SOLAAR*security*

Administrator Software Manual

9499 400 40011

010508 Issue 2

© 2008 Thermo Fisher Scientific. All rights reserved.

SOLAAR House, 19 Mercers Row, Cambridge CB5 8BZ.United Kingdom.
Telephone +44 (0) 1223 347400, Fax +44 (0) 1223 347402.
www.thermofisher.com

Thermo
SCIENTIFIC

This page is intentionally blank.

Contents

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 1 System Overview

This page is intentionally blank.

Product Structure

The SOLAARsecurity software comprises of four separate Windows applications which work in conjunction with the Windows 2000 (SP4) / XP Prof (SP2) / Vista Ultimate operating systems to provide an environment that fully supports the requirements of 21CFR Part 11.

The four SOLAAR applications are:

- **SOLAAR*security* Administrator**
  This application allows any person designated as a SOLAARsecurity Manager to define security policies for user authentication, access control, auditing of electronic records and control of electronic signatures. Typically this software will be installed on a network server to provide centralized administration for all user accounts on the network. The security policies defined using the Administrator software are stored on the network server in a secure database.

- **SOLAAR*security* Server**
  This application runs as a service on the same machine as the SOLAARsecurity Administrator application, and enforces the security policies defined by the SOLAARsecurity Manager using the Administrator program. This program is capable of servicing multiple simultaneous client applications running on different computers on the network.

- **SOLAAR*security* Data Station Client**
  This is the application used to control the Atomic Absorption spectrometer, to collect and store data, and to perform any subsequent data manipulations. 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.

- **SOLAAR*security* OQ Tests Client**

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

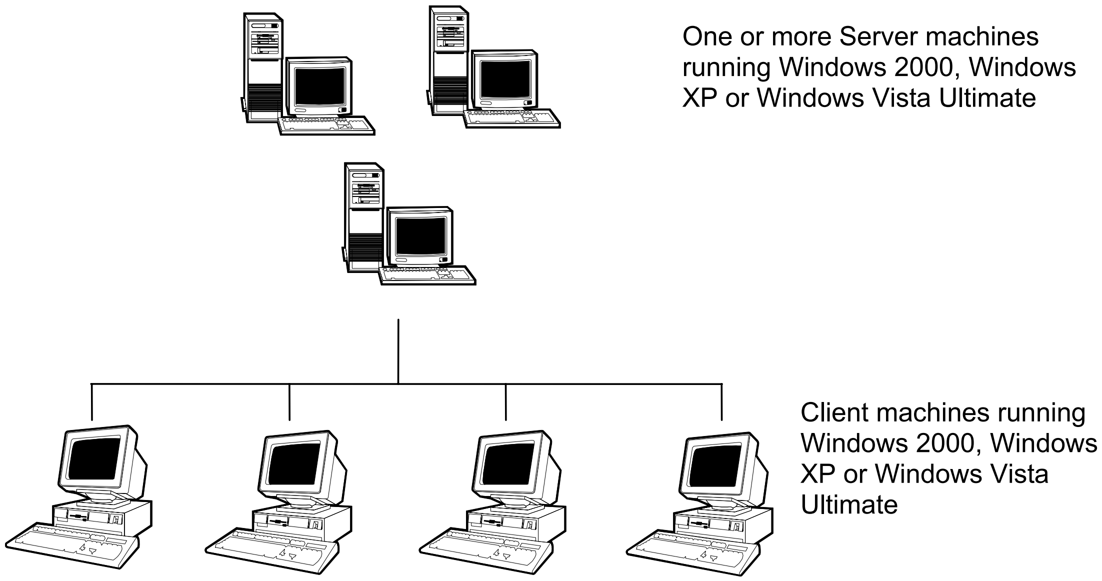
  The OQ Tests Client software also provides a comprehensive suite of User Diagnostic tools to assist in identifying and rectifying any problems that may arise with the spectrometer system. It provides facilities for creating logs of such activities, to assist in achieving compliance with the requirements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

Supported Configurations

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

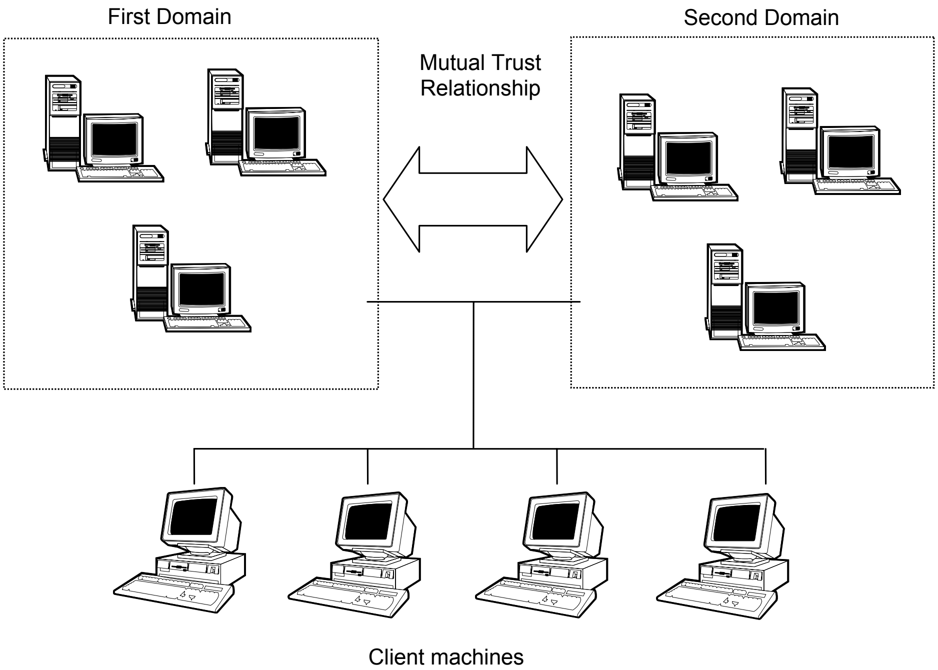
The Single Domain Model

The Administrator and Server applications are installed together on any Windows 2000 / XP / Vista Ultimate server that is a member of a domain. The SOLAAR*security* client software is installed on one or more workstations that are also members of the domain. The client workstations may be running any of Windows / 2000 / XP / Vista Ultimate.


One or more Server machines running Windows 2000, Windows XP or Windows Vista Ultimate
Client machines running Windows 2000, Windows XP or Windows Vista Ultimate

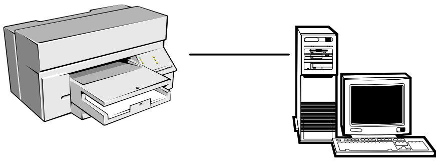
The Multiple (Trusted) Domain Model

The Administrator and Server software are installed on any Windows 2000 / XP / Vista Ultimate server that is a member of a domain. The client software is installed on client machines that are members of other, trusted domains. The client workstations may be running any of Windows 2000 / XP / Vista Ultimate.



Stand alone configuration

The SOLAARsecurity Clients, Administrator and Server software are all run on a single non-networked computer that acts as both client and server. This computer must be running Windows 2000 / XP / Vista Ultimate.



Computer running Windows 2000 Server or Professional, Windows XP Professional or Windows Vista Ultimate

System Pre-requisites

Supported Operating System Versions and pre-requisites

Operating System	Server & Administrator	Client
Windows Vista Ultimate	YES	YES
Windows XP Professional	YES	YES
Windows 2000 Server >= V5.00 SP 1	YES	YES

The Server and Administration software **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 NT LM service. (See Section 2 - Planning the Installation). 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 SOLAARsecurity Server and Administrator software 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.

However, once installed, the ability to run the SOLAARsecurity Administrator program 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.

This page is intentionally blank.

Chapter 2 Planning the Installation

This page is intentionally blank.

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 SOLAARsecurity 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 2000 / XP / VISTA operating system in order to support the requirements of 21 CFR Part 11. For example, user authentication is performed using the operating system logon 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 to which the software is to be installed and to review (existing system) or define (new system) certain aspects of system behaviour.

Please 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 section 1.2 above). 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 at least one individual concerned with the installation has Network Administrator privileges on the network domain on to 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 to which the Administrator and Server software in 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 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 is reported in audit trails together with the user account id.

- **Description**

  The contents of this field are not displayed in the SOLAAR*security* Client software, 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 logon 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 logon" to TRUE. This ensures that after the first log on 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 SOLAARsecurity 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 SOLAARsecurity 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 will be those users who 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 software. 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 each account's group membership. Access control in SOLAAR*security* 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 behaviour 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

Whilst the SOLAAR*security* client software generate their own audit trails for all records that they create and modify, 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's Audit Policy allows you to define system and security events that are to be logged in the operating system's System and Security event logs. 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 Software User Manual.

Domain Trust Relationships

If you require users from multiple domains on your network to be able to access the SOLAAR*security* Client software 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 software.

Event Log configuration

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

The operating system can also write events into its Security and System event logs **if the operating system's audit policy has been appropriately configured**. For example failed attempts to access a user account can be logged in order to meet 21 CFR 11.3000 (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 behaviour 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 software installed on a single computer. This is intended for small laboratories with no network facilities.

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 allowed access 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 logon attempts cannot be reported in an immediate and urgent manner to system management.

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

NT LM Service

The process of user authentication that forms the basis of user logon and electronic signature generation is based around the Microsoft NT LM challenge/response protocol. To enable this protocol, the NT LM Security Support Provider service must be running on the server and client computers. This is usually installed and set up by default on Windows 2000, and Windows XP and Windows Vista systems.

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

This page is intentionally blank.

Chapter 3 Installation of the SOLAAR*security* Administrator Software

This page is intentionally blank.

Initial Installation

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 are described in the AA Series Validator Log Book. 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.

Pre-Installation procedures are described in the SOLAARsecurity Pre-Installation Manual. 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 confirm 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 500Mbytes 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.

You will need:

- **The SOLAAR*security* CD**
- **The SOLAAR 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 computer and log on to the operating system and network.
2. When the operating system has loaded, and Windows desktop is displayed on the screen, insert the SOLAAR*security* CD into the CD drive.
3. The CD will automatically start the installation, and will display the first installation dialogue.
   - 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 on the file ***autorun.exe***.

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 SOLAARsecurity 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 dialogue.
   - 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 on the file ***autorun.exe.***
7. The **SOLAAR Install** dialogue will be displayed.

Note: That this CD also contains software for older AA instruments. This software is NOT compatible with SOLAAR*security.*

8. On the SOLAAR Install dialogue, select Install SOLAAR Security Server. The first dialogue of the Install Wizard will then be displayed. The Install Wizard will ask you for the information it needs to install the software. Carefully read each dialogue when it is displayed, and provide the information requested. Click on the Next button to move on the next dialogue, or click the Back button 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 dialogue, 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 on the **Back** button to reach the relevant dialogue, make the changes that you want, then click on the **Next** buttons until you reach this dialogue again. When you are satisfied with your settings, click the Next button 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 ‘Administer Security Database’ Access Control to at least one individual or group (the SOLAARsecurity 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 SOLAARsecurity Manager can complete these tasks later.

11. When you have finished, use the File.Save command, or click on the File.Save button, to save the Security database, then use the File.Exit command to close the application.
12. The final Install Wizard dialogue will then be displayed. Click on the Finish button to complete the installation, and remove the CD from the CD drive.

The Install Wizard will create a short cut to the Administrator program, and place it in the **SOLAAR Security** program group that will appear on the **Start** menu. You can, if you wish, use the facilities provided by Windows to create other short cuts as required. You may find it convenient to create a short cut on the Windows desktop, for example. Any shortcuts that you create must point to the file

```
C:\Program Files\SolaarSecurity\Admin.exe.
```

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

```
C:\Program Files\SolaarSecurity\SOLAAR
Security.sdb.
```

If the files on the machine on which you have installed the SOLAAR*security* Administrator application are not regularly backed up, you may wish to make special arrangements to ensure that a back-up copy of this file 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.

Updates, Repairs and Uninstallation

From time to time, we may release updated versions of the SOLAARsecurity 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 User database.

To repair an existing 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 **SOLAARsecurity Admin/Server.** Click on the **Change/Remove** button to display the Installation Wizard.
4. Select the **Repair** radio button, and then click the **Next** button to repair your installation.

You can uninstall the SOLAARsecurity Administrator and Server applications. Note, however, that if the Server application is not running, the SOLAARsecurity Client software will not be able to run either.

To uninstall the SOLAAR*securit*y Administrator and Server software:

1. Refer to your Windows documentation and Help files, and open the Windows Control Panel.
2. Select the **Add/Remov**e Programs command.
3. In the list of Currently Installed Programs that will be displayed, select **SOLAARsecurity Admin/Server.** Click on the **Change/Remove** button to display the Installation Wizard.
4. Select the **Automatic** radio button, and then click the **Next** button to uninstall the applications.

Chapter 4 Using the SOLAAR*security* Administrator Software

This section is intended to assist SOLAAR*security* Managers with the day-to-day administration of the SOLAAR*security* Users database. If required, some explanations of the terms and concepts involved in networked systems are provided in the Reference section of this manual.

The following functions, which are outside the scope of the SOLAAR*security* software, must be carried out by a System Administrator:

- Adding new users to the system
- Setting up and changing user groups
- Making necessary checks and adjustments to operating system configuration

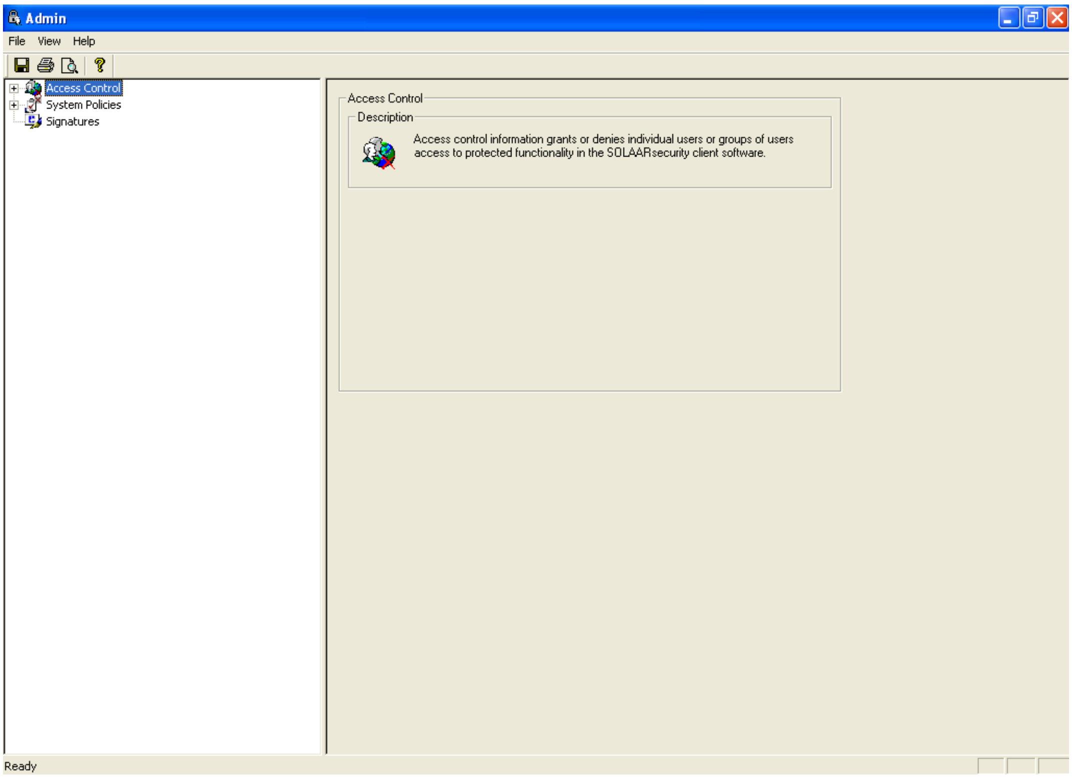
This page is intentionally blank.

Starting the SOLAAR*security* Administrator

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

Finding your way around

When the SOLAAR*security* Administrator is started the program work area is displayed.



Access control information grants or denies individual users or groups of users access to protected functionality in the SOLAARsecurity client software.

The Menu Bar

The Menu Bar contains File, View and Help menus.

The File Menu
The File menu contains the following commands:

- **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 leaving the previous Security Database unchanged.

- **Print Commands**

  The Print, Print Preview and Print Setup commands are used to print the contents of the Security Database, and have their usual significance.

- **Exit**

  Closes the SOLAAR*security* Administrator software.

The View Menu

This enables you to toggle display of the Toolbar and the Status Bar.

Help

SOLAAR*security* Administrator software does not have on-line help. The Help item enables you to access the About page, which displays the full name and version number of the software.

The Tool Bar

The Tool Bar contains buttons that provide immediate access to commonly used commands.

- 💾 Save

  This saves the current version of the Security database.

- 🖨 Print

  This prints the current version of the Security database to the default printer.

- 🔍 Print Preview

  This displays a print preview of the current version of the Security database.

- ? Help

  This displays the Help About dialogue, showing the version of the software.

The Navigation Pane

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

- Access Controls

  These allow you to set up the permissions of individual users or groups of users to access the protected functions of the software.

- System Policies

  These enable or disable security policies that apply to all users of the software.

- Signatures

  This allows you to set up the signature meanings that will be available on the system.

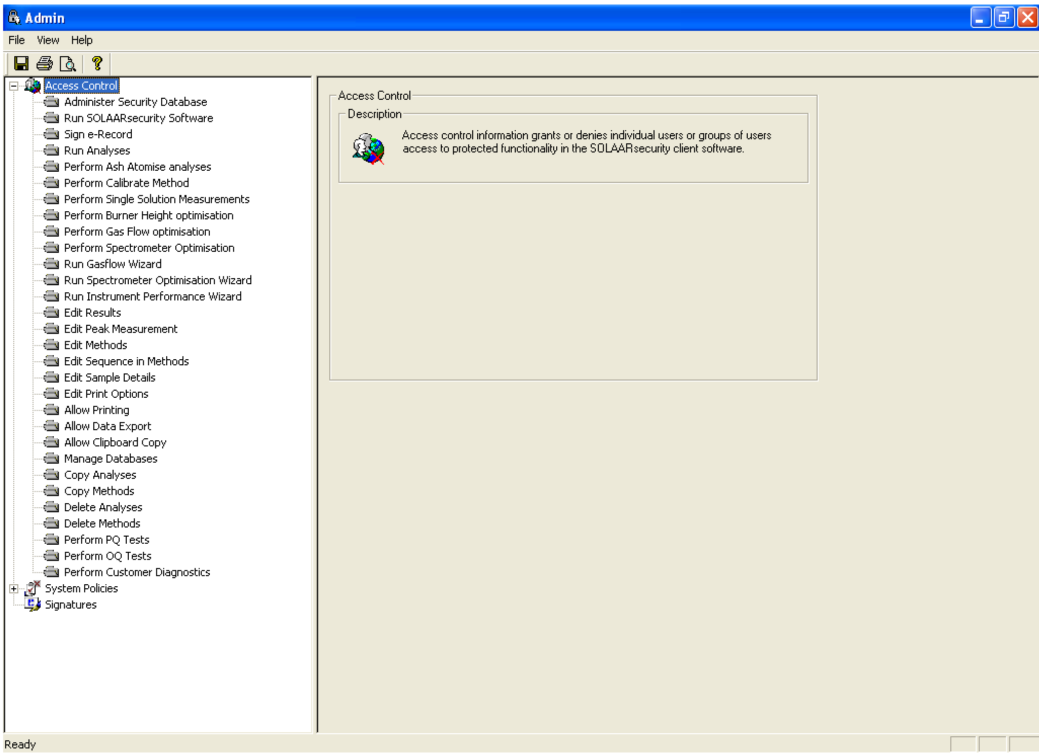
Working Area

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 Controls

Introduction to Access Controls

When the Access Control branch has been expanded (by clicking on its + sign) the navigation pane will contain the list of the available Access Controls, that is, operations for which access control is available.



- Access Control
  - Administer Security Database
  - Run SOLAARsecurity Software
  - Sign e-Record
  - Run Analyses
  - Perform Ash Atomise analyses
  - Perform Calibrate Method
  - Perform Single Solution Measurements
  - Perform Burner Height optimisation
  - Perform Gas Flow optimisation
  - Perform Spectrometer Optimisation
  - Run Gasflow Wizard
  - Run Spectrometer Optimisation Wizard
  - Run Instrument Performance Wizard
  - Edit Results
  - Edit Peak Measurement
  - Edit Methods
  - Edit Sequence in Methods
  - Edit Sample Details
  - Edit Print Options
  - Allow Printing
  - Allow Data Export
  - Allow Clipboard Copy
  - Manage Databases
  - Copy Analyses
  - Copy Methods
  - Delete Analyses
  - Delete Methods
  - Perform PQ Tests
  - Perform OQ Tests
  - Perform Customer Diagnostics
- System Policies
- Signatures

Access Control

Description

Access control information grants or denies individual users or groups of users access to protected functionality in the SOLAARsecurity client software.

Ready

When an item on the Access Control list is selected the work area will contain the following elements:

- 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 have to run analyses on the spectrometer, either to generate analytical results from samples, or to set up and optimise 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 that such users do not alter 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 Atomise Analyses'
- 'Perform Calibrate Method'
- 'Perform Single Solution Measurement'
- 'Perform Burner Height Optimisation'
- 'Perform Gas Flow Optimisation'
- 'Perform Spectrometer Optimisation'

SOLAAR Wizards provide similar functionality to the individual optimisation 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 Optimisation 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 organisations overall 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 organisation 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 SOLAARsecurity 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 SOLAARsecurity 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:

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.
On the Access Control User List and checked.	Permission to use the Access Control has been granted.
On the Access Control User List and unchecked.	Permission to use the Access Control has been explicitly denied. This will over-ride 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 alleach of the groups of which s/he is a member.

To set up Access Control permissions for Users and Groups:

2. Expand the **Access Control** list in the navigation pane by clicking on its + sign.

3. Select the Access Control for which User permissions are to be set up.

4. 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.

   - 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 on the **Add** button. The name of the user or group will be added to the Access Control list.

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

5. Continue in this way 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 s/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 in the check box to restore the check mark.

8. To remove a user or group from the Access Control list, click on the user name to select it and then click on 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 use the **Save** icon on the toolbar.

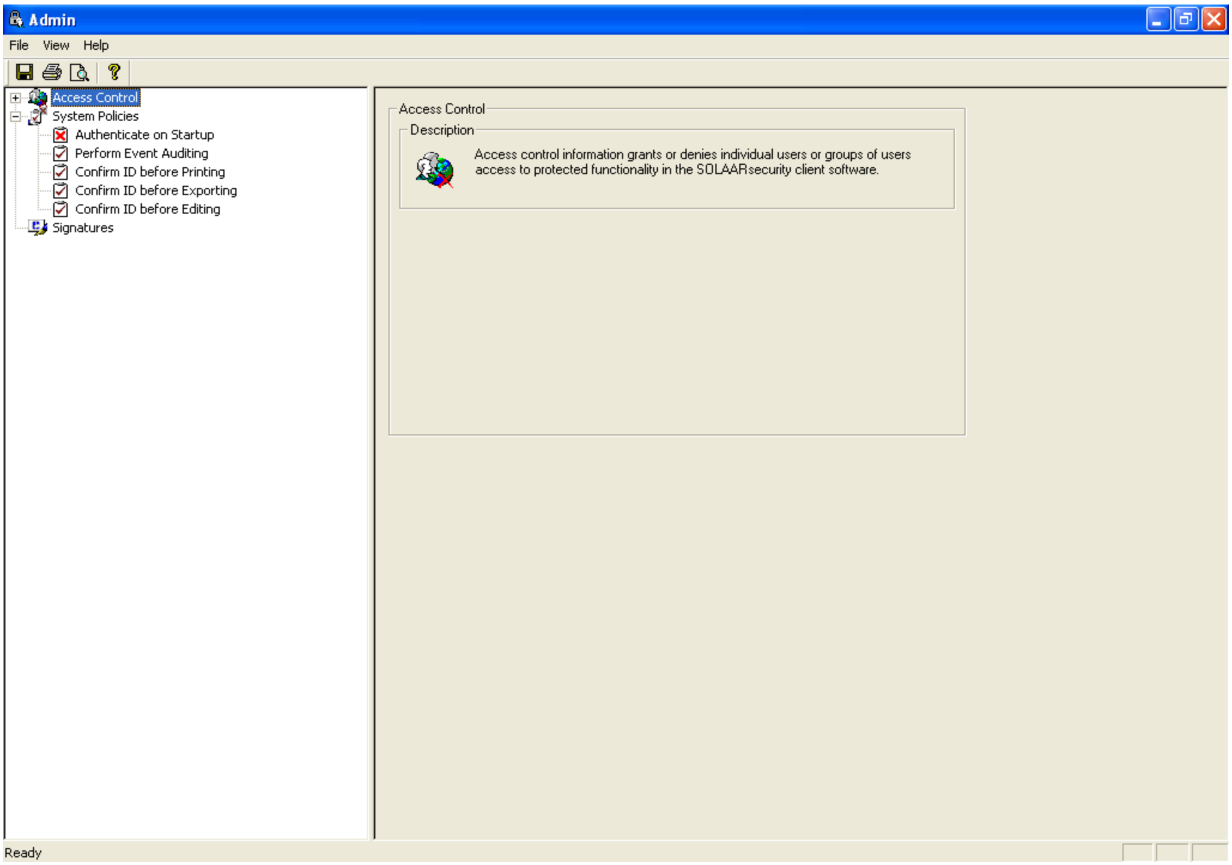
Note: If a user, or a group of users, is granted or denied permission to use the 'Run SOLAAR Security s/w' Access Control, the Users Security database must be saved, and the SOLAAR*security* Service must be stopped and restarted in order for the changes to take effect. The procedure for stopping and starting the SOLAAR*security* Service is described in Chapter 5.

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 (by clicking on its + sign) the navigation pane will contain the list System Policies available in Client software.



Access control information grants or denies individual users or groups of users access to protected functionality in the SOLAARsecurity client software.

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 SOLAAR*security* 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 SOLAAR*security* 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, SOLAAR*security* 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.

Note: If the user logged on to the workstation does not have permission to run the SOLAAR*security* 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 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 SOLAAR*security* software package will pass details of certain events to the SOLAAR*security* 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 in 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 D_2 Hours.** The deuterium (D_2) 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 D_2 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.** he 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 SOLAAR*security* 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 SOLAAR*security* 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 SOLAAR*security* software

Event logs can be viewed by on the server computer.

To view the Applications event log:

1. Click on **Start.Settings.Control Panel.Administrative Tools. Event Viewer** in Windows 2000 / XP / Vista or use S**tart. Programs.Admin Tools.Event Log** in Windows NT 4 or higher.
2. In the left hand pane, click on **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 SOLAAR*security* 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 to signatures

Users who have been assigned the right to execute electronic signatures will be able to sign following SOLAAR*security* 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 SOLAAR*security*. When a properly authorised 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 are unlikely to exactly meet the requirements of your organization. The SOLAAR*security* Manager should review the Signature Meanings and amend them as necessary.

To add a new signature meaning:

1. Click on the **Signatures** item in the navigation pane.
   - The Signatures dialogue appears in the work area.
2. To add a new meaning to the list, click on the Add button.
3. The **Signature Meaning** dialogue opens. Enter the new meaning and click on **OK** to accept it or on **Cancel** to close the dialogue leaving the Meanings list unchanged.

To delete a signature meaning:

1. Click on the **Signatures** item in the navigation pane.
   - The **Signatures** dialogue appears in the work area.
2. Click on the meaning that you wish to delete to select it, and then click on the **Delete** button to remove the meaning from the list.

To edit a signature meaning:

1. Click on the **Signatures** item in the navigation pane.
   - **The Signatures** dialogue appears in the work area.
2. Click on the meaning that you wish to edit to select it, then click on the **Edit** button.
   - The **Signature Meaning** dialogue opens with the meaning in the Edit field. Make the changes required. Click on **OK** to accept the amended meaning or on **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 **File.Save Settings** command, or use the **Save** icon on the toolbar.

Chapter 5 The SOLAAR*security* Service

Introduction

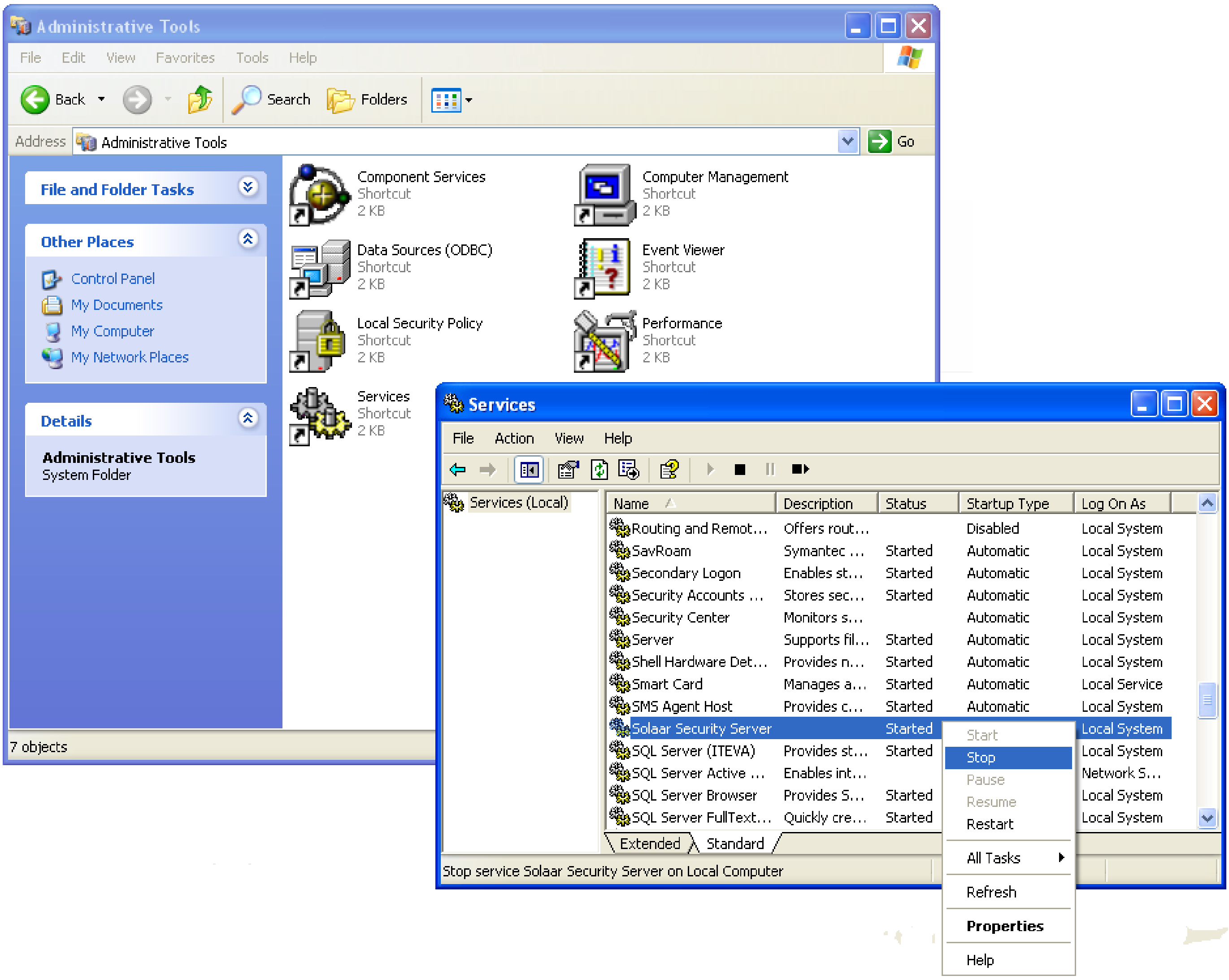
The SOLAAR*security* Service enforces the Security Policies and Access Controls that are defined by the SOLAAR*security* Manager using the Administration program. The SOLAAR*security* Service is automatically installed with the Administrator program. It enforces the security policies simultaneously across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

This page is intentionally blank.

Stopping and starting the SOLAAR*security* Service

In some circumstances it is necessary to stop and restart the SOLAAR*security* Service. In particular, when changes have been made to the list of users with the right to run the SOLAAR*security* software it is necessary to stop and restart the SOLAAR*security* Service in order to give effect to these changes. The SOLAAR*security* Service can only be started and stopped by a user with Network Administrator rights.

Note: All other changes to the SOLAAR*security* database take effect as soon as the changed database is saved, with no need to start and stop the Service application.



Name	Description	Status	Startup Type	Log On As
Routing and Remot…	Offers rout…		Disabled	Local System
SavRoam	Symantec …	Started	Automatic	Local System
Secondary Logon	Enables st…	Started	Automatic	Local System
Security Accounts …	Stores sec…	Started	Automatic	Local System
Security Center	Monitors s…		Automatic	Local System
Server	Supports fil…	Started	Automatic	Local System
Shell Hardware Det…	Provides n…	Started	Automatic	Local System
Smart Card	Manages a…	Started	Automatic	Local Service
SMS Agent Host	Provides c…	Started	Automatic	Local System
Solaar Security Server		Started		Local System
SQL Server (ITEVA)	Provides st…	Started		Local System
SQL Server Active …	Enables int…			Network S…
SQL Server Browser	Provides S…	Started		Local System
SQL Server FullText…	Quickly cre…	Started		Local System

Stop service Solaar Security Server on Local Computer

To stop the SOLAAR*security* Server application:

1. Click on **Start.Settings.Control Panel.Administrative Tools. Services.**
2. Select **SOLAAR Security Server** from the list.
3. Right click on **SOLAAR Security Server** to display the context menu, or open the **Action** menu.
4. Click on **Stop** command.

To start the SOLAAR*security* Server application:

1. Click on **Start.Settings.Control Panel.Administrative Tools. Services.**
2. Select **SOLAAR Security Server** from the list.
3. Right click on **SOLAAR Security Server** to display the context menu, or open the **Action** menu.
4. Click on the **Star**t command.

Chapter 6 Reference

This page is intentionally blank.

Network Concepts

Introduction

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 2000 (SP4) / XP (SP2) / Vista 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 logon 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 Windows NT/2000 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 SOLAARsecurity 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 SOLAAR*security* Manager may or may not be the same person as the Network Administrator, depending which server the SOLAAR*security* Server and Administration software is installed on, and the size of the network on which SOLAAR*security* is running.

After the Network Administrator has carried out the functions listed above, the SOLAAR*security* 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 SOLAAR*security* 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 SOLAAR*security* 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 SOLAAR*security* System Policies that may be required.
- Make any changes that are needed to the list of signature meanings.

The SOLAAR*security* 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.