Security Administration User's Guide

Thermo
SCIENTIFIC

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

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

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

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

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

269-228600, Rev A

Contents

Introduction

This manual explains how to use Thermo Scientific Security Administration software. You can use the software to set and enforce security policies for one or more Thermo Scientific client applications that have been programmed to work with the software. Typically a client application comes with a manual explaining how to set its specific policies.

Security Administration comprises two separate applications that work in conjunction with your Windows® Vista™ or Windows XP Professional operating system to provide a secure environment that supports the requirements of 21 CFR Part 11.

- **Security Administration** lets users, typically people designated as a system or network administrator, define security policies for access control, auditing of electronic records and control of electronic signatures. Typically this software is installed on a network server to provide centralized administration for all user accounts on the network. The security policies defined using this software are stored on the network server in a secure database where they are then queried by the Security Administration software.

- **Thermo Security Service** runs as a service under Windows and enforces the security policies defined with the Security Administration program. Thermo Security Service can service multiple simultaneous Thermo Scientific client applications running on different computers on the network.

Security Administration also includes Thermo Log Service, which logs application events and changes to files, and Thermo File Service, which allows a client application to write data to locations to which the current user does not have access rights. These services are installed on the client application computers, not with Security Administration.

When a Thermo Scientific client application is running, it is in constant communication with Thermo Security Service in order to enforce the defined security policies.

If you have just purchased Security Administration and want to use it to administer a supported client application in a secure environment, you need to perform the following general steps:

Step 1: Set up Windows administration. See “Windows administration for network computers” or “Windows administration for stand-alone computers” in the “Setting Up Windows Administration” chapter. To help prepare you for this task, you can read the overview of network concepts and Windows security features provided in the “Overview of Windows Administration” chapter. If you are using a network, you should also set your service accounts so that they are not running as local system accounts. See the “Setting Service Accounts” chapter.

Step 2: Install Security Administration. See the “Installing the Software” chapter.

Step 3: Install the client application and add it to the security database. Typically a client application is not installed on the same computer as Security Administration unless a stand-alone, non-networked computer is being used. See the documentation that came with the application for installation instructions. See “Adding a client application” in the “Using Security Administration” chapter of this manual for instructions for adding a client application to the database.

Step 4: Perform Installation Qualification (IQ) and Operation Qualification (OQ) if required. See the documentation that came with your client application.

Step 5: Set up the client application accounts and file permissions. See the “Setting Up Client Application Accounts” chapter and the documentation that came with the application.

Requirements

If you use Security Administration with a network, the network must be running Windows Vista or Windows XP Professional. The network can be a client-server network or a peer-to-peer workgroup.

Any computer on which you install and use Security Administration must meet the following minimum requirements:

- Network interface card, if you are using a network.
- Windows Vista, or Windows XP Professional with Service Pack 2.

Your client application may have additional requirements. See the documentation that came with it for more information.

Manual conventions

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

Note Notes contain helpful supplementary information. ▲

Notice Follow instructions labeled “Notice” to avoid damaging the system hardware or losing data. ▲

⚠ Caution Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury. It may also be used to alert against unsafe practices. ▲

⚠ Warning Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury. ▲

⚠ Danger Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. ▲

Tips ➡ This symbol marks the start of a list of helpful tips for using the feature being discussed.

Questions or concerns

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

Overview of Windows Administration

Setting up Windows administration is necessary before you can install and use Security Administration. This chapter provides an overview of network concepts and Windows security features and will prepare you for setting up the Windows groups and user accounts for Security Administration and your client applications.

Basic network concepts

Security Administration is designed to run in a networked environment or in a stand-alone configuration. The security functionality of Security Administration is fundamentally linked to the security features of your Windows network operating system. As a Security Administration system administrator, you do not need to be familiar with these security features unless you are also a network administrator. However, an understanding of some of the concepts and terms may give you more confidence in using the Security Administration software.

Network terms

The definitions in the next sections explain some commonly used network terms.

Servers and clients

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

A client is the requesting program or user in a client-server relationship.

Client-server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request.

Domains and domain controllers

A domain is a logical grouping of network servers and other computers that share common security and user account information. The network administrator creates one 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 and use this information to authenticate users logging on to domain accounts.

Grouping computers into domains provides benefits to both network administrators and users. The domain controllers form a single administrative unit, sharing security and user account information. This means that the network administrator 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 consists 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

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 individual 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 (explained below), which apply to specific objects.

Permissions

A permission is a rule associated with an object (usually a directory, file or printer). Permissions regulate 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.

Note Security Administration uses standard Windows users and groups; it does not create its own users or groups. ▲

There are two types of group accounts:

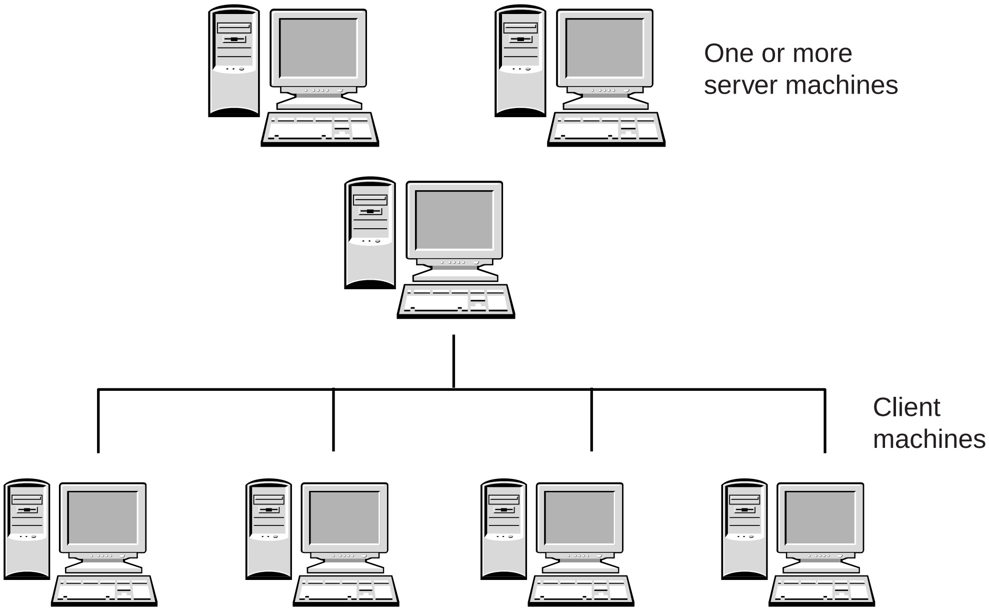
A global group consists of several user accounts from one domain that are grouped together under one group account name. A global group can contain user accounts from only one domain—the domain in which the global group was created. “Global” indicates that the group can be granted rights and permissions 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.

Supported configurations

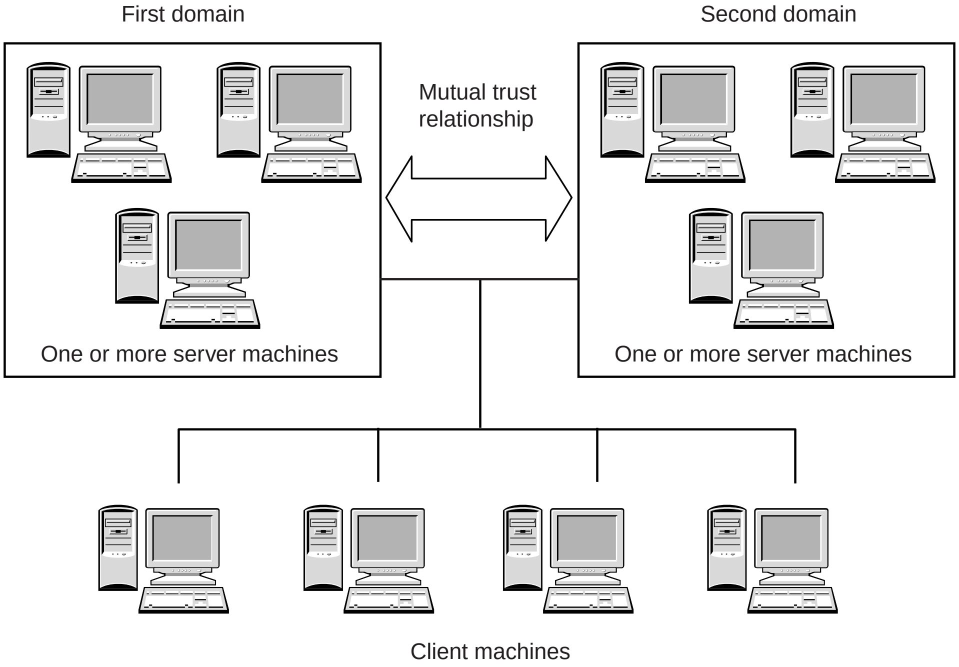
You can use Security Administration to set and enforce security policies in four types of network and other configurations:

In the **single domain** model, Security Administration and Thermo Security Service are installed together on any Windows Vista or Windows XP Professional machine that is a member of the domain. The client application is installed on multiple workstations that are members of the domain. The client workstations run Windows Vista or Windows XP Professional.



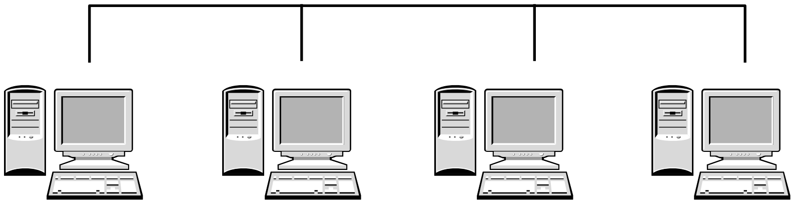
Single domain model

In the **multiple (trusted) domain** model, Security Administration and Thermo Security Service are installed on any Windows Vista or Windows XP Professional machine that is a member of either domain. The client application is installed on multiple client machines that are members of either domain. The client workstations run Windows Vista or Windows XP Professional.


First domain
Second domain
Mutual trust relationship
One or more server machines
One or more server machines
Client machines

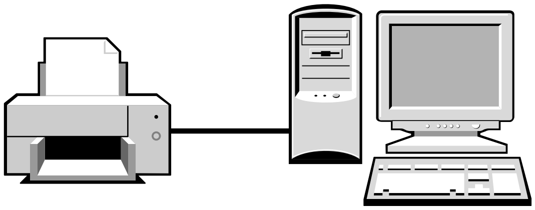
Multiple (trusted) domain model

In a peer-to-peer **workgroup**, Security Administration and Thermo Security Service are installed and run along with the client applications on two or more linked computers. The computers run Windows Vista or Windows XP Professional. This configuration eliminates the need to buy a server version of Windows; however, you need to set up user accounts on each computer in the workgroup, not just on a server. Each user must have the same user name and password on every computer in the workgroup.



Peer-to-peer workgroup

In the **stand-alone configuration**, Security Administration and Thermo Security Service are installed and run along with the client applications on a single non-networked computer that acts as both client and server. This computer runs Windows Vista or Windows XP Professional.



Computer connected to optional printer

Stand-alone configuration

Stand-alone configurations are intended for small laboratories with no network facilities. If you run Security Administration on a stand-alone system, pay special attention to the following points:

- Each stand-alone computer must have a unique name.
- Each user must have a unique local user account.

- Users other than an 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.

The role of the network administrator

A network administrator is a person who belongs to the network Administrators group and can create new users and groups on the network.

Only a user who is a member of the operating system Administrators group can perform installation and initial configuration of Security Administration and Thermo Security Service for the computer on which Security Administration is installed.

Before software installation qualification is performed, the network administrator should perform the following tasks:

- Review the operating system configuration and make any changes required to ensure compatibility with the requirements of 21 CFR Part 11.
- Set up a group of users with the right to run the Security Administration program.

Before the Security Administration system administrator can use the Security Administration software to set up the rights of users of the client application, the network administrator will also need to:

- Put the names of the users of the software onto the system, if this has not already been done. Users must be either on the domain in which Security Administration and Thermo Security Service are running, or on a domain with which a mutual trust relationship exists.
- Set up any groups of users needed by the system administrator.

After the installation and initial setup the network administrator may need to:

- Add new users to the system
- Make any changes that are needed to the composition of user groups.

The role of the system administrator

The Security Administration system administrator may or may not be the same person as the network administrator, depending on which computer Security Administration and Thermo Security Service are installed on and the policies of the network on which Security Administration is running.

After the network administrator has carried out the tasks listed in the preceding section, the system administrator needs to:

- Set up the lists of users and groups permitted to perform each of the protected functions of the client application.
- Review the Security Administration system policies and disable any policies that are not required. The system administrator may also add new policy groups and disable policies for groups of users.
- Set up the list of meanings that can be attached to electronic signatures and specify who can use those meanings.

After the initial setup the system administrator will need to perform the following maintenance tasks:

- Make changes to the rights of users and groups permitted to perform each of the protected functions of the client application.
- Make any changes that are needed to the list of signature meanings.

The system administrator will not be able to:

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

These functions can be performed only by a network administrator.

Setting up Windows users

In order for users to start a client application, they must have access to the workstation and must have been granted access to the client application by Security Administration. This means that each user must be assigned a Windows user name and password to log on to the system. The Windows local administrator must add each user to the list of users who can access the workstation. The user name will be the user’s logon name when accessing the workstation.

Through User Accounts in Windows, the administrator can add each user’s network user name to access the workstation or can create new users specifically for that workstation. The administrator can also specify the rights and privileges each user has to the workstation.

Windows passwords are required for each user of the client application to start and use the application. Windows passwords are required for digitally signing files and also for providing data security within the client application.

The administrator should take into consideration the Windows Workstation security features described in the next section when deciding the rights and privileges that should be assigned to users.

Windows security features

Security Administration runs within the Windows Vista or Windows XP Professional operating system, which provides logon authentication and security features for client applications. Security Administration uses the password authentication features in Windows Workstation to provide access to the software. User accounts can be locked out after a specified number of failed attempts to log on (see the next section for details).

Note When we use the term “Windows Workstation,” we are referring to Windows Vista and Windows XP Professional. ▲

Note The items mentioned in this section can be accessed by an administrator through User Accounts in Windows. The administrator can find more information regarding these features in the Windows Workstation Help files or the Windows Workstation documentation. ▲

The next sections describe some of the features available in Windows Workstation that the administrator can take into consideration to better secure client applications and the workstation.

Logon security features

Local Security Policy (available through Administrative Tools in Control Panel) in Windows has many features to make passwords and logging on to the workstation more secure:

- The administrator can assign user passwords and prevent users from changing those assigned passwords, or can require users to change their passwords the next time they log on. Requiring users to change their passwords at the next logon session helps to ensure that only users know their own passwords. If users forget their passwords, the passwords can be reassigned by the administrator and the users can then change those assigned passwords at their next logon session. These settings can be changed for each user by using User Accounts in Windows.

- The administrator can specify whether passwords must have minimum and maximum ages and minimum lengths. The administrator can also specify password uniqueness by setting the system to remember a certain number of passwords and to prohibit their reuse. These password settings can be changed for the workstation by using Local Security Policy (available through Administrative Tools in Control Panel) in Windows.

- The administrator can specify that user accounts be locked out after a specified number of failed attempts to log on. The account can remain disabled for a specified period of time or until the administrator resets the account. These settings can be changed for the workstation by using Local Security Policy (available through Administrative Tools in Control Panel) in Windows.

Note To comply with 21 CFR Part 11, your organization must have a mechanism in place to ensure that the same logon name is never given to two different people. ▲

Locking a workstation

Users or the administrator can specify that workstations be locked by modifying screen saver settings. The screen saver can activate after the system is inactive for a specified amount of time (we recommend using a short period of time), and the currently logged-on user must enter his or her password to unlock the screen saver.

Individual users can set this option by going into their Windows settings and opening the Display Properties dialog box in Windows, or the administrator can set this option for all users by designing a user profile and assigning it to the users as a mandatory profile. See “User profiles” for more information.

Note Some client applications have a security policy in Security Administration for controlling the screen saver. See the documentation that came with the application for details. ▲

If a client application was running when the screen saver activated, it will be in its previous state when a user enters the correct screen saver password.

If the administrator has specified a maximum allowed number of log-in attempts, that restriction also applies to the entering of screen saver passwords.

Event logging

To provide an audit trail, Security Administration uses the Event Log service in Windows to record Security Administration and client application operations, or “events,” in a log that you can view with Event Viewer. A separate log is used for these events to isolate them from other system events. Every event logged by the service includes fields containing some or all of the kinds of information listed below. By recording this information, Security Administration allows your system to meet the audit trail requirements of 21 CFR Part 11.

- The date the event occurred.
- The time the event occurred.
- The name of the client application that was being used when the event occurred (in Windows XP only).
- The type of event that occurred.
- The user name of the person who was logged in when the event occurred.

- The identification of the computer that was being used when the event occurred (in Windows XP only).

Once Security Administration and one or more client applications have been installed, the event log on the computer where Security Administration is installed automatically begins recording significant operations performed with the applications on any computers on the network where the applications are installed. Changes you make to security policies in Security Administration are recorded in the log when you save the changes with Save Settings in the File menu.

The Event Log service allows all file operations to be logged, both within and outside of all applications that are run on the system. Thus, the service will log any attempt to modify any records on the system, even if a client application is not running.

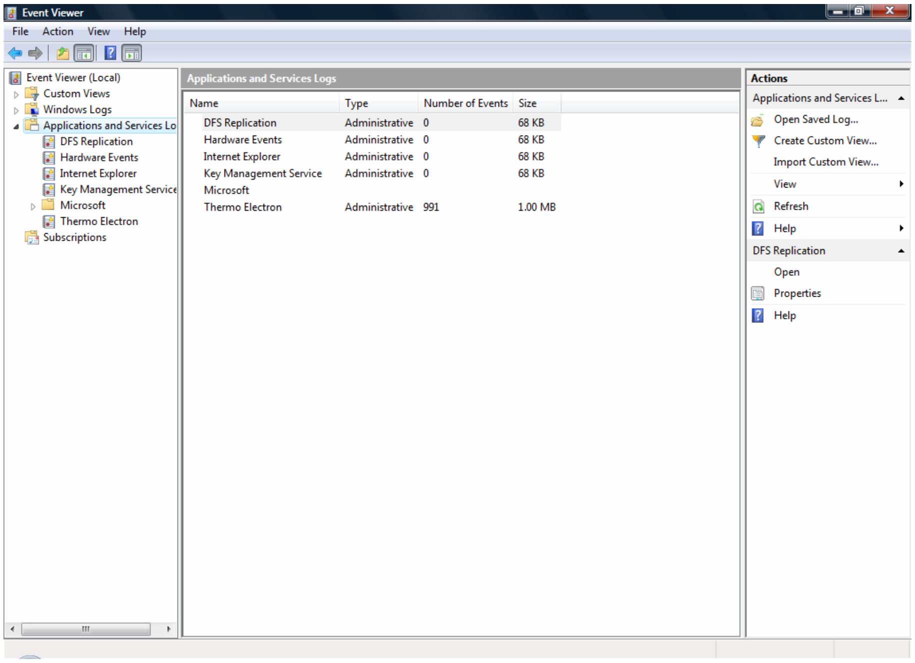
To view the log of events for Security Administration and your client applications, follow the steps below. If you need more detailed information while you are using Event Viewer, choose Help from its Action menu.

1. **Start Event Viewer.**

   Click the Start button on the Windows taskbar and choose Control Panel.

   In Control Panel double-click the Administrative Tools icon. In the Administrative Tools window, double-click the Event Viewer icon. Event Viewer appears.

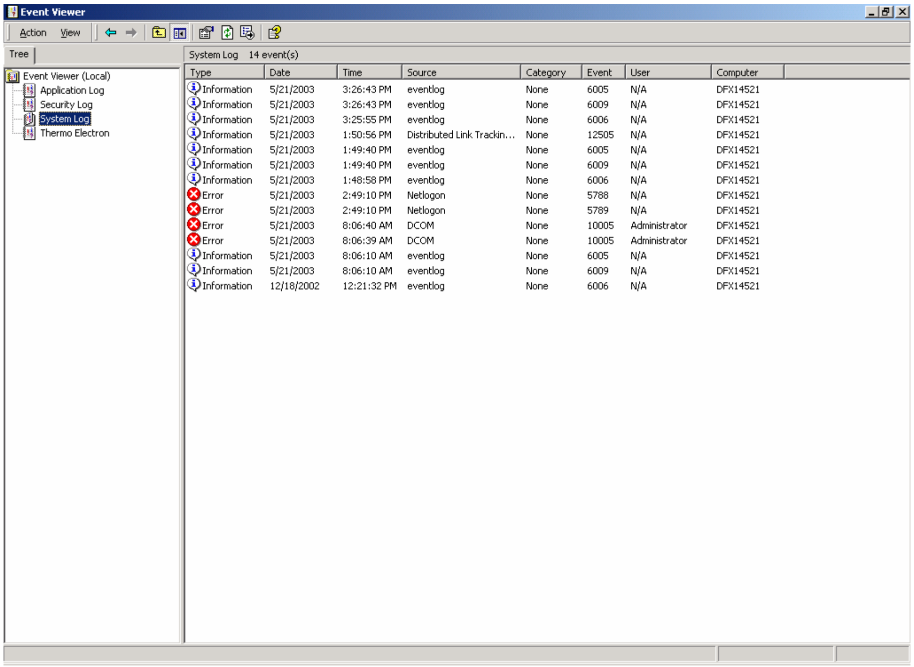
Here is an example in Windows Vista:



Applications and Services Logs

Name	Type	Number of Events	Size
DFS Replication	Administrative	0	68 KB
Hardware Events	Administrative	0	68 KB
Internet Explorer	Administrative	0	68 KB
Key Management Service	Administrative	0	68 KB
Microsoft			
Thermo Electron	Administrative	991	1.00 MB

Here is an example in Windows XP Professional:



System Log 14 event(s)

Type	Date	Time	Source	Category	Event	User	Computer
Information	5/21/2003	3:26:43 PM	eventlog	None	6005	N/A	DFX14521
Information	5/21/2003	3:26:43 PM	eventlog	None	6009	N/A	DFX14521
Information	5/21/2003	3:25:55 PM	eventlog	None	6006	N/A	DFX14521
Information	5/21/2003	1:50:56 PM	Distributed Link Trackin...	None	12505	N/A	DFX14521
Information	5/21/2003	1:49:40 PM	eventlog	None	6005	N/A	DFX14521
Information	5/21/2003	1:49:40 PM	eventlog	None	6009	N/A	DFX14521
Information	5/21/2003	1:48:58 PM	eventlog	None	6006	N/A	DFX14521
Error	5/21/2003	2:49:10 PM	Netlogon	None	5788	N/A	DFX14521
Error	5/21/2003	2:49:10 PM	Netlogon	None	5789	N/A	DFX14521
Error	5/21/2003	8:06:40 AM	DCOM	None	10005	Administrator	DFX14521
Error	5/21/2003	8:06:39 AM	DCOM	None	10005	Administrator	DFX14521
Information	5/21/2003	8:06:10 AM	eventlog	None	6005	N/A	DFX14521
Information	5/21/2003	8:06:10 AM	eventlog	None	6009	N/A	DFX14521
Information	12/18/2002	12:21:32 PM	eventlog	None	6006	N/A	DFX14521

The navigation pane at the left shows the available logs. The first three, described below, are standard Windows logs. The administrator can specify the events to log by using Local Security Policy (available through Administrative Tools in Control Panel) in Windows. Settings for the logs, such as the maximum size of the log and when to overwrite events, can be modified; choose Help from the Action menu for more information.

- The Application Log tracks specific events logged by programs, such as a file error. Program items that appear in this log are controlled by the developer of the application.

- The Security Log tracks security events, such as attempts to log on a local computer or events related to use of resources (for example, creating, opening or deleting files).

- The System Log tracks events logged by the Windows components, such as failure of a driver or other system component to load during startup.

Security Administration adds the Thermo Electron log to Event Viewer. It contains information about events related to your Thermo Scientific client applications that are designed for use with the Security Administration system. Once Security Administration and your client applications have been installed, there are several sources of these logged events:

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

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

Thermo Log Service – Tracks changes to files that are associated with the client applications. This tracking occurs whether or not these applications are running. It will generate events only for file changes that occur on local drives of the computer it is installed on. If you are going to store data to network drives, you will need to install Thermo Log Service on computers that host the network drives you are writing to. See "Installing the Software" for instructions on installing this service.

Note These audit records occur on the computer where Security Administration is installed, not on the computers where Thermo Log Service is installed. ▲

Thermo client application(s) – Tracks activity in the client application (such as OMNIC™) and changes to files while client application is running.

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

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

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

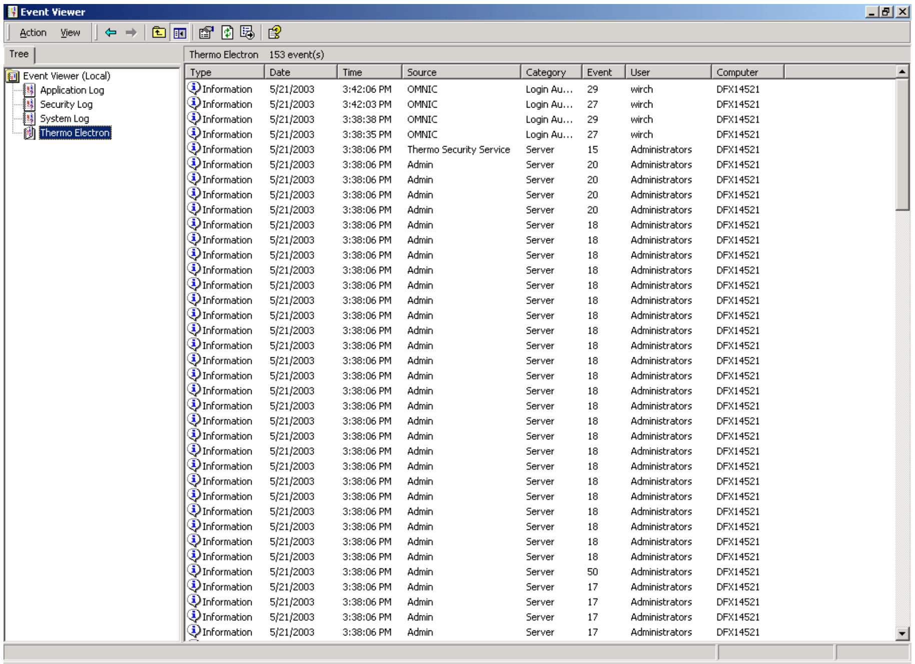
Thermo Log Service
File created
File modified
File deleted
File renamed

Thermo client application(s)
Log on
Log off
Log on failed
File created
File signed
File signing failed
File modified
File deleted
Fail to verify files signature (file tampering)

Note Other specific events may be included for the client applications you use. ▲

2. **Click the Thermo Electron icon.**

   A log of significant events that occurred while your client applications were being used appears in the right pane. Here is an example:



Thermo Electron 153 event(s)

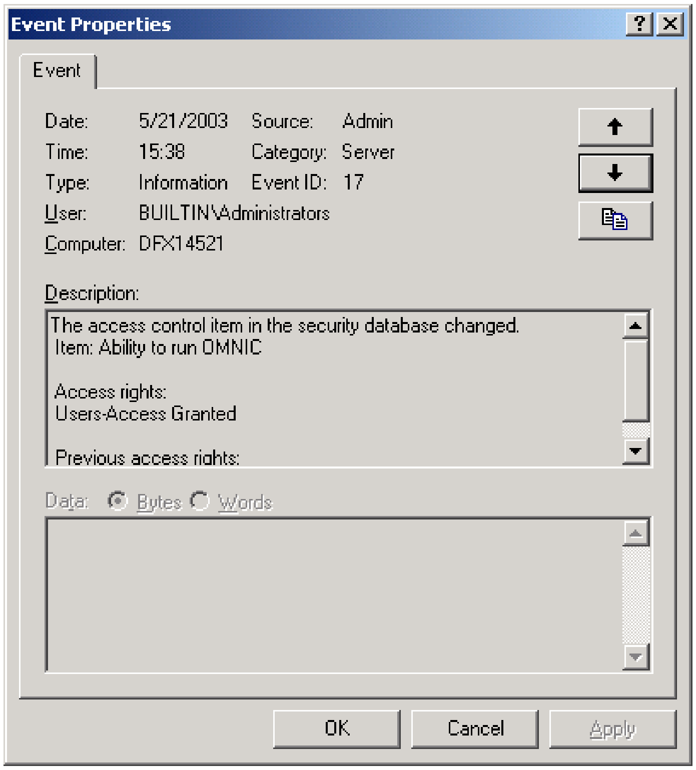
Type	Date	Time	Source	Category	Event	User	Computer
Information	5/21/2003	3:42:06 PM	OMNIC	Login Au...	29	wirch	DFX14521
Information	5/21/2003	3:42:03 PM	OMNIC	Login Au...	27	wirch	DFX14521
Information	5/21/2003	3:38:38 PM	OMNIC	Login Au...	29	wirch	DFX14521
Information	5/21/2003	3:38:35 PM	OMNIC	Login Au...	27	wirch	DFX14521
Information	5/21/2003	3:38:06 PM	Thermo Security Service	Server	15	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	20	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	20	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	20	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	20	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	18	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	50	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	17	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	17	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	17	Administrators	DFX14521
Information	5/21/2003	3:38:06 PM	Admin	Server	17	Administrators	DFX14521

   You can sort the events according to date, category, user and so on by clicking the column headings.

3. **To see detailed information about an event, select it and then choose Properties from the Action menu.**

   You can also just double-click the event.

The Event Properties dialog box appears. Here is an example:



Date: 5/21/2003 Source: Admin
Time: 15:38 Category: Server
Type: Information Event ID: 17
User: BUILTIN\Administrators
Computer: DFX14521

Description:

The access control item in the security database changed.
Item: Ability to run OMNIC

Access rights:
Users-Access Granted

Previous access rights:

If the event was the signing of a file, the signature meaning appears in the dialog box.

To see information about the preceding event in the list, click the up arrow button. To see information about the next event in the list, click the down arrow button.

You can export the list of events by choosing Export List from the Action menu. In the Save As dialog box that appears, specify where to save the list and the type of file to use. Then choose Save to save the list. You can use a word processing program or other program to open the saved file and print the list or work with it in other ways.

4. When you are finished using Event Viewer, close it by clicking the Close button (labeled “X”) in the upper-right corner of the window.

Local and global user groups and rights

The administrator can set up local or global user groups to manage users more efficiently. A local group is a group of users associated with a particular workstation. A global group is a group of users associated with a network domain, which can include more than one workstation. Local groups can contain global groups from a network domain. Rights and permissions can be assigned to a local group, and users or global groups can be added and deleted from the local group.

In Windows Vista, set up local and global groups by creating users and groups by using Computer Management available through Administrative Tools. In Windows XP Professional, use New Group in the Action menu in the Local Users And Groups in Computer Management.

Rights and privileges can then be assigned or unassigned to those groups by using Local Security Policy (available through Administrative Tools in Control Panel). Some of the rights that can be assigned or removed include:

- The right to access the workstation from a network. This right must be granted to every user of the client application.
- The right to change the system date and time.
- The right to log on to the system locally.
- The right to shut down the system.
- The right to take ownership of files or other objects.
- The right to manage the event viewer.

Note Restricting the right to change the system date and time is an important security feature. If this right is removed from a user group, the users in that group cannot collect data under a falsified date and time. ▲

User profiles

The administrator can assign users mandatory profiles that control the users' desktop settings and prohibit users from permanently changing their desktop settings. In Windows Vista, the administrator can assign profiles by using Local Security Policy to manage policies on the PC for desktop settings and restrict software use if desired. In Windows XP Professional, use Local Users And Groups in Computer Management.

Other security features

If the workstation will be connected to a network with Windows Server, or if Windows Server client-based administration tools are installed on the workstation, the administrator can take the following additional security features into consideration:

- Allowing users to have access to the network or workstation only during specified hours.
- Restricting users from logging on or allowing users to log on to specific workstations on a network.
- Specifying user account expiration dates.

Complying with 21 CFR Part 11

Security Administration integrates with many of the security and auditing features of Windows to support the requirements of 21 CFR Part 11. To comply with that regulation, you must ensure that several Windows features are properly configured:

- Each user of Security Administration or a client application requires a user account. The user's full name and password must be associated with the account. A user description may be associated with the account.
- Review the group membership of each user account as well as the rights or privileges associated with each account and group.
- Review the account policy (password restrictions, account lockout behavior, etc.) to assess the suitability of the policy for compliance with 21 CFR Part 11 and for conformity with your own organization's standards and procedures.

- Review the access control settings for those locations where users will be permitted to save, modify or delete files.

- If users from multiple domains need to be able to access a client application, and the access rights for these users is managed centrally in a single security database, there must be a mutual (bidirectional) trust relationship between the domain where Security Administration is installed and each of the domains that have user accounts and groups managed by Security Administration.

- Configure the regional settings on every client computer so that the time format is HH:mm:ss. The upper-case “H” denotes that the 24 hour clock will be used.

Setting Up Windows Administration

Setting up Windows administration is necessary before you can install and use Security Administration. The sections in this chapter take you through the steps of setting up Windows software on network computers as well as stand-alone computers.

Windows administration for network computers

Follow the instructions in this section if your computer is connected to a network. If your computer is not connected to a network, read the "Windows administration for stand-alone computers" section.

You must use the procedure in this section before you use Security Administration for the first time. You will not be able to start a client application if you have not performed these steps. These procedures set up the administrative features of your Windows 2003 Server software for Security Administration. You must be a member of the Windows Administrators group to perform this procedure. Use this procedure even if you plan to install Security Administration on one or more computers that are running Windows Vista or Windows XP Professional and that are part of a network administered using Windows 2003 Server.

Note You can use a Windows NT network, but the computers on which the client application and Security Administration are installed must be running Windows Vista or Windows XP Professional. The information that follows is for Windows 2003 Server. ▲

Note You can use Security Administration to administer a client application running on two or more computers in a peer-to-peer workgroup. This eliminates the need to buy a server version of Windows; however, you need to set up user accounts on each computer in the workgroup, not just on a server. Each user must have the same user name and password on each computer in the workgroup. The "Windows administration for stand-alone computers" section later in this chapter contains instructions for creating groups and adding users to them. Use the section that applies to your version of Windows. ▲

Typically organizations set up different levels of access and control for categories (groups) of users of their client applications. The groups described below are an example of this. The groups you use may have different names.

- Users in the **Administrators** group will be able to use all the features in the client applications as well as those in Security Administration. Typically these users are system administrators or laboratory managers.

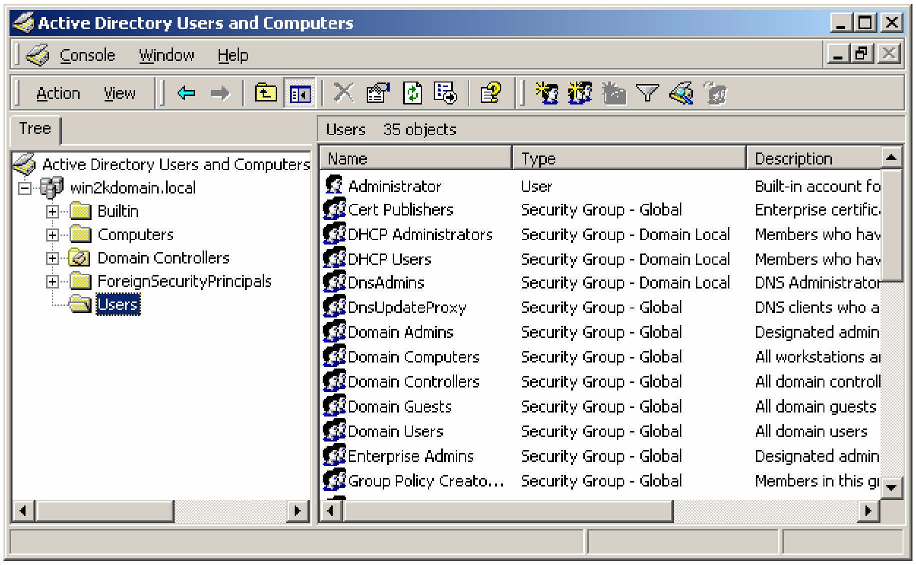
Note The Administrators group was created automatically when you installed Windows. You can use this group or create a new, differently named group of administrators to isolate administration of Security Administration and your client applications from the rest of the system administration. ▲

- Users in the **Scientists** group will be able to use all the features in the client applications but will not be able to use Security Administration.

- Users in the **Technicians** group will be able to use only specified features in the client applications and will not be able to use Security Administration.

You can create the groups you need and then add the appropriate users to them. To see which users and groups exist, use the Administrator tools provided with Windows.

Here is an example from viewing the Active Directory Users And Computers window:


Active Directory Users and Computers
Console Window Help
Action View
Tree
Active Directory Users and Computers
win2kdomain.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users

Users 35 objects

Name	Type	Description
Administrator	User	Built-in account fo
Cert Publishers	Security Group - Global	Enterprise certific.
DHCP Administrators	Security Group - Domain Local	Members who hav
DHCP Users	Security Group - Domain Local	Members who hav
DnsAdmins	Security Group - Domain Local	DNS Administrator
DnsUpdateProxy	Security Group - Global	DNS clients who a
Domain Admins	Security Group - Global	Designated admin
Domain Computers	Security Group - Global	All workstations ar
Domain Controllers	Security Group - Global	All domain controll
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Global	Designated admin
Group Policy Creato…	Security Group - Global	Members in this g

When you are setting up new users, we recommend selecting User Must Change Password At Next Logon. However, your company's policies may require you to set the options in this dialog box differently from what is shown in the illustration above.

Note Later, after you have used Security Administration to specify access control and signature permissions for your user groups, adding a new user to a group will automatically set these rights for that user. There is no need to use Security Administration to set these rights for users individually. (You will still need to set system policies for individual users.) ▲

Windows administration for stand-alone computers

Follow the instructions in this section if your computer is not connected to a network. If your computer is connected to a network, read the "Windows administration for network computers" section.

You must use the appropriate procedure in the following sections before you use Security Administration for the first time. You will not be able to start a client application if you have not performed these steps. This procedure sets up the administrative features of your Windows Vista or Windows XP Professional software for Security Administration. You must be a member of the Windows Administrators group to perform this procedure.

Note You can use Security Administration to administer a client application running on two or more computers in a peer-to-peer workgroup. This eliminates the need to buy a server version of Windows; however, you need to set up user accounts on each computer in the workgroup, not just on a server. Each user must have the same user name and password on each computer in the workgroup. The following sections contain instructions for creating groups and adding users to them. Use the section that applies to your version of Windows. ▲

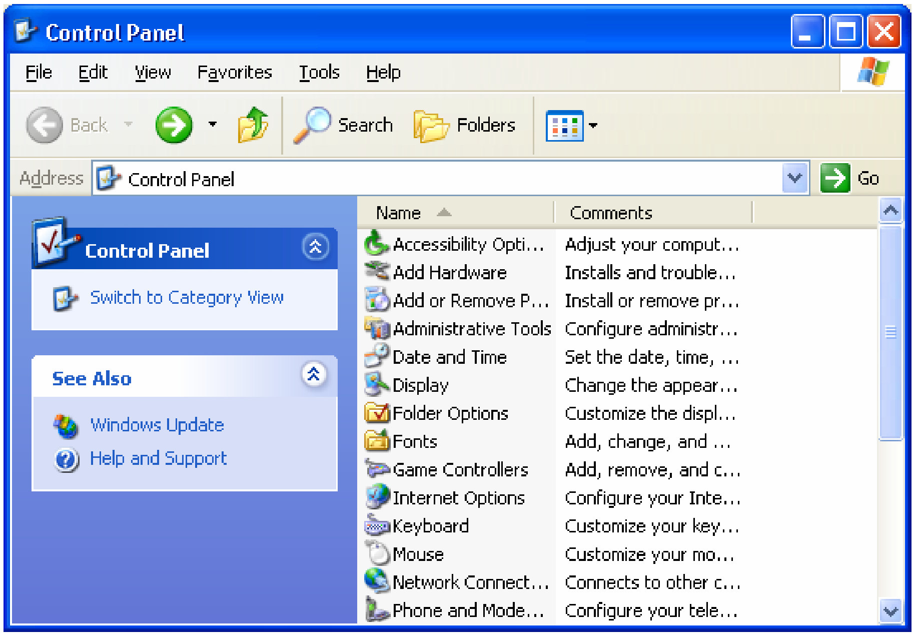
Setting up Windows Vista or Windows XP Professional administration for a stand-alone computer

Follow these steps to set up Windows Vista or Windows XP Professional administration for a stand-alone computer:

1. **Start Control Panel.**

2. **Choose Switch To Classic View if it appears near the left side of Control Panel.**

   If you don’t see this feature, you are already using the classic view of Control Panel, shown below.



Name	Comments
Accessibility Opti...	Adjust your comput...
Add Hardware	Installs and trouble...
Add or Remove P...	Install or remove pr...
Administrative Tools	Configure administr...
Date and Time	Set the date, time, ...
Display	Change the appear...
Folder Options	Customize the displ...
Fonts	Add, change, and ...
Game Controllers	Add, remove, and c...
Internet Options	Configure your Inte...
Keyboard	Customize your key...
Mouse	Customize your mo...
Network Connect...	Connects to other c...
Phone and Mode...	Configure your tele...

3. **If you are using Windows XP Professional, double-click User Accounts. If you are using Windows Vista, skip to step 8.**

Note The purpose of steps 3 to 7 is to ensure that the user must log on if using Windows XP Professional. If User Accounts is not present, the computer is already set up to require logging on; skip steps 3 through 7. ▲

   You may need to scroll to locate this item.

   The User Accounts window appears.

4. **Click the Change The Way Users Log On Or Off item.**

   The Select Logon And Logoff Options features appear.

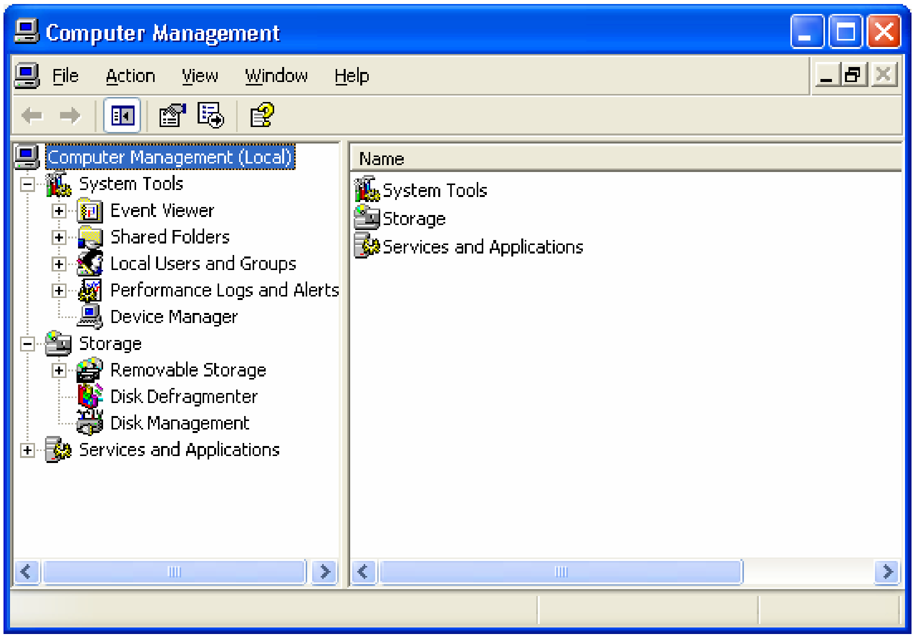
5. **Turn off Use The Welcome Screen.**

   If this item is already unchecked, skip to the next step.

6. **Click the Apply Options button.**

7. **Close the User Accounts window.**

8. **Create new users and groups as needed with the Administrative Tools and Computer Management options provided by Windows.**



You can find additional information in the Help Topics included with Windows. See these topics:

> “Create a new local group”
> “Create a new user account”

Typically organizations set up different levels of access and control for categories (groups) of users of their client applications.

Note The Administrators group was created automatically when you installed Windows. You can use this group or create a new, differently named group of administrators to isolate administration of Security Administration and your client applications from the rest of the system administration. ▲

Users in the **Administrators** group will be able to use all the features in the client applications as well as those in Security Administration. Typically these users are system administrators or laboratory managers.

The groups described below are examples of custom groups created to establish different levels of access and control in a typical laboratory. The groups you use may have different names.

- Users in the **Scientists** group will be able to use all the features in the client applications but will not be able to use Security Administration.

- Users in the **Technicians** group will be able to use only specified features in the client applications and will not be able to use Security Administration.

You can create the groups you need and then add the appropriate users to them.

To see which users and groups exist, open the Local Users And Groups folder and then the respective folders.

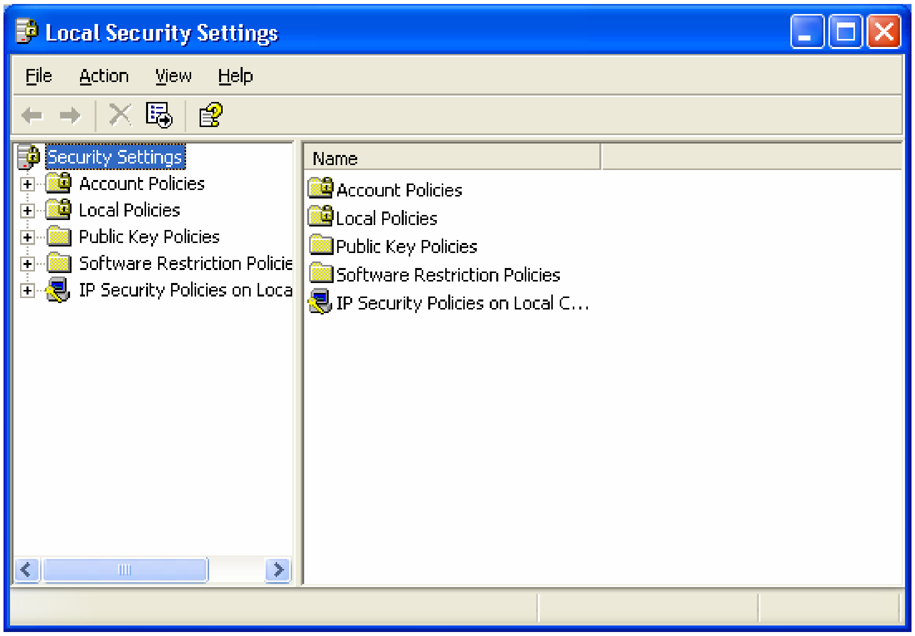
Note When adding users to a group, *make sure both Built-In Security Principles and Users are selected.* ▲

Setting the local security policy

Follow these steps to set the local security policy for a stand-alone computer:

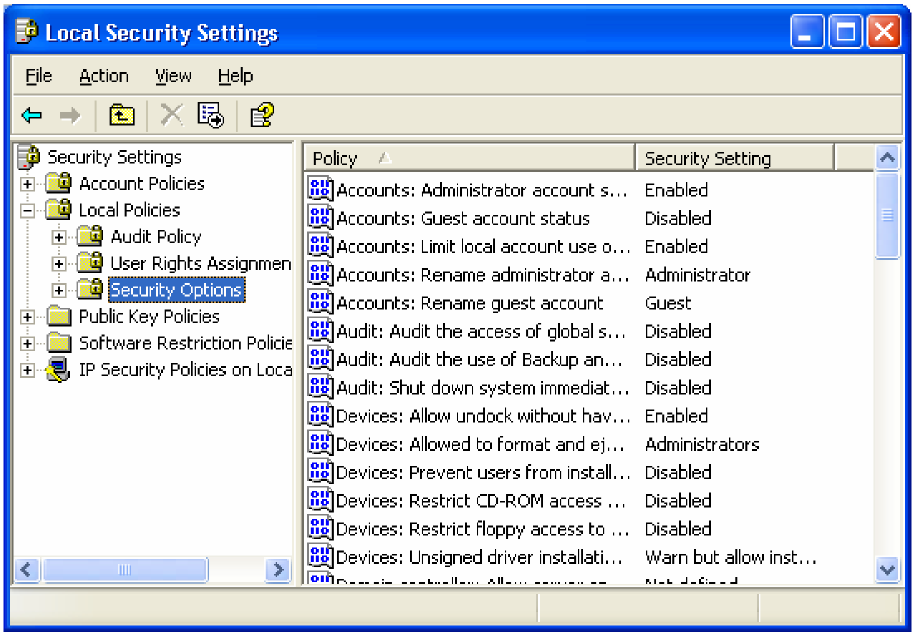
1. **Double-click Local Security Policy in the Administrative Tools window.**

   A dialog box appears (Local Security Policy in Windows Vista; Local Security Settings in Windows XP).



2. **Open the Local Policies folder and then open the Security Options folder.**

   The local policies are listed in the right pane:



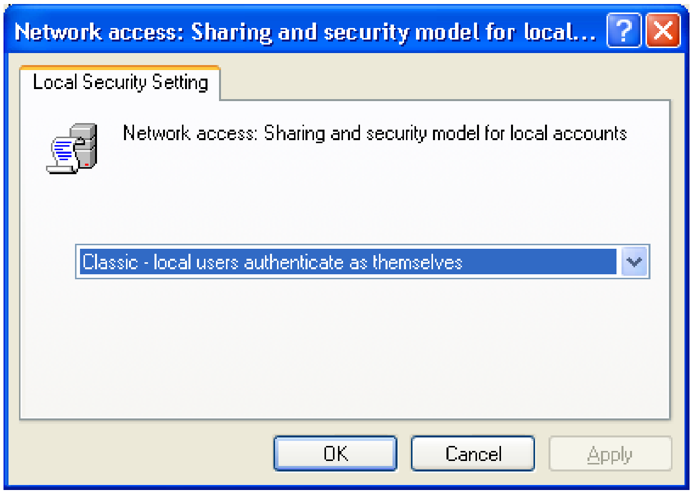
- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignmen
    - Security Options
  - Public Key Policies
  - Software Restriction Policie
  - IP Security Policies on Loca

Policy	Security Setting
Accounts: Administrator account s…	Enabled
Accounts: Guest account status	Disabled
Accounts: Limit local account use o…	Enabled
Accounts: Rename administrator a…	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global s…	Disabled
Audit: Audit the use of Backup an…	Disabled
Audit: Shut down system immediat…	Disabled
Devices: Allow undock without hav…	Enabled
Devices: Allowed to format and ej…	Administrators
Devices: Prevent users from install…	Disabled
Devices: Restrict CD-ROM access …	Disabled
Devices: Restrict floppy access to …	Disabled
Devices: Unsigned driver installati…	Warn but allow inst…

3. **Double-click Network Access: Sharing And Security Model For Local Accounts in the list of policies.**

   You may need to scroll to locate this item.

   The Network Access dialog box appears:



Network access: Sharing and security model for local accounts

Classic - local users authenticate as themselves

4. **Select Classic - Local Users Authenticate As Themselves from the drop-down list box and then choose OK.**

5. **Click the Close button (labeled “X”) to close the Local Security Settings dialog box.**

6. **Click the Close button (labeled “X”) to close the Administrative Tools window.**

   You can now install Security Administration and your client application as explained in the “Installing the Software” chapter. After the software is installed, follow the instructions in the “Setting Up Client Application Accounts” chapter to set up the user accounts for the application.

Setting Service Accounts

After you have set up Windows administration for a network as explained in the “Setting Up Windows Administration” chapter, you can set your service accounts to ensure that they are not running as local system accounts. (You may wish to set these accounts on a stand-alone computer as well.) There are several reasons to do this:

- To reduce the access privileges of the services so that they present less of a security risk, as recommended by Microsoft Corporation.

- To give access to an event log on a server computer running Security Administration.

- To give access to a shared network location for saving data.

Your client application uses two services to implement security features. The Thermo Log Service watches for changes to files with relevant extensions and generates event log records for these changes. The event log records are written to the event log of the computer where Security Administration is running. When it is installed, this service is set to run under the Local System account, which is appropriate for situations where Security Administration is running on the same computer as the client application. If Security Administration is running on a different computer, the Local System account on the client computer will not have permission to write to the event log of that computer. To remedy this, you need to set the account that the Thermo Log Service runs under to any account that is known to the computer running the Security Administration server.

The Thermo File Service acts as an agent for Security Administration to move files to protected areas of storage where the logged-on client-application user does not have permission to modify files. The client application uses this service to place files in these protected areas so they cannot be tampered with, renamed or deleted by restricted users. The Thermo File Service can write files only to locations where it has been given access. When it is installed, this service is run under the Local System account, which can be given access to any local directory through the Local Administrators group. If you want files able to be moved to a network drive, you must run the Thermo File Service under an account that has permission to write to the network drive.

Note that the Thermo Log Service and the Thermo File Service must run under the same account. An error will occur when you start the second service if you set the services to run under different accounts. The general solution is to set both services to an account that is known to the computer running the Security Administration server (for the Thermo Log Service) and also has permission to write to the network drive where the Thermo File Service will be sending files.

Follow these steps to ensure that your service accounts are not running as local system accounts:

1. **Click the Start button on the Windows taskbar and then choose Control Panel.**

2. **Double-click Administrative Tools.**

3. **Double-click Computer Management.**

4. **Open the Services And Applications item in the tree.**

5. **Click the Services item in the tree.**

6. **Double-click Thermo File Service in the Name column.**

7. **Click the Log On tab.**

8. **Select This Account.**

9. **Enter information for the account you want to use.**

10. **Choose OK.**

11. **Repeat steps 6 through 10 for Thermo Log Service.**

12. **Close the Computer Management window.**

13. **Close the Administrative Tools window.**

14. **Close the Control Panel window.**

Installing the Software

Security Administration must be installed on a disk or partition that is formatted with the NTFS file system. Only this file system is capable of using security attributes on files, an essential capability for protecting your security database and user files from unauthorized access.

Follow the steps below to install Security Administration after you have set up Windows administration as explained in the “Setting Up Windows Administration” chapter.

1. **Start Windows if it is not already running, and log on as the administrator.**

2. **Install Security Administration.**

   To do this, insert the Thermo Security Administration CD into the CD drive of the computer that will be used to administer the client application. The installation starts automatically. (If your system is not set to start CDs automatically, double-click the setup.exe file on the root of the CD to start the installation.) Follow the instructions that appear on the screen.

   During the installation you are allowed to change the location where files will be installed. If you do this, always use the same location each time you install the software so that files are upgraded correctly when subsequent versions are installed. Typically the default locations are used for installation, although you may wish to change the drive letter to install the software on the desired drive.

   During the installation you are asked whether to install the program for anyone who uses the computer or only for the administrator. Normally the program should be installed only for the administrator.

3. **Install the client application if needed.**

   This step is necessary for using the client application on a stand-alone computer (a computer not connected to a network).

   See the documentation that came with the application for instructions. Typically you insert the CD that contains your client application into the CD drive and then follow the instructions that appear on the screen. Install the application on each computer where you will plan to run it.

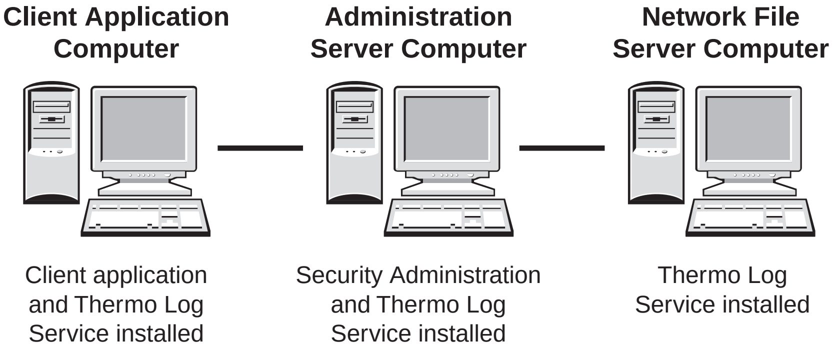
4. **Install Thermo Log Service on file servers that host network drives used by your application.**

   This service makes it possible to keep a record of when files are created, modified, renamed or deleted—even when the client application is not running.

   To install this service, load the Security Administration CD into the computer you are using as a file server. If the installation of the Security Administration program starts automatically, cancel that installation. Use Explorer to browse to the AuditChangesToFileSystem.msi file, located on the root of the CD, and double-click the file. This will launch the Thermo Log Service installer.

   As part of the installation process, a dialog box will let you specify where the Security Administration Server program is installed. You can manually type the name of the computer running the Security Server or use the search feature to locate the server. When the server is located and the installer finishes, the Thermo Log Service will watch for changes on the file server and write event records to the event log located on the computer running the Security Administration Server. This coalesces all change event records in one event log.

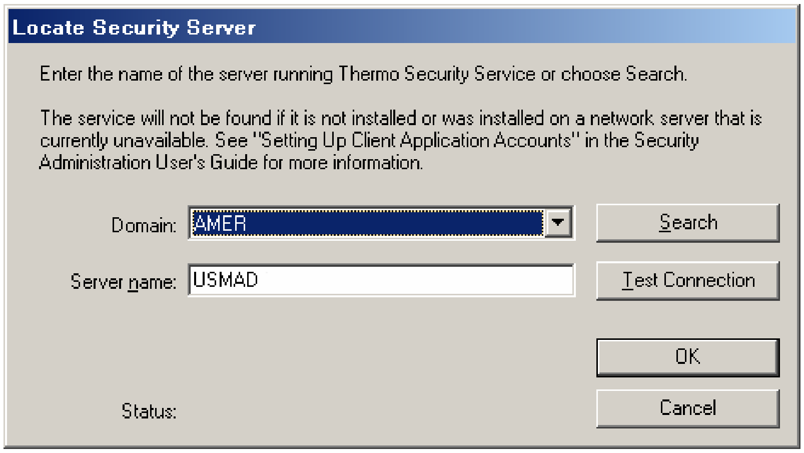
The AuditChangesToFileSystem.msi installer can be installed on as many file servers as needed to record events for all network drives being used by your application. The example below shows where software is installed on computers in a typical single-domain configuration. (Many other configurations are possible.)


Client Application Computer
Administration Server Computer
Network File Server Computer
Client application and Thermo Log Service installed
Security Administration and Thermo Log Service installed
Thermo Log Service installed

In this example, the administration server computer contains the audit trail for all files that are created, modified, renamed or deleted on any of the three computers. It is also the computer where access rights, system policies and signature reasons for users can be modified.

5. **Restart the computer.**

Note The first time you log onto a computer with a client application whose security is controlled by Security Administration, you are asked to specify the server where Security Administration (which includes Thermo Security Service) is installed. Here is an example:



Locate Security Server

Enter the name of the server running Thermo Security Service or choose Search.

The service will not be found if it is not installed or was installed on a network server that is currently unavailable. See "Setting Up Client Application Accounts" in the Security Administration User's Guide for more information.

Domain: AMER

Server name: USMAD

Status:

Type the name in the Server Name text box and choose OK, or use the Search button to locate the server. To search a different domain, first select the desired domain from the Domain drop-down list box. When you choose Search, the software searches first on the local computer and then on any other computers in the domain. Depending on the size and speed of the network, searching for the server may take several minutes to several hours. (For example, a network of all users at facilities located in multiple countries may require a search of many thousands of computers.) When a copy of Thermo Security Service is found, its location appears in the Server Name text box. After you use the Search button, its name changes to Resume Search. You can then click the button to find another location of Thermo Security Service, if one exists. Once the desired location is shown in the Server Name text box, you can choose Test Connection to verify that communication with Thermo Security Service is established. Choose OK when you are finished. ▲

After the computer has restarted, you can log on as the administrator and start Security Administration by double-clicking the Security Administration shortcut on the Windows desktop.

For every client application that will be controlled by Security Administration, you need to use Add Application in the File menu to add the application's .XML file to the security database. This is explained in the procedure in the next chapter, which also explains how to set up your client application accounts. If you are going to perform software installation qualification (IQ), follow the software IQ instructions in the documentation that came with the client application before using the next chapter.

Setting Up Client Application Accounts

After you have installed Security Administration and your client application and performed installation qualification (if needed), follow the steps below to set up the user accounts for the application. Then set file permissions to control which Windows file operations—such as overwriting a file—can be performed by specified users. See the manual that came with your client application for detailed instructions.

Follow these steps to set up user accounts:

1. **Place the client application installation CD into the CD-ROM drive if it is not already in the drive.**

Note If the client software's installation program starts automatically when you insert the CD, exit that installer. ▲

2. **Start Security Administration by double-clicking the Security Administration shortcut on the Windows desktop.**

   The Security Administration window appears. The features of this window are explained in detail in the "Using Security Administration" chapter.

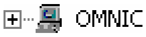
3. **If you have not already added the client application, choose Add Application from the File menu. If you have already added the application, go to step 5.**

   The Add Application dialog box appears.

4. **Browse to the CD drive, select the client application's .XML file (on the root of the CD) and choose Open.**

   For example, OMNIC's file is named OMNIC.XML.

An icon representing the application appears in the navigation pane. Here is an example:

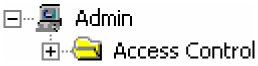


OMNIC

Note The example icons and other security items shown in this manual may be different from those for your client application. See the manual that came with your application for specific instructions. ▲

5. **Click the plus sign to the left of the Admin icon.**

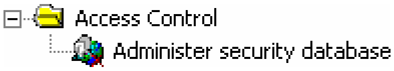
   The Access Control folder appears:



Admin
Access Control

6. **Click the plus sign to the left of the Access Control folder.**

   The Administer Security Database icon appears.



Access Control
Administer security database

7. **Click the Administer Security Database icon.**

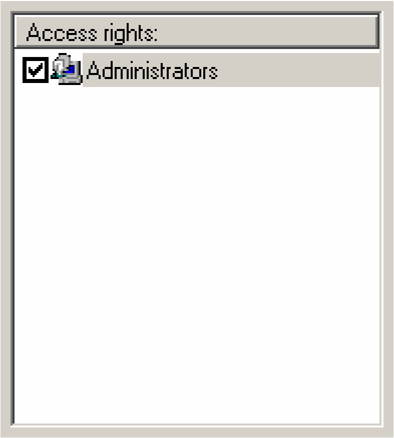
   A list of access rights appears in the right pane. You can use features in the pane to specify the users who will be able to use Security Administration.

   If the Administrators group is in the Access Rights box and is checked, go to step 10. If it is not, follow steps 8 and 9 to add the group and check it. This grants access rights to run Security Administration to users in the Administrators group.

8. **Select Administrators in the Names list.**

9. **Click the Add button.**

   The Administrators group appears in the Access Rights box.



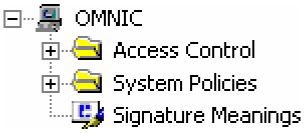
Access rights:

☑ Administrators

   The check mark indicates that members of the group can use the Security Administration software.

10. **Click the plus sign to the left of the client application icon, and then use the displayed features to set the security policies for the application.**

    Here is an example showing the three kinds of security policies that you can set:



```
⊟ OMNIC
   ⊞ Access Control
   ⊞ System Policies
     Signature Meanings
```

    Access Control lets you set the rights of users to use protected functions in the application. By default, every user has access to every feature in the client application. You must restrict access as needed to achieve the desired control over which users can use specific features. See “Controlling access to client application features” in the “Using Security Administration” chapter for general instructions. Then see the manual that came with the client application for more specific instructions for controlling access to its functions.

System Policies lets you set policies covering such things as preventing the overwriting of files and requiring electronic signatures. See “Setting system policies for the client application” in the “Using Security Administration” chapter for general instructions. Then see the manual that came with the client application for more specific instructions for setting its system policies.

Signature Meanings lets you specify the meanings that will be available for electronic signatures supplied by users of the application. The available signature meanings vary depending on the client application. See “Assigning signature meanings” in the “Using Security Administration” chapter for general instructions. Then see the manual that came with the client application for more specific instructions for specifying which signature meanings will be available.

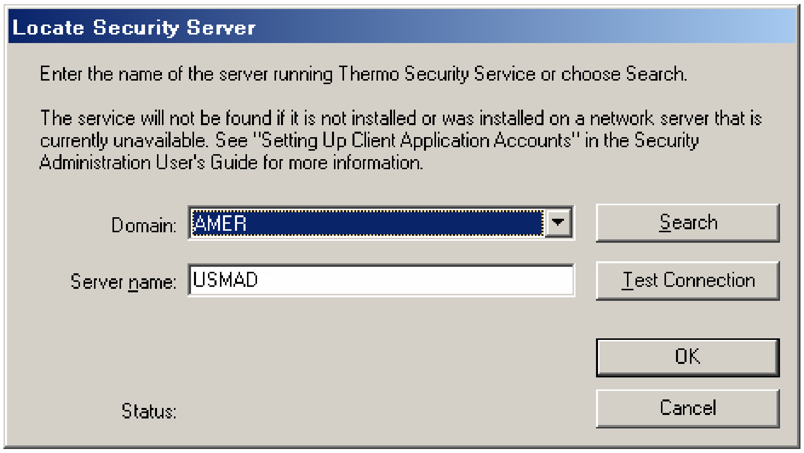
11. **Choose Save Settings from the File menu.**

    This saves the changes you made to the client application accounts. See “Saving your security policy settings” in the “Using Security Administration” chapter if you need help.

12. **Choose Exit from the File menu.**

    You are now ready to set file permissions as explained in the manual that came with your client application.

Note The first time you log onto a computer with a client application whose security is controlled by Security Administration, you are asked to specify the server where Thermo Security Service is installed. Here is an example:



Locate Security Server

Enter the name of the server running Thermo Security Service or choose Search.

The service will not be found if it is not installed or was installed on a network server that is currently unavailable. See "Setting Up Client Application Accounts" in the Security Administration User's Guide for more information.

Domain: AMER

Server name: USMAD

Status:

Type the name in the Server Name text box and choose OK, or use the Search button to locate the server. To search a different domain, first select the desired domain from the Domain drop-down list box. When you choose Search, the software searches first on the local computer and then on any other computers in the domain. Depending on the size and speed of the network, searching for the server may take several minutes to several hours. (For example, a network of all users at facilities located in multiple countries may require a search of many thousands of computers.) When a copy of Thermo Security Service is found, its location appears in the Server Name text box. After you use the Search button, its name changes to Resume Search. You can then click the button to find another location of Thermo Security Service, if one exists. Once the desired location is shown in the Server Name text box, you can choose Test Connection to verify that communication with Thermo Security Service is established. Choose OK when you are finished. ▲

Using Security Administration

To start Security Administration, double-click the Security Administration shortcut on the Windows desktop.

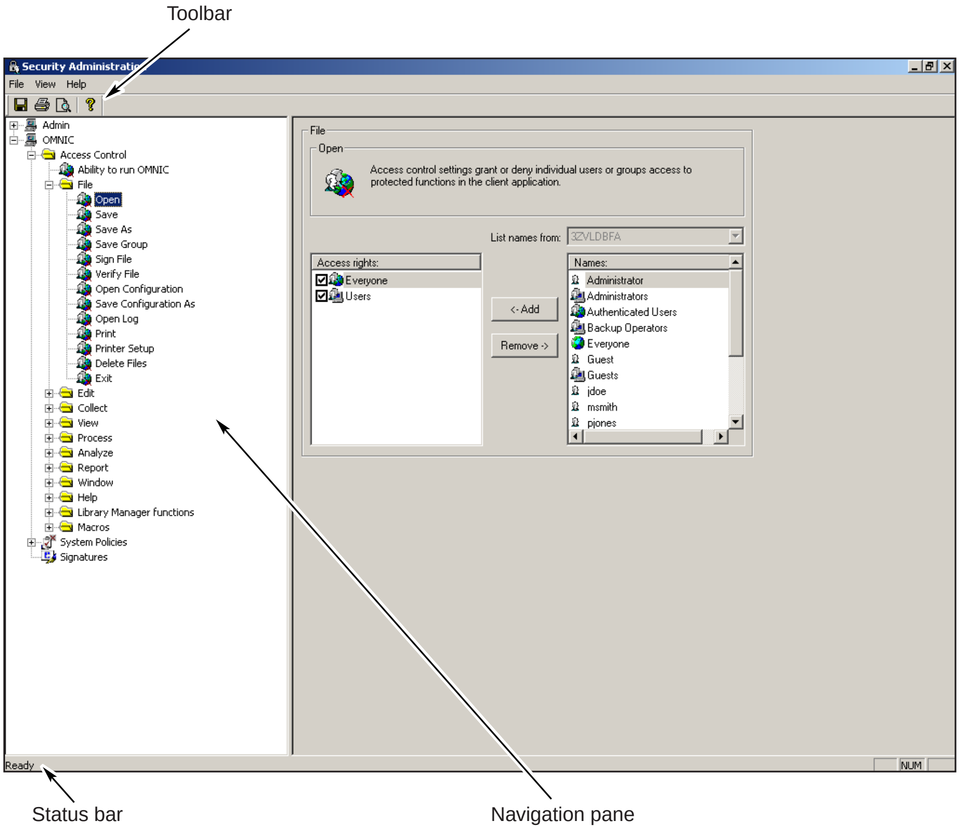
Alternatively, you can click the Start button on the Windows taskbar, point to All Programs, click the Thermo folder, and then click the Security Administration program.

Note If you have just installed a new version of a client application that has new features controlled by Security Administration, use Add Application in the File menu to add the new version's .XML file. This merges the new features into the existing settings you have specified for the application. Typically the .XML file is in the root directory of the client application installation CD. See "Adding a client application" for more information. ▲

The next section explains the features contained in the Security Administration window.

About the display

When you start Security Administration, the Security Administration window appears. Here is an example of the window showing some features for setting security policies for an added client application:



Access control settings grant or deny individual users or groups access to protected functions in the client application.

List names from: 3ZVLDBFA

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

Displaying the toolbar

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

You may find it convenient to choose a command by clicking its toolbar button instead of choosing the command from a menu. To see the name of the command associated with a button or a description of its function, point to the button and wait for the name to appear.

Follow these instructions to display the toolbar:

Choose Toolbar from the View menu. The toolbar appears below the menu bar, and a check mark appears to the left of the command name. To remove the toolbar from the display, choose Toolbar from the View menu when the check mark is present.

Displaying the status bar

Use Status Bar in the View menu to display a status bar showing information such as the purpose of the currently highlighted menu command. Follow these instructions:

Choose Status Bar from the View menu. The status bar appears below the navigation pane, and a check mark appears to the left of the command name. To remove the status bar from the display, choose Status Bar from the View menu when the check mark is present.

Using the keyboard to select items in the navigation pane

Use Status Bar in the View menu to display a status bar showing information such as the purpose of the currently highlighted menu command. Follow these instructions:

If you have selected a security feature for a client application in the navigation pane (for example, a system policy), you can use Select Previous in the View menu to select the previous item in the tree (if there is one). Normally you would do this by using the command's keyboard shortcut: hold down the Ctrl key and press the up arrow key. Similarly, you can use Select Next in the View menu to select the next item in the tree. To use this command's keyboard shortcut, hold down the Ctrl key and press the down arrow key.

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

Displaying Help information

Security Administration provides both general and context-sensitive Help information for its features and those of client applications. (See “Adding a client application” for details about adding a client application to the navigation pane.) The next sections explain how to display this information.

Note Since Security Administration and client applications have separate Help systems, displayed in their own windows, you will find information for only one program within a particular Help system. ▲

When you are finished viewing Help information, close the Help system by clicking the Exit button (if available) or the Close button (labeled “X”) in the upper-right corner of the Help window.

Help for Security Administration

To find information about using Security Administration, choose Security Administration Help Topics from the Help menu. The Help window that appears includes Contents, Index and Search tabs containing standard Windows features for finding information.

Help for client applications

To display Help information for a particular feature in the navigation pane, select the feature and then click the Help button in the toolbar:

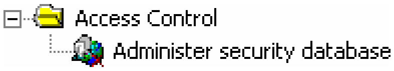
?

The Help system that appears depends on which program contains the selected feature.

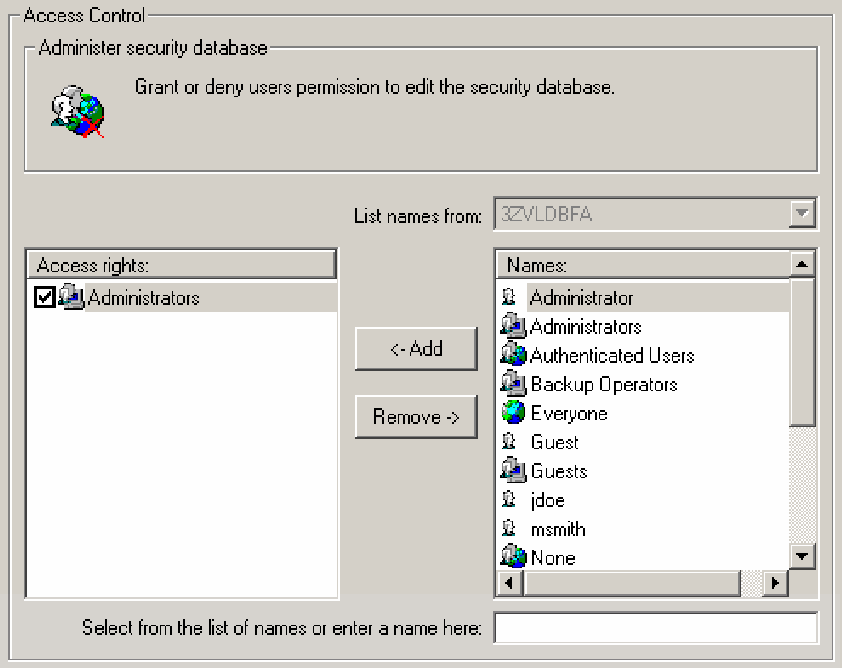
Note This capability may not be available for some client applications. ▲

Controlling access to Security Administration

Setting up security for your system must include controlling who can run Security Administration. When you open the Admin icon in the navigation pane, the Access Control folder appears. When you open it, the Administer Security Database icon appears:



When you click the Administer Security Database icon, a list of access rights and other features appear in the right pane. Here is an example:



Access Control

Administer security database

Grant or deny users permission to edit the security database.

List names from: 3ZVLDBFA

Access rights:

☑ Administrators

Names:

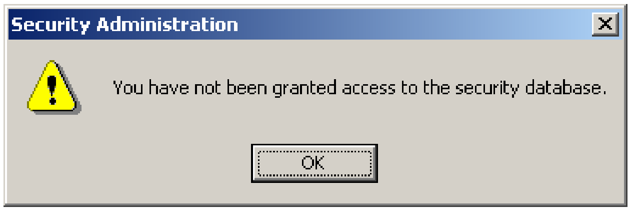
Administrator
Administrators
Authenticated Users
Backup Operators
Everyone
Guest
Guests
jdoe
msmith
None

Select from the list of names or enter a name here:

You can use features in the right pane to specify which users can start Security Administration.

If the computer is connected to one or more networks, selecting a network or the local computer from the List Names From drop-down list box lists the users and groups on that network or computer in the Names box. This lets you control access to Security Administration for the users and groups on the networks and computer. If the computer is not connected to a network, the List Names From drop-down list box is not available, and the users and groups on the computer are listed in the Names box.

The users and groups on the selected network or computer for whom access to the software has been specified appear in alphabetical order in the Access Rights box. If a check mark appears to the left of a name, that user or group can start the software. If no check mark appears, that user or group is denied the right to start the software. If a user without access attempts to start the software, the following message appears:



Security Administration

You have not been granted access to the security database.

If you click a check box to remove its check mark, denying a user or group access to start the software, this denial takes priority over any other settings that grant the user or group access. To prevent confusion, you should generally deny access only for individual users and not for groups. Typically, access is granted to a group and then denied to particular members of the group.

Important *If a user is a member of two groups with different access control specifications, the more restrictive specification takes priority for that user.* To simplify specifying access control, we recommend that you assign a user to only one group you have created. Also, keep in mind that all users are automatically members of the Users group, so checking an individual user in the Access Rights box and then unchecking the Users group does *not* grant access to that user. Instead, it denies access to all users, and since all individuals are also users, no one has access. In general, *avoid unchecking the Users group* or most other groups; it is usually better to check a group and then uncheck individual users in the group to deny them access. ▲

To specify access for a user or group not listed in the Access Rights box, select it in the Names box or type it in the text box below the list, and then choose Add.

If you type the name, use the following syntax:

```
<domainname>\<accountname>
```

where “domainname” is the name of the domain location of the user or group, and “accountname” is the account name of the user or group. The user or group is added to the list in the Access Rights box, with access granted by default. You can then change the access specification.

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

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

To fully control access to Security Administration, be sure to specify access as explained above for the all users and groups on the local computer and all the networks available in the List Names From drop-down list box.

When you are finished, save your settings in the security database. See “Saving your security policy settings” for details.

Adding a client application

Use Add Application in the File menu to add a client application to the navigation pane. You can then set security policies for the application.

If you have just installed a new version of a client application that has new features controlled by Security Administration, be sure to use Add Application to add the new version’s .XML file. Typically the file is in the root directory of the client application installation CD. This merges the new features into the security database and preserves all of your existing settings.

Follow these steps to add a client application:

1. **Choose Add Application from the File menu.**

   The Open dialog box appears.

2. **Locate and select the client application file you want to open.**

   Typically the application file is in the root of the client application installation CD.

Note Some .XML files are available in different languages. The language is indicated by its standard Windows abbreviation included in the file name. For example, OMNIC_DEU.XML is the German version of the OMNIC.XML file. Use these language versions of the .XML files if you want the Access Control and System Policies settings displayed in a language other than English. If the English .XML file has been loaded, you can switch to a different language by loading a different .XML file. All of the text will be changed to the selected language, but the settings made in English will be retained. ▲

3. **Choose Open.**

   The application appears as an icon in the tree in the navigation pane. See "Setting security policies for client applications" for instructions for setting security policies for the application.

Important After you add a client application, restart the computer so that Thermo Log Service will be able to monitor the new file extensions that were added. ▲

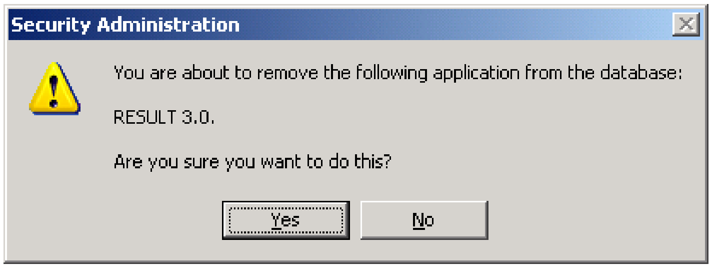
Removing a client application

Use Remove Application in the File menu to remove a client application from the navigation pane.

Follow these steps to remove a client application:

1. **Choose Remove Application from the File menu.**

   A message appears. Here is an example:



You are about to remove the following application from the database:

RESULT 3.0.

Are you sure you want to do this?

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

   Choose No if you don’t want to remove the application.

Setting security policies for client applications

When you open the icon for a client application, three kinds of security functions for the application become available in the navigation pane:

Using **Access Control**, you can set the rights of individual users or groups of users to use the protected functions of the client application. See “Controlling access to client application features” for more information.

With **System Policies** you can set policies covering such things as preventing the overwriting of files and requiring electronic signatures. See “Setting system policies for the client application” for details.

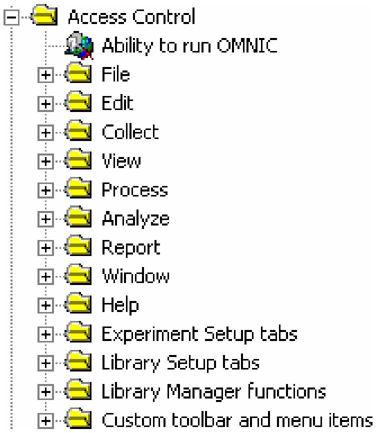
The **Signature Meanings** features let you specify the meanings that will be available for electronic signatures supplied by users of the system. See “Assigning signature meanings” for more information.

After you use these features to set security policies for the client applications, you can save your settings in the security database and print the database. See “Saving your security policy settings” and “Printing the database” for details.

Controlling access to client application features

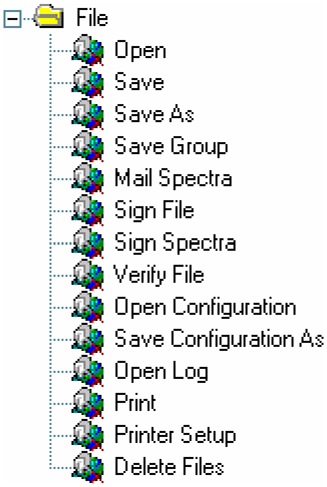
Use Access Control to set the rights of individual users or groups of users to use the protected functions of the client application. A feature in the application will be available only if the logged-in user has the right to use it.

When you open the Access Control folder for the client application by clicking its plus sign, a tree of folders and other items appears. Here is an example:



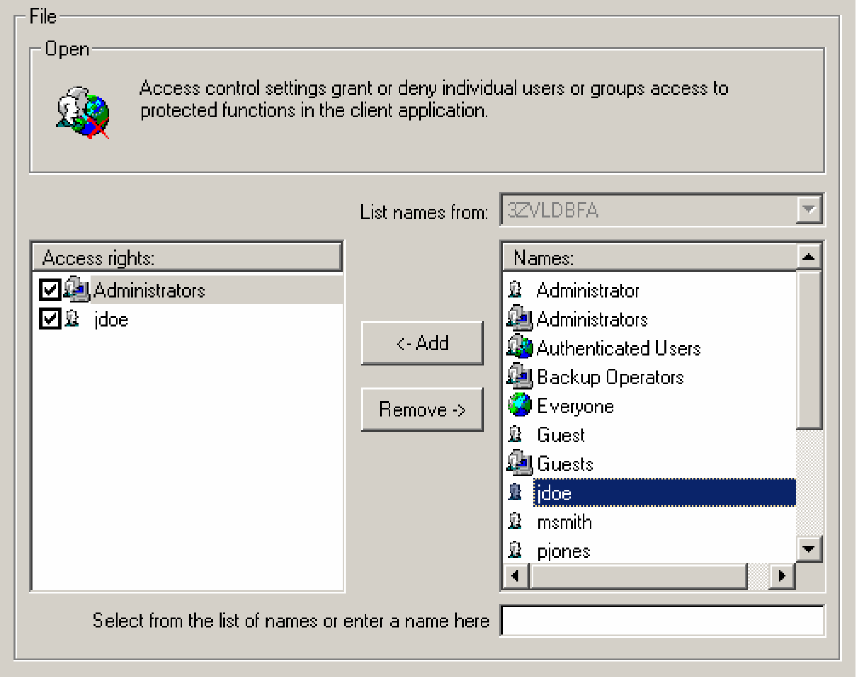
- Access Control
  - Ability to run OMNIC
  - File
  - Edit
  - Collect
  - View
  - Process
  - Analyze
  - Report
  - Window
  - Help
  - Experiment Setup tabs
  - Library Setup tabs
  - Library Manager functions
  - Custom toolbar and menu items

Each item in the tree represents a protected function or group of functions in the client application; that is, operations for which access control is available. If there is a plus sign to the left of a folder, the folder represents a group of functions such as a menu of commands. When you open one of these folders by clicking its plus sign, a tree of icons appears. Here is an example showing icons that represent commands in a menu:



- File
  - Open
  - Save
  - Save As
  - Save Group
  - Mail Spectra
  - Sign File
  - Sign Spectra
  - Verify File
  - Open Configuration
  - Save Configuration As
  - Open Log
  - Print
  - Printer Setup
  - Delete Files

You can click a function to display features for controlling access to that function. Here is an example:



File

Open

Access control settings grant or deny individual users or groups access to protected functions in the client application.

List names from: 3ZVLDBFA

Access rights:
- ☑ Administrators
- ☑ jdoe

Names:
- Administrator
- Administrators
- Authenticated Users
- Backup Operators
- Everyone
- Guest
- Guests
- jdoe
- msmith
- pjones

Select from the list of names or enter a name here

The features provided depend on the client application you are setting up. See the documentation that came with your client application for more specific information about controlling access to its protected functions.

If the computer is connected to one or more networks, selecting a network or the local computer from the List Names From drop-down list box lists the users and groups on that network or computer in the Names box. This lets you specify access to the function for the users and groups on the networks and computer. If the computer is not connected to a network, the List Names From drop-down list box is not available, and the users and groups on the computer are listed in the Names box.

The users and groups on the selected network or computer for whom access to the function has been specified appear in alphabetical order in the Access Rights box. If a check mark appears to the left of a name, that user or group can use the function. If no check mark appears, that user or group cannot use the function.

If you click a check box to remove its check mark, denying a user or group access to the function, this denial takes priority over any other settings that grant the user or group access. To prevent confusion, you should generally deny access only for individual users and not for groups. Typically, access is granted to a group and then denied to particular members of the group.

To specify access control for a user or group not listed in the Access Rights box, select it in the Names box or type it in the text box below the list, and then choose Add.

If you type the name, use the following syntax:

```
<domainname>\<accountname>
```

where “domainname” is the name of the domain location of the user or group, and “accountname” is the account name of the user or group. The user or group is added to the list in the Access Rights box, with access granted by default. You can then change the access specification.

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

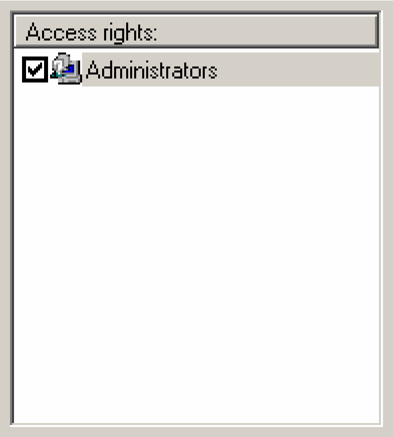
This removes that user’s or group’s right to use the function. (There is an exception to this: If a removed user is a member of a group that has the right to use the function, the user will have that right.)

Important *If a user is a member of two groups with different access control specifications, the more restrictive specification takes priority for that user.* To simplify specifying access control, we recommend that you assign a user to only one group you have created. Also, keep in mind that all users are automatically members of the Users group, so checking an individual user in the Access Rights box and then unchecking the Users group does *not* grant access to that user. Instead, it denies access to all users, and since all individuals are also users, no one has access. In general, *avoid unchecking the Users group* or most other groups; it is usually better to check a group and then uncheck individual users in the group to deny them access. ▲

Note You can use Add To All Access Control Items in the File menu to quickly grant or deny a user access to all the features of an application whose access is controlled by Security Administration. Similarly, you can use Remove From All Access Control Items in the File menu to remove the grant or deny designation for a user from all the features of an application whose access is controlled by Security Administration. See the next two sections for details. ▲

By specifying access control for logical combinations of groups and individual users, you can quickly specify that some, but not all, of the members of a group have access to a command. Consider this example:

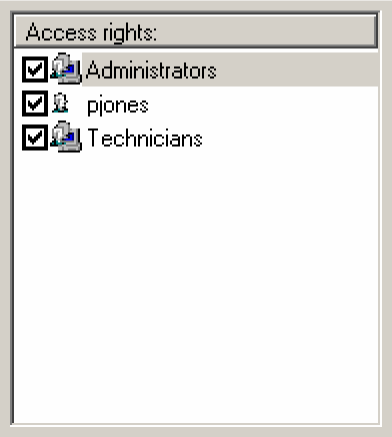
Currently only the members of the Administrators group have access to a command:


Access rights:

☑ Administrators

You want all the members of the Technicians group except Pat Jones (whose user name is “pjones”) to have access to the command as well. This can be accomplished in two simple steps.

First, use the Add button to add Technicians and pjones to the Access Rights box. Initially, check marks appear (by default) to the left of the two added names in the Access Rights box:

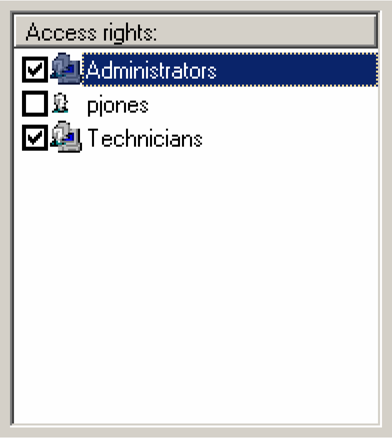


Access rights:

☑ Administrators
☑ pjones
☑ Technicians

These initial settings give all members of the Technicians group (and the Administrators group) access to the command.

Next, to deny Pat Jones access, click the check box to the left of pjones to remove the check mark:



Access rights:

☑ Administrators
□ pjones
☑ Technicians

The access rights are now set as desired and ready to be saved.

To fully control access to a function, be sure to specify access control as explained above for the all users and groups on the local computer and all the networks available in the List Names From drop-down list box.

When you are finished, save your settings in the security database. See “Saving your security policy settings” for details.

Granting or denying a user access to all the protected functions of an application

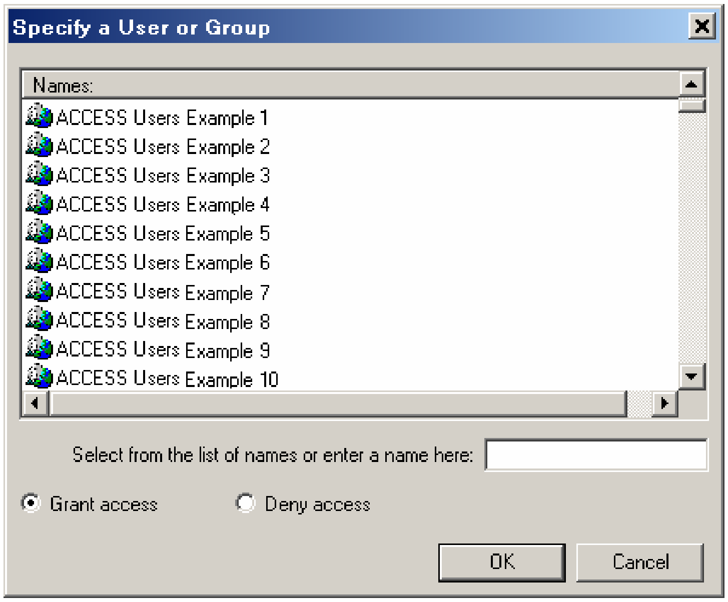
Use Add To All Access Control Items in the File menu to quickly grant or deny a user or user group access to all of the protected functions of Security Administration or a client application. This has the same effect as granting or denying the user or user group access to all of the functions individually. Follow these steps:

1. **Select the application for which you want to grant or deny access.**

   You can select Security Administration or a client application. Click the appropriate icon in the navigation pane to select an application.

2. **Choose Add To All Access Control Items from the File menu.**

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



Specify a User or Group

Names:

ACCESS Users Example 1
ACCESS Users Example 2
ACCESS Users Example 3
ACCESS Users Example 4
ACCESS Users Example 5
ACCESS Users Example 6
ACCESS Users Example 7
ACCESS Users Example 8
ACCESS Users Example 9
ACCESS Users Example 10

Select from the list of names or enter a name here:

● Grant access ○ Deny access

3. **Specify the user or user group to whom you want to grant or deny access.**

   To do this, select an item in the list box or type a name in the text box.

4. **Specify whether to grant or deny access by selecting Grant Access or Deny Access.**

5. **Choose OK.**

Removing a user's access designation for all the protected functions of an application

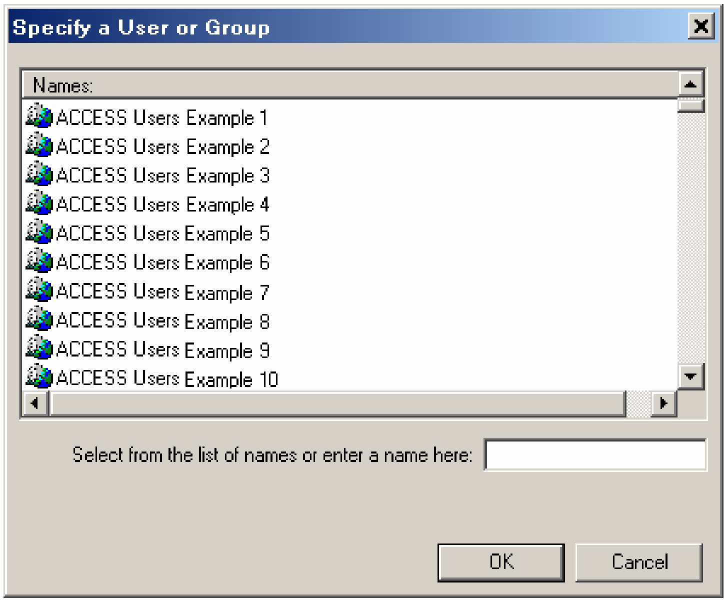
Use Remove From All Access Control Items in the File menu to quickly remove a user's or user group's grant or deny designation for all of the protected functions of Security Administration or a client application. This has the same effect as removing the designation for all of the functions individually. Follow these steps:

1. **Select the application for which you want to remove the user's access designation.**

   You can select Security Administration or a client application. Click the appropriate icon in the navigation pane to select an application.

2. **Choose Remove From All Access Control Items from the File menu.**

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



Specify a User or Group

Names:

ACCESS Users Example 1
ACCESS Users Example 2
ACCESS Users Example 3
ACCESS Users Example 4
ACCESS Users Example 5
ACCESS Users Example 6
ACCESS Users Example 7
ACCESS Users Example 8
ACCESS Users Example 9
ACCESS Users Example 10

Select from the list of names or enter a name here:

3. **Specify the user or user group to whom you want to deny access.**

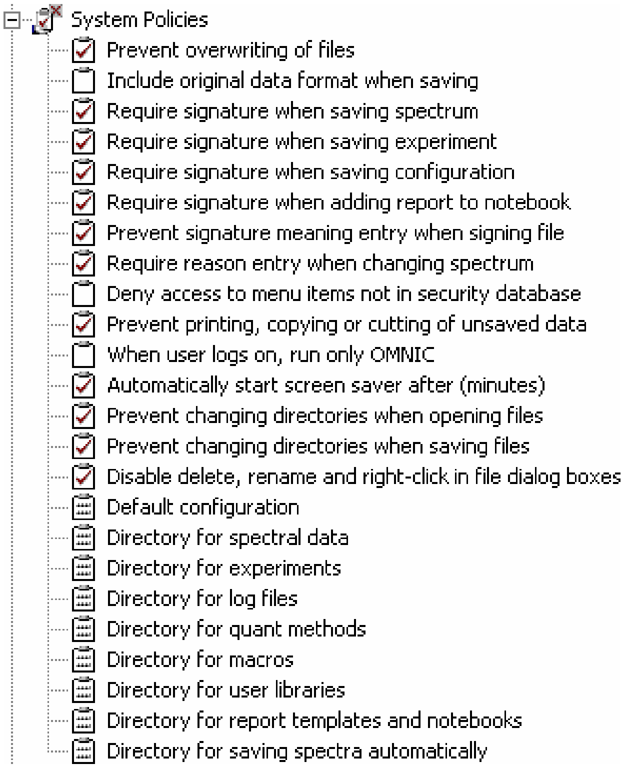
   To do this, select an item in the list box or type a name in the text box.

4. **Choose OK.**

Setting system policies for the client application

Use System Policies to set policies covering such things as preventing the overwriting of files and requiring electronic signatures. Normally all of the system policies for a client application are selected to provide the most restrictive and controlled environment.

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



- System Policies
  - ☑ Prevent overwriting of files
  - □ Include original data format when saving
  - ☑ Require signature when saving spectrum
  - ☑ Require signature when saving experiment
  - ☑ Require signature when saving configuration
  - ☑ Require signature when adding report to notebook
  - ☑ Prevent signature meaning entry when signing file
  - ☑ Require reason entry when changing spectrum
  - □ Deny access to menu items not in security database
  - ☑ Prevent printing, copying or cutting of unsaved data
  - □ When user logs on, run only OMNIC
  - ☑ Automatically start screen saver after (minutes)
  - ☑ Prevent changing directories when opening files
  - ☑ Prevent changing directories when saving files
  - ☑ Disable delete, rename and right-click in file dialog boxes
  - ▦ Default configuration
  - ▦ Directory for spectral data
  - ▦ Directory for experiments
  - ▦ Directory for log files
  - ▦ Directory for quant methods
  - ▦ Directory for macros
  - ▦ Directory for user libraries
  - ▦ Directory for report templates and notebooks
  - ▦ Directory for saving spectra automatically

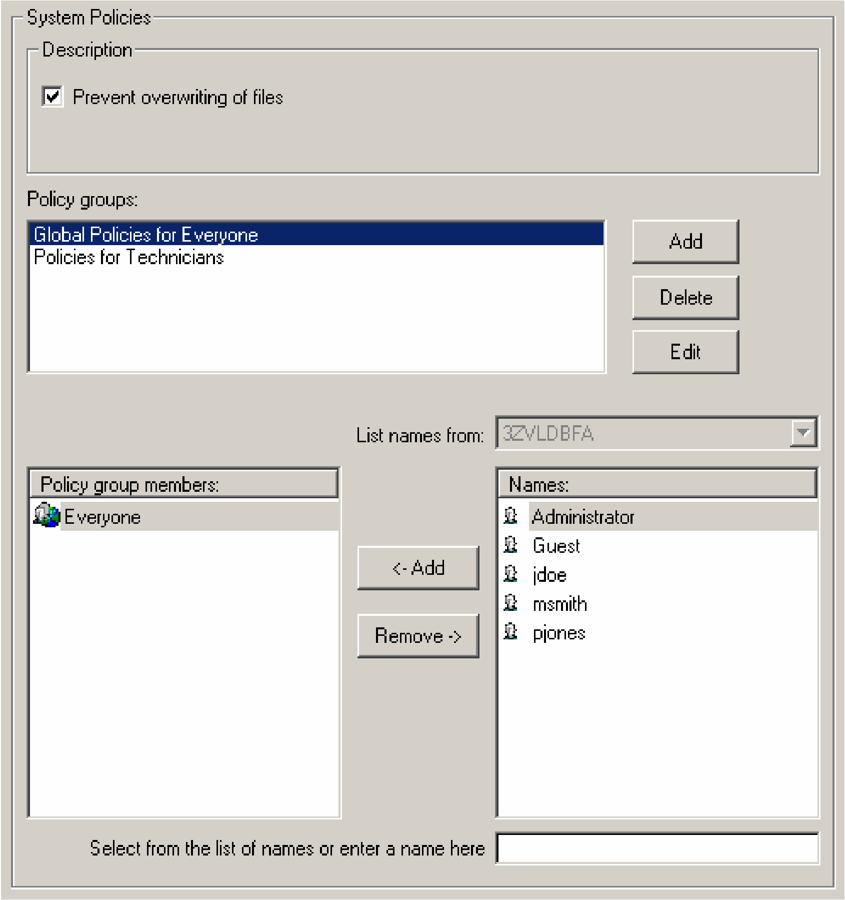
The available polices depend on the client application you are setting up.

If a check box appears to the left of a policy, you can specify whether it is selected or not selected for different “policy groups.” A policy group is a group of users for whom you can set system policies. You can create policy groups and add users to them; this is explained later in the “Creating a policy group, deleting a group or editing a group’s name” and “Adding users or removing users from a policy group” sections.

One policy group, Global Polices For Everyone, is present for every system policy. Its purpose is to provide policy settings for users whom you have not yet assigned to a group. All users are automatically members of this group. You cannot delete the group, change its name, delete users from it or add users to it. *If a user is a member of another group, that group’s policy settings for the user are used instead of the settings of the Global Policies For Everyone group.*

If no check box appears to the left of a policy in the navigation pane (see Default Configuration in the illustration), it is not the type of policy that can be selected or not selected for different policy groups. Instead, it lets you specify a system attribute, such as a default configuration or default directory, for policy groups. An example of this is explained later in this section.

You can click a policy to display features for specifying that policy. Here is an example:



System Policies

Description

☑ Prevent overwriting of files

Policy groups:

Global Policies for Everyone
Policies for Technicians

List names from: 3ZVLDBFA

Policy group members:

Everyone

Names:

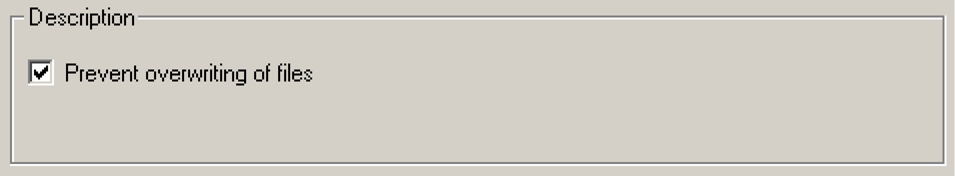
Administrator
Guest
jdoe
msmith
pjones

Select from the list of names or enter a name here

The features provided depend on the type of policy and the client application you are setting up. See the documentation that came with your client application for more specific instructions for setting its system policies.

When you select a policy group in the Policy Groups box, that group's settings for the selectable policies appear in the tree in the navigation pane (a check mark appears or does not appear in the check box to the left of each policy name). This lets you see all of the group's selectable settings at a glance. In addition, the members of the selected group are listed in alphabetical order in the Policy Group Members box.

Once you have selected a policy group, you can click a policy in the navigation pane in order to set that policy for the group. You do this by using either a check box that appears in the Description box or other special features that are explained in the manual that came with the client application. Here is an example showing the check box for a selectable policy:

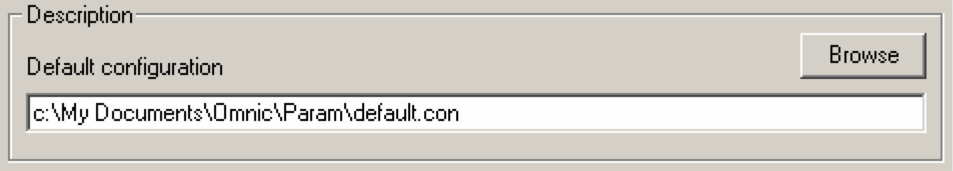


Description

☑ Prevent overwriting of files

To change the setting, click the check box. A check mark in the check box means the policy will be in effect for the group after you save the security database.

Policies that let you specify a system attribute, such as a default configuration or default directory, include whatever special features are needed for setting the policy. These features are explained in the manual that came with the client application. In the OMNIC example below, the Default Configuration policy is used to specify a default configuration file to be used for different policy groups who run a client application. To set this policy, you would type the pathname of the desired configuration in the Default Configuration text box or use the Browse button to locate and select a path.



Description

Default configuration: c:\My Documents\Omnic\Param\default.con

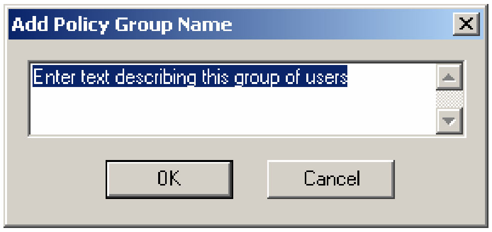
When you are finished setting the system policies, save your settings in the security database. See “Saving your security policy settings” for details.

Creating a policy group, deleting a group or editing a group's name

You can create a new policy group, delete a policy group or edit a policy group's name.

To create a new policy group, click the Add button to the right of the Policy Groups box.

The Add Policy Group Name dialog box appears:



Enter text describing this group of users

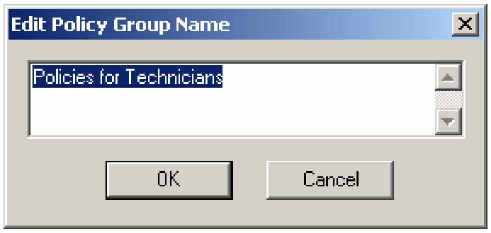
Type a description for the group (for example, "Technicians") and choose OK. The new group appears in the Policy Groups box, with a name that includes the description you entered; for example, "Policies for Technicians." You can then add users to the group by using the Add button to the right of the Access Rights box, as explained later in this section.

To delete a policy group (other than the Global Policies For Everyone Group), select the group in the Policy Groups box and click the Delete button.

The group is removed from the list.

To edit the name of a policy group (other than the Global Policies For Everyone Group), select the group in the Policy Groups box and click the Edit button.

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



Type a new description for the group and choose OK. The edited group name appears in the Policy Groups box.

Adding users or removing users from a policy group

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

To add a user to the policy group, select the desired user in the Names box or type the name in the text box below the list, and then choose Add.

If you type the name, use the following syntax:

```
<domainname>\<accountname>
```

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

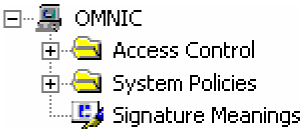
To remove a user from the policy group, select the user in the Policy Group Members box and then choose Remove.

Assigning signature meanings

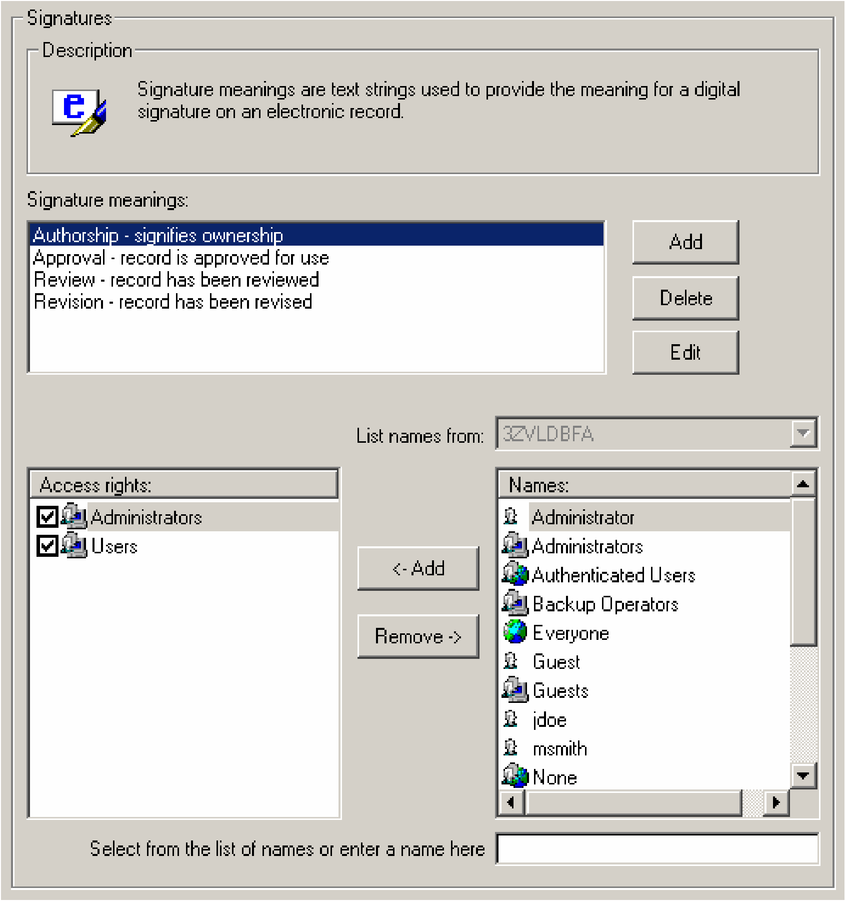
Use Signature Meanings to specify the meanings that will be available for electronic signatures supplied by users of the client application. Each client application has its own default list of available signature meanings. You can edit or delete these meanings and add new meanings. You can also specify which users or groups can use particular meanings.

Note Some client applications include a system policy that specifies whether users can enter custom signature meanings. See the documentation that came with your client application for more information. ▲

To see the current signature meaning assignments, click the Signature Meanings icon for the client application. If the Signature Meanings icon is not visible, click the plus sign to the left of the application's icon in the tree. Here is an example showing the Signature Meanings icons:



The Signature Meanings features appear in the right pane. Here is an example:



Signature meanings are text strings used to provide the meaning for a digital signature on an electronic record.

Signature meanings:

Authorship - signifies ownership
Approval - record is approved for use
Review - record has been reviewed
Revision - record has been revised

List names from: 3ZVLDBFA

Access rights:

☑ Administrators
☑ Users

Names:

Administrator
Administrators
Authenticated Users
Backup Operators
Everyone
Guest
Guests
jdoe
msmith
None

Select from the list of names or enter a name here

The listed available signature meanings depend on which client application you are working with, whether the default signature meanings have been edited or deleted, and whether any signature meanings have been added.

Note If you make changes to the list of signature meanings and later want to restore the default list, see the manual that came with your client application and edit the list to match the manual illustration that shows the default list. ▲

When you select a signature meaning in the list by clicking it, the Access Rights box lists the user groups whose permission to select that signature meaning has been specified. If a check mark appears to the left of a listed user group, those users can select that signature meaning when signing a file. If no check mark appears, users in that group cannot select that signature meaning. If a user group is not listed in the Access Rights box, those users also cannot select that signature meaning unless they have been granted permission individually to select that meaning. (Some exceptions to these rules are explained in the next section.)

The next sections explain how to change the permission specifications for the selected signature meaning and change the list of available signature meanings. When you are finished, save your settings in the security database. See "Saving your security policy settings" for details.

Changing signature meaning assignments

This section discusses changing the permission specifications for the currently selected signature meaning. Keep in mind that the changes you make apply only to that signature meaning. To make changes for a different signature meaning, first select it in the list of available meanings.

If the computer is connected to one or more networks, selecting a network or the local computer from the List Names From drop-down list box lists the users and groups on that network or computer in the Names box. This lets you specify the signature meaning permissions for the users and groups on the networks and computer. If the computer is not connected to a network, the List Names From drop-down list box is not available, and the users and groups on the computer are listed in the Names box.

If you click a check box to remove its check mark, denying a user or group permission to select the signature meaning, this denial takes priority over any other settings that grant the user or group permission. To prevent confusion, you should generally deny permission only for individual users and not for groups. We recommend that you assign a user to only one group you have created. Also, keep in mind that all users are automatically members of the Users group, so checking an individual user in the Access Rights box and then unchecking the Users group does *not* give permission to that user. In general, *avoid unchecking the Users group* or most other groups; it is usually better to check a group and then uncheck the appropriate members of the group individually to deny them permission.

To specify permission for a user or group not listed in the Access Rights box, select the desired user or group in the Names box by clicking it or type the name in the text box below the list, and then choose Add.

If you type the name, use the following syntax:

```
<domainname>\<accountname>
```

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

The user or group appears in the Access Rights box, with permission granted by default. You can then change the permission specification.

To remove a listed user or group from the Access Rights box, select the user or group by clicking it and then choose Remove.

This removes that user's or group's permission for the signature meaning, just as if you have removed the check mark to the left of the name of the user or group. (There is an exception to this: If a removed user is a member of a group that has permission for the meaning, the user will have permission.)

To fully specify permissions for a signature meaning, be sure to specify permissions as explained above for the all users and groups on the local computer and all the networks available in the List Names From drop-down list box.

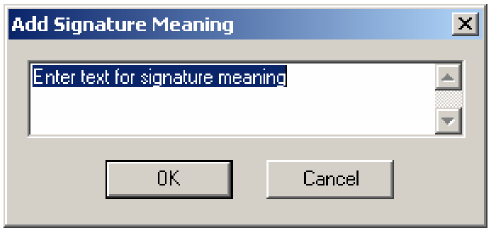
When you are finished, save your settings in the security database. See “Saving your security policy settings” for details.

Changing the available signature meanings

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

To add a new signature meaning to the list of available meanings, choose Add.

The Add Signature Meaning dialog box appears. Here is an example:



Enter text for signature meaning

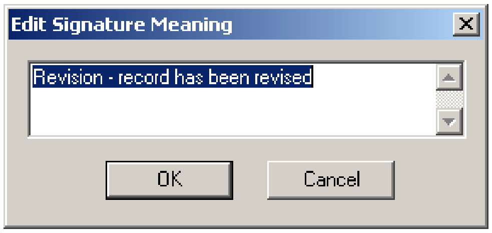
Type the desired text in the text box and then choose OK. The text you entered appears in the list of available signature meanings. You can then use the instructions in the preceding section to specify which user groups can select this signature meaning when signing a file.

To delete a signature meaning from the list of available meanings, select the meaning by clicking it and then choose Delete.

The meaning will no longer be available to users when they sign files.

To edit a signature meaning in the list of available meanings, select the meaning by clicking it and then choose Edit.

The Signature Meaning dialog box appears. Here is an example:



Revision - record has been revised

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

Saving your security policy settings

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

After you save your settings, you can see them in the database and also print the database. See “Previewing the security database” and “Printing the database” for more information.

Note If you have made changes to any security policy settings and then exit Security Administration without first saving your settings, you will be prompted to save the settings. See “Exiting Security Administration” for details. ▲

Follow these instructions to save your security policy settings:

Choose Save Settings from the File menu.

Your security policy settings are saved in the security database.

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

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

Note Every change you make to the security database is logged in the system event log when you save your settings. ▲

Printing the security database

The File menu contains three commands that let you preview the security database before printing it, set options that affect printing, and print the contents of the database. Printing the database lets you keep a hard-copy record of your most recently saved settings. The next sections explain how to use the commands.

Previewing the security database

Use Print Preview in the File menu to view the contents of the security database before printing it.

Note Only settings that you have saved will appear in the database. See “Saving your security policy settings” for information about saving your security policy settings. ▲

Follow these steps to preview the security database:

1. **Choose Print Preview from the File menu.**

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

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

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

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

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

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

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

If you want to print the database, click the Print button. Set the print options in the dialog box that appears and then choose OK. If you need help, right-click a feature or see your Windows documentation. Since this also closes the preview window, the procedure is finished.

Note You can also print the database using Print in the File menu. See "Printing the database" for details. ▲

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

Setting the print options

Choose Print Setup from the File menu to set options that affect the printing of the security database before printing the database. See "Printing the database" for instructions for printing the database.

Printing the database

Choose Print from the File menu to print the contents of the security database. If you would like to view the database before printing it, use Print Preview in the File menu. (You can also print the database using the Print button in the preview window.) See “Previewing the security database” for details. If you would like to set some print options such as paper size and page orientation, use Print Setup in the File menu. See “Setting the print options” for details.

Exiting Security Administration

Choose Exit from the File menu to exit Security Administration.

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

Troubleshooting

The troubleshooting table below will help you solve problems that may occur when you log into a client application. If you are unable to solve a problem after following the provided instructions, use the information at the beginning of this document to contact us.

Problem	What To Do
When a user attempts to log into a client application, an error message says the user name or password did not match.	Verify that the user has the right to access the computer from the network. See “Local and global user groups and rights” in the “Overview of Windows Administration for All Systems” chapter for more information. If you are using Windows XP, verify that the “Classic” setting is in effect, as explained in the procedure in “Setting up Windows Vista or Windows XP Professional administration for a stand-alone computer” in the “Setting Up Windows Administration” chapter.
A user with a blank password can log on to Windows XP Professional but cannot log into a client application or Security Administration.	Assign the user a non-blank password.
The security database does not display correctly when you use Print Preview in the File menu; for example, the text is too large.	Make sure an appropriate printer driver is installed on the computer.

Problem	What To Do
When a user attempts to log into a client application, the log-in fails and this error message appears: “The dwFlags parameter is CRYPT_NEWKEYSET but the key already exists.”	This occurs because Windows turns off the ability to sign data if the password is changed by an administrator rather than by the account owner. This can be caused by a permissions problem on a computer with an NTFS file system. Make sure the user has appropriate permissions in the locations described below. (Note: This information applies *only* to NTFS file systems.) 1. In Windows Explorer enable the ability to see hidden files. 2. Browse to `<root drive letter>:\Documents and settings\<user name>\Application data\Microsoft\Crypto\RSA`. For example, the path for the administrator on a computer with only a C drive would be `C:\Documents and Settings\Administrator\Application Data\Microsoft\Crypto\RSA`. 3. Right-click the RSA folder and choose Properties from the pop-up menu. 4. In the RSA Properties dialog box click the Security tab. (If there is no Security tab, you do not have an NTFS file system; this procedure does not apply to your system.) 5. Make sure Full Control for the folder is enabled for the current user and for a user named “SYSTEM.”

Problem	What To Do
When a user attempts to start a client application, this message appears: "Unable to communicate with Thermo Security Service."	Make sure that Security Administration is installed, and make sure that the network cables are connected and there are no other network problems that would prevent normal communication. An incorrect network server may be specified. Use ChangeServer.exe on the Security Administration Software CD to specify the correct server. A Windows firewall program may be preventing programs—such as Security Administration and a client application—from communicating over the network. To allow communication, without allowing the spread of viruses and worms, add an exception to the firewall as explained below. In Windows Vista: 1. Start Windows Firewall: In Windows standard view, start Security from Control Panel and then choose Windows Firewall. 2. Click the Change Settings link in Windows Firewall. 3. On the Exceptions tab in the Windows Firewall dialog box, click File And Printer Sharing so that it becomes highlighted. 4. Click the Add Port button. 5. In the Add A Port dialog box , set Name to Thermo Security Service, set Port Number to 139, and set Protocol to TCP. Then choose OK. 6. Choose OK to close the Windows Firewall Settings dialog box, close Windows Firewall, and then close Control Panel. In Windows XP Professional: 1. Start Windows Firewall: In Windows standard view, start Security Center from Control Panel and then choose Windows Firewall. In Windows classic view, start Windows Firewall from Control Panel. 2. On the Exceptions tab in the Windows Firewall dialog box, click File And Printer Sharing so that it becomes highlighted. 3. Click the Edit button. 4. In the Edit A Service dialog box, select TCP 139 so that its check box contains a check mark and then choose OK. 5. Choose OK to close the Windows Firewall dialog box, close the Windows Security Center window if it is open, and then close Control Panel.

Index