-28
 Compressing and Repairing PQ Results databases..... 3-28
 Copying PQ Tests Result records..... 3-29
 Working with OQ Test Results records 3-31
 Creating OQ Tests Result records..... 3-31
 Viewing OQ Tests Result records 3-31
 Viewing an OQ Tests Result record Audit Trail 3-32
 Viewing OQ Tests Result record Signatures..... 3-32
 Signing an OQ Tests Result record 3-33
 Printing OQ Tests Result records 3-34
 Managing OQ Tests Results records 3-34
 Repairing OQ Tests databases..... 3-35

Working with Access Controls	3-36
Administer Security Database.....	3-36
Run SOLAAR <i>security</i> Software.....	3-36
Sign e-record.....	3-36
Run Analyses.....	3-37
Perform Ash Atomize analyses.....	3-37
Perform Calibrate Method	3-37
Perform Single Solution Measurements.....	3-37
Perform Burner Height optimization	3-38
Perform Gas Flow optimization	3-38
Perform Spectrometer optimization	3-38
Run Gas Flow Wizard.....	3-39
Run Spectrometer Optimization Wizard.....	3-39
Run Instrument Performance Wizard	3-39
Edit Results.....	3-39
Edit Peak Measurement	3-40
Edit Methods	3-40
Edit Sequence in Methods	3-40
Edit Sample Details in Methods.....	3-41
Edit Print Options	3-41
Allow Printing.....	3-41
Allow Data Export	3-41
Allow Clipboard Copy	3-41
Manage Databases.....	3-42
Copy Analyses.....	3-42
Copy Methods	3-42
Delete Analyses	3-42
Delete Methods.....	3-42
Perform PQ Tests	3-42
Perform OQ Tests	3-42
Perform Customer Diagnostics	3-43
Working with System Policies.....	3-43
Authenticate on Startup	3-43
Perform Event Auditing.....	3-43
Confirm ID before Printing.....	3-43
Confirm ID before Exporting	3-43
Confirm ID before Editing	3-44
Working with Signature Meanings.....	3-45
Upgrade Considerations.....	3-46
Database Considerations	3-46
Permissions and Users.....	3-46

Chapter 4	SOLAAR<i>security</i> Administrator Software	4-1
	Starting the Administrator Applications	4-1
	The User Interface	4-2
	Access Control	4-5
	Access Control support of User Groups	4-11
	User Access Control of Delete Results and Delete Methods.....	4-13

User Access Control of Burner Up and Burner Down.....	4-13
Display of the Spectrometer Status.....	4-14
User Access Control for Changing Lamp	4-14
User Access Control of New and Close Results	4-15
User Access Control of Fuel Up and Fuel Down.....	4-15
Audit Trail tracking of User Access (System Log).....	4-16
The Local Group Policy Editor	4-17
SOLAAR <i>security</i> System Log.....	4-20
System Policies.....	4-21
Signatures	4-25
The SOLAAR <i>security</i> Service.....	4-27
Introduction to SOLAAR <i>security</i> Service.....	4-27
Stopping and Starting the SOLAAR <i>security</i> Service...	4-27
Reference	4-30
Network Concepts	4-30
The Role of the Network Administrator.....	4-32
The Role of the SOLAAR <i>security</i> Manager.....	4-33
Chapter 5	
The 21 CFR Part 11 Rule.....	5-1
Open and Closed Systems.....	5-2
Electronic Records	5-3
Audit Trails.....	5-5
Electronic Signatures.....	5-6
Authority and Device Checks.....	5-8

Using this Manual

This chapter provides information about this manual.

Contents

- [About this Manual](#) on page 1
- [Related Documentation](#) on page 2
- [Typographical Conventions](#) on page 3
- [Contacting Us](#) on page 5

About this Manual

This SOLAAR*security* Software Manual introduces the Thermo Scientific™ SOLAAR*security* Software and describes the configuration and operation of the iCE 3000 Series Atomic Absorption Spectrometer with SOLAAR*security*. For information about the operating procedures for the iCE 3000 Series AAS system, we recommend that you read the *iCE 3000 Series AAS Operating Manual*.

Who Uses this Guide

This SOLAAR*security* Software Manual is intended for all personnel the need to perform measurements with the iCE 3000 Series mass spectrometer.

Scope of this Guide

The SOLAAR*security* Software Manual includes the following chapters:

- [Chapter 1: “Introduction”](#) gives a general introduction into the SOLAAR*security* Software.
- [Chapter 2: “Pre-Installation and Installation”](#) describes supported system configurations and how to review the operating system configuration.
- [Chapter 3: “SOLAAR*security* Client Software”](#) describes the installation and use of the Client application.

- [Chapter 4: “SOLAARsecurity Administrator Software”](#) describes the installation and use of the Administrator application.
- [Chapter 5: “The 21 CFR Part 11 Rule”](#) describes how the Electronic Records, Electronic Signatures Rule is implemented in the SOLAARsecurity Software.

Related Documentation

In addition to this SOLAARsecurity Software Manual, Thermo Fisher Scientific provides the following documents for the iCE 3000 Series AAS instruments:

- *iCE 3000 Series AAS Pre-Installation Requirements Guide*
- the *iCE 3000 Series AAS Operating Manual* – this describes the installation, alignment and use of the Spectrometer and accessories.
- the *Atomic Absorption Spectrometry Methods Manual* – this describes the physical and chemical principles underlying the technique of Atomic Absorption Spectrometry, and gives practical guidance on sample preparation and related topics.
- the *iCE 3000 Series AAS SOLAAR Software Manual* – this gives a detailed description of the software, together with instructions on how to carry out all the main operations.

The *iCE 3000 Series AAS Operating Manual* represents the Original Operating Instructions. Thermo Fisher Scientific provides this SOLAARsecurity Software Manual as additional reference documents for the iCE 3000 Series AAS instruments.

The SOLAAR Software also provides Help.

A printed version of the *iCE 3000 Series AAS Operating Manual* is shipped with the instrument. A printed version of the *iCE 3000 Series AAS Pre-Installation Requirements Guide* is part of the Pre-Installation Kit. This kit is sent to your laboratory before the arrival of the iCE 3000 Series AAS.

Typographical Conventions

This section describes typographical conventions that have been established for Thermo Fisher Scientific manuals.

Signal Words

Make sure you follow the precautionary statements presented in this manual. The special notices appear different from the main flow of text:

Tip Points out possible material damage and other important information in connection with the instrument.

Data Input

Throughout this manual, the following conventions indicate data input and output via the computer:

- Messages displayed on the screen are represented by capitalizing the initial letter of each word and by italicizing each word.
- Input that you enter by keyboard is identified by quotation marks: single quotes for single characters, double quotes for strings.
- For brevity, expressions such as “choose **File > Directories**” are used rather than “pull down the File menu and choose Directories.”
- Any command enclosed in angle brackets < > represents a single keystroke. For example, “press <**F1**>” means press the key labeled *F1*.
- Any command that requires pressing two or more keys simultaneously is shown with a plus sign connecting the keys. For example, “press <**Shift**> + <**F1**>” means press and hold the <Shift> key and then press the <F1> key.
- Any button that you click on the screen is represented in bold face letters. For example, “click **Close**”.

Topic Headings

The following headings are used to show the organization of topics within a chapter:

Chapter Name





Second Level Topics

Third Level Topics

Fourth Level Topics

Contacting Us

There are several ways to contact Thermo Fisher Scientific. You can use your smartphone to scan a QR Code, which opens your email application or browser.

Contact	Link / Remarks	QR Code
Brochures and Ordering Information	www.thermofisher.com/aas	
Service Contact	www.unitylabservices.com	
Technical Documentation SharePoint	<ul style="list-style-type: none"> ❖ To get user manuals for your product 1. With the serial number (S/N) of your instrument, request access on our customer SharePoint as a customer at www.thermoscientific.com/Technicaldocumentation 2. For the first login, you have to create an account. Follow the instructions given on screen. Accept the invitation within six days and log in with your created Microsoft™ password. 3. Download current revisions of user manuals and other customer-oriented documents for your product. Translations into other languages may be available there as well. 	
Customer Feedback	<ul style="list-style-type: none"> ❖ To suggest changes to this manual <p>You are encouraged to report errors or omissions in the text or index. Send an email message to the Technical Editor at documentation.bremen@thermofisher.com.</p>	

Introduction

Welcome to the Thermo Scientific™ SOLAAR*security*™ Software for the Thermo Scientific Atomic Absorption iCE 3000 Series spectrometers.

SOLAAR*security* is a software product released for use with Thermo Fisher Scientific's iCE 3000 Series Atomic Absorption Spectrometers and accessories. As well as providing flexible and versatile control of the spectrometer and its accessories, this software has been designed to provide tools and facilities that will assist you in creating and maintaining electronic records containing analytical data that meet the requirements of the US Government's Food and Drug Administration 21 CFR Part 11 Rule (herein referred to as "the Rule") – Electronic Records; Electronic Signatures.

The deployment of the SOLAAR*security* Software itself, however, is only one aspect of achieving regulatory compliance. Installation and operation of the software and associated analytical instrumentation must be performed within a much broader framework of organizational structure, IT infrastructure, standards and supporting procedures (SOPs).

For example, it is assumed that if your organization has chosen to comply with the electronic signatures part of the Rule, then it will have:

- Performed the necessary verification of the identity of the proposed signers
- Submitted the necessary certification to the FDA
- Created written policies to hold individuals accountable for the validity and veracity of data held in electronic records carrying the signature of the individual.

The scope of this manual is limited to those aspects of the software and analytical instrumentation that have a direct impact on the role that the SOLAAR*security* Software plays in helping your organization to achieve compliance. This manual does NOT cover the analytical use of the software and instrumentation; this is discussed in detail in the *SOLAAR Software Manual*, and in the *On-Line Help* system supplied with the software.

This manual shows you how to install and use the SOLAAR*security* Software. It should be used in conjunction with the other AA Series User Documentation supplied with your system.

SOLAARsecurity Components

The SOLAARsecurity Software comprises four inter-related Windows applications, which work together to provide these facilities and functions.

Administrator and Server Applications

The SOLAARsecurity **Administrator** application provides facilities for creating and maintaining the SOLAAR Users Security database. This contains details of the authorised users of the SOLAAR Atomic Absorption system, the Access Controls that allow them to use its facilities, and certain System Policies that control the behaviour of the system.

The SOLAARsecurity **Server** application runs as a service on the same machine as the SOLAARsecurity Administrator application, and provides communications links between the SOLAARsecurity Client applications and the operating system security features. This program is capable of servicing multiple simultaneous client applications running on different computers on the network.

The purposes and uses of these two components are described in the SOLAARsecurity Administrator chapter, see [“SOLAARsecurity Administrator Software”](#) on page 4-1.

Client Applications

The SOLAARsecurity **Data Station Client** application is used to control the Atomic Absorption Spectrometer and associated accessories, to perform analyses, and to collect and store the analytical results. When this software is running it is in constant communication with the SOLAARsecurity Server Software in order to enforce the security policies defined by the SOLAARsecurity Manager.

The SOLAARsecurity **OQ Tests Client** application provides facilities for automatically performing the OQ (Operational Qualifications) Tests on the spectrometer, and collecting and storing the OQ data. The Calibration Validation Unit must be installed, in order to use these facilities.

The OQ Tests Client software also provides a comprehensive suite of User Diagnostic tools to assist in identifying and rectifying any problems that may arise with the spectrometer system. It provides facilities for creating logs of such activities, to assist in achieving compliance with the requirements of the 21 CFR Part 11 Rule. It is NOT necessary to have the Calibration Validation Unit accessory installed in order to use these User Diagnostic tools and facilities.

When the Client applications are installed as part of the complete SOLAAR*security* package, a further set of functions becomes available. This set of functions provides the facilities that are necessary to create and store electronic records containing analytical data that can satisfy the requirements of the 21 CFR Part 11 Rule, and are discussed in this manual, see [“The 21 CFR Part 11 Rule”](#) on [page 5-1](#).

Introduction

SOLAARsecurity Components

Pre-Installation and Installation

This chapter shows the supported operating system versions, the management of user rights, and the Pre-installation Report form.

Contents

- [System Overview](#) on page 2-1
- [System Prerequisites](#) on page 2-4
- [Planning the Installation](#) on page 2-6
- [SOLAARsecurity Pre-installation Report](#) on page 2-12
- [Installation](#) on page 2-13

System Overview

The following diagrams illustrate some common network architectures supported by the SOLAARsecurity Software.

The Single Domain Model

The Administrator and Server applications are installed together on any Windows XP, Windows Vista Ultimate, Windows 7 Professional, or Windows 10 Professional server that is a member of a domain.

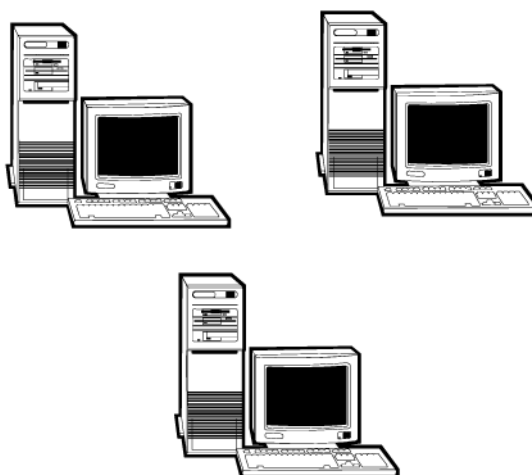


Figure 2-1. One or more Server machines with Windows OS

The SOLAAR*security* Client application is installed on one or more workstations that are also members of the domain. The Client workstations may be running any of Windows XP Professional (SP2), Windows Vista Ultimate, Windows 7 Professional, and Windows 10 Professional.

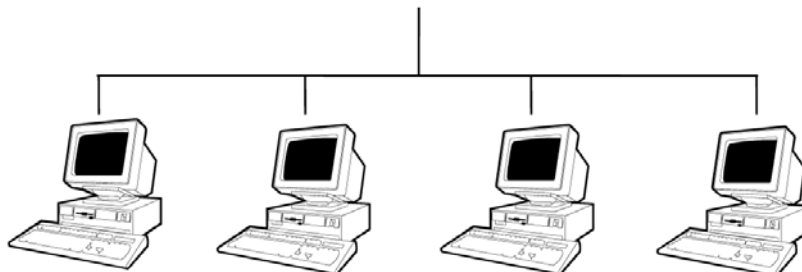


Figure 2-2. Client machines with Windows OS

The Multiple (Trusted) Domain Model

The Administrator and Server applications are installed on any Windows XP Professional (SP2), Windows Vista Ultimate, Windows 7 Professional, and Windows 10 Professional server that is a member of a domain. The Client application is installed on machines that are members of other, trusted domains. The Client machines may be running Windows XP Professional (SP2), Windows Vista Ultimate, Windows 7 Professional, and Windows 10 Professional.

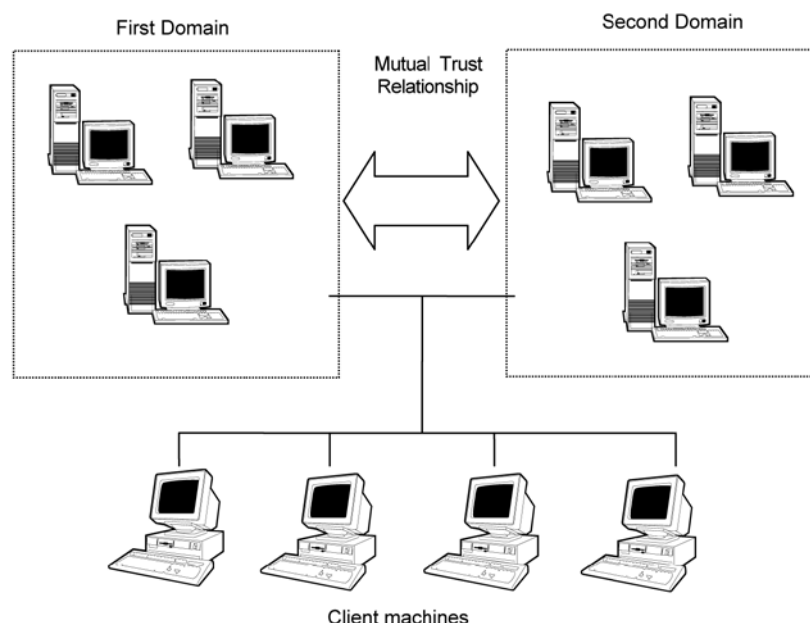


Figure 2-3. Server and Client machines in multiple domains

Stand alone Configuration

The SOLAAR*security* Clients, Administrator and Server applications are all run on a single non-networked computer that acts as both client and server. This computer must be running Windows XP Professional (SP2), Windows Vista Ultimate, Windows 7 Professional, or Windows 10 Professional.

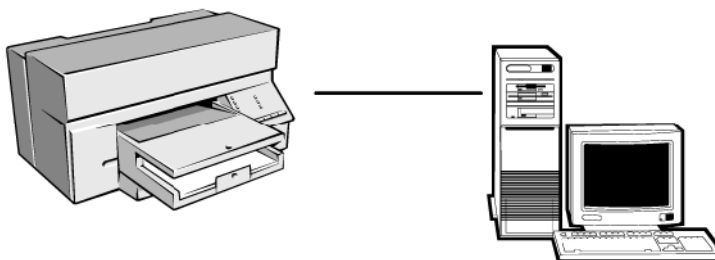


Figure 2-4. Computer with Windows OS running all SOLAAR*security* applications

System Prerequisites

The Server / Administrator PC and the Client PC may run with the operating system version as shown in [Table 2-1](#).

Table 2-1. Supported Operating System versions and prerequisites

Operating System	Server / Administrator	Client
Windows XP Professional	Yes	Yes
Windows Vista Ultimate	Yes	Yes
Windows 7 Professional	Yes	Yes
Windows 10 Professional	Yes	Yes

The Server and Administration applications **MUST** be installed on to a disk or partition formatted with the NTFS file system and the Server and Client computers **MUST** be running the NTLM service (if applicable), see [“Planning the Installation”](#) on [page 2-6](#). All configurations require that Internet Explorer version 4.01 SP2 or higher must be installed.

Installation and Configuration Prerequisites

Installation and initial configuration of the SOLAAR*security* Server and Administrator applications can only be performed by a user who has membership of the operating system Administrators group. This user **MUST** have the necessary knowledge and authority to perform the required checks and configuration changes.

Additional information for Vista Ultimate and Windows 7 Professional Users: Windows Vista, Windows 7, and Windows_10 utilize Microsoft User Account Control (UAC) Technology. This control is responsible for prompts that require confirmation of an administrator name and password to continue with an action that normally requires administrator rights. One element of the UAC is “Admin Approval Mode”. This is an operating mode (which runs as default) and means Windows users who are defined as members of the Windows Administrators group are, by default, run with the privilege of standard users. This means they cannot perform functions, which require administrator rights without further action. Members of the Windows Administrator group are switched (elevated) to true Administrator mode by request. This occurs “on-demand” when the user right-clicks on a program and selects “Run as Administrator”. This can also happen automatically when a program recognizes a user as a true administrator.

Once installed, the ability to run the SOLAAR*security* Administrator application can be granted by the operating system administrator to any user(s) or group(s) of users as required. This allows day-to-day

administration of SOLAAR*security* to be performed by authorized individuals other than operating system administrators. Such individuals and groups are described as SOLAAR*security* Managers.

Planning the Installation

Scope

The SOLAAR*security* Software has been designed specifically to assist your organization in achieving compliance with the 21 CFR Part 11 Rule – “Electronic Records and Electronic Signatures”. The deployment of the SOLAAR*security* Software itself is, however, only one aspect of achieving regulatory compliance. Installation and operation of the software must be performed within a much broader framework of organizational structure, IT infrastructure, standards and supporting procedures (SOPs).

The scope of the following guidelines is limited to those aspects of the operating system and immediate network environment that have a direct impact on the role that the SOLAAR*security* Software plays in helping your organization to achieve compliance.

For example, it is assumed that if your organization has chosen to comply with the electronic signatures part of the Rule then you will have:

- Performed the necessary verification of the identity of proposed signers.
- Submitted the required certification to the FDA.
- Created written policies to hold individuals accountable for actions initiated under their electronic signatures.

Reviewing the Operating System Configuration

The SOLAAR*security* Software integrates with many of the security and auditing features of the Windows operating system in order to support the requirements of 21 CFR Part 11. For example, user authentication is performed using the operating system login procedures, password policies are those of the operating system, and access control is based on operating system user account and group membership.

For compliance with 21 CFR Part 11 it is necessary to ensure that several operating system features are suitably configured.

The first step in planning the installation is therefore to identify the target system on which the software is to be installed and to review (existing system) or define (new system) certain aspects of system behavior.

Tip Refer to your operating system documentation for details of how to perform the necessary checks and configuration changes.

SOLAAR*security* Software can be installed in a ‘stand-alone’ or networked environment (see “[System Prerequisites](#)” on [page 2-4](#)). For a ‘stand-alone’ installation, it is necessary that at least one individual concerned with the installation has an *Administrator* account on the local machine on which the software is to be installed. For a networked installation, it is necessary that at least one individual concerned with the installation has *Network Administrator* privileges on the network domain on which the software is to be installed. For convenience, these individuals will be referred to as the System Administrators in the following documentation.

User Accounts

Each user of the SOLAAR*security* Software requires a user account. If the software is running on a stand-alone machine, this must be a local user account, and if the software is running in a networked environment, then it must be a network user account. The System Administrator must create these accounts. A network user account may either be on the same domain as the computer on which the Administrator and Server software is being installed or it may be on another domain that shares a bi-directional trust relationship with this domain.

The following information is associated with each user account:

- Users Full Name

This information must be supplied for compliance with the electronic signatures part of the 21 CFR Part 11 Rule, since it is a mandatory component of a signature manifestation. Even if your organization does not require electronic signatures, it is strongly recommended that this information be supplied, since the user’s full name is reported in audit trails together with the user account ID.

- Description

The contents of this field is not displayed in the SOLAAR*security* Client application, but can serve to provide useful additional information (such as job title) about the user if required.

- Password

The user’s password is one of the components used to generate an electronic signature and is also used to authenticate users during login and when using certain facilities provided by the software. When creating a new user account, the System Administrator should assign an initial password, and set “User Must Change Password at next login” to *True*. This ensures that after the first login the System Administrator no longer has any knowledge of the user’s password.

Group Membership

Access to operating system resources (such as files and folders) and features within the SOLAAR*security* Software can often be managed more efficiently through the use of groups. For example groups can be created to reflect the different roles within your organization, such as SOLAAR*security* Managers, Senior Analysts, and Instrument Operators. The System Administrator must set up these groups at the operating system level.

Individual users can be assigned membership of one or more of these groups and access rights can then be granted on a group basis rather than on an individual basis. The groups need not be mutually exclusive, but if users belong to more than one group, they will have only the rights that are common to all groups of which they are members.

It is recommended that at least one global group be created whose members are to be assigned the right to administer the SOLAAR*security* system – the SOLAAR*security* Managers. After installation and initial configuration by the System Administrator it is this list of users who will be able to assign access rights, define signature meanings and perform other administrative functions using the SOLAAR*security* Administrator application. By creating a specific group to perform this function, and transferring the administration right to members of this group, you can remove the need for System Administrators to be involved in day-to-day administration of the SOLAAR*security* Software.

User Rights Policy

The user rights and privileges associated with each user account and group should be reviewed as should group membership. Access control in SOLAAR*security* Software is performed with respect to the identity of a user (as defined by their user account) and the groups to which that user belongs. It is particularly important to restrict membership of groups with administrator rights to the appropriate user accounts.

Account Policy

An Account Policy defines password restrictions and account lockout behavior for all accounts on the system. The Account Policy should be reviewed to assess the suitability of the policy for compliance with 21 CFR Part 11.300 and for conformity with your own organization's standards and procedures.

Audit Policy

While the SOLAAR*security* Client application generates its own audit trails for all records that are created and modified, only the operating system can audit events that occur to electronic records outside the scope of the SOLAAR*security* Software, for example, the deletion of a file from a folder by a user.

The operating system audit policy allows you to define system and security events that are to be logged in the operating system event logs of System and Security. It is particularly important to review the policy settings for file access for those locations where users of the software will be permitted to save, modify, or delete files.

File/Folder Access Control

In conjunction with the audit policy, the access control settings for the locations where users of the software will be permitted to save, modify or delete files should be reviewed. There are some special considerations related to authorized user access to SOLAAR*security* Client files and folders that are described in detail in the SOLAAR*security* Client chapter, see “[SOLAAR*security* Client Software](#)” on [page 3-1](#).

Domain Trust Relationships

If you require users from multiple domains on your network to be able to access the SOLAAR*security* Client application; and for the access rights for these users to be managed centrally in a single security database, you must first ensure that the appropriate trust relationships exist between the domains.

There must exist a mutual (bi-directional) trust relationship between the domain on to which the SOLAAR*security* Server and Administrator software is installed and each of the domains that hold the user accounts and groups you wish to manage using the SOLAAR*security* Administrator application.

Event Log Configuration

If event logging has been enabled, the Server software will write the details of significant events into the operating system Application event log on the machine on which the SOLAAR*security* Server application is running. Such events are, for example, successful and failed attempts to log on to the SOLAAR*security* Clients.

The operating system can also write events into its Security and System event logs **if the operating system audit policy has been appropriately configured**. For example, failed attempts to access a user account can be

logged in order to meet 21 CFR Part 11.300 (d) “Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.”

The maximum size and event log wrapping behavior must be configured for these event logs so as to prevent loss of event log entries between backups.

Special Considerations for Stand-alone Systems

SOLAAR*security* may be configured to run as a stand-alone system with the Client and Administrator/Server applications installed on a single computer. This is intended for small laboratories with no network facilities.

Tip It is **not recommended** that multiple computers be configured this way for the following reasons:

- Each computer will have its own security database making the job of administration difficult.
- Each user could potentially have multiple signatures if access is allowed to multiple computers.
- The uniqueness of computer and account names and passwords cannot be enforced by the operating system.
- Date and time stamping of audit trail entries will not be synchronized to a single time source.
- Failed, unauthorized login attempts can not be reported in an immediate and urgent manner to system management.

Tip When running SOLAAR*security* as a stand-alone system, special attention should be given to the following:

- Each stand-alone computer must be given a unique name
- Unique local user accounts must be created for each user
- Users other than the System Administrator must not have access to the local administrator account
- Users must not be able to change the date and time on the local system clock.

NTLM System

The process of user authentication that forms the basis of user login and electronic signature generation for Windows XP is based around the Microsoft NTLM (NT Lan Manager) challenge/response protocol. To enable this protocol, the NTLM Security Support Provider service must be running on the server and client computers. This is usually installed and set up by default on Windows XP.

If the NTLM service is not present user authentication can not take place, and operations requiring user authentication cannot be performed.

Tip This is not applicable to Windows Vista, Windows 7, and Windows 10.

SOLAARsecurity Pre-installation Report

Please complete this form and send it (via fax or email) to your local support organization before your installation visit.

SOLAARsecurity Pre-installation Report Please complete this form and fax to your local support organization, before your installation visit.

Name of the network administrator who will be present for the installation		
Contact Details	Phone:	E-mail:
Location of Server PC		
Location of Client PC (Data Station)		
Pre-installation checks		
Operating system:	Server:	Client:
OR	Standalone:	
File system of disk or partition on which the Administration and Server software will be installed:		
Internet Explorer installed on Client PC(s)		Yes/No/Version:
Operating system configuration review		
User accounts	Reviewed	Yes/No
Groups	Reviewed	Yes/No
User rights	Reviewed	Yes/No
Account policy	Reviewed	Yes/No
Audit policy	Reviewed	Yes/No
File/Folder access control	Reviewed	Yes/No
Domain trust relationships	Reviewed	Yes/No
Event log configuration	Reviewed	Yes/No
NT LM service (if applicable)	Reviewed	Yes/No/N/A
Regional settings	Reviewed	Yes/No

I have read the pre-installation information and have made relevant checks as indicated above.
 Signature: _____ Date: _____

Name: _____ Position: _____

Figure 2-5. SOLAARsecurity Pre-Installation Report

Installation

Tip See “[Planning the Installation](#)” on page 2-6 for details on the NTLM Service.

Validation

In order to fully comply with the requirements of the Rule, the SOLAAR*security* Software installation and operation must be validated. Installation Qualification (IQ) and Operational Qualification (OQ) procedures for the Client Software are described in the AA Series Validator Logbook. If you are performing a validated installation, you **MUST** follow the procedures set out in the relevant section of the Log Book, referring where necessary to the instructions below.

Regional Options - Time Settings

The Server Software retrieves the time from the server computer in 24-hour format and sends it to the Client Software, which stores it in 24-hour format. However, when the time is displayed or printed, for example, in an audit trail, the Client Software formats it according to the regional options in place on the client computer.

If the client computer uses a 12-hour clock, the time will be displayed or printed in that format, resulting in ambiguous time stamps on audit trail entries.

The regional settings on every client computer need to be configured as follows in order to display and/or print the time stamp unambiguously.

❖ To configure the regional settings

1. Open Control Panel > Regional and Language Options.
2. Click the **Customize** button.
3. Select the Time tab.
4. Select *HH:mm:ss* for the time format. The capital H denotes that the 24-hour clock will be used.

File and Folder Protection

By default, the SOLAAR*security* installation does NOT protect the folders that contain the executable and data files that the applications require. If you are installing the Client Software on a machine that is

running a version of Windows that supports the NTFS file system, you can use the facilities provided by the operating system to protect these files.

The SOLAAR*security* Client Software installation will, by default, create the following folder structure on the hard drive:

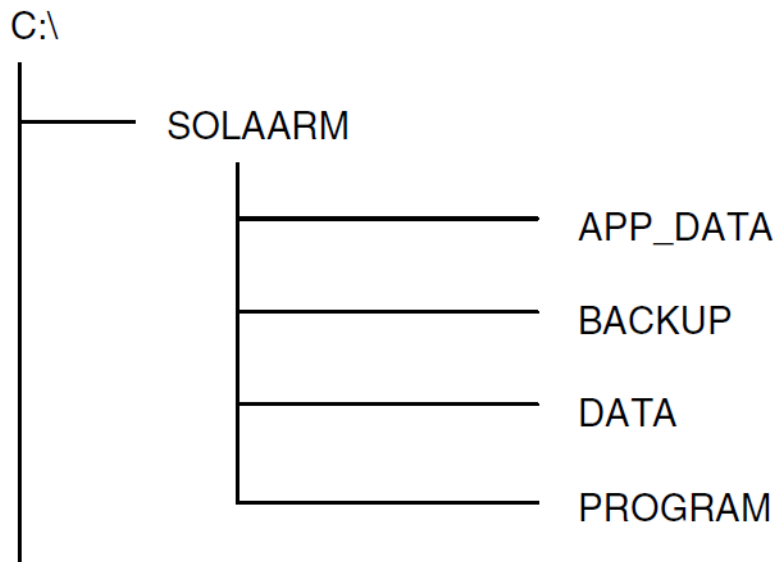


Figure 2-6. Folder structure of Thermo SOLAAR*security* Client PC

The C:\SOLAARM\APP_DATA folder will only exist if the SOLAAR Applications Library has been installed. The C:\SOLAARM\BACKUP folder will only exist if you have upgraded an earlier version of SOLAAR Software, and have chosen to save the previous version.

The C:\SOLAARM\PROGRAM folder is the location of the executable and other files required to run the Client applications. All users of the Client applications will require read/write access to this folder.

The C:\SOLAARM\DATA folder is the default location for Results (*.slr), Methods (*.slm), PQ Test Results (*.slr), and OQ Test Results (*.oqr) databases. All users will require read/write access to this folder if this default location is used. However, it is possible to set up DATA folders in any location accessible from the workstation. A user who has to read or write data to/from these files will require read/write access to the appropriate folder. We recommend that, for ease of use, at least the SOLAAR*security* Manager should have read/write access to the DATA folder.

Initial Installation

Pre-Installation procedures are described in the SOLAAR*security* Pre-Installation chapter, see “[Pre-Installation and Installation](#)” on [page 2-1](#). A Pre-Installation report template is included in this manual; you should confirm that you have a properly completed and signed copy of this form before starting the installation.

Before performing the installation, you should confirm that the computer hardware and Windows operating system are fully functional. If possible, we recommend that the software should be installed on a new machine, with a fresh installation of the Windows operating system.

You should check that:

- The Disk Check utility provided with Windows (Scandisk or Checkdisk) does not report any errors on the drive where you intend to install the software.
- There is at least 500 MBytes of free disk space available.
- Windows itself starts up and runs without error.
- Any other applications that have been installed on the machine also start up and run without errors.

We recommend that the SOLAAR*security* Administrator and Server applications should be installed before the Client applications. If you intend to install the software with the networked security option enabled, you must know the Computer Name of the machine on which the SOLAAR*security* Server application has been installed.

You will need:

- The SOLAAR Software CD.
 - The SOLAAR*security* Software CD.
 - Administrator rights on the machine where the software is to be installed.
- ❖ **To install the SOLAAR*security* Administrator and Server applications**
1. Start up the machine and log on to the operating system and network.
 2. When the operating system has loaded and the Windows desktop is displayed on the screen, insert the SOLAAR*security* Software CD into the CD drive.
 3. The CD will automatically start the installation, and will display the first installation dialog.

If you have disabled the Auto Run facility in the CD Drive Properties of your computer, use **Windows Explorer** or **My Computer** to navigate to the root folder of the CD drive, then double-click the **secure.exe** file.

4. Follow the instructions on the screen to install the first part of the SOLAAR*security* Administrator software.
5. When this process has been completed, remove the SOLAAR*security* CD from the CD drive.
6. Insert the SOLAAR Software CD into the CD drive. The CD will automatically start the installation, and will display the first installation dialog.

If you have disabled the Auto Run facility in the CD Drive Properties of your computer, use **Windows Explorer** or **My Computer** to navigate to the root folder of the CD drive, then double-click the **autoplay.exe** file.

7. The installation process will then start.
8. On the **SOLAAR Install** dialog, select **Install SOLAAR Security Server**. The Install Wizard will ask you for the information it needs to install the software. Carefully read each dialog when it is displayed, and provide the information requested. Click **Next** to move on to the next wizard page, or click **Back** to return to the previous one if you want to change the information you have provided.

The Install Wizard will suggest default locations for the software installation. We recommend that you accept these defaults, unless you have good reason not to use them, as this will ensure that instructions and procedures contained in the documentation that we supply will correctly describe your installation.

9. On the last dialog, you will have the final opportunity to review and change your install settings before the software is installed. If you want to change any of the settings you have made, click the **Back** button to reach the relevant dialog, make the changes that you want, then click the **Next** buttons until you reach this dialog again. When you are satisfied with your settings, click **Next** to start the installation.
10. When the installation has been completed, the SOLAAR*security* Administrator program will automatically be started. Refer to the section below, and grant permission to use the 'Administrator Security Database' Access Control to at least one individual or group (the SOLAAR*security* Manager), and grant permission to use the 'Run SOLAAR*security* Software' Access Control to at least one individual or group.

- If you do not grant these permissions at this time, the default settings of the Access Controls are such that only a member of the Administrators group on the local machine will be able to run the Administrator application, and no one will be able to run the Client software.
 - You can also grant or deny other permissions to use the various Access Controls, set the required System Policies, and define Signature meanings at this time, if you wish. Alternatively, the SOLAAR*security* Manager can complete these tasks later.
11. When you have finished, use the File > Save command, or click **File > Save** to save the Security database, then use the **File > Exit** command to close the application.
 12. The final Install Wizard page will be displayed. Click **Finish** to complete the installation, and remove the CD from the CD drive.

The Install Wizard will create shortcuts to the Administrator program in the Thermo SOLAAR program group that will appear on the Start menu. Optionally, use the facilities provided by Windows to create other shortcuts as required. You may find it convenient to create a shortcut on the Windows desktop, for example. Any shortcuts to the Administrator program that you create must point to the file:

C:\Program Files (x86)\SOLAARSecurity\Admin.exe

Details of SOLAAR*security* Users and their permissions, and other security information is held in the database file:

C:\Program Files (x86)\SOLAARSecurity\SolaarSecurity.sdb

If the files of the SOLAAR*security* Administrator application on the machine are not regularly backed up, you may wish to make special arrangements to ensure that a back-up copy of these files is maintained in a secure location.

The Install Wizard will install the SOLAAR*security* Server application as a Windows service, and will set it to start automatically each time Windows is started.

❖ **To install the SOLAAR*security* Client applications**

1. Start up the machine and log on to the operating system and network.
2. When the operating system has loaded and the Windows desktop is displayed on the screen, insert the SOLAAR Software CD into the CD drive.
3. The CD will automatically start the installation, and will display the first installation dialog.

If you have disabled the Auto Run facility in the CD Drive Properties of your computer, use **Windows Explorer** or **My Computer** to navigate to the root folder of the CD drive, then double-click the **autoplay.exe** file.

4. The installation process will then start.
5. On the **SOLAAR Install** dialog, select **Install SOLAAR Data Station**. The **Security Installation** dialog will then be displayed.
6. Select the type of security installation that you require, and click **OK**.
 - Do **not** select the option to install the software with no security, as this will install the software without any of the tools and facilities that are necessary to meet the requirements of the 21 CFR Part 11 Rule.
 - If you have selected the option to install a stand-alone security system, the Install Wizard will then start.
 - If you have selected the option to install a networked security system, the **Identify Security Server** dialog will be displayed. Enter the name of the computer on which the *SOLAARsecurity* Server is running, then click **OK**. The Install Wizard will then start.
7. The Install Wizard will ask you for the information it needs to install the software. Carefully read each dialog when it is displayed, and provide the information requested. Click **Next** to move on to the next wizard page, or click **Back** to return to the previous one if you want to change the information you have provided.

The Install Wizard will suggest default locations for the software installation. We recommend that you accept these defaults, unless you have good reason not to use them, as this will ensure that instructions and procedures contained in the documentation that we supply will correctly describe your installation.
8. On the last dialog, you will have the final opportunity to review and change your install settings before the software is installed. If you want to change any of the settings you have made, click the **Back** button to reach the relevant dialog, make the changes that you want, then click the **Next** buttons until you reach this dialog again. When you are satisfied with your settings, click **Next** to start the installation.
9. When the installation has been completed, the final Install Wizard page will be displayed. Click **Finish** to complete the installation, and remove the CD from the CD drive.

The Install Wizard will create shortcuts to the Client programs in the Thermo SOLAAR program group that will appear on the Start menu. Optionally, use the facilities provided by Windows to create other shortcuts as required. You may find it convenient to create a shortcut on the Windows desktop, for example. Any shortcuts to the Data Station Client that you create must point to the file

C:\SOLAARM\program\SOLAAR32.exe and shortcuts to OQ Test Client must point to C:\SOLAARM\program\oqtest.exe.

Updates, Repairs and Uninstalls

From time to time, we may release updated versions of the SOLAAR*security* Software that contain enhanced features and functions. When an installation is updated, any data created by the previous version will be retained. The procedure for updating the software will, in general, be the same as the initial Installation procedure, although the Install Wizard may require additional or different information.

The Install Wizard is also capable of repairing an existing installation, if for example, one or more of the files required become damaged. Again, this will NOT change any information stored in the SOLAAR databases.

❖ To repair or uninstall an installation of the SOLAAR*security* Administrator and Server software

1. Refer to your Windows documentation and Help files, and open the Windows **Control Panel**.
2. Select the **Add/Remove Programs** command.
3. In the list of Currently Installed Programs that will be displayed, select **Solaar Security Admin/Server**. Click the **Change/Remove** or **Uninstall/Change** button (depending on your Operating System) to display the Installation wizard.
4. Select the **Repair** option, and then click **Next** to repair your installation.
-or-
Select the **Automatic** option, and then click **Next** to uninstall your installation.

You can uninstall the SOLAAR*security* Administrator and Server applications.

Tip However, if the Server application is not running, the SOLAAR*security* Client software will not be able to run either.

❖ **To repair or uninstall an installation of the SOLAAR*security* Client software**

1. Refer to your Windows documentation and Help files, and open the Windows **Control Panel**.
2. Select the **Add/Remove Programs** command.
3. In the list of Currently Installed Programs that will be displayed, select **Thermo SOLAAR**. Click the **Change/Remove** or **Uninstall/Change** button (depending on your Operating System) to display the Installation wizard.
4. Select the **Repair** option, and then click **Next** to repair your installation.
-or-
Select the **Automatic** option, and then click **Next** to uninstall your installation.

You can uninstall the SOLAAR*security* Client applications.

SOLAAR*security* Client Software

This chapter shows the supported operating system versions, the management of user rights, and the Pre-installation Report form.

Contents

- [Starting the Client Applications on page 3-1](#)
- [Working with Analysis Results Records on page 3-3](#)
- [Working with Method Records on page 3-13](#)
- [Working with PQ Tests Results Records on page 3-22](#)
- [Working with OQ Test Results records on page 3-31](#)
- [Working with Access Controls on page 3-36](#)
- [Working with Signature Meanings on page 3-45](#)
- [Upgrade Considerations on page 3-46](#)

Starting the Client Applications

If you have been granted permission to use the Access Control 'Run SOLAAR*security* Software', you can start and use the Client Applications.

Before you can start one of the SOLAAR*security* Client applications, you must first start and log on to the workstation. You will have to provide your User Name and Password to allow the Windows Operating System to start. You should refer to your System Administrator if you can not start or log on the workstation.

❖ To start the Client application

1. Click on the **Start** button to display the Start menu.
2. Select the **Thermo SOLAAR** item to display available SOLAAR applications.
3. Click the name of the client application that you want to use.

Tip If you are not the person who started up and logged on to the workstation, you must shut down the workstation, restart it, and log on with your own identity before you can use the Client software.

The start up procedure is described in more detail in the main *iCE 3000 Series AAS SOLAAR Software Manual*.

Tip Note that the procedure described above is the default start up procedure. There are other start up options available that can be set up on the workstation, some of which are described in the *iCE 3000 Series AAS SOLAAR Software Manual*. If one or more of these options have been set up, please refer to any documentation or instruction that describes their use.

If the Client software does not start, but displays an error message indicating that Access is denied, you do not have permission to use it. If you think that you should be able to use it, refer to your SOLAARsecurity Manager.

If the 'Authenticate on Startup' System Policy has NOT been set, the Client software will start up immediately, ready for use.

If the 'Authenticate on Startup' System Policy HAS been set, the Authenticate User dialog will be displayed, so that you can confirm your identity before using the software.

❖ **To log on to a Client Application**

1. On the **Authenticate User** dialog, type your User Name and Password. These **MUST** be the same as those you used to log on to the Workstation.
2. Click **OK** to start the Client software.

The Client software will not start up if you have attempted to log on incorrectly, either because you are not the same person that logged on to the workstation, or because you have entered you User Name and/or Password incorrectly. Make a note of the content of any prompts or error messages displayed, and refer to your System Administrator or SOLAARsecurity Manager.

If the 'Perform Event Auditing' System Policy has been set, successful and unsuccessful attempts to log on to the Client software will generate events that will be logged in the Event Audit Trail (the Windows Applications Event Log on the server machine).

Tip Note that an event will NOT be generated if you can not start the Client software because you have not been granted permission to do so.

Working with Analysis Results Records

Analysis Results records are created by the Data Station Client software, and stored in a Results database. Each database can hold a very large number of records, limited only by the free disk space available to the workstation, and the Data Station Client can create an unlimited number of databases.

You can freely open and close Results databases using the commands provided on the **File** menu. Note that your SOLAARsecurity Manager may have restricted access to certain database files by using the Security properties of the files. If you get error messages indicating that the file is in use, or that you do not have access to it, you should refer to the appropriate authority to confirm that you should have access to this file before investigating further.

Creating Analysis Results Records

If you have been granted permission to use any of the following the Access Controls, you will be able to create Analysis Results records:

- 'Run Analyses'
- 'Perform Ash Atomize Analyses'
- 'Perform Calibrate Method'
- 'Perform Single Solution Measurement'
- 'Run Instrument Performance Wizard'

Analysis Results records are created automatically when you use any of the following Data Station Client functions:

- Action > Analyze (or clicking the **Analyze** toolbar button).
- Action > Single Solution (or clicking the **Single Solution** toolbar button)
- Action > Calibrate Method
- Action > Ash Atomize
- Action > Run Dual Analysis (or clicking on the Dual Analysis toolbar button)
- Check Instrument Performance Wizard

Tip The Action > Run Dual Analysis command will actually generate two Results Records.

Viewing Analysis Results records

You can view Analysis Results records in the Analysis Results window, and display any or all the Analysis Results records that are contained in the open Results database. Various options are available to allow you to search for specific records and select the information to be displayed. These are described in the *iCE 3000 Series AAS SOLAAR Software Manual*, and in detail in the *On-Line Help* system.

The Analysis Results window display is color coded to indicate the signature status of the records displayed. Records displayed against a white background have not had any signatures executed to them. Records displayed against a light green background have had one or more signatures executed to the record, and at least one of the signatures is valid. Records displayed against a yellow background have had one or more signatures executed to the record, but none of the signatures are now valid.

❖ To select Analysis Results record to display

1. Use the Options command on the Results menu or the Results Window shortcut menu to display the Results Display Options dialog.
2. Then use the facilities provided on this dialog to locate and select the Analysis Results record(s) that you want.
3. Close the Results Display Options dialog when you have completed your selection.

Click the **Help** button on the Results Display Options dialog to learn how to use the various functions provided.

Viewing an Analysis Results record Audit Trail

You can view the Audit Trail of any Analysis Results record from the Results Window.

❖ To view a Results Record Audit Trail

1. In the Results window, select a result that is part of the record that you are interested in to highlight it.
2. Open the Results menu, or right-click to display the **Results Window** shortcut menu, and then click **View Audit Trail**.

The Audit Trail will be displayed for you to review it. When you have finished, click **Close** to close the Audit Trail.

Viewing Analysis Results record Signatures

You can view the Signatures that have been executed to an Analysis Results record from the Results window.

❖ To view the Signatures associated with an Analysis Results record

1. In the Results window, select a result that is part of the record that you are interested in to highlight it.
2. Open the Results menu, or right-click to display the **Results Window** shortcut menu, and then click **View Signatures**. Details of any signatures that have been executed to the Analysis Results record will be displayed.

If a signature appears in crossed through text, it indicates that the signature is invalid. This is because something has happened to the Analysis Results record to change the data that it contains since the time that it was signed.

Signatures are also recorded and can be viewed in the Analysis Results record Audit Trail.

Signing an Analysis Results record

If you have been granted permission to use the 'Sign e-record' Access Control, you can execute an electronic signature to an Analysis Results record.

❖ To sign an Analysis Results record

1. Use the **Options** command on the Results menu or the Results Window shortcut menu to display the Results Display Options dialog.
2. Then use the facilities provided on this dialog to locate and select the Analysis Results record(s) that you want.
3. Close the Results Display Options dialog.
4. In the Results Window, select a result that is part of the record that you are interested in to highlight it.
5. Open the Results menu, or right-click to display the Results Window shortcut menu, and then click **Sign Results**. The User Authentication dialog will be displayed.
6. Type your User Name and Password.

If this is the first time the **User Authentication** dialog has been used since you started the Client application, you must enter both your User Name and your Password. However, if you have used this

dialog previously in the current session, your User Name will be remembered, and you will only have to enter your password. This behavior is consistent with that described in Section 11.200 (a) (1) of the Rule.

7. Select one of the **Signature Meanings** from the drop-down menu.
8. Click **OK** to execute the signature to the Analysis Results record.
 - An acknowledgment prompt will be displayed confirming the details of your signature.
 - You can view your signature as described in [“Viewing Analysis Results record Signatures”](#) on page 3-5.

Editing an Analysis Results record

If you have been granted permission to use any of the ‘Edit Results’, ‘Edit Peak Measurement’ or ‘Edit Sample Details’ Access Controls, you will be able to edit Analysis Results records.

Analysis Results records can be edited from the **Results Window**, by using the Results Editing functions located on the Results menu, and on the **Results Window** shortcut menu. The Results Editing functions are:

- Results > Delete Result
- Results > Restore Result
- Results > Use Height for calculations
- Results > Use Area for calculations
- Results > Edit Peak Measurement
- Results > Edit Sample Details

The use and effects of these editing tools are described in detail in the **Editing Results** topic of the On-Line Help system.

❖ To edit Analysis Results records

1. Use the **Options** command on the Results menu or the Results Window shortcut menu to open the Results Display dialog, to select and display the Analysis Results records you require.
2. Select a result contained in the appropriate Analysis Results record to highlight it.
3. Select the Results Editing command that you require from the Results menu or from the Results Window shortcut menu.

4. If the System Policy 'Confirm ID before editing' has been set, the Authenticate User dialog will be displayed. Type in your User Name (if necessary) and Password, and then click **OK**.

The results in the Analysis Record will then be re-calculated to take account of the effect of your edit, and entries to Audit Trail will be made that record the details of the edit.

Printing Analysis Results records

If you have been granted permission to use the 'Allow Printing' Access Control, you will be able to print Analysis Results records. If you have this permission, you will also be able to preview the printed output.

Printing the data contained in Analysis Results records can be accomplished through the commands available on sub-menus displayed when the File > Print and File > Print Preview commands are selected. The **Print a Report** wizard also allows printing of the data contained in Analysis Results records.

The layout and content of the printed report of the data contained in an Analysis Results record is controlled by the options set on the Print Options dialog. You must have permission to use the 'Edit Print Options' Access Control before you can change these options. The SOLAARsecurity Data Station Client allows a user who has been granted permission to edit the Print Options, to save one or more sets of Print Options as pre-defined templates. You can select one of these to use, even if you do not have permission to edit the Print Options directly.

❖ To print an Analysis Results record

1. Ensure that the printer that you intend to use has been properly installed, and that the appropriate options for paper size, print quality etc. have been selected. You can access these functions from the dialog displayed when you use the File > Print Setup command, but the options available will depend on the type of printer that has been installed.
2. Use the **Options** command on the Results menu or the Results Window shortcut menu to open the Results Display dialog, to select and display the Analysis Results records you require.

Either

3. Open the Wizard Launcher dialog and select the Print wizard, then follow the instructions displayed on the screen.
 - If the Confirm ID before printing System Policy has been set, the Authenticate User dialog will be displayed when the wizard has finished. You must enter your User Name (if it is not already displayed) and Password before the printing will start.

Or

4. Select the **File > Print Options** command to display the Print Options dialog.
5. Select the Print Options that you require, or load the template that you want to use, then close the Print Options dialog.
6. Select the **File > Print Preview > Results** command to preview your printed output.
 - If the Confirm ID before printing System Policy has been set, the Authenticate User dialog will be displayed. You must enter your User Name (if it is not already displayed) and Password before you can preview your printed output.
 - If you are satisfied with your preview, click **Print** on the Preview toolbar.
7. If you do not want to pre-view your printed output, select the **File > Print > Results** command to print your Report immediately.
 - If the Confirm ID before printing System Policy has been set, the Authenticate User dialog will be displayed. You must enter your User Name (if it is not already displayed) and Password before your Report will be printed.

Exporting Analysis Results records

If you have been granted permission to use the 'Allow Data Export' and/or 'Allow Clipboard Copy' Access Controls, you will be able to export the data contained in Analysis Results records for use in other applications.

Exporting the data contained in Analysis Results records as text files can be accomplished through the commands available on sub-menus displayed when the File > Export command is selected. Data from Analysis Results records can also be copied to the Windows Clipboard using the commands on the Edit > Copy sub-menu.

❖ **To export the data contained in an Analysis Results record**

1. Use the Options command on the Results menu or the Results Window shortcut menu to open the Results Display dialog, to select and display the Analysis Results records you require.
2. Open the **File > Export** sub-menu, and select the type of data that you wish to export, and text format that you want to export it in. The Result Export dialog will be displayed.

- If the Confirm ID before exporting System Policy has been set, the Authenticate User dialog will be displayed. You must enter your User Name (if it is not already displayed) and Password before you can pre-view your printed output.
3. Select the details of the data that you want to export, and click **OK** to display the Save As dialog.
 4. Specify a file name and location for the exported data, and then click **OK** to create the file.
- ❖ **To copy the data contained in an Analytical Results record to the Windows Clipboard**
1. Use the **Options** command on the Results menu or the Results Window context menu to open the Results Display dialog, to select and display the Analysis Results records you require.
 2. Open the **Edit > Copy** sub-menu, and select the type of data that you wish to copy to the clipboard, and format that you want to copy it in. The Result Export Options dialog will be displayed.
 3. Select the details of the data that you want to copy, and click **OK**.
 - If the Confirm ID before exporting System Policy has been set, the Authenticate User dialog will be displayed. You must enter your User Name (if it is not already displayed) and Password before you can pre-view your printed output.
 4. Navigate to the destination application, and then use that applications **Edit > Paste** command to transfer the data.

Managing Analysis Results records

The SOLAARsecurity Data Station Client software provides facilities for managing and maintaining Analysis Results records. To use these facilities, you must have been granted permission to use the 'Manage Databases', 'Copy Analyses', 'Delete Analyses' and 'Delete Signals' Access Controls.

You can access the Database Management functions from sub-menus displayed when you select the **File > Database Management** command. This command is available only when no Results database is open. You must first therefore use the **File > Close Results** command to close any open Results database before you can the database management functions.

Full descriptions of the database management functions are provided in the *On-Line Help* system, especially in the topic **How to >Work with Results > Work with Results Databases**, and will not be repeated here.

Compressing and Repairing Results databases

Compressing a Results database has no effect on the Analysis Results that it contains. The command simply reclaims any empty space caused by deleting Analysis Results records that may exist in a database.

If a Results database has become corrupted, perhaps because of a fault in Data Station hardware, it may be possible to repair it using the **Repair Database** command. Thermo Fisher Scientific does not guarantee that this function will always repair a damaged database, nor that the data originally contained in the damaged database can be recovered after the command has been used. If it is important that the databases remain undamaged, provision should be made for them to be saved to a secure location that is regularly backed up.

Before attempting to use the Repair Database command, you must first use the facilities provided in the Windows operating system to ensure that the file that contains the database is not itself corrupted. Running the Repair command on a database contained in a corrupted file is likely to result in the complete loss of data contained in the database. You should refer to the How to... topics of the *On-Line Help* system before using this function.

If the Repair function does successfully repair a database, the Analysis Results records contained in the database will be restored to their original state, including any signatures that have been executed to the records.

❖ To compress an Analysis Results database

1. Use the **File > Close Results** command to close any open Results databases.
2. Select the **File > Database Management > Compress Database** command to display the Database to Compress dialog.
3. Select the database that you want to compress, and click **OK**. The database will then be compressed.

❖ To repair an Analysis Results database

1. Use the **File > Close Results** command to close any open Results databases.
2. Select the **File > Database Management > Repair Database** command to display the Database to Repair dialog.
3. A prompt will be displayed, asking you to confirm that you have checked the file integrity with the tools provided with your Windows operating system.
4. Select the database that you want to repair, and click **OK**. The database will be repaired.

Copying Analysis Results records

If you have permission to use the 'Copy Analyses' Access Control, you can copy Analysis Results records from one Results database to another. When you use this function, an entire Analysis Results record, including its Audit Trail and any Signatures executed to it, are copied.

The copied record will contain an entry in its Audit Trail that identifies the database that it was copied from.

❖ To copy an Analysis Results record

1. Use the **File > Close Results** command to close any open Results databases.
2. Select the **File > Database Management > Copy Analyses** command to display the Database to Copy From dialog.
3. Select the database that contains the Analysis Results record that you want to copy, and click **OK**. The Copy Analyses dialog will be displayed.
4. In the Selected Analyses pane, select the Analysis Results record that you want to copy.
 - Facilities are provided on this dialog for applying filters to the database to locate the record(s) that you want to copy. Click **Help** to learn how to use these.
5. Click **Add** to move the selected record to the Analyses to Copy pane. Repeat this procedure for as many records as you want to copy.
6. Type the name and path to the destination database in the Database to copy to field, or click the **Browse** button to locate it.
7. Click the **Copy** command to copy the records.

Deleting Analysis Results records

If you have permission to use the 'Delete Analyses' Access Control, you can delete Analysis Results records from a Results database. When you use this function, an entire Analysis Results record, including its Audit Trail and any Signatures executed to it, is deleted.

Use of this function generates an event that is recorded in the Event Audit Trail, if the 'Perform Event Auditing' System Policy is set. The event will contain details of the Analysis Results record that has been deleted, and the database from which it was deleted.

NOTICE

It is not possible to restore a deleted Analysis Results record. The granting of permission to use this function should therefore be considered carefully, and the circumstances in which it may be used should be clearly set out in an appropriate SOP.

❖ **To delete an Analysis Results record**

1. Use the **File > Close Results** command to close any open Results databases.
2. Select the **File > Database Management > Delete Analyses** command to display the Database to Delete Analysis From dialog.
3. Select the database that contains the Analysis Results record that you want to delete, and click **OK**. The Delete Analyses from Database dialog will be displayed.
4. In the Selected Analyses pane, select the Analysis Results record that you want to delete.
 - Facilities are provided on this dialog for applying filters to the database to locate the record(s) that you want to copy. Click **Help** to learn how to use these.
5. Click **Add** to move the selected record to the Analyses to Delete pane. Repeat this procedure for as many records as you want to delete.
6. Click **Delete** to delete the records.

Working with Method Records

Method records are created by the Data Station Client software, and stored in a Methods database. A Method record is also copied and stored in every Analysis Results record. Each database can hold a very large number of records, limited only by the free disk space available to the workstation, and the Data Station Client can create an unlimited number of databases. The currently open Methods database is normally referred to as the Methods Library.

You can open and close Methods Libraries using the **Browse** command provided on the **Methods Library** dialog. Note that your SOLAARsecurity Manager may have restricted access to certain database files by using the Security properties of the files. If you get error messages indicating that the file is in use, or that you do not have access to it, you should refer to the appropriate authority to confirm that you should have access to this file before investigating further.

SOLAARsecurity Data Station Client software makes use of the concept of a Current Method that is distinct from a Method record. The Current Method is the Method that is displayed when you open the **Method** dialog, and it is the Method that will be used when you run analyses, perform single solution measurements, and carry out other functions in the software that are concerned with making measurements. If you have been granted permission to use the 'Edit Methods' Access Control, you can freely edit the Current Method on the Method dialog, and the effects of your edits can be investigated immediately. However, the Current Method is NOT a Method record in the context of the Rule – it is a transient copy of a Method record, and is primarily intended for method development purposes. A Method record is created only when the Current Method is saved in the Methods Library for the first time. At this point, a Method Audit Trail is created, and can be viewed from the commands available on the Methods Library dialog. If a saved Method is loaded from the library, edited, and saved again, the Audit Trail will record the differences between the saved versions – it will NOT record all the individual edits themselves that created the differences between the versions.

If a Method is loaded from the Library, edited, then used to create an Analysis Results record, the edited Method record will be saved in the Analysis Results record, and its Audit Trail will be updated.

Tip If you have been granted permission to use the 'Sign e-record' Access Control, you will be able to sign any Method record that has been saved in the Methods Library. You CANNOT sign the Current Method.

Most of the functions required to work with Method records and Method databases can be found on the **Methods Library** dialog.

❖ **To open the Methods Library dialog**

1. Select the **Edit > Method** command, or click on the Edit Method toolbar button, to open the tabbed Method dialog.
2. If necessary, move to the General tab of Method dialog.
3. Click on the **Library** button to display the Methods Library dialog.

Creating Method records

You can create Method records if you have been granted permission to use the 'Edit Methods' Access Control. A Method record is created when the Current Method is saved to the Methods Library. If you want to create a new Method, you should use the New button on the General tab of the Method dialog to reset the Current Method to the default parameters for the first element that you intend to measure and then immediately provide a name for the Method and use the Save button to create the record in the Methods Library. This will create a new, empty Audit Trail for the Method record. You can then edit the Method as required, and save the final version. By following this procedure, the Method record Audit Trail will start with all parameters at their known, default values, and all subsequent changes to them will be recorded.

❖ **To create a new Method record from the Method dialog**

1. Select the Edit > Method command, or click the **Edit Method** toolbar button, to open the tabbed Method dialog.
2. If necessary, move to the General tab of Method dialog.
3. Click the **New** button to display the Element dialog.
4. Select the first element that you want to use in your Method, and Technique that you want to use to measure it.
 - Click the **Help** button of the Method dialog for a detailed discussion of the issues associated with creating a new Method.
5. Click **OK** to close the Element dialog. You have now re-set the Current Method to the default parameters for the selected element.
6. On the General page of the Method, type a meaningful Method name and Description of the Method into the relevant fields.
7. Click the **Save** button to save the new Method record in the Methods Library. A prompt will be displayed asking you to confirm that you want to save the Method record with the Method Name that you entered. Click **OK** to confirm this, and the Method record will be saved in the Method Library.

Alternatively, you can create a new Method using the Method Wizard to guide and prompt you. When the Method Wizard finishes, the new Method you have created will be the Current Method. You must save this in the Methods Library by following [step 7](#) above to create a new Methods record.

Viewing Method records

Method records can be viewed on the **Methods Library** dialog.

The **Methods Library** dialog display is color coded to indicate the signature status of the records displayed. Records displayed against a white background have not had any signatures executed to them. Records displayed against a light green background have had one or more signatures executed to the record, and at least one of the signatures is valid. Records displayed against a yellow background have had one or more signatures executed to the record, but none of the signatures are now valid.

❖ To view a Method record

1. Open the **Methods Library** dialog.
2. Click the **Method Name** of the Method record to select it.
3. The description of the Method record will be displayed.

If you want to see the actual Method parameters, you must use the **Load** button to load the Method record from the Library into the Current Method. You can then view the entire Method in the **Method** dialog.

❖ To view a Method record Audit Trail

1. Open the **Methods Library** dialog.
2. Click the **Method Name** of the Method record to select it.
3. Click the **Audit Trail** button to display the Audit Trail for the selected record.

❖ To view a Method record Signatures

1. Open the **Methods Library** dialog.
2. Click the **Method Name** of the Method record to select it.
3. Click the **Signatures** button to display the Signature history for the selected record.

Signing Method records

If you have been granted permission to use the 'Sign e-record' Access Control, you can execute an electronic signature to a Method record.

Method records can be signed on the **Methods Library** dialog.

❖ To sign a Method record

1. Open the **Methods Library** dialog.
2. Click the **Method Name** of the Method record to select it.
3. Click the **Sign** button to display the User Authentication dialog.
4. Type in your User Name and Password.
 - If this is the first time the User Authentication dialog has been used since you started the Client application, you must enter both your User Name and your Password. However, if you have used this dialog previously in the current session, your User Name will be remembered, and you will only have to enter your password. This behavior is consistent with that described in Section 11.200 (a) (1) of the Rule.
5. Select one of the Signature Meanings from the drop-down menu.
6. Click **OK** to execute the signature to the Method record.

Loading Method records

If you want to use a Method record to perform an analysis, or if you want to review, edit or print the Method parameters, you must load the Method record, so that it becomes the Current Method and is displayed in the **Method** dialog.

❖ To load a Method record

1. Open the **Methods Library** dialog.
2. Click the Method Name of the Method record to select it.
3. Click the **Load** button to load the Method record as the Current Method.
4. Close the Methods Library dialog.

If you have not been granted permission to use the 'Edit Method' Access Control, a warning prompt will be displayed.

Editing and Saving Method records

If you have been granted permission to use the 'Edit Method' Access Control, you can edit and save a Method record.

The tabbed Method dialog provides facilities for you to edit the Sequence Table and Action Matrix, and the Sample Details, even though these are not part of the Method record. If you have not been granted permission to use the 'Edit Method' Access Control, then you will not be able to edit these settings on the Method dialog. However, if you have permission to use the 'Edit Sequence' and 'Edit Sample Details' Access Controls, then you will be able to edit these on separate dialogs. Note that editing the Sequence Table and Action Matrix, and the Sample Details, will NOT invalidate any signatures that have been executed to the Method record.

❖ To Edit and Save a Method record

1. Load a Method record from the Methods Library as described in [“Loading Method records”](#) on [page 3-16](#).
2. Select the Edit > Method command, or click the **Edit Method** tool bar button to open the tabbed Method dialog.
3. Edit the Method parameters as required.
4. Click the **Save** button to save the new Method record in the Methods Library. A prompt will be displayed asking you to confirm that you want to save the Method record with the Method Name that you entered. Click **OK** to confirm this, and the Method record will be saved in the Method Library.
 - It is not essential to provide a new Method Name for your edited Method record. However, you may find it useful to include a summary of your edits in either the Method Name or in the Description field, so that you can easily distinguish the edited and original versions of the Method record in the Methods Library dialog.

Printing Method records

A printed copy of a Method record can be made by loading the Method record from the Method Library into the Current Method, then selecting the File > Print > Method or File Print Preview > Method commands. You must have been granted permission to use the 'Allow Printing' Access Control before you can print a Method record. If the 'Confirm ID before Printing' System Policy has been set, you will have to properly complete the User Authentication dialog before printing.

❖ **To print a Method record**

1. Load a Method record from the Methods Library as described in “Loading Method records” on page 3-16.
 - Ensure that the printer that you intend to use has been properly installed, and that the appropriate options for paper size, print quality etc. have been selected. You can access these functions from the dialog displayed when you use the File > Print Setup command, but the options available will depend on the type of printer that has been installed.
2. Select the File > Print Preview > Method command to preview your printed output.
 - If the Confirm ID before printing System Policy has been set, the Authenticate User dialog will be displayed. You must enter your User Name (if it is not already displayed) and Password before you can preview your printed output.
 - If you are satisfied with your preview, click the **Print** button on the Preview tool bar.
3. If you do not want to pre-view your printed output, select the File > Print > Method command to print your Report immediately.
 - If the Confirm ID before printing System Policy has been set, the Authenticate User dialog will be displayed. You must enter your User Name (if it is not already displayed) and Password before your Report will be printed.

Managing Method records

The SOLAARsecurity Data Station Client software provides facilities for managing and maintaining Method records. To use these facilities, you must have been granted permission to use the ‘Manage Databases’, ‘Copy Methods’ and ‘Delete Methods’ Access Controls.

You can access the Database Management functions from sub-menus displayed when you select the File > Database Management command. This command is available only when no Results database is open. You should first therefore use the File > Close Results command to close any open Results database before using the database management functions.

Full descriptions of the database management functions are provided in the On-Line Help system, especially in the topic How to > Work with Methods > Work with Method Databases, and will not be repeated here.

Compressing and Repairing Methods databases

Compressing a Methods database has no effect on the Method records that it contains. The command simply reclaims any empty space that may have been caused by deleting Method records.

If a Methods database has become corrupted, perhaps because of a fault in Data Station hardware, it may be possible to repair it using the Repair Database command. Thermo Fisher Scientific does not guarantee that this function will always repair a damaged database, nor that the data originally contained in the damaged database can be recovered after the command has been used. If it is important that the databases remain undamaged, provision should be made for them to be saved to a secure location that is regularly backed up.

Before attempting to use the Repair Database command, you must first use the facilities provided in the Windows operating system to ensure that the file that contains the database is not itself corrupted. Running the Repair command on a database contained in a corrupted file is likely to result in the complete loss of data contained in the database. You should refer to the How to... topics of the On-Line Help system before using this function.

If the Repair function does successfully repair a database, the Method records contained in the database will be restored to their original state, including any signatures that have been executed to the records.

❖ To compress a Methods database

1. Use the File > Close Results command to close any open Results databases.
2. Select the File > Database Management > Compress Database command to display the Database to Compress dialog.
3. Select the database that you want to compress, and click **OK**. The database will then be compressed.

❖ To repair a Methods database

1. Select File > Close Results to close any open Results databases.
2. Select the File > Database Management > Repair Database command to display the Database to Compress dialog.
3. A prompt will be displayed, asking you to confirm that you have checked the file integrity with the tools provided with your Windows operating system. If you have done this, click **OK** to start the repair process.
4. Select the database that you want to compress, and click **OK**.

The database will then be repaired, if possible.

Copying Method records

If you have permission to use the 'Copy Methods' Access Control, you can copy Method records from one Methods database to another. When you use this function, an entire Method record, including its Audit Trail and any Signatures executed to it, are copied. The Sequence Table, Analysis Matrix and Sample Details associated with the Method record are also copied.

The copied record will contain an entry in its Audit Trail that identifies the database that it was copied from.

❖ To copy a Method record

1. Use the File > Close Results command to close any open Results databases.
2. Select the File > Database Management > Copy Method command to display the Database to Copy From dialog.
3. Select the database that contains the Method record that you want to copy, and click **OK**. The Copy Method dialog will be displayed.
4. In the Selected Methods pane, select the Method record that you want to copy.
 - Facilities are provided on this dialog for applying filters to the database to locate the record(s) that you want to copy. Click the **Help** button to learn how to use these.
5. Click the **Add** button to move the selected record to the Methods to Copy pane. Repeat this procedure for as many records as you want to copy.
6. Type the name and path to the destination database in the Database to copy to field, or click the Browse button to locate it.
7. Click the **Copy** command to copy the records.

Deleting Method records

If you have permission to use the 'Delete Methods' Access Control, you can delete Method records from a Methods database. When you use this function, an entire Method record, including its Audit Trail and any Signatures executed to it, and the associated Sequence Table, Action Matrix and Sample Details are deleted.

Use of this function generates an event that is recorded in the Event Audit Trail, if the 'Perform Event Auditing' System Policy is set. The event will contain details of the Method record that has been deleted, and the database from which it was deleted.

NOTICE

It is not possible to restore a deleted Method record. The granting of permission to use this function should therefore be considered carefully, and the circumstances in which it may be used should be clearly set out in an appropriate SOP.

❖ To delete a Method record

1. Use the File > Close Results command to close any open Results databases.
2. Select the File > Database Management > Delete Method command to display the Database to Delete Method From dialog.
3. Select the database that contains the Method record that you want to delete, and click **OK**. The Delete Method from Database dialog will be displayed.
4. In the Selected Methods pane, select the Method record that you want to delete.
 - Facilities are provided on this dialog for applying filters to the database to locate the record(s) that you want to copy. Click the **Help** button to learn how to use these.
5. Click the **Add** button to move the selected record to the Methods to Delete pane. Repeat this procedure for as many records as you want to delete.
6. Click the **Delete** command to delete the records.

Working with PQ Tests Results Records

PQ Tests Results records are created by the Data Station Client software, and stored in a PQ Results database. Each database can hold a very large number of records, limited only by the free disk space available to the workstation, and the Data Station Client can create an unlimited number of databases.

You can freely open and close PQ Results databases using the commands provided on the File menu. Note that your SOLAARsecurity Manager may have restricted access to certain database files by using the Security properties of the files. If you get error messages indicating that the file is in use, or that you do not have access to it, you should refer to the appropriate authority to confirm that you should have access to this file before investigating further.

Creating PQ Analysis Results records

If you have been granted permission to use the 'Perform PQ Tests' Access Control, you will be able to create PQ Tests Results records.

PQ Tests Results records are created automatically when you use the Action/Run PQ Tests command.

The new PQ Tests Results record will be stored in the PQ Results database that is selected at the time that it is created. You can select the PQ Results database that will be used to store the PQ Tests Result record by using the Edit > OQ/PQ Database Locations command to display the OQ/PQ Database Locations dialog.

At the same time that a PQ Tests Results record is created, a new Data Audit Trail is created, and attached to the record. The first entry in the Audit Trail will record the creation of the record.

Viewing PQ Tests Results records

You can view PQ Tests Results records in the Results window, and display any or all the PQ Tests Results records that are contained in the open PQ Results database. Various options are available to allow you to search for specific records and select the information to be displayed. These are described in the SOLAAR Users Manual, and in detail in the On Line Help system.

The Results display is color coded to indicate the signature status of the records displayed. Records displayed against a white background have not had any signatures executed to them. Records displayed against a light green background have had one or more signatures executed to the

record, and at least one of the signatures is valid. Records displayed against a yellow background have had one or more signatures executed to the record, but none of the signatures are now valid.

❖ **To select PQ Test Results record to display**

1. Use the File > Open Results command to select the PQ database that contains the records that you want to view.
 - The only distinction between a PQ Results database and a normal Results database is the type of Results records that they contain.
2. Use the **Options** command on the Results menu or the Results Window context menu to display the Results Display Options dialog, then use the facilities provided on this dialog to locate and select the PQ Tests Results record(s) that you want. Close the Results Display Options dialog when you have completed your selection.
 - Click the **Help** button on the Results Display Options dialog to learn how to use the various functions provided.

Viewing a PQ Test Results record Audit Trail

You can view the Audit Trail of any PQ Tests Results record from the Results window.

❖ **To view a PQ Test Results record Audit Trail**

In the Results window, click a result that is part of the record that you are interested in to highlight it.

1. Open the Results menu, or right click to display the Results Window shortcut menu, and then click the **View Audit Trail** command.

The Audit Trail will be displayed for you to review it. When you have finished, click the **Close** button to close the Audit Trail.

Viewing PQ Test Results record Signatures

You can view the Signatures that have been executed to a PQ Tests Result record from the **Results** window.

❖ **To view the Signatures executed to a PQ Tests Result record**

1. In the Results window, click a result that is part of the record that you are interested in to highlight it.

2. Open the Results menu, or right click to display the Results Window shortcut menu.
3. Click the **Signatures** command to review any signatures that have been executed to the PQ Tests Result record.

If a signature appears in crossed through text, it indicates that the signature is invalid. This is because something has happened to the Analysis Results record to change the data that it contains since the time that it was signed.

Signatures are also recorded and can be viewed in the PQ Tests Result record Audit Trail.

Signing a PQ Tests Result record

If you have been granted permission to use the 'Sign e-record' Access Control, you can execute an electronic signature to a PQ Tests Result record.

❖ To sign a PQ Tests Result record

1. Use the **Options** command on the Results menu or the Results Window context menu to display the Results Display Options dialog, then use the facilities provided on this dialog to locate and select the PQ Tests Result record(s) that you want. Close the Results Display Options dialog.
2. In the Results window, click a result that is part of the record that you are interested in to highlight it.
3. Open the Results menu, or right click to display the Results Window shortcut menu, and then click the Sign Results command. The User Authentication dialog will be displayed.
4. Type your User Name and Password.
 - If this is the first time the User Authentication dialog has been used since you started the Client application, you must enter both your User Name and your Password. However, if you have used this dialog previously in the current session, your User Name will be remembered, and you will only have to enter your password. This behavior is consistent with that described in Section 11.200 (a) (1) of the Rule.
5. Select one of the Signature Meanings from the drop-down menu.
6. Click **OK** to execute the signature to the PQ Analysis Results record.
7. An acknowledgment prompt will be displayed confirming the details of your signature. Click **OK** to close this.

You can view your signature as described in the section above.

Printing PQ Tests Result records

If you have been granted permission to use the 'Allow Printing' Access Control, you will be able to print PQ Tests Result records. If you have this permission, you will also be able to preview the printed output.

Printing the data contained in PQ Tests Result records can be accomplished through the commands available on sub-menus displayed when the File/Print and File/Print Preview commands are selected. The Print a Report Wizard also allows printing of the data contained in Analysis Results records.

The layout and content of the printed report of the data contained in a PQ Tests Result record is controlled by the options set on the Print Options dialog. You must have permission to use the 'Edit Print Options' Access Control before you can change these options. The SOLAARsecurity Data Station Client allows a user who has been granted permission to edit the Print Options to save one or more sets of Print Options as pre-defined templates. You can select one of these to use, even if you do not have permission to edit the Print Options directly.

❖ To print a PQ Tests Result record

1. Ensure that the printer that you intend to use has been properly installed, and that the appropriate options for paper size, print quality etc. have been selected. You can access these functions from the dialog displayed when you use the File/Print Setup command, but the options available will depend on the type of printer that has been installed.
2. Use the Options command on the Results menu or the Results Window context menu to open the Results Display dialog, to select and display the PQ Tests Results records you require.

Either

3. Open the Wizard Launcher dialog and select the Print Wizard, then follow the instructions displayed on the screen.
 - If the Confirm ID before printing System Policy has been set, the Authenticate User dialog will be displayed when the Wizard has finished. You must enter your User Name (if it is not already displayed) and Password before the printing will start.

Or

4. Select the File/Print Options command to display the Print Options dialog.

5. Select the Print Options that you require, or load template that you want to use, then close the Print Options dialog.
6. Select the File > Print Preview Results command to preview your printed output.
 - If the Confirm ID before printing System Policy has been set, the Authenticate User dialog will be displayed. You must enter your User Name (if it is not already displayed) and Password before you can pre-view your printed output.
 - If you are satisfied with your pre-view, click the Print button on the preview tool bar.
7. If you do not want to pre-view your printed output, select the File/Print/Results command to print your Report immediately.
8. If the Confirm ID before printing System Policy has been set, the Authenticate User dialog will be displayed. You must enter your User Name (if it is not already displayed) and Password before your Report will be printed.

These procedures will print a Report containing the analytical results that have been generated during the PQ Test. It is also possible to print a summary of the test results.

❖ **To print the Test Results contained in a PQ Tests Result record**

1. Ensure that the printer that you intend to use has been properly installed, and that the appropriate options for paper size, print quality etc. have been selected. You can access these functions from the dialog displayed when you use the File/Print Setup command, but the options available will depend on the type of printer that has been installed.
2. Use the **Options** command on the Results menu or the Results Window context menu to open the Results Display dialog, to select and display the PQ Tests Result records you require. Close the Results Display dialog.
3. Open the Results menu, or right-click to display the Results Window context menu.
4. Select the View PQ Results command to display the PQ Test Results dialog.
5. Click **Print** to print the PQ Test Report.
 - If the Confirm ID before printing System Policy has been set, the Authenticate User dialog will be displayed. You must enter your User Name (if it is not already displayed) and Password before your Report will be printed.

Exporting PQ Tests Result records

If you have been granted permission to use the 'Allow Data Export' and/or 'Allow Clipboard Copy' Access Controls, you will be able to export the data contained in PQ Tests Result records for use in other applications. Note that you can only export the analytical results. You cannot export the Test Results information displayed on the PQ Test Results dialog.

Exporting the data contained in PQ Tests Result records as text files can be accomplished through the commands available on sub-menus displayed when the File/Export command is selected. Data from PQ Tests Result records can also be copied to the Windows Clipboard using the commands on the Edit/Copy sub-menu.

❖ To export the data contained in a PQ Tests Result record

1. Use the **Options** command on the Results menu or the Results Window context menu to open the Results Display dialog, to select and display the PQ Tests Result records you require.
2. Open the File > Export sub-menu, and select the type of data that you wish to export, and text format that you want to export it in. The Result Export dialog will be displayed.
 - If the Confirm ID before exporting System Policy has been set, the Authenticate User dialog will be displayed. You must enter your User Name (if it is not already displayed) and Password before you can pre-view your printed output.
3. Select the details of the data that you want to export, and click **OK** to display the Save As dialog.
4. Specify a file name and location for the exported data, and then click **OK** to create the file.

❖ To copy the data contained in a PQ Tests Result record to the Windows Clipboard

1. Use the **Options** command on the Results menu or the Results Window context menu to open the Results Display dialog, to select and display the Analysis Results records you require.
2. Open the Edit > Copy sub-menu, and select the type of data that you wish to copy to the clipboard, and format that you want to copy it in. The Result Export Options dialog will be displayed.
3. Select the details of the data that you want to copy, and click **OK**.
 - If the Confirm ID before exporting System Policy has been set, the Authenticate User dialog will be displayed. You must enter your User Name (if it is not already displayed) and Password before you can pre-view your printed output.

4. Navigate to the destination application, and then use that applications Edit > Paste command to transfer the data.

Managing PQ Tests Result records

The SOLAARsecurity Data Station Client software provides facilities for managing and maintaining PQ Tests Result records. To use these facilities, you must have been granted permission to use the 'Manage Databases' and 'Copy Analyses' Access Controls.

You can access the Database Management functions from sub-menus displayed when you select the File > Database Management command. This command is available only when no Results database is open. You should first therefore use the File > Close Results command to close any open Results database before using the database management functions.

Full descriptions of the database management functions are provided in the On-Line Help system, especially in the topic How to > Work with Results/Work with Results Databases, and will not be repeated here.

Compressing and Repairing PQ Results databases

Compressing a PQ Results database has no effect on the PQ Analysis Results that it contains. The command simply reclaims any empty space that may exist in the database.

If a PQ Results database has become corrupted, perhaps because of a fault in Data Station hardware, it may be possible to repair it using the Repair Database command. Thermo Fisher Scientific does not guarantee that this function will always repair a damaged database, nor that the data originally contained in the damaged database can be recovered after the command has been used. If it is important that the databases remain undamaged, provision should be made for them to be saved to a secure location that is regularly backed up.

Before attempting to use the Repair Database command, you must first use the facilities provided in the Windows operating system to ensure that the file that contains the database is not itself corrupted. Running the Repair command on a database contained in a corrupted file is likely to result in the complete loss of data contained in the database. You should refer to the How to... topics of the *On Line Help system* before using this function.

If the Repair function does successfully repair a database, the PQ Tests Result records contained in the database will be restored to their original state, including any signatures that have been executed to the records.

❖ **To compress a PQ Test Results database**

1. Use the File > Close Results command to close any open Results databases.
2. Select the File > Database Management/Compress Database command to display the Database to Compress dialog.
3. Select the database that you want to compress, and click **OK**. The database will then be compressed.

❖ **To repair a PQ Test Results database**

1. Use the File > Close Results command to close any open Results databases.
2. Select the File > Database Management/Repair Database command to display the Database to Compress dialog.
3. A prompt will be displayed, asking you to confirm that you have checked the file integrity with the tools provided with your Windows operating system. If you have done this, click **OK** to start the repair process.
4. Select the database that you want to compress, and click **OK**. The database will be repaired.

Copying PQ Tests Result records

If you have permission to use the 'Copy Analyses' Access Control, you can copy PQ Tests Result records from one PQ Results database to another. When you use this function, an entire PQ Tests Result record, including its Audit Trail and any Signatures executed to it, are copied. Note that you CANNOT copy PQ Analysis Results records to a normal Results database, nor can you copy normal Analysis Results records to a PQ Results database. However, either type of record can be copied into an empty Results database – it is the type of record that the database contains that determines whether it is a normal or a PQ Results database.

The copied record will contain an entry in its Audit Trail that identifies the database that it was copied from.

❖ **To copy a PQ Tests Result record**

1. Use the File > Close Results command to close any open Results databases.
2. Select the File > Database Management > Copy Analyses command to display the Database to Copy From dialog.

3. Select the database that contains the Analysis Results record that you want to copy, and click **OK**. The Copy Analyses dialog will be displayed.
4. In the Selected Analyses pane, select the PQ Tests Result record that you want to copy.
 - Facilities are provided on this dialog for applying filters to the database to locate the record(s) that you want to copy. Click the **Help** button to learn how to use these.
5. Click the **Add** button to move the selected record to the Analyses to Copy pane. Repeat this procedure for as many records as you want to copy.
6. Type the name and path to the destination database in the Database to copy to field, or click the **Browse** button to locate it.
7. Click the **Copy** command to copy the records.

Working with OQ Test Results records

OQ Tests Result records are created by the OQ Tests Client software, and stored in an OQ Results database. Each database can hold a very large number of records, limited only by the free disk space available to the workstation, and the OQ Tests Client can create an unlimited number of databases.

You can freely open and close OQ Results databases using the commands provided on the File menu. Note that your SOLAARsecurity Manager may have restricted access to certain database files by using the Security properties of the files. If you get error messages indicating that the file is in use, or that you do not have access to it, you should refer to the appropriate authority to confirm that you should have access to this file before investigating further.

Creating OQ Tests Result records

If you have been granted permission to use the 'Perform OQ Tests' Access Control, you will be able to create OQ Tests Results records.

OQ Tests Result records are created automatically when you use the Action/Start Test Sequence command or click on the Start Test Sequence tool bar button.

The new OQ Tests Result record will be stored in the OQ Results database that is open at the time that it is created

At the same time that an OQ Tests Results record is created, a new Data Audit Trail is created, and attached to the record. The first entry in the Audit Trail will record the creation of the record.

Viewing OQ Tests Result records

You can view OQ Tests Result records in the OQ Results window, and display any or all the OQ Tests Result records that are contained in the open OQ Results database. Various options are available to allow you to search for specific records and select the information to be displayed. These are described in the SOLAAR Users Manual, and in detail in the On Line Help system.

The OQ Results window display is color coded to indicate the signature status of the records displayed. Records displayed against a white background have not had any signatures executed to them. Records displayed against a light green background have had one or more signatures executed to the record, and at least one of the signatures is valid. Records displayed against a yellow background have had one or more signatures executed to the record, but none of the signatures are now valid.

❖ **To select OQ Tests Result records to display**

1. Use the File > Open Results command to select the OQ database that contains the records that you want to view.
2. Use the Display Options command on the OQ Results menu or the OQ Results Window context menu to display the Results Display Options dialog, then use the facilities provided on this dialog to locate and select the OQ Tests Result record(s) that you want. Close the Results Display Options dialog when you have completed your selection.
 - Click the **Help** button on the Results Display Options dialog to learn how to use the various functions provided.

Viewing an OQ Tests Result record Audit Trail

You can view the Audit Trail of any OQ Tests Results record from the OQ Results window.

❖ **To view an OQ Tests Result record Audit Trail**

1. In the OQ Results Window, click on a result that is part of the record that you are interested in to highlight it.
2. Open the Results menu, or right-click to display the Results Window context menu, and then click the **View Audit Trail** command.

The Audit Trail will be displayed for you to review it. When you have finished, click the **Close** button to close the Audit Trail.

Viewing OQ Tests Result record Signatures

You can view the Signatures that have been executed to an OQ Tests Result record from the OQ Results Window.

❖ **To view the Signatures associated with an OQ Tests Result record**

1. In the Results Window, click a result that is part of the record that you are interested in to highlight it.
2. Open the Results menu, or right-click to display the OQ Results Window context menu.
3. Click the **View Signatures** command to review any signatures that have been executed to the OQ Tests Result record.

If a signature appears in crossed through text, it indicates that the signature is invalid. This is because something has happened to the OQ Tests Result record to change the data that it contains since the time that it was signed.

Signatures are also recorded and can be viewed in the OQ Tests Result record Audit Trail.

Signing an OQ Tests Result record

If you have been granted permission to use the 'Sign e-record' Access Control, you can execute an electronic signature to an OQ Tests Result record.

❖ To sign an OQ Tests Results record

1. Use the Display Options command on the Results menu or the OQ Results Window context menu to display the Results Display Options dialog, then use the facilities provided on this dialog to locate and select the OQ Tests Result record(s) that you want. Close the Results Display Options dialog.
2. In the OQ Results Window, click on a result that is part of the record that you are interested in to highlight it.
3. Open the Results menu, or right-click to display the OQ Results Window context menu, and then click the Sign Results command. The User Authentication dialog will be displayed.
4. Type your User Name and Password.
 - If this is the first time the User Authentication dialog has been used since you started the Client application, you must enter both your User Name and your Password. However, if you have used this dialog previously in the current session, your User Name will be remembered, and you will only have to enter your password. This behavior is consistent with that described in Section 11.200 (a) (1) of the Rule.
5. Select one of the Signature Meanings from the drop-down menu.
6. Click **OK** to execute the signature to the OQ Tests Result record.
7. An acknowledgment prompt will be displayed confirming the details of your signature. Click **OK** to close this.

You can view your signature as described in the section above.

Printing OQ Tests Result records

If you have been granted permission to use the 'Allow Printing' Access Control, you will be able to print OQ Tests Result records. If you have this permission, you will also be able to preview the printed output.

Printing the data contained in OQ Tests Result records can be accomplished through the commands available on sub-menus displayed when the File/Print and File/Print Preview commands are selected.

❖ To print an OQ Tests Result record

1. Ensure that the printer that you intend to use has been properly installed, and that the appropriate options for paper size, print quality etc. have been selected. You can access these functions from the dialog displayed when you use the File > Print Setup command, but the options available will depend on the type of printer that has been installed.
2. Use the Display Options command on the Results menu or the OQ Results Window context menu to open the Results Display dialog, to select and display the OQ Tests Result records you require.
3. Select the File > Print Preview > Full Report command to preview your printed output.
 - If the Confirm ID before printing System Policy has been set, the Authenticate User dialog will be displayed. You must enter your User Name (if it is not already displayed) and Password before you can preview your printed output.
 - If you are satisfied with your preview, click the Print button on the preview tool bar.
4. If you do not want to pre-view your printed output, select the File > Print > Full Report command to print your Report immediately.
 - If the Confirm ID before printing System Policy has been set, the Authenticate User dialog will be displayed. You must enter your User Name (if it is not already displayed) and Password before your Report will be printed.

Managing OQ Tests Results records

The SOLAARsecurity OQ Tests Client software provides facilities for maintaining OQ Tests Results databases. To use these facilities, you must have been granted permission to use the 'Manage Databases' Access Control.

You can access the Database Management functions from sub-menus displayed when you select the File > Database Management command. This command is available only when no OQ Results database is open. You should first therefore use the File > Close Results command to close any open OQ Results database before using the database management functions.

Repairing OQ Tests databases

If an OQ Tests Results database has become corrupted, perhaps because of a fault in Data Station hardware, it may be possible to repair it using the Repair Database command. Thermo Fisher Scientific does not guarantee that this function will always repair a damaged database, nor that the data originally contained in the damaged database can be recovered after the command has been used. If it is important that the databases remain undamaged, provision should be made for them to be saved to a secure location that is regularly backed up.

Before attempting to use the Repair Database command, you must first use the facilities provided in the Windows operating system to ensure that the file that contains the database is not itself corrupted. Running the Repair command on a database contained in a corrupted file is likely to result in the complete loss of data contained in the database. You should refer to the How to... topics of the On Line Help system before using this function.

If the Repair function does successfully repair a database, the OQ Tests Results records contained in the database will be restored to their original state, including any signatures that have been executed to the records.

❖ To repair an OQ Tests database

1. Use the File > Close Results command to close any open Results databases.
2. Select the File > Database Management > Repair Database command to display the Database to Repair dialog.
3. A prompt will be displayed, asking you to confirm that you have checked the file integrity with the tools provided with your Windows operating system. If you have done this, click **OK** to start the repair process.

The database will be repaired.

Working with Access Controls

Access Controls are provided to limit the functionality of the Client software that is available to a specific user in a controllable way, to meet the requirements of Section 11.10 paragraph (g) of the Rule.

An individual may be granted or denied permission to use any of the functions that are subject to Access Controls. These permissions are granted or denied to users by the SOLAARsecurity Manager, who will use the facilities provided in the SOLAARsecurity Administrator application to do this.

When a user has logged in to the SOLAARsecurity Data Station Client, the status of the permissions to use the Access Controls can be viewed on the Security Permissions dialog.

❖ To view your Security Permissions

1. Select the Security menu command to display the Security Permissions dialog.
 - Access Controls that you have been granted permission to use will be marked with a tick.

Each Access Control and the functions that it controls, is described in detail below.

Administer Security Database

If you have permission to use this Access Control you can start up and use the SOLAARsecurity Administrator application to set up the Access Controls and other security features for all other users of the system. Special considerations apply to the use of this Access Control, which are described in the SOLAARsecurity Administrator Users Manual.

Run SOLAARsecurity Software

If you have permission to use this Access Control you can start up and run the SOLAARsecurity Data Station and OQ Tests Client applications.

Sign e-record

If you have permission to use this Access Control you can execute electronic signatures to electronic records created by the SOLAARsecurity Data Station and OQ Tests Client applications.

Run Analyses

If you have permission to use this Access Control you can use the Action > Analyze and the Action > Run Dual Analysis commands and the equivalent tool bar buttons in the SOLAARsecurity Data Station application to carry out atomic absorption analyses.

Perform Ash Atomize analyses

If you have permission to use this Access Control you can use the Action > Ash Atomize command, the equivalent tool bar button and the Furnace Optimization Wizard in the SOLAARsecurity Data Station application to perform an ash atomize experiment. When the experiment has been completed, you will be offered the option of transferring the optimized parameters to the Current Method, and you will be able to do this even if you do not have permission to use the 'Edit Method' Access Control. You can then use the modified Current Method to run an analysis. However, without permission to use the 'Edit Method' Access Control, you will not be able to save the modified Current Method in the Method Library.

Perform Calibrate Method

If you have permission to use this Access Control you can use the Action > Calibrate Method command in the SOLAARsecurity Data Station application to calibrate the Current Method. When the experiment has been completed, the Current Method will automatically be updated with the calibration data. You will be able to do this even if you do not have permission to use the 'Edit Method' Access Control. You can then use the modified Current Method to run an analysis. However, without permission to use the 'Edit Method' Access Control, you will not be able to save the calibrated Current Method in the Method Library.

Perform Single Solution Measurements

If you have permission to use this Access Control you can use the Action > Single Solution command and the equivalent tool bar button in the SOLAARsecurity Data Station application to measure a single solution using the Current Method parameters. A Single Solution measurement would typically be used to confirm that the instrument has been set up and adjusted correctly before starting an analysis.

Perform Burner Height optimization

If you have permission to use this Access Control you can use the Action > Optimize > Burner Height command in the SOLAARsecurity Data Station application to perform a burner height optimization experiment. When the experiment has been completed, the optimized burner height parameter will automatically be transferred to the Current Method. You will be able to do this even if you do not have permission to use the 'Edit Method' Access Control. You can then use the modified Current Method to run an analysis. However, without permission to use the 'Edit Method' Access Control, you will not be able to save the modified Current Method in the Method Library.

Note that this Access Control has no effect on the Optimize Burner Height parameter in the Flame parameters section of the Method. If this parameter is set, a Burner Height optimization will be automatically performed when the Method is run.

Perform Gas Flow optimization

If you have permission to use this Access Control you can use the Action > Optimize > Gas Flow command in the SOLAARsecurity Data Station application to perform a fuel Gas Flow optimization experiment. When the experiment has been completed, the optimized Gas Flow parameter will automatically be transferred to the Current Method. You will be able to do this even if you do not have permission to use the 'Edit Method' Access Control. You can then use the modified Current Method to run an analysis. However, without permission to use the 'Edit Method' Access Control, you will not be able to save the modified Current Method in the Method Library.

Note that this Access Control has no effect on the Optimize Fuel Flow parameter in the Flame parameters section of the Method. If this parameter is set, a Fuel Gas flow rate optimization will be automatically performed when the Method is run.

Perform Spectrometer optimization

If you have permission to use this Access Control you can use the Action > Optimize > Spectrometer command in the SOLAARsecurity Data Station application to perform a Spectrometer optimization experiment. When the experiment has been completed, the optimized Spectrometer parameters will automatically be transferred to the Current Method. You will be able to do this even if you do not have permission to use the 'Edit Method' Access Control. You can then use the modified Current Method to run an analysis. However, without permission to use the 'Edit Method' Access Control, you will not be able to save the modified Current Method in the Method Library.

Note that this Access Control has no effect on the Optimize Spectrometer parameter in the Spectrometer parameters section of the Method. If this parameter is set, a Spectrometer parameters optimization will be automatically performed when the Method is run.

Run Gas Flow Wizard

If you have permission to use this Access Control you can use the Optimize Gas Flow and Burner Height Wizard in the SOLAAR*security* Data Station application to perform fuel Gas Flow and Burner Height optimization experiments. When the experiments have been completed, the optimized Gas Flow and Burner Height parameters can be transferred to the Current Method. You will be able to do this even if you do not have permission to use the 'Edit Method' Access Control. You can then use the modified Current Method to run an analysis. However, without permission to use the 'Edit Method' Access Control, you will not be able to save the modified Current Method in the Method Library.

Run Spectrometer Optimization Wizard

If you have permission to use this Access Control you can use the Optimize Spectrometer Parameters Wizard in the SOLAAR*security* Data Station application to perform a Spectrometer Parameters optimization experiment. When the experiment has been completed, the optimized Spectrometer parameters can be transferred to the Current Method. You will be able to do this even if you do not have permission to use the 'Edit Method' Access Control. You can then use the modified Current Method to run an analysis. However, without permission to use the 'Edit Method' Access Control, you will not be able to save the modified Current Method in the Method Library.

Run Instrument Performance Wizard

If you have permission to use this Access Control you can use the Instrument Performance Wizard in the SOLAAR*security* Data Station application to measure the sensitivity and detection limit of your instrument when it is running the Current Method.

Edit Results

If you have permission to use this Access Control you can use the following commands to edit and re-calculate the results displayed in the Results Window:

- Results > Delete Result

- Results > Restore Result
- Results > Delete Resample
- Results > Restore Resample
- Results > Use Height for Calculation
- Results > Use Area for Calculation
- Results > Change Line Fit

Edit Peak Measurement

If you have permission to use this Access Control you can use the Results > Edit Peak Measurement command to edit the peak measurement parameters and re-calculate the results displayed in the Results Window.

Edit Methods

If you have permission to use this Access Control you can use the Edit > Method command and its equivalent tool bar button to display the Current Method in the Method dialog. You can then freely edit the Current Method, and save the edited Method as a Method record in the Method Library. You can also create new Methods, and edit and save them in the Methods Library as required.

Edit Sequence in Methods

If you have permission to use this Access Control you can use the Edit > Sequence command to display and edit the Sequence Table and Analysis Matrix for the Current Method, even if you do not have permission to use the 'Edit Method' Access Control. This function allows you to change the Sequence Table and Analysis Matrix to suit a particular batch of samples, while ensuring that other Method parameters cannot be changed – for example, the Method may have been set up with 20 samples in the Sequence Table, but you now want to measure 25. You can edit the Sequence Table by adding more Sample actions, without affecting any other Method parameters.

If you do have permission to use the 'Edit Methods' Access Control, you can edit the Sequence Table and Analysis Matrix on the Sequence tab of the Method dialog, irrespective of your permissions status for this Access Control.

Edit Sample Details in Methods

If you have permission to use this Access Control you can use the Edit > Sample Details command to display and edit the Sample Details for the Current Method, even if you do not have permission to use the 'Edit Method' Access Control. This function allows you to change the Sample Details to suit a particular batch of samples, while ensuring that other Method parameters cannot be changed.

You can also use the File > Import Sample Details command to import a set of Sample Details from a file.

If you do have permission to use the 'Edit Methods' Access Control, you can edit the Sample Details by using the **Sample Details** button on the Sequence tab of the Method dialog, irrespective of your permissions status for this Access Control.

Edit Print Options

If you have permission to use this Access Control you can use the File > Print Options command to display the Print Options dialog, where you can edit the Print Options, and save sets of Print Options as Templates.

Even if you do not have permission to use this Access Control, you can open the Print Options dialog and load pre-defined Templates.

Allow Printing

If you have permission to use this Access Control you can use the File > Print and File > Print Preview commands to print a variety of Reports. You can also use the Print a Report wizard, which will provide step-by-step guidance for setting up Print Options and printing a Results Report.

Allow Data Export

If you have permission to use this Access Control you can use the File > Export command to export data in the form of text files.

Allow Clipboard Copy

If you have permission to use this Access Control you can use the Edit > Copy command to copy data on to the Windows clipboard. You can then use the Edit > Paste command in another application to transfer the data into that application.

Manage Databases

If you have permission to use this Access Control you can use the File > Database Management > Compress Database and ...Repair Database commands to carry out maintenance tasks on the SOLAAR*security* databases used by the Client applications.

Copy Analyses

If you have permission to use this Access Control you can use the File > Database Management > Copy Analyses command to copy Analysis Results records from one Results database to another.

Copy Methods

If you have permission to use this Access Control you can use the File > Database Management > Copy Methods command to copy Method records from one Methods database to another.

Delete Analyses

If you have permission to use this Access Control you can use the File > Database Management > Delete Analyses command to delete Analysis Results records from a Results database.

Delete Methods

If you have permission to use this Access Control you can use the File > Database Management > Delete Methods command and the **Delete** button on the Method Library dialog to delete Method records from a Methods database.

Perform PQ Tests

If you have permission to use this Access Control you can use the Action/Run PQ Tests command to create a new PQ Tests Results record.

Perform OQ Tests

If you have permission to use this Access Control you can use the Action > Start Test Sequence command or the Start Test Sequence button on the OQ Tests dialog of the OQ Tests Client application to create a new OQ Tests Results record.

Perform Customer Diagnostics

If you have permission to use this Access Control you can use the View > Customer Diagnostics command of the OQ Tests Client application to display the Customer Diagnostics dialog, and use the facilities and functions it contains to diagnose problems with your Atomic Absorption system hardware.

Working with System Policies

System Policies affect all users of the SOLAARsecurity Client software, and are set up by the SOLAARsecurity Manager using the SOLAARsecurity Administrator application.

Authenticate on Startup

If this System Policy is set, all users will have to log in to the SOLAARsecurity Client software. The User Authentication dialog will be displayed when the Client software is started, and all users will have to confirm their identity by entering their User name and Password. A check will be made to confirm that the user attempting to start the application is the same person as logged on to the Data Station, and that User name and Password are correct.

Perform Event Auditing

If this System Policy is set, the SOLAARsecurity Client applications will use the Windows Application Event Log of the machine on which the Server software is running, to log significant events that may affect the electronic records created and maintained by the Client applications. This process is not visible to users of the Client applications.

Confirm ID before Printing

If this System Policy is set, all users will have to confirm their identity on the User Authentication dialog before they can print electronic records.

Confirm ID before Exporting

If this System Policy is set, all users will have to confirm their identity on the User Authentication dialog before they can export electronic records.

Confirm ID before Editing

If this System Policy is set, all users will have to confirm their identity on the User Authentication dialog before they can edit electronic records. A Comment field is provided on the User Authentication dialog, so that a reason for the edit can be provided. The comment is stored in the records Audit Trail.

Working with Signature Meanings

The SOLAAR*security* Manager is able to set up one or more Signature Meanings using the SOLAAR*security* Administrator application. These will be displayed on a drop down list on the User Authentication dialog when you execute a signature to an electronic record, and you must select one to successfully sign the record.

Upgrade Considerations

If you are upgrading an earlier installation of SOLAAR software (previous to v10.0) to SOLAAR*security*, there are some issues of which you should be aware. The development of the new features in SOLAAR*security* has involved substantial changes in the both the software itself, and in the databases that are used to store the electronic records.

SOLAAR*security* used with SOLAAR Software v10.0 onwards can be upgraded to the current version of SOLAAR Software with no modification of databases necessary. All audit trails will be maintained.

Database Considerations

Databases created by earlier version of the SOLAAR software (previous to v10.0) will appear as READ ONLY when opened with the SOLAAR*security* Client applications. You will be able to view, print and export the records contained in these databases, but you will NOT be able to add new records, nor change the existing records.

If you want to bring such historical data under the same controls (audit trails and signatures) that are available for new records created by the Client applications, you must copy the records from the old database into a database created by the SOLAAR*security* Client. Analysis Results records copied in this way will take their Audit Trails with them, and a new entry will be added showing where the record has been copied from. Other records created in earlier versions of SOLAAR do not have audit trails; when these are copied, a new audit trail will be created for each record, and the first entry in it will record that the record has been copied, and the source database it was copied from.

When historical records have been copied into new SOLAAR*security* databases in this way, you will be able to execute signatures to them, and their Audit Trails will record any changes, in exactly the same way as new records. After the new records have been created in the SOLAAR*security* database they will no longer be accessible using your earlier SOLAAR software.

Permissions and Users

Earlier versions of SOLAAR Data Station (previous to v10.0) and SOLAAR OQ Tests applications had a limited security system that allowed users to identified, and granted permission to use certain facilities. **This user information will not be carried over if the installation is upgraded to the full SOLAAR*security* software package.**

After the software has been upgraded, all Users must be identified and granted permission to use the software, as described in the *SOLAARsecurity Administrator Software Manual*.

SOLAAR*security* Administrator Software

This chapter describes the SOLAAR*security* Administrator application and the SOLAAR*security* Service. A Reference section is appended to describe the network concepts, the role of the network Administrator, and the role of the SOLAAR*security* Manager.

Contents

- [Starting the Administrator Applications](#) on page 4-1
- [Access Control support of User Groups](#) on page 4-11
- [The Local Group Policy Editor](#) on page 4-17
- [The SOLAAR*security* Service](#) on page 4-27
- [Reference](#) on page 4-30

Starting the Administrator Applications

From the Windows Start menu, select the SolaarSecurity > Administer Solaar Security options command. The Administrator application will start, and will automatically load the current version of the SOLAAR*security* Users database.

Tip SOLAAR*security* must be run as Administrator. To do so, right-click the program entry in the Start menu and select Run as administrator.

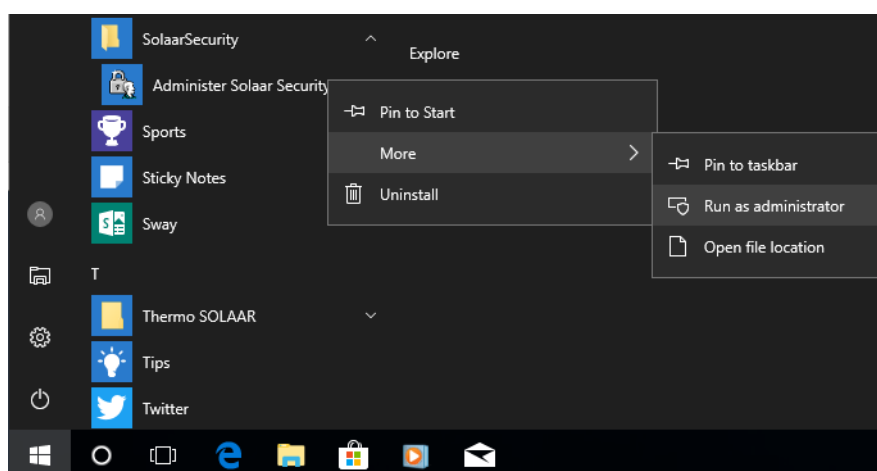


Figure 4-1. The SOLAAR*security* Administration tool in the Start menu

The User Interface

After the SOLAARsecurity Administrator tool is started the program window is displayed.

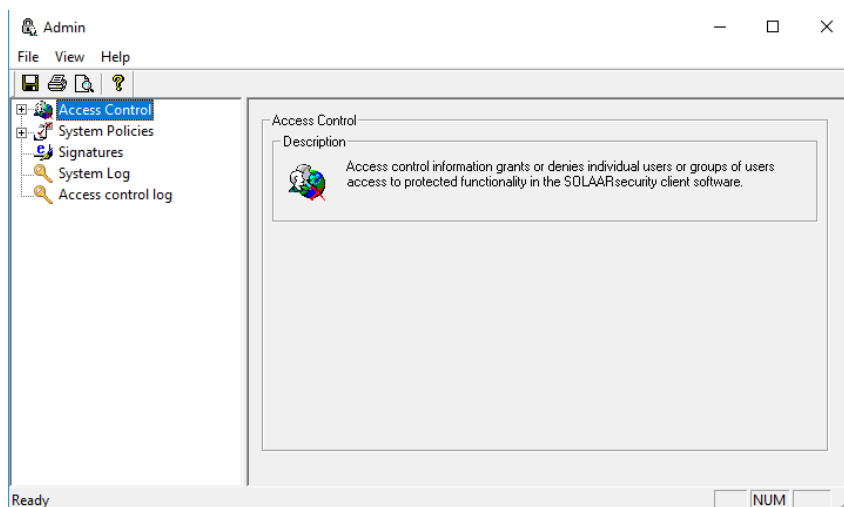


Figure 4-2. SOLAARsecurity Admin program window

The program window shows a menu bar with File, View, and Help menus, which are described in [Table 4-1](#), a Toolbar (see [Table 4-2](#)), the Navigation Pane, and the Work Area.

The Menu Bar

Table 4-1. Menu items

Menu	Comment
File > Save Settings	Save Settings enables you to save the current version of the Security Database. This must be done before any changes that have been made can take effect. If the Security Database has not been saved when the Administrator software is shut down, you will be prompted to save and given the option to close the Administration software without saving changes.
File > Print	The Print, Print Preview and Print Setup commands are used to print the contents of the Security Database and to configure the printer.

Table 4-1. Menu items, continued

Menu	Comment
File > Export System Log	Opens the Export System Log to PDF dialog to save the SOLAAR AA Report as a PDF:

The screenshot shows a table titled 'SOLAAR AA Report' with the following columns: Index, Keywords, Date and Time, Source, Event ID, Task Category, Computer, and Message. The table contains 34 rows of data, all with 'Success' as the keyword and 'Microsoft Windows Security-Auditing' as the source. The messages describe various system events such as 'Special Logon', 'Key migration operation', and 'Special privileges assigned to new logon'.

This menu item is only enabled after the System Log has been saved.

File > Exit	Closes the SOLAARsecurity Administrator software.
View	This enables you to toggle display of the Toolbar and the Status Bar.
Help	SOLAARsecurity Administrator does not have an <i>On-line Help</i> . The Help menu item enables you to access the About page, which displays the full name and version number of the Administrator software.

The Toolbar

The Toolbar contains buttons, which provide quick access to commonly used commands.

Table 4-2. Toolbar items

Icon/Button	Description
Save	Saves the current version of the Security database.
Print	Prints the current version of the Security database to the default printer.
Print Preview	Displays a print preview of the current version of the Security database.
Help	Displays the Help About dialog, showing the version of the software.

The Navigation Pane

The Navigation Pane shows a tree structure holding a couple of groups of security functions that the program controls. The security functions are:

- **Access Control**
Multiple entries allow you to set up the permissions of individual users or groups of users to access the protected functions of the software. See “[Access Control](#)” on page 4-5.
- **System Policies**
These entries enable or disable security policies that apply to all users of the software. See “[System Policies](#)” on page 4-21.
- **Signatures**
This item allows you to set up the signature meanings that will be available on the system. See “[Signatures](#)” on page 4-25.
- **System Log**
Shows the System Logs as a table with *Index, Keywords, Date and Time, Source, Event ID, Task Category, Computer, and Message* columns.

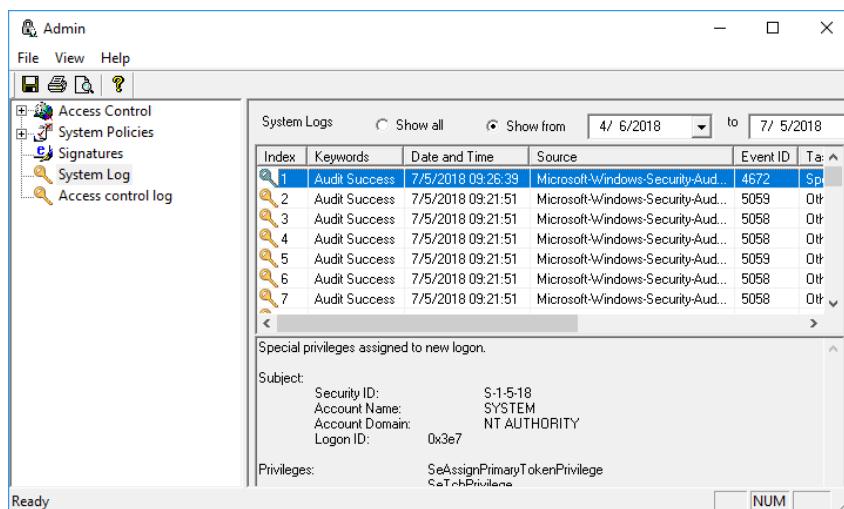


Figure 4-3. SOLAARsecurity Admin System Log view

Select an entry to show details in the lower pane. Click the **To** and **From** date fields to open a calendar, where you can select a date range to filter the System Logs. See “[SOLAARsecurity System Log](#)” on page 4-20.

- **Access control log**
Shows the Access Control Logs as a table with *Date, Time, User, Event ID, Message, and Additional Info* columns.

The Working Area

The Working Area to the right of the Navigation Pane contains an information area, which displays the currently selected security function, and a brief description of its purpose. Below this, other controls will appear as required by the specific function selected.

Access Control

Introduction to Access Control

When the Access Control branch has been expanded, the navigation pane will show the list of the available Access Controls, that is, operations for which access control is available.

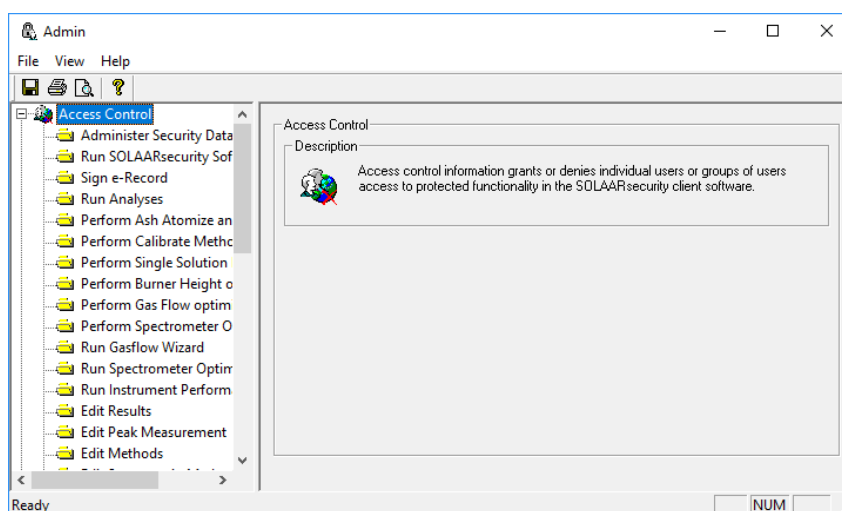


Figure 4-4. Expanded Access Control tree

Select an item on the Access Control list to show the elements in the work area as follows:

- A drop-down list that will include the logged on domain and any trusted domains that are available on the network.
- A list of the individual users and/or groups of users on the currently selected domain.
- A list of the individual users and/or groups of users with permission to perform the currently selected function, and/or users from whom permission is explicitly withheld.
- Buttons for adding and removing individual users and/or groups of users from the list of users and/or groups with the right to perform the currently selected function.

Access Controls

The SOLAAR*security* functions that are subject to Access Controls have been chosen to provide flexible sets of permissions that are appropriate to the requirements of different types of users of the software, spectrometer and its accessories. It is therefore necessary to have some understanding of the operation of the instrument and software before setting up the users of these Access Controls. The scheme described below shows examples of the Access Controls and their relevance to the different types of user.

Management and Authority Functions

Users who have responsibility for administering the SOLAAR*security* Users Security database will require permission to use the 'Administer Security Database' Access Control.

All users who have to use the Data Station Client software to set up or run analyses, and review, edit, export and print analytical results will require permission to use the 'Run SOLAAR*security* Software' Access Control.

Users who have responsibility for signing electronic records created by the system will require permission to use the 'Sign e-record' Access Control.

Analysis Functions

Users who run analyses on the spectrometer, either to generate analytical results from samples, or to set up and optimize Methods, will require permission to use the 'Run Analyses' Access Control.

Users who are required to run pre-defined Methods on different batches of samples will require permission to use the 'Edit Sample Details' Access Control, and, in some cases, permission to use the 'Edit Sequence in Method' Access Control as well. However, we also suggest that when it is important to control pre-defined Methods, permission for them to use the 'Edit Method' Access Control should be explicitly denied.

Method Development Functions

Experienced users who have responsibility for developing and verifying analytical methods on the spectrometer and its accessories will require permission to use some or all of the following Access Controls:

- Edit Methods
- Perform Ash Atomize Analyses
- Perform Calibrate Method

- Perform Single Solution Measurement
- Perform Burner Height Optimization
- Perform Gas Flow Optimization
- Perform Spectrometer Optimization

SOLAAR Wizards provide similar functionality to the individual optimization functions listed above. However, they provide a controlled user interface, with step-by-step, guided instructions that may be more appropriate for less experienced users who nevertheless have responsibility for developing and verifying analytical methods on the spectrometer and its accessories. Use of these Wizards is controlled by the following Access Controls:

- Run Gasflow Wizard
- Run Spectrometer Optimization Wizard
- Run Instrument Performance Wizard

Results Editing Functions

The SOLAAR*security* Data Station Client provides facilities for editing analytical results in various ways. Such edits are always Audit Trailed and are fully reversible. However, we suggest that granting permission to use the Access Controls for these functions should be carefully considered in the context of your organizational data integrity policies. Users who need the ability to edit analytical results require permission to use the following Access Controls:

- Edit Results
- Edit Peak Measurement

Printing and Exporting Functions

The SOLAAR*security* Clients provide a variety of facilities for printing and exporting the information contained in the e-records that they create and manage. Information that has been printed or exported from the SOLAAR*security* e-records, however, moves outside the scope of the security and data auditing tools provided in the software. If the analytical record keeping procedures in your organization require exported or printed information, you should consider carefully who is given permission to use these Access Controls. The relevant Access Controls are:

- Allow Printing
- Allow Data Export

- Allow Clipboard Copy

Database Management Functions

The SOLAAR*security* Clients provide facilities for copying e-records between databases, deleting e-records, and performing other database maintenance tasks, such as attempting to recover records from a corrupt database. Following the traceability requirements of the 21 CFR Part 11 Rule, all these operations can be recorded in the Event Log, but as they can result in substantial changes to the databases, you should consider carefully who is given permission to use these Access Controls. The Access Controls concerned are:

- Manage Databases
- Copy Analyses
- Copy Methods
- Delete Analyses
- Delete Methods

Setting up and Maintaining Access Control

At installation, permission to administer the SOLAAR*security* database is granted only to members of the Administrators group of the local machine, and no other users have permission to use any of the Access Controls. By default, permission to use the 'Sign e-record', 'Perform PQ Tests' and 'Perform OQ Tests' Access Controls is explicitly denied to members of the Everyone group, which normally includes all registered users of the system.

During installation, the Administrator installing the software has the opportunity to grant permission to administer the SOLAAR*security* database to the SOLAAR*security* Manager(s), who will have day-to-day responsibility for running the SOLAAR*security* database.

Permission to use Access Controls will be denied to all users and groups to whom permission has not been explicitly granted, either as individuals or as members of a group. It is therefore normally only necessary to explicitly deny permission to users or groups in order to over-ride access that has been granted through group membership.

The status of a user or group may be one of the following:

Table 4-3. User, Group and Permission status

User or Group	Permission status
Not on the Access Control User List	Permission has not been granted. However, an individual may have access to the function by virtue of their membership of a group that has been granted permission.
Checked on the Access Control User List	Permission to use the Access Control has been granted.
Not checked on the Access Control User List	Permission to use the Access Control has been explicitly denied. This will overrule any permissions that have been granted through group membership.

If a user is a member of more than one group, that user will have only those rights that are the sum of those accessible through common to all of the groups of which she or he is a member.

❖ **To set up Access Control permissions for Users and Groups**

1. Click [+] to expand the Access Control list in the navigation pane.
2. Select the Access Control for which User permissions are to be set up.
3. From the Names list, click on the first user or group that you wish to add to the Access Control user list to highlight it.

Tip If you are using a system with multiple trusted domains, use the drop-down list to select the domain on which the users and/or groups are listed.

4. Click the **Add** button. The name of the user or group will be added to the Access Rights list.

Tip Note that domain names will be shown explicitly only when the user is part of a domain other than the logged on domain.

5. Repeat [step 4](#) until all required users and groups from the selected domain have been added to the list of users of the Access Control.
6. If the users are located on more than one domain, select the next domain and add users from it as above.
7. If you wish to explicitly deny permission to use the Access Control to a user or group in the user list, click in the check box to remove the check mark. If a user has been explicitly denied permission to use an Access Control, this will override any entry that has granted the user permission to use that Control. Thus, if a user is part of a

group that has been granted permission, the group setting can be overridden for a specific user by denying permission in this way.

- This facility may be used, for example, to accommodate a new recruit. The System Administrator will add the new staff member to the system in the group to which she or he will ultimately belong. The SOLAAR*security* Manager can then deny permission to use the Access Control for operations for which the recruit has not yet been trained, then grant permission progressively as training proceeds. Permissions can be restored by clicking the check box to restore the check mark.
8. To remove a user or group from the Access Control list, click the user name to select it and then click the **Remove** button. The selected user or group will be removed from the Access Control list.
 9. When you have finished setting up the Access Control user lists, the new settings must be saved in the Security Database. Use the File > Save Settings menu command, or click **Save** on the toolbar.

Tip If a user, or a group of users, is granted or denied permission to use the 'Run SOLAAR Security s/w' Access Control, the Users Security database must be saved, and the SOLAAR*security* Service must be stopped and restarted in order for the changes to take effect. The procedure for stopping and starting the SOLAAR*security* Service is described in [“Stopping and Starting the SOLAARsecurity Service”](#) on page 4-27.

Access Control support of User Groups

In this release, permissions can be applied to existing User Groups and not just individual Users.

Open the **SOLAARsecurity Administration** tool and expand the Access Control tree and provide access to the selected Access Control item by **Adding** the selected user group or user from the **Names** pane to the **Access Rights** pane.

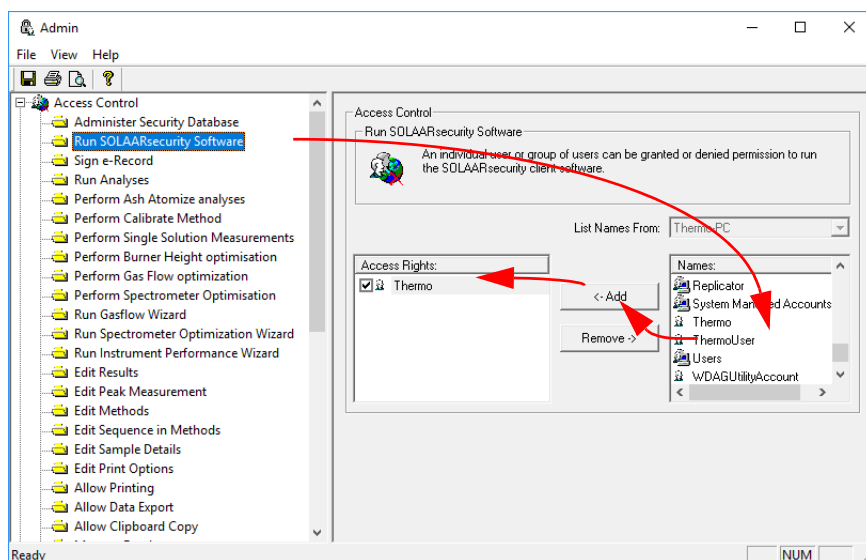


Figure 4-5. Adding a user group to the permission list for an Access Control item

After all permissions are assigned, click the **Save** icon in the toolbar to save the updated permissions.

Any changes made to the User Access Rights defined in SOLAARsecurity Administration can be displayed from within the SOLAAR software by clicking the **Security** menu to show the Security - Permissions window.

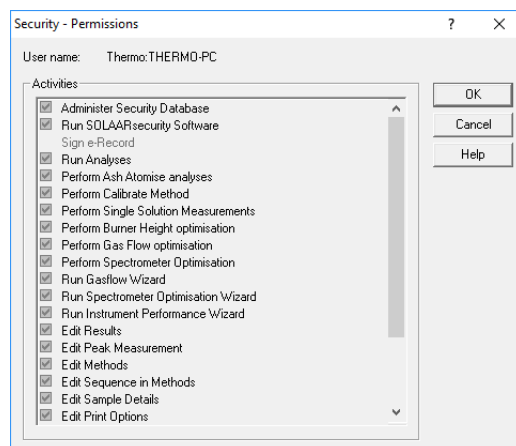


Figure 4-6. SOLAAR Security Permissions dialog with rights for logged-in user

❖ **To define the access control permissions**

Open the **SOLAARsecurity Administration** tool (see [Figure 4-7](#)) where you can define the permissions for supported action within SOLAAR.

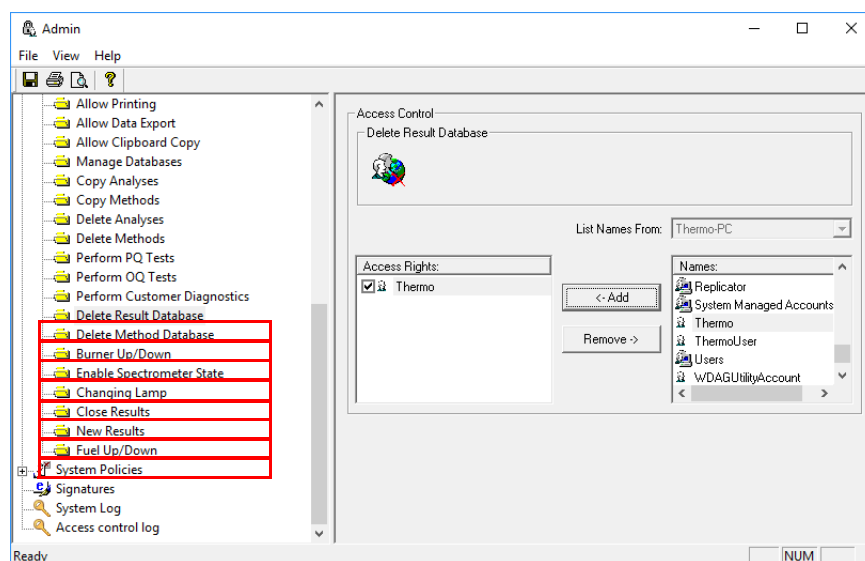


Figure 4-7. Access Control section of SOLAARsecurity tool showing the commands that can now assigned permissions

User Access Control of Delete Results and Delete Methods

Through the permissions defined for the items *Delete Result Database* and *Delete Method Database*, access to the menu commands **File > Delete > Results Database** and **File > Delete > Method Library** in SOLAAR can be controlled.

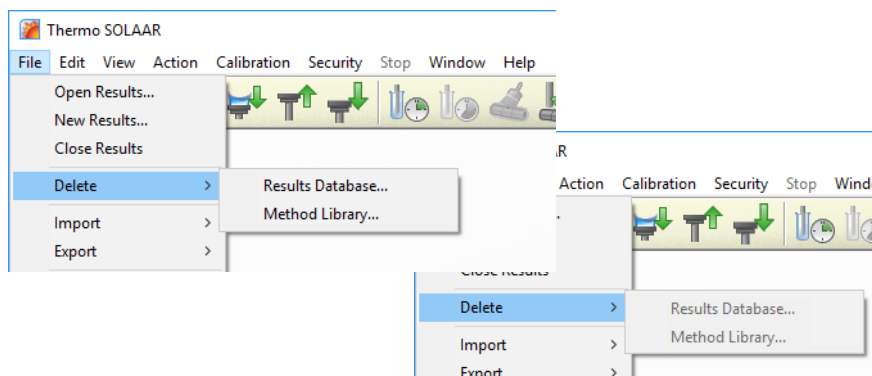


Figure 4-8. SOLAAR File > Delete menu commands active (left) and inactive (right)

If the current user does not have the appropriate permissions, the menu commands **Delete > Results Database** and **Delete > Method Library** are inactive.

User Access Control of Burner Up and Burner Down



Through the permissions defined for the item *Burner Up/Down*, access to the menu commands **Action > Flame > Burner Up** and **Action > Flame > Burner Down** and toolbar icons in SOLAAR can be controlled.

Display of the Spectrometer Status

Through the permissions defined for the item *Enable Spectrometer State*, the **Spectrometer Status** window displays a warning message or the required information.

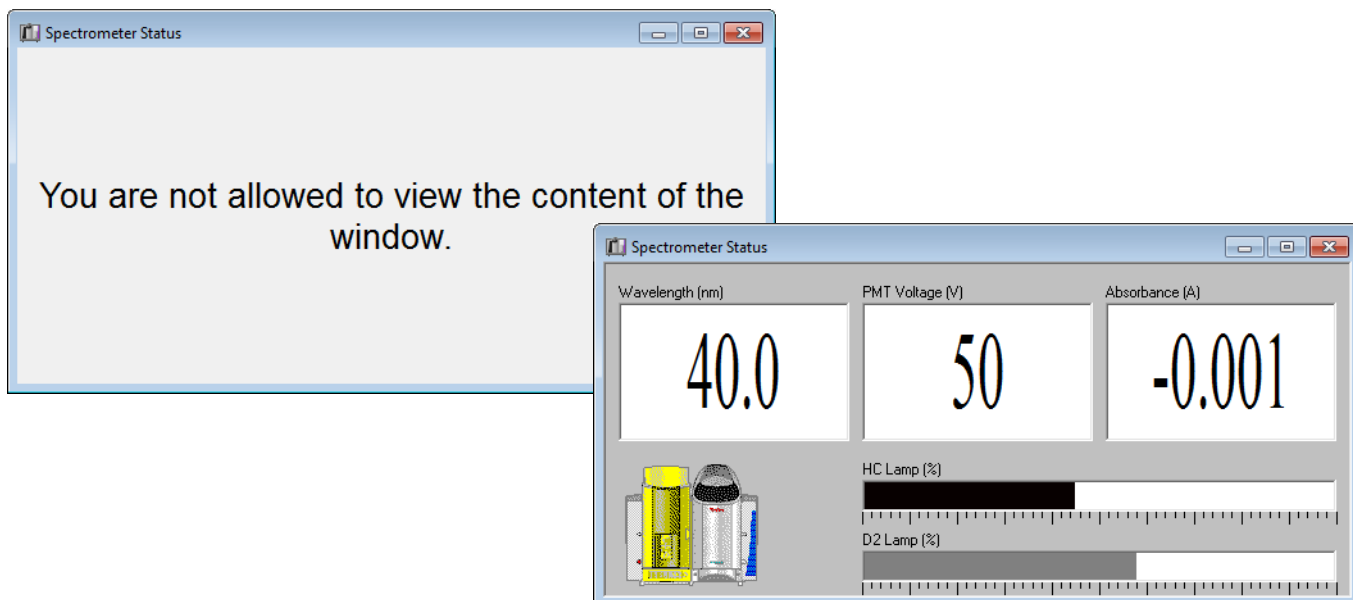


Figure 4-9. Spectrometer Status window displays for user accounts with and without the required permissions

User Access Control for Changing Lamp

Through the permissions defined for the item *Changing Lamp*, the **Lamp Usage** dialog provides active **Add Lamp** and **Delete Lamp** buttons.

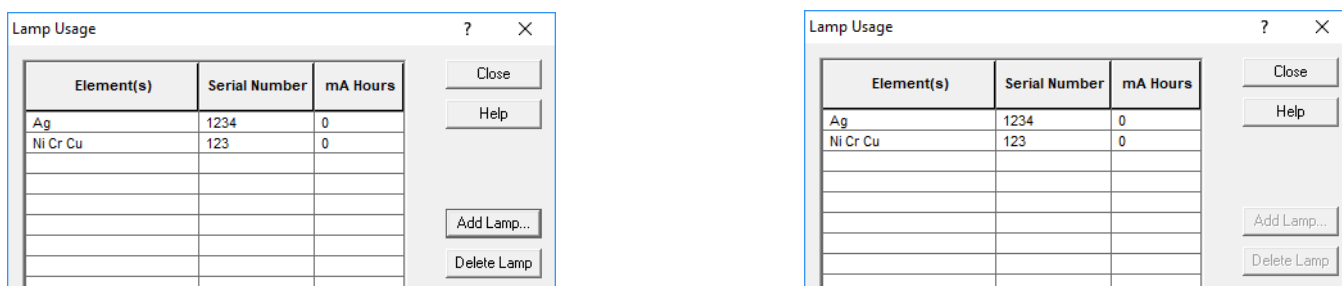


Figure 4-10. SOLAAR Lamp Usage dialog with Add Lamp/Delete Lamp buttons active (left) and inactive (right)

Tip Selecting a lamp for deletion will not show a security message when you click **Delete Lamp**.

User Access Control of New and Close Results

Through the permissions defined for the items *New Results* and *Close Results*, access to the menu commands **File > New Results** and **File > Close Results** in SOLAAR can be controlled.

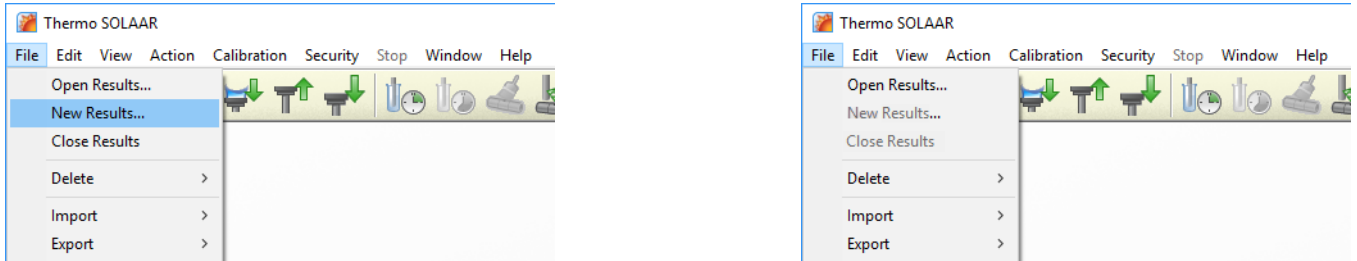


Figure 4-11. SOLAAR File > New Results / File Close Results menu commands active (left) and inactive (right)

User Access Control of Fuel Up and Fuel Down

Through the permissions defined for the item *Fuel Up/Down*, access to the menu commands **Action > Flame > Fuel Up** and **Action > Flame > Fuel Down** in SOLAAR can be controlled.

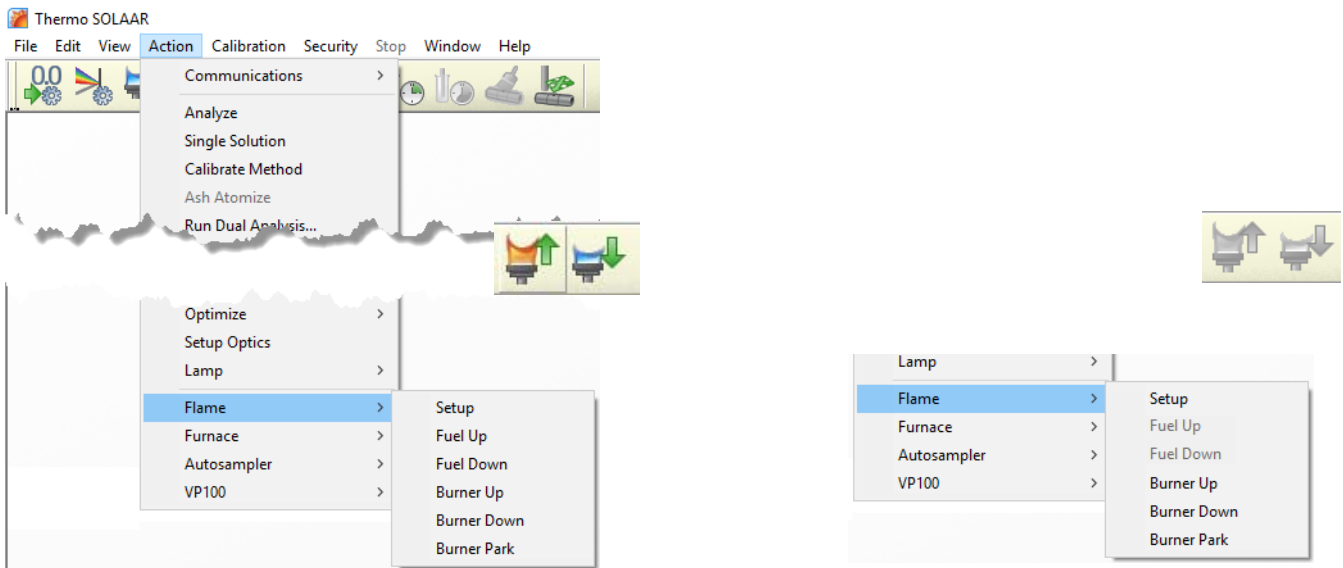


Figure 4-12. SOLAAR Action > Flame > Fuel Up / Fuel Down menu commands and toolbar icons active (left) and inactive (right)

Without permission, the user cannot increase or decrease the fuel flow to control the flame. That means the fuel flow specified in the Method (depending on the selected element) is maintained.

Audit Trail tracking of User Access (System Log)

While the Audit Trail window of SOLAAR shows all messages tracked from the software controlling the AA spectrometer, additional modifications in the SOLAAR environment, for example, user management, can now be tracked in a System Log in the SOLAAR*security* Administrator application. The SOLAAR System Log displays the events captured by the Windows operating system. Before the SOLAAR*security* System Log can be used to view these changes, an Administrator must configure the Windows operating system.

Tip The controls above and below are taken from a Windows 7 based installation. The same functionality is available under Windows 10.

The Local Group Policy Editor

❖ **To configure the Windows logging system**

1. Start **gpedit.msc** with the Run command of Windows.
2. In the **Local Group Policy Editor**, expand the tree Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policies - Local Group Policy Object to see the **Account Management**.

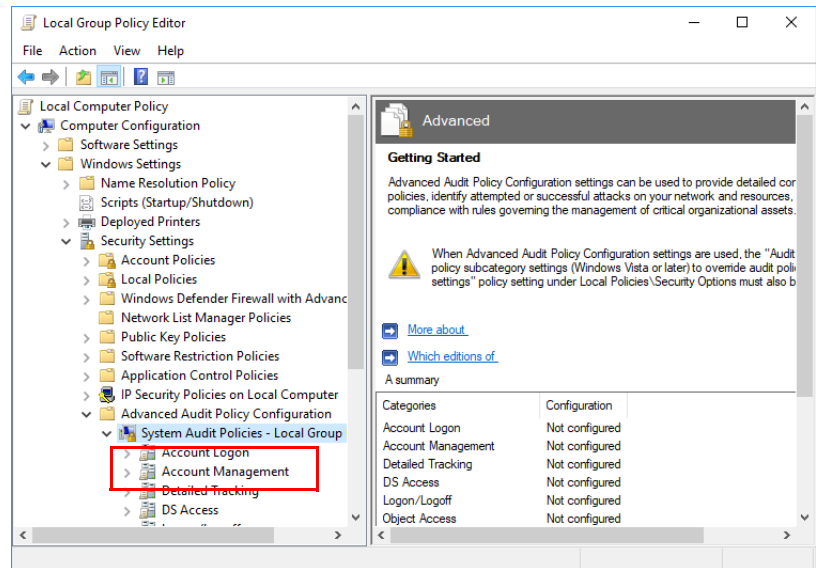


Figure 4-13. Windows Local Group Policy Editor with expanded tree to see Account Management

3. Under **Account Management**, **Logon/Logoff**, **Policy Change**, and **System**, right-click the Subcategory item and select Properties to

change the Audit Events according to the following screen shots, see [Figure 4-14](#) to [Figure 4-18](#).

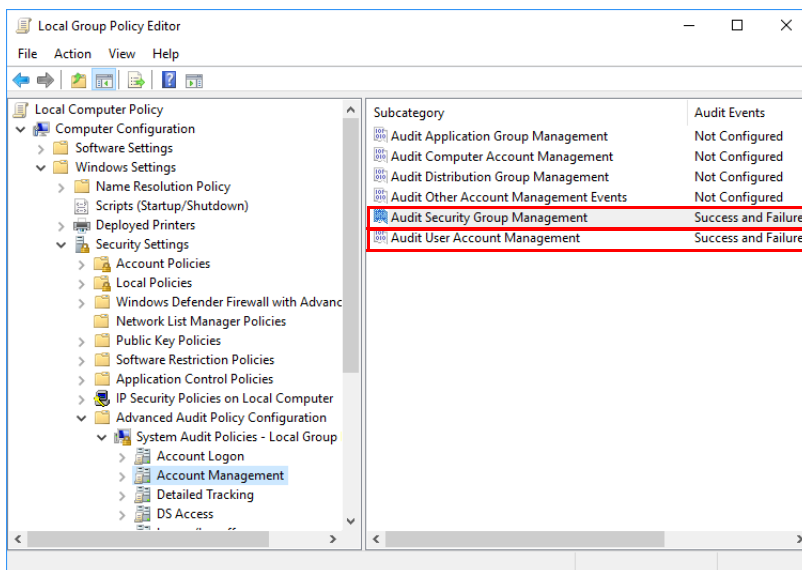


Figure 4-14. Windows Local Group Policy Editor with Account Management

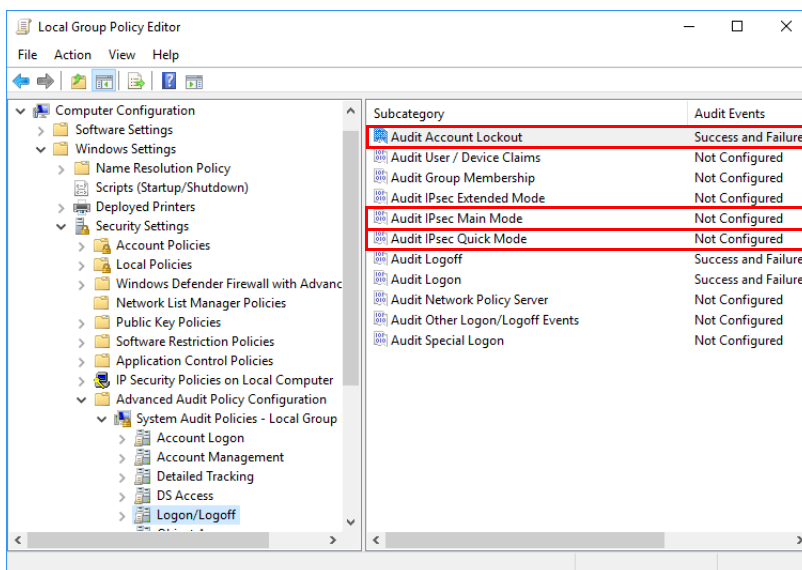


Figure 4-15. Windows Local Group Policy Editor with Logon/Logoff

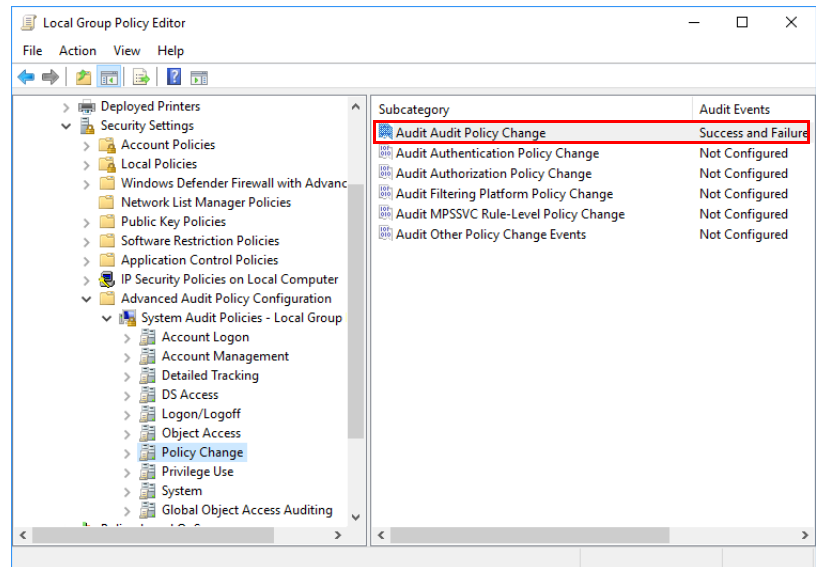


Figure 4-16. Windows Local Group Policy Editor with Policy Change

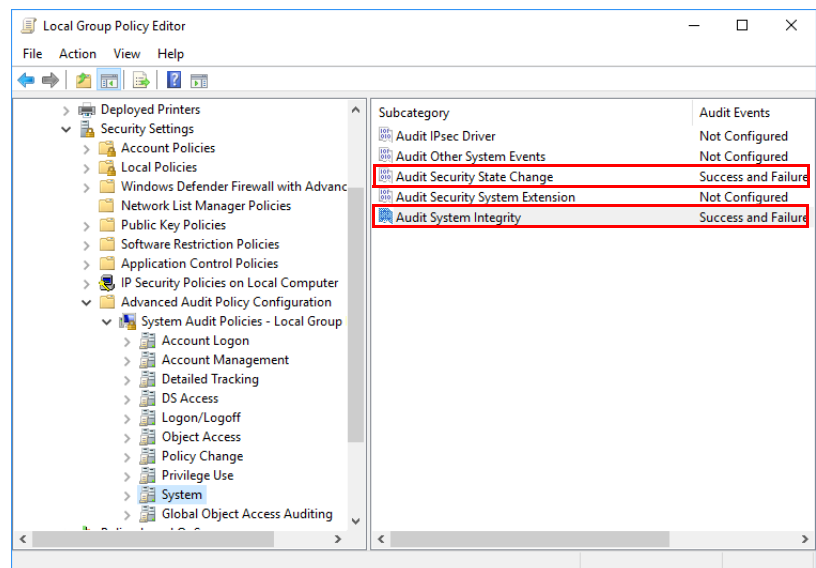


Figure 4-17. Windows Local Group Policy Editor with System

4. To activate the changes in the Windows log, navigate to Local Computer Policy > Computer Configuration

> Windows Settings > Security Settings > Local Policies > Security Options and change the item as shown in [Figure 4-18](#) to *Enabled*.

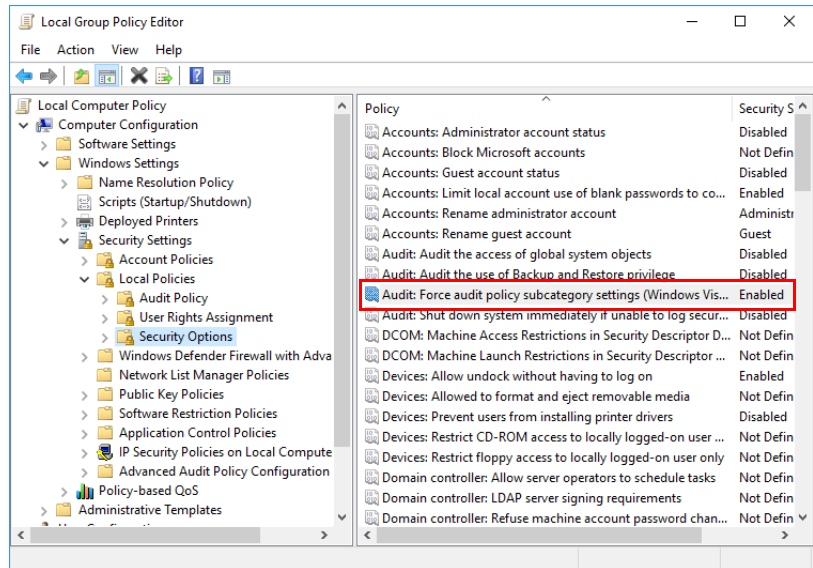


Figure 4-18. Windows Local Group Policy Editor with Security Options

5. Restart your Computer.
6. With these Windows operating system changes made, events will start to be recorded in the SOLAARsecurity System Log.

SOLAARsecurity System Log

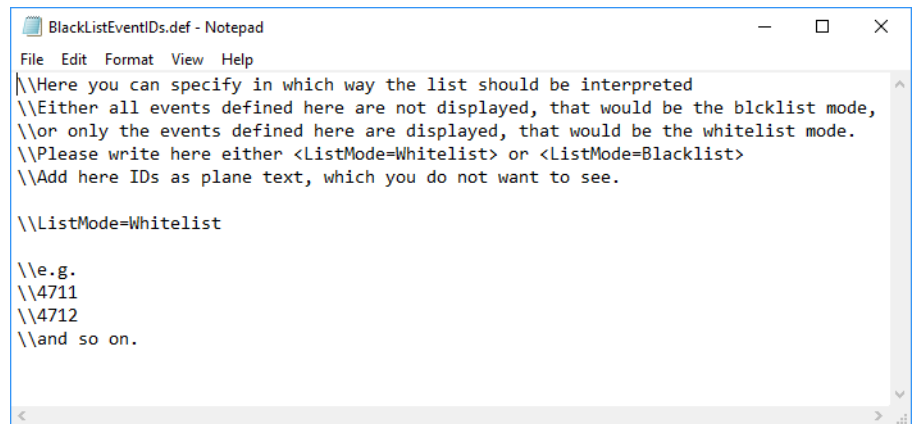
The SOLAARsecurity System Log tracks all changes to user rights that create a Windows Eventlog entry (Event ID 1100) or a Windows Security Auditing entry (for example, Logon or Logoff events with ID 4624 or 4647).

The SOLAARsecurity Audit Trail captures all changes in the System Log as the Windows System Log is read by the SOLAAR software.

The System Log can be filtered to minimize irrelevant information. There are two ways to achieve this:

- Create a ‘blacklist’ of Windows Event IDs that you do not want displayed in the SOLAARsecurity System Log. This is the default process.
- or-
- Create a ‘whitelist’ of Windows Event IDs that you do want displayed in the SOLAARsecurity System Log.

After the first start of SOLAAR*security*, the file `BlackListEventIDs.def` is created under `C:\Users\. The file may be edited with a text editor to list the IDs of Windows Events, which you do not want to see displayed in the SOLAARsecurity System Log.`



```

BlackListEventIDs.def - Notepad
File Edit Format View Help
\\Here you can specify in which way the list should be interpreted
\\Either all events defined here are not displayed, that would be the blcklist mode,
\\or only the events defined here are displayed, that would be the whitelist mode.
\\Please write here either <ListMode=Whitelist> or <ListMode=Blacklist>
\\Add here IDs as plane text, which you do not want to see.

\\ListMode=Whitelist

\\e.g.
\\4711
\\4712
\\and so on.
  
```

Figure 4-19. BlackListEventIDs.def file opened in Notepad

Alternatively, this file can be used as a ‘whitelist’ to show only the IDs of Windows Events that you want to see in the SOLAAR*security* System Log. To enable this function, add `ListMode=Whitelist` as the first row in the `BlackListEventIDs.def` file. Then list the Windows Event IDs, which shall be shown in the SOLAAR*security* System Log. Rows beginning with two backslashes `\\` are used for comments only (as seen in [Figure 4-19](#)) and are therefore not recognized by the software.

System Policies

Introduction to System Policies

System policies are security features that are applied uniformly to all users at all times.

When the System Policies branch has been expanded the navigation pane will show the list System Policies available in the Client software.

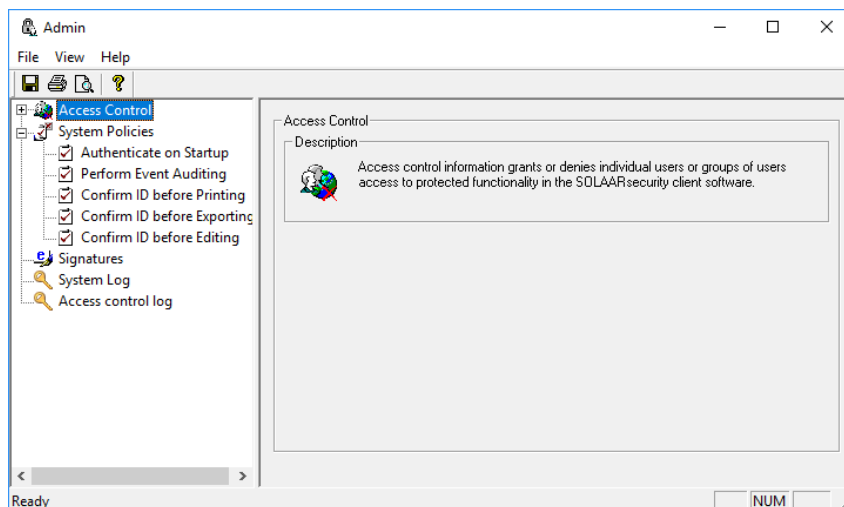


Figure 4-20. Expanded System Policies tree

The following sections describe the effects of enabling and disabling each of the System Policies.

Authenticate on Startup

When Authenticate on Startup is enabled the User Authentication process will take place when the Client software is started. This process confirms that the user attempting to start the SOLAARsecurity Client software is the same user who logged on to the workstation. If the user is not the current logged on Windows user, or if the password is not recognized, access to the SOLAARsecurity Client software will be denied, and the unsuccessful log on attempt will be logged in the Windows Applications Event Log.

If Authenticate on Startup is not enabled, SOLAARsecurity will assume that the individual who is starting up the Client software is the user currently logged on the workstation, and will not check their identity, nor require that they enter their valid password.

Tip If the user logged on to the workstation does not have permission to run the SOLAARsecurity software (i.e., permission to use the Access Control has not been granted to them), they will be denied access, but this will NOT cause an event to be recorded in the Event Log.

It would be normal to have the Authenticate on Startup System Policy enabled when working in a secure 21 CFR Part 11 environment.

Perform Event Auditing

When Perform Event Auditing is enabled, the various component parts of the SOLAARsecurity software package will pass details of certain events to the SOLAARsecurity Server application, that will in turn write an entry to the Windows Application Event Log on the machine on which the Server is running.

❖ **The events that can be audited this way are:**

1. **Event 0.** The Diagnostics section of the OQ Tests Client provides a variety of tests that can be performed on the spectrometer and Data Station hardware, together with facilities for re-calibrating the Burner Height and Monochromator mechanisms. When any of these facilities are used, an Event 0 will be generated, and the description of the event will include the test or action performed, and the result (*success* or *failure*). In addition, a function has been provided that enables a user to create an Event Log entry. The text associated with this can be specified when the Event Log entry is created. This function is provided to allow unknown or unanticipated events, such as emergency service activities, to be logged.
2. **Program Close.** One of the Client applications has been closed normally.
3. **Reset D₂ Hours.** The deuterium (D₂) lamp is a user replaceable component of the spectrometer background correction system, and the Data Station Client software monitors its usage automatically. A command is provided to reset the lamp usage counter back to zero, which is normally done when a new lamp is fitted. Using this command creates a Reset D₂ Hours Event Log entry.
4. **Data Deleted.** The Database Management functions in the Data Station Client software have been used to delete an e-record from a database. The identity of the record, and the database from which it has been deleted, is recorded.
5. **File Created.** The File > New command in one of the Client applications has been used to create a new database.
6. **OQ Validation.** The OQ Tests Client software has been used to create a new OQ Results e-record.
7. **PQ Validation.** The PQ Test command in the Data Station Client software has been used to create a new PQ Results e-record.
8. **User Authenticate Succeeded.** A user has successfully confirmed his identity. This event can occur when any of the Authenticate on Startup, Confirm ID before Printing, Confirm ID before Exporting and Confirm ID before Editing System Policies are set.

9. **User Authenticate Failed.** A user has failed to successfully confirm his identity, and has been denied access to the Client software or function concerned. The reason for the failure is logged. This event can occur when any of the Authenticate on Startup, Confirm ID before Printing, Confirm ID before Exporting and Confirm ID before Editing System Policies are set.
10. **Database Deleted.** A SOLAARsecurity database has been deleted using the facilities provided within one of the Client Applications. Note that this event will NOT occur if a database is deleted using the facilities provided by the Windows Operating System – if it necessary to log operating system events, the security facilities provided in the operating system must be used.

In addition to these events, the SOLAARsecurity Server will also generate events when it is installed, when it is started, when it is stopped, and when it is uninstalled. These messages provide auditable confirmation that the system is working correctly, so that the other events will be successfully logged.

The following information is associated with each logged event, and is placed in the Windows Applications Event Log:

- Time and date at which the event information is written to the event log.
- The User ID of the user who was logged in when the event occurred.
- The full name of the user who was logged in when the event occurred.
- The name of the computer on which the event occurred.
- The ID number and description of the event which occurred.
- The version number of the SOLAARsecurity software.

Event logs can be viewed by on the server computer.

❖ **To view the Applications event log**

1. Navigate to The Event Viewer through Administrative Tools located in the Control Panel.
2. In the left hand pane, click **Applications Log**.
 - Facilities are provided to allow the Event Log entries to be filtered and sorted to allow you to easily locate the entries that you want to view. You can display only the entries created by the SOLAARsecurity system, by setting the Source filter to **Solaar Security Server**.

Confirm ID before Printing

When this System Policy is set, a user with permission to use the relevant Access Controls will have to confirm his identity before the Printing and Print Preview functions can be used to make paper copies of electronic records.

Confirm ID before Exporting

When this System Policy is set, a user with permission to use the relevant Access Controls will have to confirm his identity before the Export and Copy to Clipboard functions can be used to export the data contained in electronic records to other applications.

Confirm ID before Editing

When this System Policy is set, a user with permission to use the relevant Access Controls will have to confirm his identity before using any of the Results Edit functions to modify the data contained in Results e-records.

Signatures

Introduction

Users who have been assigned the right to execute electronic signatures will be able to sign following SOLAARsecurity electronic records:

- Analysis Results records
- Method Results records
- PQ Results records
- OQ Results records

Signature meanings are required by 21 CFR Part 11, and the meaning is a mandatory component of an electronic signature in SOLAARsecurity. When a properly authorized user signs an e-record, a list of meanings for the signature will be presented. That list is created and maintained using the Signatures function in the Administrator application. A default set of meanings is supplied, but these may not meet the requirements of your organization. The SOLAARsecurity Manager should review the Signature Meanings and amend them if required.

❖ To add a new signature meaning

1. Click the Signatures item in the navigation pane.

The Signatures dialog opens in the work area.

2. To add a new meaning to the list, click the **Add** button.
3. The Signature Meaning dialog opens. Enter the new meaning and click **OK** to accept it or **Cancel** to close the dialog leaving the Meanings list unchanged.

❖ **To delete a signature meaning**

1. Click the Signatures item in the navigation pane.
The Signatures dialog opens in the work area.
2. Select the meaning that you wish to delete, and then click **Delete** to remove the meaning from the list.

❖ **To edit a signature meaning**

1. Click the Signatures item in the navigation pane.
The Signatures dialog opens in the work area.
2. Select the meaning that you wish to edit, and then click the **Edit** button.
The Signature Meaning dialog opens with the meaning in the Edit field. Make the changes required. Click **OK** to accept the amended meaning or **Cancel** to close the dialog leaving the existing meaning unchanged.

When you have finished setting up the signature meanings, the new settings must be saved in the Security Database. Use the File > Save Settings command, or click **Save** on the toolbar.

The SOLAARsecurity Service

Introduction to SOLAARsecurity Service

The SOLAARsecurity Service enforces the Security Policies and Access Controls that are defined by the SOLAARsecurity Manager using the Administration program. The SOLAARsecurity Service is automatically installed with the Administrator program. It enforces the security policies simultaneously across all of the SOLAARsecurity Client applications running on the network.

Stopping and Starting the SOLAARsecurity Service

In some circumstances it is necessary to stop and restart the SOLAARsecurity Service. In particular, when changes have been made to the list of users with the right to run the SOLAARsecurity software it is

necessary to stop and restart the SOLAARsecurity Service in order to give effect to these changes. The SOLAARsecurity Service can only be started and stopped by a user with Administrator rights.

Tip All other changes to the SOLAARsecurity database take effect as soon as the changed database is saved, with no need to start and stop the Service application.

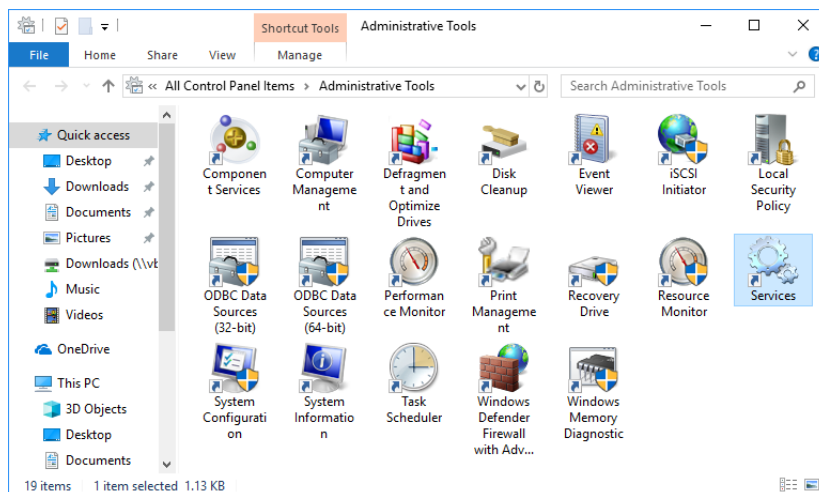


Figure 4-21. Services from the Administrative Tools

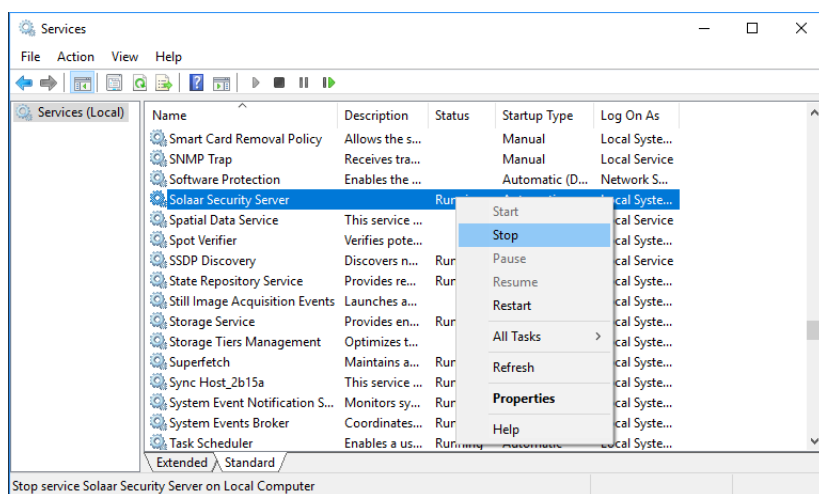


Figure 4-22. The Solaar Security Server shortcut menu

❖ **To stop the SOLAARsecurity Server application**

1. Click Start > Settings > Control Panel > Administrative Tools > Services, see [Figure 4-21](#).
2. Select Solaar Security Server from the list.
3. Right-click Solaar Security Server to display the shortcut menu, or open the Action menu, see [Figure 4-22](#).
4. Click the **Stop** command.

❖ **To start the SOLAARsecurity Server application**

1. Click Start > Settings > Control Panel > Administrative Tools > Services, see [Figure 4-21](#).
2. Select Solaar Security Server from the list.
3. Right-click Solaar Security Server to display the shortcut menu, or open the Action menu, see [Figure 4-22](#).
4. Click the **Start** command.

Reference

Network Concepts

SOLAAR*security* is designed to run in a networked environment or in a stand-alone configuration.

The security functionality is fundamentally linked to the security features in the Windows XP Professional / Windows Vista Ultimate / Windows 7 Professional / Windows 10 Professional network operating systems.

A SOLAAR*security* Manager does not need to be familiar with these security features, unless s/he is also a Network Administrator. However an understanding of some of the concepts may give you more confidence in using the SOLAAR*security* Administrator software.

Servers

A network server is a computer or device that provides information or services to other computers on a network.

Domains

A domain is a logical grouping of network servers and other computers that share common security and user account information. The Network Administrator creates a user account for each user. Users then log on to a domain, not to an individual server within the domain.

Within a domain, domain controllers manage all aspects of user-domain interactions. Domain controllers are computers running server software. They store security and user account information for the entire domain. Domain controllers use this information to authenticate users logging on to domain accounts.

Grouping computers into domains provides benefits to both network managers and users. The domain controllers form a single administrative unit, sharing security and user account information, which means that the Network Manager needs to manage only one account for each user. Each user needs to use (and remember the password for) only one account. When users browse the network for available resources, they see the network grouped into domains, rather than seeing all of the network servers and printers at once.

Trust Relationships

Security across multiple domains is administered through trust relationships. A trust relationship is a link between two domains where the trusting domain honors the login validations from the trusted domain. Two domains can thus be combined into one administrative unit that can authorize access to resources in both domains.

In a one-way trust relationship, one domain trusts the domain controllers in another domain to validate user accounts to use its resources. The resources that become available are in the trusting domain, and the accounts that can use them are in the trusted domain.

A two-way (mutual) trust relationship is composed of two one-way trust relationships, in which each domain trusts users in the other domain. Users can log on from computers in either domain to the domain that contains their account. Each domain can have both accounts and resources. Global user accounts and global groups can be used from either domain to grant rights and permissions to resources in either domain. In other words, both domains are trusted domains.

Rights and permissions

A right authorizes a user to perform certain actions on a computer system, such as backing up files and directories, logging on to a computer interactively, or shutting down a computer system. Rights exist as capabilities for using either domain controllers at the domain level or workstations or member servers at the local level. Rights can be granted to groups or to user accounts.

A user who logs on to an account belonging to a group to which the appropriate rights have been granted can carry out the corresponding actions. When a user does not have appropriate rights to perform an action, an attempt to carry out that action is blocked.

Rights apply to the system as a whole and are different from permissions, which apply to specific objects.

A permission is a rule associated with an object (usually a directory, file, or printer), and it regulates which users can have access to the object and in what manner. Most often the creator or owner of the object sets the permissions for the object.

Users and Groups

System Administrators typically group users according to the types and degrees of network access their jobs require. By using group accounts, Administrators can grant rights and permissions to multiple users at one

time. Other users can be added to an existing group account at any time, immediately gaining the rights and permissions granted to the group account.

There are two types of group accounts:

A global group consists of several user accounts from one domain that are grouped together under one group account name. A global group can contain user accounts from only one domain - the domain in which the global group was created. "Global" indicates that the group can be granted rights and permissions to use resources in multiple (global) domains. A global group can contain only user accounts and can be created only on a domain, not on a workstation or member server.

A local group consists of user accounts and global groups from one or more domains, grouped together under one account name. Users and global groups from outside the local domain can be added to the local group only if they belong to a trusted domain. "Local" indicates that the group can be granted rights and permissions to use resources in only one (local) domain. A local group can contain users and global groups but no other local groups.

The Role of the Network Administrator

The SOLAAR*security* installation procedure requires a member of the network Administrators group to:

- Review the operating system configuration and make any changes required to ensure compatibility with the requirements of 21 CFR Part 11.
- Enable event auditing in the Applications Event log, System Event log and Security Event log so as to configure the system to meet the requirements of 21 CFR Part 11.
- Set up a group of users with the right to run the SOLAAR*security* Administration program.

Before the SOLAAR*security* Manager can use the SOLAAR*security* Administrator software to set up the rights of users of the Client software, the Network Administrator will also need to:

- Put the names of the users of the software on to the system, if this has not already been done. Users must be either on the domain in which the SOLAAR*security* Server and Administration software are running, or on a domain with which a mutual trust relationship exists.
- Set up any groups of users needed by the SOLAAR*security* System Administrator.

After installation and initial set-up the Network Administrator will need to:

- Add new users to the system.
- Make any changes that are needed to the composition of user groups.
- Start and stop the SOLAARsecurity service if required.

The Role of the SOLAARsecurity Manager

The SOLAARsecurity Manager may or may not be the same person as the Network Administrator, depending which server the SOLAARsecurity Server and Administration software is installed on, and the size of the network on which SOLAARsecurity is running.

After the Network Administrator has carried out the functions listed above, the SOLAARsecurity Manager needs to:

- Set up the lists of users and groups granted permission to use the Access Controls for each of the protected functions of the Client software.
- Review the SOLAARsecurity System Policies and disable any policies that are not required.
- Set up the list of meanings that can be attached to electronic signatures.

After initial set-up the SOLAARsecurity Manager will need to perform the following maintenance tasks:

- Make changes to the permission granted or denied to users and groups permitted to use the Access Controls for each of the protected functions of the Client software.
- Make any changes to the SOLAARsecurity System Policies that may be required.
- Make any changes that are needed to the list of signature meanings.

The SOLAARsecurity Manager will not be able to:

- Add new users to the system.
- Change the composition of groups of users.

These functions can only be performed by a Network Administrator.

The 21 CFR Part 11 Rule

The Food and Drugs Administration is a United States Government Agency that has responsibility for ensuring the safety of pharmaceutical and related healthcare products supplied to American consumers. One method that it uses to discharge this responsibility is to regulate and approve the activities of the manufacturers of these materials, then prevent products from unapproved vendors from being sold in the US market.

The terms of the FDA regulations are strict, and involve the regular submission, by the manufacturer, of Manufacturing Quality Control and other records to the FDA. Manufacturers are regularly inspected and audited by FDA inspectors to ensure, amongst other things, that their record keeping systems meet the requirements that the FDA considers to be necessary to ensure the validity and veracity of these records.

On August 20th, 1997, the US FDA released Part 11 “Electronic Records; Electronic Signatures” of Title 21 of the Code of Federal Regulations, usually referred to as the 21 CFR Part 11 Rule¹. This Rule sets out the conditions under which the FDA is prepared to accept submission of electronic (as opposed to paper based) records from regulated manufacturers.

¹ Code of Federal Regulations, Title 21, Food and Drugs, Part 11 “Electronic Records; Electronic Signatures Final Rule”, Federal Register 62 (54), 13429-13466. A copy of the Final Rule itself can be obtained from <http://www.fda.gov/RegulatoryInformation/Guidances/ucm125067.htm>

Open and Closed Systems

The Rule defines and distinguishes two broad types of computer systems that may create, modify, maintain or transmit electronic records. These are described as:

Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

The Rule sets out separate controls that are required for closed and open systems.

The SOLAAR*security* Software package is a **closed system** under these definitions, and provides facilities and functions that will assist you in meeting the requirements for closed systems set out in section 11.10 of the Rule.

Electronic Records

Section 11.3 of the Rule deals with the definitions of various terms used in the Rule. Under these definitions, an electronic record is:

...any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

SOLAARsecurity uses database technology to create, store and maintain electronic records. Four types of database are used that contain information. According to the Rule, these databases constitute electronic records. The databases are:

1. The Results databases
2. The Method databases
3. The Operational Qualification (OQ) Tests Results databases
4. The Performance Qualification (PQ) Tests Results databases. Each database can contain many individual records, which are defined as follows:

Analysis Record

A single electronic record contained in a Results database is defined as an Analysis Record. An Analysis record is composed of a set of analytical results measured from a batch of samples, together with the Method used to measure samples, the Sequence Table and Action Matrix that defines the measurement sequence, and the Sample Details that contain sample specific information. An Audit Trail that records any changes made to the data after the analysis has been completed is also part of an Analysis Record.

Method Record

A single electronic record contained in a Methods database (generally referred to as the Methods Library) is defined as a Method Record, which is composed of sets of Analysis Parameters for each element defined in the Method, and an Audit Trail which records changes made to the Method Record since its creation.

SOLAAR Methods include sample and run dependent data, in the form of Sample Details, the Sequence Table and associated Action Matrix. This data is NOT considered to form part of the Method Record. When the Method and its associated Samples Details, Sequence Table and Action Matrix are used to measure a particular batch of samples, the Method Record itself and the Sample Details, Sequence Table and Action Matrix become part of the Analysis Record.

Operational Qualification Tests Results Record

The Operation Qualification (OQ) Tests database is created and maintained by the OQ Test Client application. A single OQ Test Results Record consists of a set of results from an OQ Test sequence, together with the pass/fail status of each test. An Audit Trail is included.

Performance Qualification Tests Results Record

The Performance Qualifications (PQ) Tests database is created and maintained by the SOLAAR Data Station client application. A single PQ Test Results Record consists of a PQ Test Analysis Record, which has similar characteristics as a normal Analysis Record.

Audit Trails

Section 11.10 paragraph (e) of the Rule requires the use of:

...secure, computer generated, time-stamped audit trails to independently record the date and time of operator entries that create, modify or delete electronic records.

SOLAAR*security* creates audit trails for each type of electronic record described above. The audit trails are created automatically, and are stored as part of the electronic record to which they pertain. They record the creation of the record, and any subsequent manipulation of the data contained in the record. These are described as Data Audit Trails. However, the definition of audit trails in the Rule is wider than this, and includes, for example, the requirement to record the deletion of an electronic record. Obviously, if the audit trail is part of the record itself, the audit trail will be deleted with the record, and so cannot record the deletion of the record. SOLAAR*security* therefore implements a second type of audit trail, known as the Event Audit Trail, to record such events. To do this, it makes use of the facilities provided by the Microsoft® Windows® Operating System.

Versions of Microsoft Windows Operating System that are based on Windows NT4 and higher (Windows XP Professional (SP2), Windows Vista™ Ultimate, Windows 7 Professional, and Windows 10) provide a feature described as the Applications Event Log. This is an audit trail that is maintained by the operating system that can be used by applications running under the operating system. SOLAAR*security* uses the Windows Applications Event Log to maintain an audit trail of events associated with its electronic records that cannot be recorded in the record itself.

Electronic Signatures

Paper records submitted to the FDA must be signed by one or more individuals. A handwritten signature is a legally binding assertion that the signing individual accepts responsibility for the content of the document, as required by the Agency Regulations.

When the FDA considered the use of electronic records, they included the concept of Electronic Signatures. Provided that Electronic Signatures conform to the requirements of the relevant parts of the Rule, the FDA will consider the Electronic Signatures to be:

...equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations.

An Electronic Signature is defined in Section 11.3 (b) paragraph (7) of the Rule as being:

...a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

Paragraph (5) of the same section defines a particular type of electronic signature, described as a Digital Signature, as being:

An electronic signature based on cryptographic methods of originator identification, computed using a set of rules and a set of parameters such that the identity of the signer and integrity of the data can be verified.

Electronic Signature components

The Rule provides for signatures that are based on biometric devices i.e. a unique physical attribute of the individual that is measured and recorded, and incorporated into the signature. SOLAARsecurity does NOT support electronic signatures based on biometrics.

The Rule also provides guidance for electronic signatures that are based on the use of identification codes in combination with passwords. SOLAARsecurity implements electronic signatures of this type.

Section 11.200 (a) paragraph (1) states that such electronic signatures shall:

Employ at least two distinct identification components such as an identification code and password.

SOLAARsecurity implements electronic signatures based on unique user identification and unique user passwords. These are derived from the user identification and password used by individuals to gain access to the Windows network or local machine operating system, and are created and maintained using facilities provided by the operating system. The

process by which the identity of a user is discovered and confirmed using this data is referred to as User Authentication. Issues associated with the creation and maintenance of this user identification and verification data, so that the requirements of the Rule are properly satisfied, are discussed in more detail in the SOLAAR*security* Administrators Manual.

Electronic Signature manifestations

Section 11.50 (a) of the Rule sets out the information that must be associated with an electronic signature:

- (1) The printed name of the signer;
- (2) The date and time when the signature was executed; and
- (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

SOLAAR*security* signatures include all this information. When an individual signs a record, he can pick one of several meanings for the signature from a list of approved meanings. This list can be set up and maintained centrally using the SOLAAR*security* Administrator application.

Signature/record linking

Section 11.70 of the Rule requires that:

Electronic ... signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied or otherwise transferred to falsify an electronic record by ordinary means.

SOLAAR*security* electronic signatures are stored as part of the electronic record to which they pertain. They can not be excised, copied or otherwise transferred to another electronic by any ordinary means provided in the SOLAAR*security* software or the Windows operating system.

Signature validity

SOLAAR*security* signatures are Digital Signatures, as defined by paragraph (5) of section 11.3 (b) of the Rule. When a signature is executed to an electronic record, a cryptographic algorithm is used to generate a code that uniquely identifies the content of the record. This code is included in the signature. When the signature associated with the record is subsequently viewed, the record data is again encrypted, and the two codes are compared. The signature is only considered to be valid when the two codes are identical. Any intended or accidental change to the record data after the signature has been executed will result

in a different code when the record is encrypted, and so the signature will become invalid. Signature validity is made visible by colour coding the display of the signed records, as well as providing a means of viewing the signatures themselves.

Authority and Device Checks

Section 11.10, paragraph (g) of the Rule requires the use of Authority Checks to:

... ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

and paragraph (h) goes on to describe Device Checks that:

... determine, as appropriate, the validity of the source of input data or operational instructions.

SOLAARsecurity provides these Authority Checks by means of Access Controls that grant or deny access to specific parts of the system to authorised individuals. Individuals can be granted or denied permission to use the Client software itself, and the various functions within it. Permissions to access controlled functions are set up in the SOLAARsecurity Administrator application, and cannot be changed from the Client software.

SOLAARsecurity also provides System Policies that implement a second level of security for certain facilities, including starting the Client software packages themselves. When the appropriate System Policy is set, additional User Authentication will be required before the facility can be used. System Policies are also set up in the SOLAARsecurity Administrator application, and cannot be changed from the Client software.

