

SecureWave
Safeguarding Tomorrow

Sanctuary Application Control Suite Administrator's Guide

www.securewave.com



Liability Notice

Information in this manual may change without notice and does not represent a commitment on the part of SecureWave.

SecureWave, S.A. provides the software described in this manual under a license agreement. The software may only be used in accordance with the terms of the contract.

No part of this publication may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without the prior written permission of SecureWave.

SecureWave claims copyright in this program and documentation as an unpublished work, revisions of which were first licensed on the date indicated in the foregoing notice. Claim of copyright does not imply waiver of other rights by SecureWave.

Copyright 2000-2007© SecureWave, S.A.
All rights reserved.

Trademarks

Sanctuary is a trademark of SecureWave, S.A.
All other trademarks recognized.

SecureWave, S.A.
Atrium Business Park
23, rue du Puits Romain
L-8070 Bertrange
Luxembourg

Phone: +352 265 364-11 (add prefix 011 when calling from USA or Canada)
Fax: +352 265 364-12 (add prefix 011 when calling from USA or Canada)
Web: www.securewave.com

Technical Support hours are Monday to Friday, 8:00 to 20:00 CET/CEST in Europe and 8:00 AM to 8:00 PM ET/EDT in North America.

You can contact our technical support team by calling:

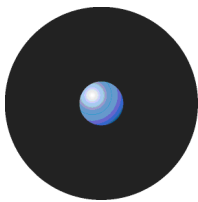
+352 265 364 300 (International),
+1-877-713-8600 (US Toll Free),
+44-800-012-1869 (UK Toll Free)

or by sending an email to support@securewave.com

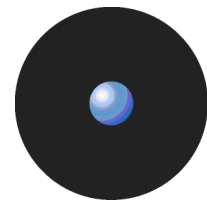
Published on: August 2007

Contents

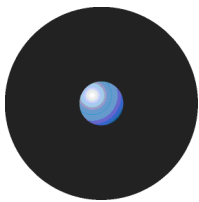
Introducing Sanctuary Application Control Suite	5
A complete portfolio of security solutions	5
What can you find in this guide	5
Conventions	6
Typographical conventions	6
Symbol conventions	6
Keyboard conventions	6
For more information	7
To contact us	7
Chapter 1: Understanding Sanctuary Application Control Suite	9
Welcome to Sanctuary Application Control Suite	9
Benefits of the white-list approach	9
How does the system know which files can be run?	10
What do you gain by using Sanctuary Application Control Suite?	11
Chapter 2: Using Sanctuary Application Control Suite	13
What is new in this version	13
Working with the Sanctuary Application Control Suite system	13
Starting up the Sanctuary Management Console	13
Connecting to a server	14
Log in as a different user	14
The Sanctuary Management Console	15
Controlling your workspace	16
The Sanctuary Application Control Suite modules	18
The Sanctuary Management Console menus and tools	18
File menu	18
View menu	18
Tools menu	19
Endpoint Maintenance	19
Reports menu	21
Explorer menu	21
Window menu	22
Help menu	22
Chapter 3: An overview of authorization strategies	23
Central authorization using digital signatures	24
Central authorization by file location (path)	25
Local authorization of executables, scripts and macros	25
Local authorization of files that are not centrally authorized	25
Preventing the malicious spread of locally authorized files	27
Deleting user's local authorization lists	27
Sending updated authorization information to computers	28
To push updates to all computers protected by Sanctuary	28
To push updates to a specific computer	28
Chapter 4: Setting up Sanctuary administrators	29
How to set up a Sanctuary system administrator	29
To define a system administrator with full management privileges	29
To define a system administrator with restricted access privileges	30
To define access privileges to specific functions and modules	30
Chapter 5: Building a white list of authorized files	33
Exporting and importing file authorization settings	33
Importing Standard File Definitions	34
Benefits of using the automatic import option during installation	35



To manually import Standard File Definitions	35
Selecting files to authorize using the Exe Explorer module	36
To select files using the Exe Explorer modules	38
Automatically scanning a computer to identify files	39
Using the Scan Explorer module	39
Using the Authorization Wizard	42
To authorize executable files using the Authorization Wizard	43
Chapter 6: Organizing files into File Groups	47
Creating and managing File Groups	47
To create a new File Group	47
To delete a File Group	48
To rename a File Group	48
To create a parent-child relationship between File Groups	48
Assigning executable, script and macro files to File Groups	50
To assign files to File Groups	50
Changing file assignments	51
To change the File Group to which a file is assigned	51
To delete a file from a File Group	52
To delete a file from the SecureWave Sanctuary Database	52
Viewing file assignments	52
To sort entries by any attribute, such as filename or File Group	53
To display a subset of the files in the database	53
Using the Groups tab	53
Chapter 7: Authorizing files by location (Path Rules)	55
Creating, changing, and deleting Path Rules	55
To create a new Path Rule that applies to everybody	55
To create a new Path Rule that applies to a specific user or user group	56
To modify an existing Path Rule	57
To delete a single Path Rule for a user or user group	57
To delete all Path Rules for a user or user group	57
Conventions for specifying paths in the rules	57
Defining and working with Trusted Owners	58
To define or delete a Trusted Owner	58
Trusted Owner and Path Rule example	59
Path Rules precedence	59
Chapter 8: Granting access using the User Explorer	61
Users and user groups	61
Direct, indirect, and not authorized File Groups	61
Assigning File Groups to users/user groups	64
To assign/remove File Groups to/from users	64
Assigning users/user groups to File Groups	65
To assign/remove users to/from a File Group	65
Chapter 9: Monitoring activities using the Log Explorer	67
Accessing the Log Explorer module	68
Log Explorer templates	69
To use an existing template	69
To create and use a new template	69
Log Explorer window	71
Navigation/Control bar	71
Column headers	72
Results panel / custom report contents	75
Criteria/Properties panel	78
Control button panel	78
Select and edit templates window	78
Template settings window	80
Simple Query tab	81
Criteria	82
Query & Output tab	83
Schedule tab	85
Format tab	85
Delivery tab	86
Using the Log Explorer module to authorize unknown files	87
To authorize a new executable, script or macro from the Log Explorer module	87
Forcing the latest log files to upload	87
Viewing administrator activity	88
Audit events	88



Generating reports of system status and settings	89
Chapter 10: Managing files using the Database Explorer	91
Viewing database records	91
Using the Database Explorer module	91
To sort entries by any attribute, such as filename or File Group	92
To expand the display to show/hide other columns	92
To save this list as a CSV file	93
Synchronizing Sanctuary accounts with Microsoft and/or Novell accounts	93
To synchronize domain members	93
SXDomain command-line tool	93
Novell's synchronization script	93
To synchronize user/account information from a workgroup (not a domain)	94
Performing database maintenance	94
Backing up the SecureWave Sanctuary Database	94
Removing old database records	94
To delete old database records	94
Removing obsolete computer connections records	95
Chapter 11: Generating Sanctuary reports	97
File Groups by User	98
Users by File Group	99
User Options	100
Machine Options	101
Online Machines	102
Server Settings Report	103
Chapter 12: Setting Sanctuary system options	105
Options set in old Sanctuary versions	105
Default options	106
To change default option settings	106
Default options for protected servers and computers	107
Client Hardening	107
eDirectory translation	108
Endpoint status	108
Execution blocking	108
Execution eventlog	109
Execution log	109
Execution notification	109
Local Authorization	109
Log upload interval	110
Log upload threshold	110
Log upload time	110
Log upload delay	110
Server address	110
Default options for users and user groups	111
Execution blocking	111
Execution eventlog	112
Execution log	112
Execution notification	112
Macro and Script protection	112
Relaxed logon	113
Relaxed logon time	113
Options that apply to specific machines or specific users	114
To override default option settings	114
Determining which option setting takes precedence	115
Precedence rules for computer options	115
Precedence rules for user and user group options	116
Precedence rules for options with both computer and user/user group values	118
Precedence rules for the Execution Blocking option	120
Informing client computers of changes	121
Chapter 13: Windows Updates and other tools	123
Authorization Service Tool	123
Microsoft Software Update Services and Windows Server Update Services	123
What does the Authorization Service Tool do?	123
Installing the Authorization Service tool	125
Configuring the Authorization Service tool	125
Versatile File Processor tool	127
Command line parameters	127



Usage notes	128
Examples	130
File Import/Export Tool	130
Command line parameters	130
Usage notes	131
Examples	131
Chapter 14: Inspecting your endpoints and authorizing software	133
The 'Discover' procedure	133
Exact match: 'High-control foundation'	134
Procedure	134
Authorizing your present installation	135
Pros and cons	135
Pragmatically: 'Average foundation'	136
Procedure	136
Authorizing your present installation	136
Pros and cons	136
Maintenance phase	137
Frequently changing programs	137
Operating system updates and patches	137
New software installations	137
Software updates	137
Changing from a test to a production environment	138
Identifying DLL dependencies	138
What are DLLs?	138
What are dependencies?	139
How are DLLs dependencies identified?	139
How to integrate dependencies with Sanctuary	139
Glossary	141
Index of Figures	145
Index of Tables	149
Index	150

Introducing Sanctuary Application Control Suite

The real world can be harsh: Trojans, worms, viruses, hackers, and even careless or disgruntled employees threaten your company's data and structure. They can undermine your business with extraordinary speed, and the cost and damage to applications, data, confidentiality, and public image, can be immense.

Your role, until now, has been to try to anticipate malicious code and actions before they occur and to react to them when they do — in a never-ending expenditure of time, money, and energy.

Sanctuary solutions stop that futile game for good. With Sanctuary software, you define what is allowed to execute on your organization's desktops and servers, and what devices are authorized to copy data. Everything else is denied by default. Only authorized programs and devices can run on your network, regardless of the source. Nothing else can get in. Nothing.

What makes Sanctuary so revolutionary is that it is proactive, not reactive. You are empowered, not encumbered. You lower and raise the drawbridge. You open and close the borders. You create calm in a chaotic world.

A complete portfolio of security solutions

SecureWave offers a complete portfolio of solutions for regulating your organization's applications and devices.

- > Our Sanctuary Application Control Suite, can be any of the following programs:
 - > **Sanctuary Application Control Custom Edition** lets you create multiple File Groups and User Groups, so you can control application execution at a more granular level.
 - > **Sanctuary Application Control Terminal Services Edition** extends application control to Citrix or Microsoft Terminal Services environments, which share applications among multiple users.
 - > **Sanctuary Application Control Server Edition** delivers application control to protect your organization's servers, such as its Web-hosting server, email server, and database server.
- > **Sanctuary Device Control** prevents unauthorized transfer of applications and data by controlling access to input/output devices, such as memory sticks, modems, and PDAs.
- > **Sanctuary for Embedded Devices** moves beyond the traditional desktop and laptop endpoints and onto a variety of platforms that include ATMs, industrial robotics, thin clients, set-top boxes, network area storage devices and the myriad of other systems running Windows XP Embedded.

What can you find in this guide

This guide explains how to use Sanctuary Application Control Suite (Sanctuary Application Control Custom Edition, Sanctuary Application Control Terminal Services Edition, and Sanctuary Application Control Server Edition - as explained in the previous section) to enable your organization's servers and computers to only run safe, approved applications.

- > *Chapter 1: Understanding Sanctuary Application Control Suite*, provides a high-level overview of the solution, how it works and benefits your organization.
- > *Chapter 2: Using Sanctuary Application Control Suite*, shows a high-level view of system modules, menus, and tools.
- > *Chapter 3: An overview of authorization strategies*, describes the various file tools and ways you can control file execution.



- > *Chapter 4: Setting up Sanctuary administrators*, tells how to set up two types of system administrators — with full or limited privileges.
- > *Chapter 5: Building a white list of authorized files*, describes four ways to load definitions of allowable executables, scripts and macros into the system.
- > *Chapter 6: Organizing files into File Groups*, describes the process of setting up File Groups and adding files to those groups.
- > *Chapter 7: Authorizing files by location (Path Rules)*, describes the process of using pathname rather than digital signature to define allowable files.
- > *Chapter 8: Granting access using the User Explorer*, describes two key ways to give users privileges to use executable files, scripts and macros.
- > *Chapter 9: Monitoring activities using the Log Explorer*, describes the logs of application-execution activity and explains how to verify the log of the system administrator activities.
- > *Chapter 10: Managing files using the Database Explorer*, describes the database in full as well as routine housekeeping functions such as system cleanup and backup.
- > *Chapter 11: Generating Sanctuary reports*, describes the HTML reports that can be easily created by the system.
- > *Chapter 12: Setting Sanctuary system options*, describes the various options that govern system operation at user, machine, group, or global levels.
- > *Chapter 13: Windows Updates and other tools*, explains how you can use Sanctuary with the technologies provided with Windows.
- > *Chapter 14: Inspecting your endpoints and authorizing software*, outlines recommended procedures for using Sanctuary in the context of a total security strategy.
- > The *Glossary* and indexes (*Index of Figures*, *Index of Tables*, and *Index*) provide quick access to specific terms or topics.

Conventions

Typographical conventions

Different typefaces have been used to outline special types of content throughout this guide:

<i>Italic text</i>	Represents fields, menu options, and cross-references.
This style	Shows messages or commands typed at a prompt.
SMALL CAPS	Represent buttons you select.

Symbol conventions

The following symbols emphasize important points:



Take note. You can find here more information about the topic in question. These may relate to other parts of the system or points that need particular attention.



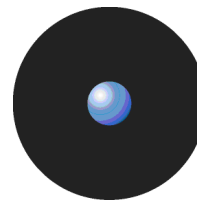
Shortcut. Here is a tip that may save you time.



Caution. This symbol means that proceeding with a course of action may result in a risk, e.g. loss of data or potential problems with the operation of your system.

Keyboard conventions

A plus sign between two keyboard keys means that you must press those keys at the same time. For example, ALT+R means that you hold down the ALT key while you press R.



A comma between two or more keys means you must press each of them consecutively. For example 'Alt, R, U' means that you press each key in sequence.

For more information

In addition to the documents and online help that come with Sanctuary, further information is available on our Web site at:

www.securewave.com

This regularly updated Web site provides you with:

- > The latest software upgrades and patches (for registered users).
- > Troubleshooting tips and answers to frequently asked questions.
- > Other general support material that you may find useful.
- > New information about Sanctuary.
- > Our Knowledge Base (KB), with FAQ (Frequent Asked Questions) and practical information of your every day use of Sanctuary solutions.

To contact us

If you have a question not found in the online help or documentation, you can contact our customer support team by telephone, fax, email, or regular mail.

Technical Support hours are Monday to Friday, 8:00 to 20:00 CET/CEST in Europe and 8:00 AM to 8:00 PM ET/EDT in North America.

You can contact our technical support team by calling:

+352 265 364 300 (International),
+1-877-713-8600 (US Toll Free),
+44-800-012-1869 (UK Toll Free)

or by sending an email to: support@securewave.com

Alternatively, you can write to customer support at:

SecureWave, S.A.
Atrium Business Park
23, rue du Puits Romain
L-8070 Bertrange
Luxembourg

Chapter 1: Understanding Sanctuary Application Control Suite

This chapter introduces Sanctuary Application Control Suite and explains how it benefits your organization. We explain:

- > How Sanctuary Application Control Suite fundamentally differs from most anti-virus and intrusion-detection systems on the market.
- > How Sanctuary Application Control Suite streamlines your costs and network administration, adding higher levels of protection.
- > How it protects your environment enforcing proper use of user's applications.
- > Enhance productivity levels not allowing unauthorized/unlicensed program installations.
- > The basic components of the Sanctuary Application Control Suite solution and what each contributes to the security strategy.
- > What happens behind the scenes to make Sanctuary Application Control Suite such a powerful, effective, yet easy-to-use solution.
- > How to navigate through the different screens and options.

Welcome to Sanctuary Application Control Suite

If you are tired of worrying about viruses, worms, and other malicious code... tired of keeping up with illegal or unlicensed software that finds its way onto crucial servers or computers... rest easy. Now you have Sanctuary.

Sanctuary Application Control Suite is a unique product that provides a new approach to network security. Rather than specifying what *cannot* run (an approach that has administrators scrambling to defend themselves against every new threat that comes along), Sanctuary security specifies what *can* run. Nothing else works, period. That means no matter how inventive and evolved some new malicious code might be, it simply does not run. You are protected.

Using Sanctuary Application Control Suite ensures that:

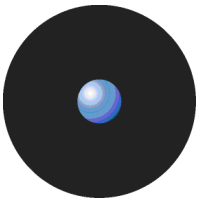
- > Your users cannot execute programs such as hacking tools, games, or unlicensed software.
- > You eliminate the threats posed by Trojans, Worms, and executable viruses, both known and unknown.

Sanctuary Application Control Suite works in exactly the opposite way to the way most security and anti-virus products on the market do. Rather than creating a 'black list' of files that are *not* allowed to run, Sanctuary uses a 'white list' of executable files, scripts and macros that *are* allowed to run.

Benefits of the white-list approach

Sanctuary Application Control Suite innovative 'white list' approach offers several significant benefits (for a complete description see the Sanctuary's Architecture Guide):

- > **Greater protection.** Even if dozens of new viruses, worms, and Trojans have been created since you installed the software, you are protected. Unknown and unauthorized executable files, regardless of their origin — email, Internet, DVD or CD — simply do not run.



- > **Early interception.** For most malicious code, the application cannot even be installed, because the self-install program itself is an executable file that does not run. That means requests for execution are intercepted long before there is any chance of running them.
- > **Simple maintenance.** You do not have to keep loading updates just to keep pace with the endless stream of new viruses. You do not even need to know exactly what software is installed on every protected system. You only have to monitor what is known and approved, not everything else.

In short, with Sanctuary, you have a robust shield protecting your organization's servers and computers. For a complete description of the advantages and disadvantages of white lists see Sanctuary's Architecture Guide.

How does the system know which files can be run?

As a Sanctuary administrator, you can specify which executable files, scripts and macros each user can activate, in a simple three-stage process:

1. Build your white list of executables, scripts and macros.

Collect files by using built-in tools to scan the servers and computers you wish to protect, or import standard file definitions provided by SecureWave for popular Windows 2000, Windows 2000 Server, Windows XP, Windows 2003 Server and Vista operating systems.

The system calculates a unique signature (a 'hash') for each executable file, script or macro, and uses this distinctive signature to identify allowable files.

2. Organize the files into File Groups.

To streamline administration, you can logically organize files into File Groups, such as grouping together all applications that would be needed by your Webmaster, all database management applications used by your database administrators, or your payroll program.



A single File Group cannot contain both executables and scripts/macros.

3. Link users with their allowed File Groups.

Having defined File Groups, Users, and User Groups, you can now specify not only which executables, scripts and macros can be used, but by whom. Once a file has been centrally authorized and it is immediately available to be run by all authorized users.

When a user wants to run an executable, script or a macro, the following actions automatically take place:

1. If the file is an executable, it is identified as such by the operating system and loaded in memory *ready* for execution (but not actually executed yet!).
2. If the file is identified by Sanctuary as a script or macro, it is again loaded in memory ready for execution.



Sanctuary can only recognize and centrally manage the following types of scripts and macros:

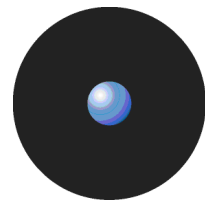
- > *VBScripts and JScripts that are interpreted by the Windows Script Host (using `cscript.exe` and `wscript.exe`). These scripts are text files written using the grammar and semantics of the appropriate language. To be recognized by Sanctuary your script files must have the appropriate file extension — either `.vbs` or `.js`.*
- > *Visual Basic scripts (VBA macros) that execute within Microsoft Office and other host applications. These are embedded in Word documents, Excel spreadsheets, and so on.*

3. Before any execution takes place, Sanctuary checks the contents of the entire file to determine the digital signature (hash) of the file that has been loaded into memory.



Visual Basic scripts (VBA macros) can be embedded in many Microsoft Office formats, such as `.doc`, `.dot`, `.xls`, and `.ppt` files. In this case, a hash is created for the whole file, not just the macro.

4. The digital signature is compared to those of files authorized to run (in the white list).



5. If and only if, the file corresponds exactly to a file on the white list, i.e. their digital signatures are identical, and the file is authorized for execution by the person/machine that has requested it, the file is executed.

If you are using Sanctuary Application Control Server Edition, the solution protects your organization's servers and, by nature, your 'users' are system administrators. For the purposes of this guide, we call them all users, even though for some of our products they are not end-users in the typical sense of the word. Sanctuary recognizes both local and domain users and groups.

Now you can have total control over applications running on your organization's servers. Authorized administrators and users can work with their applications, but they cannot run any other executable files, such as viruses, Spyware, any unauthorized scripts/macros, or other inappropriate applications — whether loaded deliberately or accidentally.

What do you gain by using Sanctuary Application Control Suite?

We have already described the benefits of a white-list approach versus the typical black-list approach — see also the Sanctuary's Architecture Guide. Looking further, Sanctuary offers a wide range of features and benefits:

- > **Strong file identification** — Sanctuary works by examining each executable, script or macro file that an administrator wishes to centrally authorize and calculating a unique digital signature based on the entire contents of that executable. This digital signature is known as a hash. Even the slightest change to a file would result in a different hash, which means the altered file would not be able to run.
- > **Software version control** — Because the solution recognizes files by content rather than by name or location, you can manage different versions of applications as different files. As a result, you cannot only control which applications are allowed but also which versions.

For example, you may decide that an older version of an application is valid up to a certain date. Old and new versions are valid during a transitional period, and only the new version may run after a designated date.

- > **Reduced total cost of ownership** — Is your organization buying software licenses on a per-computer basis rather than a per-user basis? Are you, therefore, paying for idle computers, or duplicate licenses for a single user, just to ensure compliance with software licensing terms?

If so, then you will appreciate the ability to manage application access at the user level. Since you always know exactly how many users are authorized to use each application, you can reduce the total number of licenses: one per user instead of one per computer.

- > **Preventing the installation of undesirable programs** — Not only does Sanctuary stop undesirable programs from running — in most cases, it prevents them from even being installed. That is because the installation program itself is an executable file. It does not run, because it is not authorized.
- > **Easy installation** — Despite being an extremely powerful security tool, Sanctuary is simple to install. A wizard guides you through the installation process, prompting you for any information required.
- > **The ability to grant or revoke access on the fly** — The administrator may grant or revoke access to executables, scripts and macros 'on the fly'. Users do not have to reboot or log off and then log on again for the changes to take effect.
- > **A log trail of all system activity** — Each time a user requests to run a file, a log entry is created. The File Group assignment details for the respective files can be accessed and maintained — if required — directly from the log.
- > **Integration with industry standard databases** — Sanctuary integrates with the powerful Microsoft SQL Server and MSDE databases, which offer speed, security, robustness, and interoperability with other applications. With these databases, there is virtually no limit to the number of servers and/or computers that can be protected.
- > **Non-stop protection** — Although Sanctuary is a network-based solution, its power extends to off-line systems as well. Whenever a server or computer is connected to the network, Sanctuary sends the latest authorization information. If that machine is later isolated from the network—intentionally or otherwise—it is



still managed by the authorization information stored in a secure location on its hard disk. Whenever the computer is reconnected to the network, it automatically receives an update.

- > **The ability to manage applications by their locations** — Their unique digital signatures (hashes) identify most executable files, but you can also inform the program that all files in secure locations are inherently safe. 'Path rules' enable you to define approved applications based on their location rather than on binary hash calculations.
- > **Provisional and limited local override of application denial** — You can opt to allow users to authorize an application locally if it is not on the centralized master list of previously approved executables, scripts and macros. The system displays its characteristics and potential security risks, grants provisional access, and logs the activity. To prevent the spread of malicious code, such as Trojan horses, the system can automatically disable the application if it appears on a certain number of computers in a given period.
- > **Protection from unauthorized scripts** — Optionally, Sanctuary can control the execution of VBScripts, Microsoft Office VBA macros, and JScripts. Depending on the settings, the execution can be authorized, prevented altogether, or the user can be prompted with a dialog every time a script attempts to execute on his computer.
- > **Windows Server Update Services support** — You can deploy automatic update services inside your own network: All Microsoft Authorized updates and fixes can be automatically authorized, their hash created, and the database updated.
- > **Encrypted client-SecureWave Application Server communication using TLS protocol** — Client driver-SecureWave Application Server and intra SecureWave Application Server communication can, optionally, be done using TLS protocol which encrypts all communications using a certificate signed with a private key. If this option is not activated, communication messages are signed using the private/public key pair generated during setup. See the *Sanctuary's Setup Guide* for a complete description.

Rest easy. You have Sanctuary.

Chapter 2: Using Sanctuary Application Control Suite

This chapter provides a high-level view of what it is like to work with Sanctuary. It includes:

- > The administrative tasks that determine system operation.
- > The menu selections available to authorized administrators.
- > The six key modules of the Sanctuary management console.

What is new in this version

See the *Readme.txt* file located on your CD installation disk for a full list of features and changes.

Working with the Sanctuary Application Control Suite system

From the Sanctuary Management Console, you can perform all the tasks required to configure, monitor, and maintain the solution — its database records, executable files, authorizations, and system activity.

Using a familiar Windows-styled interface with pull-down menus, pop-up dialog boxes, and Outlook-style screen displays, you can easily perform the following tasks:

- > Build a list of executable files, scripts and macros that you wish to allow.
- > Define authorizations for the identified executable files (applications), scripts and macros.
- > Organize files into File Groups and manage those File Groups. You can also create a parent-child relationship easing the task of classifying all the applications that use common components.
- > Define individuals and groups who have permission to use applications.
- > Associate File Groups with User Groups to define access privileges.
- > Manage and maintain the database of authorizations.
- > Monitor a record of system activity and settings.
- > Set and change a variety of system options.

If you have already installed solution components by using the simple installation wizards or following the steps in the Sanctuary's Setup Guide, then you are ready to get going.

Starting up the Sanctuary Management Console

As with nearly all Windows programs, you start the Sanctuary Management Console by clicking on the Windows START button and selecting *Programs* → *Sanctuary* → *Sanctuary Management Console*. You can also create a shortcut in Windows desktop for your convenience.



Connecting to a server

When you initially launch the Sanctuary Management Console, you need to connect to a SecureWave Application Server. The *Connect to SecureWave Application Server* dialog is displayed.

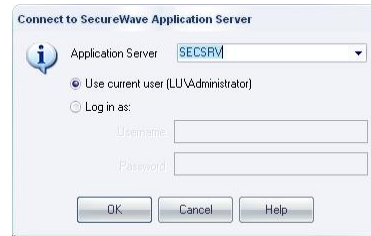


Figure 1. Connecting to the SecureWave Application Server

To connect to a server, follow these steps

1. Select the SecureWave Application Server to which you want to connect from the list (if available) or type in the name. You can use the IP address, the NetBios name or the fully qualified domain name of the SecureWave Application Server. If your Server is configured to use a fixed port, you must append the port number to the server name as in this example:

```
secrsrv.secure.com[1234]
```



Please refer to the description of the registry key settings of the SecureWave Application Server in the Sanctuary's Setup Guide for more information about how to configure the server to use a fixed port.



When the SecureWave Application Server is installed on a Windows XP SP2 or Windows 2003 SP1 computer, you should configure the Windows XP Firewall to allow the communication between the Server and the Console. See Appendix E in the 'Sanctuary's Setup Guide for more details.

2. Select to login as the current user or as a different one using the *Login as* option.
3. Click on the OK button. The Sanctuary Management Console screen appears, as shown on *Figure 3*.

If the Sanctuary Management Console screen does not appear, an error message is displayed. This indicates that there were problems when all the internal tests were carried out. Check that you have the required permissions to connect to that server, on domain rights and Sanctuary Management Console rights level. See *Chapter 4: Setting up Sanctuary administrators* on page 29.

Log in as a different user

By default, the system establishes the connection using your own credentials.



A local account is created on a single computer and is stored in its Security Account Manager (SAM) database on its hard disk. Domain accounts are created on the domain controller and stored in the Active Directory. To log onto the local machine, you need a local account. To log onto the domain you need a domain account.

If you choose to click on the *Login as* option, instead of using your own credentials you must enter the user name and password. Prefix the user name by a workstation name and slash for local accounts and by a domain name and slash for domain accounts (e.g. DOMAIN1\ADMIN1).

Once the connection established, the user's credentials are shown in the *Output* panel while the *Connection* panel show the license details. If you do not see these windows, select the VIEW → CONNECTION and/or VIEW → OUTPUT command:

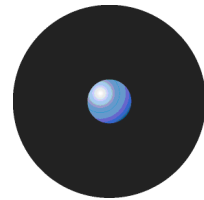


Figure 2. Connection and Output window

The Sanctuary Management Console

When you log onto the Sanctuary system, the system displays the program’s user interface. From this screen, you are only a click or two away from the full range of configuration and management functions. Take a moment to get familiar with the menu selections, tools, panels, and modules available from this screen as shown in the following image.

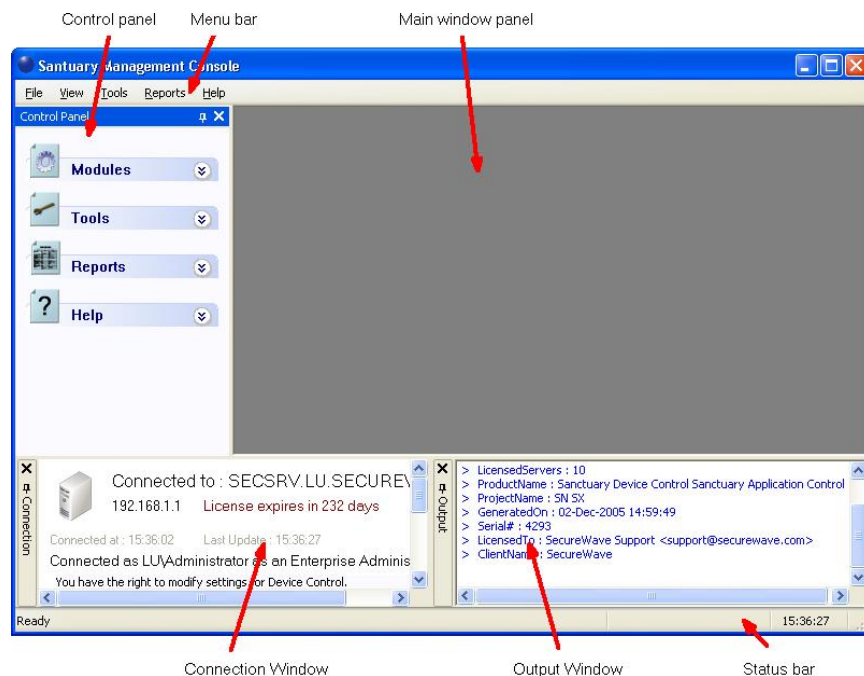


Figure 3. The main screen

The *Menu bar* in the upper part of the window let you choose different functions and commands. Some of these depend on the module you are working with. As with nearly all Windows programs, you can use the ALT key to have immediate access to the different commands. You can use, for example, Alt+R+O to get an HTML Online Machine report.

In the left part of the window, you find the *Control Panel* from where you can directly select the available modules and options without using the menu. If you do not see it, use the *View → Control Panel* command to display it.

The *Main Window panel* changes its contents depending on the module selected on the left panel. You can refine even more the resulting information in some modules. Every time you open a module, its stays open — arranged in stacked tabs — until explicitly closed. You can use the *Window* command of the menu bar to organize your workspace.

The *Connection window* shows rights information regarding the current user. Use the sidebars to navigate through the text. If you do not see it, use the *View → Connection* to display it.



The *Output* window shows you important information messages. Here you can find those messages generated by updates sent to the clients, file fetching, I/O failures, and error messages. Use the sidebars to navigate through the text. If you do not see it, use the *View* → *Output* command to display it.

The *Status bar*, at the bottom of the screen, shows important information about the condition of the console. If you do not see it, use the *View* → *Status Bar* to display it.

If you are using a time-limited license for Sanctuary then once a day, when starting the management console, you get the following screen informing you of your license status:

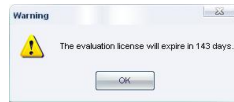





Figure 4. License status warning

This dialog contains the same data reported to the Connection window in the main screen. This event also generates a log that you can see using Windows Event Viewer.

Controlling your workspace

You can use the Pin icon  to 'pin down', or 'park' the *Control Panel*, *Connection*, or *Output* window. The icon changes to . The alternative is to 'float' the window, in which the icon changes to .

In the *Dock* mode, the panel hides itself as a tab next to the program's window border leaving more space for the main window panel. In the *Floating* mode, the windows can be moved to any position in the screen, sharing the working area with whatever module(s) is opened.



Figure 5. Docked Control panel



Figure 6. Docked window

Click again on the pin to 'float' again the window panel.

You can resize and drag the windows panes to whatever zone you prefer as in the following example:

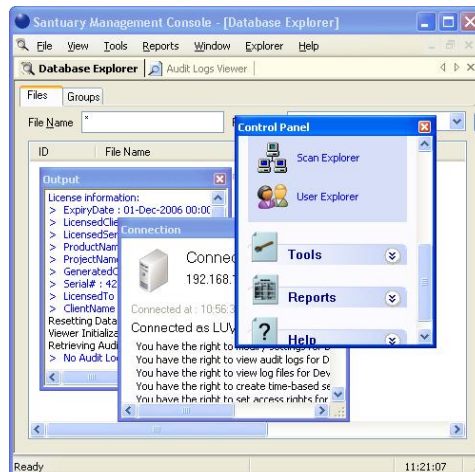


Figure 7. Floating Control panel

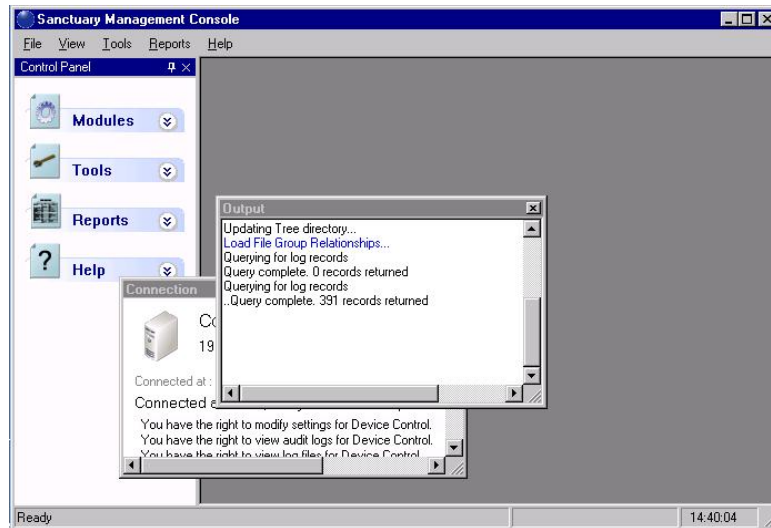
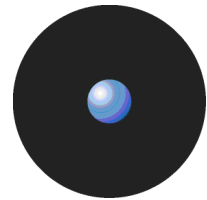


Figure 8. Floating windows

Double click on the window's title bar to dock it to its previous position once more. You can also glide the window to any edge until it docks itself — guide yourself with the rectangle shape preview before letting go the mouse button.

All open modules occupy the main window area and can be 'floated' or 'docked' at will. You can use the *Window* menu to arrange the opened module's windows in a tile, cascade, or iconize mode. Each window can also be closed, maximized, or iconized independently as needed. If several modules are already open (as shown in *Figure 7*), you can choose between them using the stacked tab bar.

You can reorder the windows located at the main window panel by dragging them using their title bar, or traverse them using the *Scroll Left* or *Scroll Right* icons ◀ ▶.

To close the active window, click on its cross icon, right-click on the title bar and select *Close*, or press Ctrl+F4.

To minimize a window, right-click on the title bar and select *Minimize*. You can also use the *Restore* and *Maximize* icons and commands as on any Windows program.

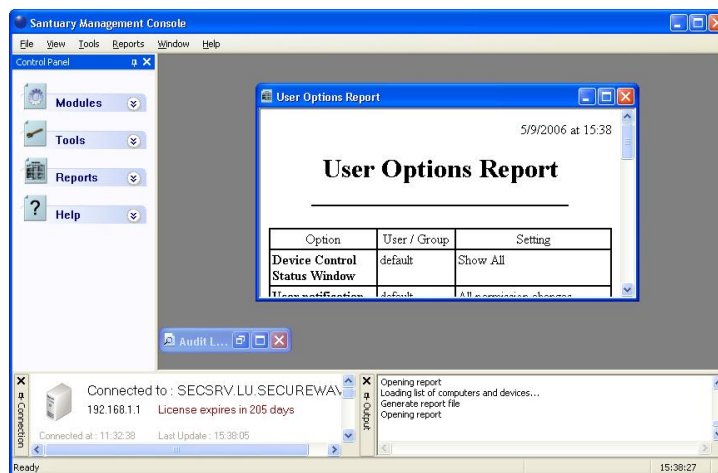
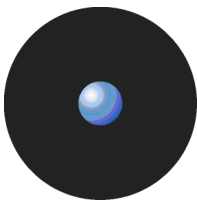


Figure 9. Minimized windows



The Sanctuary Application Control Suite modules

The functions you need for configuring and managing Sanctuary are grouped into six modules, represented by the icons in the *Modules* section of the *Control Panel* (usually located on the left side of the screen):

<i>Module</i>		<i>Use to...</i>	<i>See page</i>
<i>Database Explorer</i>		View the list of executable files, scripts and macros that have been entered into the SecureWave Sanctuary Database and manage file assignment details.	91
<i>Exe Explorer</i>		Build a list of executable files, scripts and macros that are allowed to run, assigning these files to File Groups.	36
<i>Log Explorer</i>		View logs of applications, scripts and macros that have been run, those to which access was denied, or those locally authorized after denial. If you are an Enterprise Administrator you can also view information about Administrator actions from the Audit logs.	67
<i>Scan Explorer</i>		Scan a computer or domain to identify executable files, scripts and macros that need to be authorized, and assign the files to a File Group.	39
<i>User Explorer</i>		Align users or User Groups with File Groups, to grant them permission to use the files in the File Groups.	61

Table 1. The System Modules

The procedure for assigning files to File Groups is the same, irrespective of which module you use. This is explained in *Chapter 6: Organizing files into File Groups* on page 47.

Detailed information about how to use these modules work is given in the following chapters.

The Sanctuary Management Console menus and tools

This section describes all the commands you can directly access using the *Menu bar*.

File menu

The *File* menu (on the menu bar), gives you a one-click access to the following functions:

<i>Option</i>	<i>Use to...</i>
<i>Connect</i>	Communicate with another SecureWave Application Server in other machine or/a different user name in order to carry out administrative tasks.
<i>Disconnect</i>	Detach from the current SecureWave Application Server. You need to do this in order to reconnect using a different user or server.
<i>Save As</i>	Save the contents of the main page in CSV format (only available for specific modules). You can use it to export data to any CSV compliant program, for example Excel.
<i>Print</i>	Print the active report window. You get the standard Internet Explorer print dialog where you can choose the printer and select several printer options.
<i>Exit</i>	Exit from the Sanctuary Management Console application. Note that this command does not stop the SecureWave Application Server, just your administrative session.

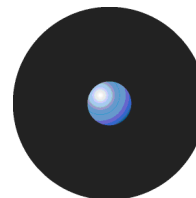
Table 2. The File Menu

View menu

The *View* menu contains the following functions that regulate the appearance of the on-screen display:

<i>Option</i>	<i>Use to...</i>
<i>Modules</i>	Show a submenu that allows you to select any available module.
<i>Control Panel</i>	Show/hide the Control Panel that allows you to select modules, tools, reports, and help from a convenient list.
<i>Output</i>	Show/hide the Output window (log of system activity).
<i>Connection</i>	Show/hide the Connection window (real-time operating information).
<i>Status bar</i>	Show/hide the status bar (program's conditions, clock, and messages).

Table 3. The View Menu



Tools menu

The *Tools* menu (on the menu bar), gives you one-click access to the following functions:

Option	Use to...	See page
<i>Synchronize Domain Members</i>	Update the SecureWave Sanctuary Database with the current list of users and groups of a domain or machine.	93
<i>Database Maintenance</i>	Delete log files and items generated from a database scan created before a specified date.	94
<i>User Access</i>	Define Sanctuary Enterprise Administrators and Sanctuary Administrators. It allows you to restrict the right to set permissions, view the audit information about Administrators actions or the shadowing information. See Sanctuary's Setup Guide to learn how to set rights to control Organizational Units/ Users/ Computers/ Groups	29
<i>Default Options</i>	Change the default option settings for computers.	105
<i>Path Rules</i>	Use path locations and file 'owners' to define which applications can run.	55
<i>Spread Check</i>	Prevent the spread of self-propagating code by disabling suspicious executables that have been locally authorized on too many computers.	27
<i>Send Updates to All Computers</i>	Dispatch the latest setting and permission changes to all computers in the SecureWave Application Server(s) online table(s). Changes can be sent in synchronous or asynchronous mode	27
<i>Send Updates to</i>	Transmit the latest setting and permission changes to one or more selected computers.	27
<i>Import Standard File Definitions</i>	Import files and their hash definitions for any server platforms supported by the Sanctuary solution (Windows 2000/XP/2003 and Vista). When you initially install Sanctuary, you can also install some file definitions. You can find new ones on our Web site: www.securewave.com .	34
<i>Export Settings</i>	Export all file permission settings to an external file that can be used to import in a client or to deploy the client component with predefined permissions. See also the Sanctuary's Setup Guide.	33
<i>Purge Online Table</i>	The SecureWave Application Server keeps a record of the connected clients. Sometimes, clients are disconnected without notifying their server that they are not available anymore. In this case orphan entries are left in the online table affecting the performance of the 'Send Updates' functionality. When you purge the online table, the SecureWave Application Server erases all information it has regarding connected clients. Every time a user logs on/off or unlocks his station the online table is modified.	95
<i>Endpoint Maintenance</i>	Create and save maintenance 'tickets' for computers/computer groups allowing protected files and/or registries to be modified. See next section for an explanation.	19, 106

Table 4. The Tools Menu



You can also find all these commands in the *Tools* module of the Control Panel.

Sanctuary keeps a copy of the users' information in its database. When a new user logs on Sanctuary stores their Security Identifier (SID) but not their name. The same applies when you add a new computer to the domain: Sanctuary identifies the computer and stores its name in the database. For performance reasons, new user's names are not resolved during logon but require an explicit synchronization (*Tools*→*Synchronize Domain Members*). The synchronization process depends on whether the protected computers are in a domain or a workgroup.

Endpoint Maintenance

When the client driver starts, it generates a 15-byte random value used for protection purposes. This key — which we call Salt — is used to guarantee that only authorized processes/users can do maintenance. The *Endpoint Maintenance* dialog is used to create and save a 'ticket' for this service. This provisional permission to modify, repair, or remove the client driver, registry keys, or special directories, can be sent to computers or users.

This key value works in conjunction with the *Client Hardening* value established in the *Default Options* dialog (see *Default options* on page 106). If the client hardening option is set to 'Basic' you do not need salt. If the client hardening option is set to 'Extended' you need to enter or query the salt and relax the protection using the endpoint maintenance. The generated 'ticket' can be saved and transported to the client computer(s) by any available mean (shared directory, email, or removable device).



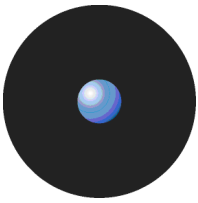
Do not use the 'Send to' right-click menu option to transfer the Maintenance ticket file, use Copy and Paste instead.



If the client machine is not reachable, you can always get the 'salt' value and 'hardening' status of the client computer by right-clicking its Sanctuary Client Driver's icon — located on the system bar — and selecting 'Endpoint Maintenance' from the context menu.



You must enable the 'Remote Registry' service on Windows Vista machines if you want to query the 'Salt' value using the Sanctuary Management Console. This service is disabled by default in this operating system. A workaround is to ask the user to provide this value.



Client ticket rules

The client ticket follows these rules:

1. The maintenance ticket is unique and per machine. You cannot generate the same ticket for several computers (even though you are allowed to do so if the client hardening option is set to 'Basic').
2. A validity period can be defined for the ticket. After this period, if the ticket has not been accepted it is no longer accepted by clients. Once the ticket is accepted, there is no time limit for its use. To deactivate the ticket you must reboot the machine.
3. If the maintenance ticket is generated for a specific user, this user must be logged to accept it. If this is not the case, the ticket is rejected.
4. If you choose to 'relax' the client hardening value by creating and using a maintenance ticket for a computer without choosing a user and another user logs into the same machine, the computer continues in a 'relaxed' state until the next reboot.
5. Your comments appear on the audit log. You can review them by using the *Log Explorer* module (see on *Chapter 9: Monitoring activities using the Log Explorer* page 67).



The client protection mechanism can also be temporary deactivated when using the Client Deployment Tool. The protection is reactivated — and reset to its previous setting — after the client's reboot. Please consult the Sanctuary's Setup Guide for more details.

To create and save maintenance 'tickets' for endpoint machines/users

1. Select the TOOLS → ENDPOINT MAINTENANCE item from the menu bar (or the *Control Panel*).
2. Select the salt value. (If the client hardening option is set to 'Basic' you do not need salt. If the client hardening option is set to 'Extended' you need to enter or query the salt for the machine you are using to relax.) Use the QUERY button to obtain the salt value directly from the client computer. Use the right-click context menu of Sanctuary Client Driver's icon when the machine is not connected to the network.
3. Select the validity period for the ticket.
4. Select the user(s) and/or computer for which this 'ticket' is valid.
5. Add any valuable comments in the corresponding field.
6. Click on the SAVE button, choose a suitable location, click on SAVE and then on CLOSE.

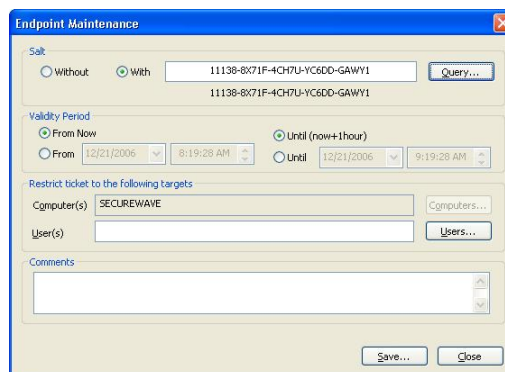
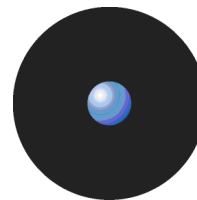


Figure 10. Endpoint Maintenance

You can save this ticket (ticket.smt) and transfer it to selected computers by means of an email or external device — the machine(s) needs to have the required permissions to access the device if using *Sanctuary Device Control*. You can also save directly to the 'ticket' directory of the necessary online machine. This 'maintenance ticket' must then be copied to the predefined ticket directory in the client computer(s). See the *Sanctuary's Setup Guide* for a description of the registry keys. As previously explained, this ticket also depends of the *Client Hardening* option value.



Reports menu

The *Reports* menu (on the menu bar), leads to the following functions:

Option	Use to...	See page
<i>File Groups by User</i>	Select one or more Users and/or Groups and generate a report of the File Groups they may use.	98
<i>Users by File Group</i>	Select one or more File Groups and generate a report of the Users and Groups given access to them.	99
<i>User Options</i>	Display all the user options defined in the system.	100
<i>Machine Options</i>	Display all the computer options defined in the system.	101
<i>Online Machines</i>	Show all machines currently recognized by the SecureWave Application Server that you are connected to.	102
<i>Server Settings</i>	Find out how your SecureWave Application Server(s) is configured. This is provides you with very useful configuration and troubleshooting information.	103

Table 5. The Reports Menu



In addition to the standard reports that are available through the Reports menu, you can define your own criteria for selecting log entries and producing reports using the Log Explorer module. For more information see Chapter 9: Monitoring activities using the Log Explorer on page 67.

Explorer menu

The *Explorer* menu (on the menu bar) changes depending on the module you are using (as selected in the *View*→*Modules* menu or using the *Control Panel*).

Option	Use to...
In the Database Explorer module	
<i>Assign</i>	Change the File Group to which a file is assigned.
<i>Manage file groups</i>	Add, rename and delete a File Group. See page 47 for more details.
<i>Choose columns</i>	To organize the panels' columns
In the Exe Explorer module	
<i>Map Network Drive</i>	Assign a drive letter (map) to any shared resource on a network. Doing this, you can quickly and easily access the resource by using the letter instead of a full path qualifier.
<i>Disconnect Network Drive</i>	Remove the letter assignment from any shared resource on a network. This is the opposite operation than that done with the <i>Map Network Drive</i> command.
<i>Assign</i>	Change the File Group to which a file is assigned.
<i>Manage File Groups</i>	Add, rename, and delete a File Group. See page 47 for more details.
<i>Choose columns</i>	To organize the panels' columns.
In the Log Explorer module	
<i>Fetch log</i>	Obtain the latest log from a client computer. See page 87 for details.
<i>Manage File Groups</i>	Add, rename, and delete a File Group. See page 47 for more details.
In the Scan Explorer module	
<i>Perform scan</i>	Scan a computer to identify executable files, scripts and macros that need to be authorized.
<i>Select scans</i>	Choose the two scans you want to compare.
<i>Assign</i>	Change the File Group to which a file is assigned.
<i>Manage File Groups</i>	Add, rename, and delete a File Group. See page 47 for more details.
<i>Choose columns</i>	To organize the panels' columns.
In the User Explorer module	
<i>No options are available in the Explorer menu for this module.</i>	

Table 6. The Explorer Menu



Window menu

The *Window* menu controls the navigation and display of various elements of the Management Console window:

Use this option	To
<i>Cascade</i>	Place all open windows in an overlapping arrangement.
<i>Tile</i>	Lay all open windows side by side in a non-overlapping fashion.

Table 7: The Window menu items

Help menu

The Help menu gives you handy access to on-line help.

Use this option	To
<i>Help</i>	Access context-sensitive help. You can also use the shortcut function key F1.
<i>Contents</i>	View the Help file by contents.
<i>Search</i>	Search for a specific topic in the Help file.
<i>Index</i>	Go directly to the help's index page.
<i>About</i>	Display information about your installed version of Sanctuary.
<i>SecureWave on the Web</i>	Go to the SecureWave's home page, where you can find up-to-date information, resources, support, etc. about this and other useful products.
<i>SecureWave Knowledgebase</i>	Direct access to SecureWave's knowledge database. An invaluable source of tips, questions and answers, and how-to articles.

Table 8. The Help Menu

Chapter 3: An overview of authorization strategies

Sanctuary protects your organization's servers and computers by permitting only authorized applications to run on them — unknown executable files that are not required for the authorized applications (or the operating system) are blocked by default. In addition, Sanctuary can also protect your system from running many unauthorized scripts and macros (as these contain commands that are interpreted either by host applications running on the computers, or the Windows operating system itself — even though they are not Win32 executables).

The Sanctuary system offers several strategies for managing the running/blocking of executables, scripts and macros. These include:

- > **Central authorization using digital signatures.** This is the main method used to secure your servers and computers against unwanted executables, scripts and macros — known or unknown. Your organization centrally manages authorizations by establishing a list of the executables, scripts and macros that are specifically approved by an authorized Sanctuary administrator (in a 'white list') and checking whether the digital signatures ('hashes') of files users want to run are in this list.
- > **Central authorization by file location (path).** This enables you to control executable files for which digital signatures are not useful or applicable. You can establish Path Rules to handle exceptions, for example, auto-changing executable files. You can also define Trusted Owners to reinforce security.
- > **Local authorization.** You can choose to grant some local users limited rights to authorize additional executables, scripts and macros — unknown files that they may require for their work.

Most executable files can be identified by their file extensions. File extensions such as .exe, .com, .dll (dynamic link library), .cpl (control panel), .scr (screen-saver), .drv, and .sys (system driver) normally denote executable files. When deciding whether a file is authorized to run Sanctuary does not rely on file extensions but lets the operating system determine whether a file is an executable. If so, Sanctuary checks whether the digital signature of the file is listed in its 'white list' of allowed files (in the case of central authorization using digital signatures).

Scripts and macros are more difficult to identify than executables. Sanctuary can only recognize, and centrally manage, the following types of scripts and macros:

- > VBScripts and JScripts that are interpreted by the Windows Script Host (using `cscript.exe` and `wscript.exe`). These scripts are text files written using the grammar and semantics of the appropriate language. To be recognized by Sanctuary your script files must have the appropriate file extension — either .vbs or .js.

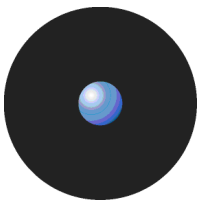


File names are only available for scripts interpreted by `cscript.exe` and `wscript.exe`. This means, for example, that Java scripts executed by Internet Explorer cannot be centrally managed.

- > Visual Basic scripts (VBA macros) that execute within Microsoft Office and other host applications. These are embedded in Word documents, Excel spreadsheets, and so on.

Sanctuary also contains a mechanism to prevent the malicious spread of locally authorized files. If it detects that an unknown executable, script or macro has been locally authorized on a certain number of servers or computers within the defined period, it can disable the executable and the local authorization capability.


We take a closer look at the various authorization strategies in the following sections.




Central authorization using digital signatures

The primary, and most powerful, method that Sanctuary uses to control executable files, scripts and macros involves identifying individual files that a user wants to run based on their digital signatures. Sanctuary either blocks these or allows them to run depending whether the files are in an authorized 'white list' and whether the user (or user group containing the user) has been granted to the right to run them.

Central authorization using digital signatures typically controls all the applications required to manage and maintain the organization's servers (including the operating system itself), and applications and scripts that are specific to your business.


 *Previous versions of Sanctuary did not let administrators authorize scripts and macros using digital signatures — only executable files.*

 *Central authorization using digital signatures works in combination with local authorization of executables, scripts and macros, and the 'Execution blocking' and 'Macro and Script protection' options to either grant or deny authorization for a particular executable file, script or macro. Also see Local Authorization on page 109, and Macro and Script protection on page 112.*


Central authorization of executables, scripts and macros using digital signatures involves the following steps:

1. **Building a list of executables, scripts and macros that are authorized to run.** This list can be assembled by running a scan of target systems (using the *Scan Explorer*), by searching designated directories (using the *Exe Explorer*), or by using the Authorization Wizard, the *Log Explorer*, or the Versatile File Processor Tool. See *Chapter 5: Building a white list of authorized files* on page 33.
2. **Creating a unique digital signature for each approved executable, script or macro.** Sanctuary examines the binary contents of the executable files, scripts and MS office macros, calculates a 20-character alphanumeric digital signature (or 'hash'), and records this information in a central repository.

The list of centrally authorized executables, scripts and macros is the 'white list' of programs trusted within your organization, and that you want all or some users/user groups to be able to run at any time.

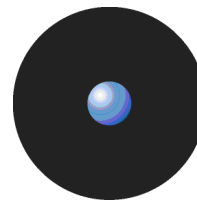
 *Visual Basic scripts (VBA macros) can be embedded in many Microsoft Office formats, such as .doc, .dot, .xls, and .ppt files. In this case, a hash is created for the whole file, not just the macro.*

3. **Organizing approved executables, scripts and macros files into File Groups.** An authorized Sanctuary administrator assigns the files identified in step 2 to particular File Groups, such as 'Windows Operating System'. This simplifies the administration of related and/or interdependent files.
4. **Associating File Groups with users or user groups.** An authorized Sanctuary administrator then determines which users, and/or user groups, have access to which File Groups. This means that a particular user can only run a particular application, script or macro if they have the appropriate privileges to do so.
5. **Downloading authorization information to protect your computers.** The digital signatures of centrally approved files are downloaded to each user's machine and stored in a secure location on their local hard drive. Sanctuary references this locally stored authorization list whenever the user (or a server administrator) attempts to launch an executable file or run an identifiable script or macro.

 *It is particularly important to centrally authorize operating system files and driver files (such as the video card user interface, *atiptaxx.exe*) that execute before the user logs on.*

You can set up and maintain the white list of files Sanctuary uses for central authorization using:

- > The Database Explorer module (see *Chapter 10: Managing files using the Database Explorer* on page 91).
- > The Exe Explorer module (see *Selecting files to authorize using the Exe Explorer* on page 36).
- > The Log Explorer module (see *Using the Log Explorer module to authorize unknown files* on page 87).
- > The Scan Explorer module (see *Using the Scan Explorer module* on page 39).



— or —

- > Authorization Wizard, FileTool.exe, or the AuthSrv.exe tools (see *Using the Authorization Wizard* on page 42).

For more information see *Chapter 5: Building a white list of authorized files* on page 33.

Central authorization by file location (path)

For a small number of applications, security based on file hashes simply does not work. For example, some executables are modified as part of the installation procedure, typically to embed licensing information. In some cases, internal applications change frequently, however you trust the modified files, as they are run under the control of trusted administrators.



You cannot authorize scripts and macros by file location (Path Rules) — only executable files.

To allow for applications of this sort, Sanctuary lets you to authorize all executables that run from a specified location, determined by the path of the file: Executable files in the specified directory location are exempted from normal hash checking. They are presumed to be from a trusted source, so they are allowed to run.

To add a layer of protection to this type of authorization, you can have the system check the identity of the file's owner — and only execute files that belong to trusted owners.

Central authorization by file location is set up using the *Path Rules* option of the *Tools* menu (or from the *Control Panel*). See *Chapter 7: Authorizing files by location (Path Rules)* on page 55 for more information.

Local authorization of executables, scripts and macros

Local authorization relies on local users' discretion to determine for themselves at the time of running a file, whether it should be allowed or denied. By default, Sanctuary does not permit users to perform local authorization. Occasionally however, you may wish to give a user the right to locally authorize an application required for their productivity, such as to run a special executable, macro or script once.



In order to permit local authorization of executables, scripts and macros the 'Local Authorization', 'Execution blocking' and 'Macro and Script protection' options must have the required values. See Chapter 12: Setting Sanctuary system options on page 105.



*For a user to be asked if they want to authorize or deny an executable, script or macro, the file must be assigned to a File Group **and** the user must be assigned permission to use files in that File Group (either explicitly as a user, or through membership of a User Group).*



Sanctuary contains a spread check mechanism to prevent the malicious spread of locally authorized files. If Sanctuary detects that an unknown executable, script or macro has been locally authorized too many times within the defined period, it disables the local authorization capability and the executable.



When a user creates or records a new macro in Microsoft Office (i.e. not by loading it from a file), the macro is not intercepted and the user can run it without notification.

Local authorization of files that are not centrally authorized

Let us consider the situation when a user attempts to run an executable, script or macro that has not been centrally authorized, i.e. whose digital signature (hash) has not been included in the white list of files that are authorized to run (provided the user has the appropriate permissions).

We also assume that:

- > The *Local Authorization* option (see *Local Authorization* on page 109) has an 'Enabled' value either by default (for all machines) or for the specific computer on which the user wants to run the file.



— and —

- > The *Local Authorization* option has not been disabled because the *Spread Check* mechanism is enacted to stop self-propagating code. See *Preventing the malicious spread of locally authorized files* on page 27 for more information.

— and —

- > The *Execution Blocking* option has a value of 'Ask user for *.exe only' or 'Ask user always' either for the user, one of the groups of which he is a member, specific computer on which the user wants to run the file, or by default (for all users or machines). See *Examples of the precedence of Execution Blocking options* on page 121 for more information.

In addition, in the case of a script or a macro, the *Macros and script protection* option must either have a value of 'Ask User' or 'Disabled' either for the user, one of the groups of which he is a member, or by default (for all users).

When the user attempts to execute a file that is not centrally authorized the following takes place:

1. The user gets an alert message explaining that the executable, script or macro has not been centrally authorized. This alert message emphasizes the potential risks of authorizing this file and displays details about it, such as its path, internal name, filename, description, and alleged source of origin.

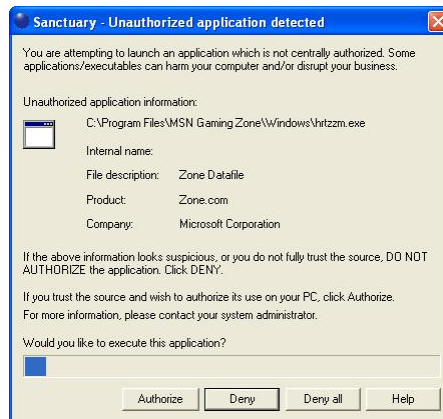


Figure 11: Local authorization dialog

2. Within the alert dialog, the user can then choose one of the following actions:
 - > *Authorize* — To allow the script or macro to execute for this one time and one computer only. Once authorized, this prompt does not appear again.
 - > *Deny* — To prevent the execution, as the source of the executable, script or macro is not fully trusted.
 - > *Deny all* — To prevent execution of this and future scripts and macros.



You can reset the 'Deny all' local authorization setting, if required, by right-clicking on the Sanctuary Client icon in the system tray of the machine running the client and selecting the option in the context menu.

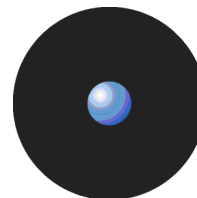


If the user does not respond within the time-out period (two minutes by default), the dialog automatically disappears and the file is denied.



Some applications, such as Windows Media Player, start several scripts when they are loaded. The user is prompted for each script launched by the application if the 'Ask User' option is set.

Whether the executable is authorized or denied, the Sanctuary system logs the action.



Preventing the malicious spread of locally authorized files

Sanctuary contains a mechanism to prevent the malicious spread of locally authorized files. If the Sanctuary system detects that an unknown executable, script or macro has been locally authorized on a certain number of servers or computers within the defined period, it immediately disables the executable and the local authorization capability. This does not disable the already running authorized executables, however self-propagating viruses and worms are stopped in their tracks.



If you have more than one SecureWave Application Server on your network, only one of them should be assigned the job of spread checking.

To set up spread checking:

1. Select *Spread Check* from the *Tools* menu (or from the *Control Panel*). The system displays the following dialog.

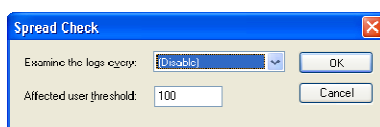


Figure 12. Spread Check dialog

2. Select how frequently the system should check activity logs for suspicious propagation of locally authorized files, for example, every 5 minutes or 15 minutes.
3. Enter the number of users that, if locally authorizing a particular unknown executable, script or macro, triggers the spread checking mechanism. This threshold of suspicion is, by default, set to one hundred users.
4. Click on OK.

Once the Sanctuary administrator has investigated the reason why the spread check mechanism was triggered, and possibly cleaned up any infected machines, local authorization can be turned back on.

Deleting user's local authorization lists

Although local authorization should only be granted to trusted users, there are situations where you may want to delete the list of all the applications that the user has locally allowed to run. This can arise because:

- > You decide that if a user really needs an authorization, it is your job to authorize it centrally, regaining control.
- > Your company's policies have changed and all authorization is to be strictly controlled.
- > You no longer trust a particular individual.
- > The user made a mistake and wants to 'un-authorize' an application.

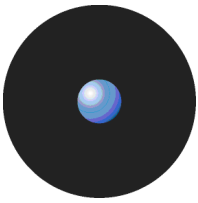
All local authorizations are kept in a local file located in the %WINDOWS%\sxddata folder. To 'un-authorize' all locally authorized applications, simply erase all .locauth files located in this directory. You can either do this on a per-user basis or delete them at every startup by defining a task in the Windows Scheduler (a simple batch file does the job).



An administrator or a 'normal' user cannot erase these files if the hardening option is activated. You need to emit a Maintenance Ticket or disable the Client hardening option for the machine.

Alternatively, you can disable all previously user-authorized executables, scripts or macros as follows:

1. Create a File Group called 'Not allowed' or similar.
2. Add all applications that should not be allowed to this new File Group.
3. Do not assign this File Group to any user/user group.
4. Send updates to all computers.



Since this File Group has not been assigned, it supersedes local authorization and, thus, disables all previously user-authorized programs — see *Local Authorization* on page 109.

Sending updated authorization information to computers

When you change any system setting — options, parameters, file authorizations, etc. — you must distribute these changes to servers and computers protected by the Sanctuary system. If you do not push updates to computers, they are automatically downloaded whenever a server or computer logs on to the network.

To push updates to all computers protected by Sanctuary

If you want to update all computers running the Sanctuary Client, simply select *Send Updates to All Computers* from the *Tools* menu (or the *Control Panel*). Updates are distributed to all clients in the SecureWave Application Server(s) online table(s). All clients are sent an update signal. The clients that respond to this contact the SecureWave Application Server and get the new hashes.

When you select the *Send Updates to All Computers* option, you are prompted for a decision as to whether to send the updates:

- > Synchronously (if you click on the YES button). Sanctuary may take a long time sending updates and the *Sanctuary Management Console* has to wait for the SecureWave Application Server to finish sending the updates to all machines in the online table.
- > Asynchronously (if you click on the No button). In this case, the *Sanctuary Management Console* does not wait for the SecureWave Application Server to finish and you can continue working while the update is done in the background.

To push updates to a specific computer

To update a specific computer you can either:

1. Activate the *User Explorer* module. To do this, click on the 👤 icon located in the Modules section of the *Control Panel* of the main window or use the *View→Modules* command.
2. Right-click on the target computer.
3. Select *Send Updates to <name>* from the popup menu.

— or —

1. Select the *Send Updates to* item from the *Tools* menu (or the *Control Panel*).
2. Choose the computer you want to update using the *Select Computer* dialog.
3. Click on the OK button to close the dialog and send the updates.

Chapter 4: Setting up Sanctuary administrators

Within Sanctuary, there are two types of administrators:

- > **Sanctuary administrators** have permission to use management functions that affect the operation of the Sanctuary system itself, such as building lists of executable, script and macro files, setting and changing authorizations, and viewing logs of system activity.

A *Sanctuary Enterprise Administrator* has full access to all management functions.

Regular *Sanctuary Administrators* have restricted privileges that are defined in the system by the Enterprise Administrator.

- > **Administrators** have permission to use functions specific to their server or computer software. For instance, your Webmasters would be considered server administrators and be granted access to use applications pertaining to their job functions. They would not be able to modify the operations of the Sanctuary system. In the context of Sanctuary, administrators are only users.

Once an Enterprise Administrator has been defined, he is the only one allowed to assign other users as regular Administrators. This chapter describes the process of setting up administrators to manage the Sanctuary system: an authorized Sanctuary *Enterprise Administrator* and a Sanctuary *Administrator(s)*.

How to set up a Sanctuary system administrator

To protect your security system itself from illegal access, only authorized administrators can access Sanctuary management functions. The use of any of the administration tools requires administrative privileges. Moreover, you must have administrative privileges in order to set up other administrators.

To define a system administrator with full management privileges

1. Select *Tools*→*User Access* from the menu bar at the top of the management console display (or from the *Control Panel*). The system displays the *User Access* dialog shown below.

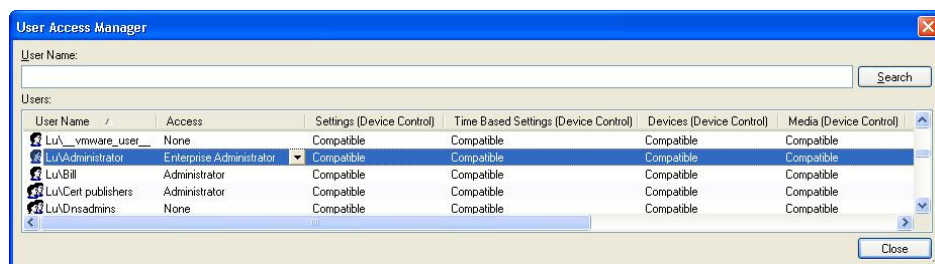
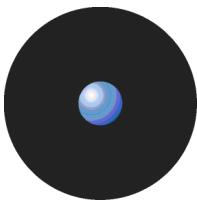


Figure 13. User Access Manager dialog

2. Enter a user name in the *User Name* field.
3. Click on the SEARCH button to locate the user or group to whom you want to grant administrative rights.
4. When that user's name appears in the *Users* list box, select it.
5. Click on the *Access* column and set that user as an *Enterprise Administrator*. This user now has rights to connect to the SecureWave Application Server to manage any object (users, groups, computers, default options, Standard File Definitions, Path Rules, and database maintenance).



By default, any member of the Windows Administrators groups on any SecureWave Application Server has the privileges of a full Enterprise Administrator. However, once you designate an official Enterprise Administrator, access privileges automatically are reduced for the other members of the local Administrators group. These individuals no longer have access to management functions unless specifically authorized.



Since all programs of our suite share the same database, some options you set for the Console users are also enforced for other programs of our Suite. For instance, changing a user from Enterprise Administrator to a 'normal' Administrator for Sanctuary Application Control Suite also changes his role for Sanctuary Device Control.



When adding or removing Administrators from the list, make sure there is always at least one Enterprise Administrator set. Be careful not to block yourself out.

To define a system administrator with restricted access privileges

In the *User Access Manager* dialog, click the *Access* column and set the user as an *Administrator* instead of an *Enterprise Administrator*. This user now has rights to use designated management functions but cannot promote other users to be Administrators or Enterprise Administrators. Be sure to have at least one Enterprise Administrator. Only Enterprise Administrators have access to the *Tools* menu.

To define access privileges to specific functions and modules

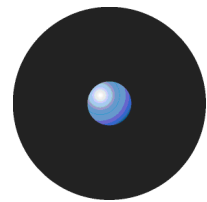
1. In the *User Access* dialog, click the *Settings (App.Control)* header. Set this attribute to:
 - Yes This Administrator can change permissions and system option for the objects for which he/she has write permissions in the Active Directory.
 - No This Administrator can view users' access permissions but not change them, cannot change system options, and cannot authorize applications using the Authorization Wizard.

*Compatible**
2. Click on the *Audit (App.Control)* header. Set this attribute to:
 - Yes This Administrator can view and search audit logs of system activity (in the *Log Explorer*).
 - No This Administrator cannot view or search audit logs.

*Compatible**
3. Click on the *Execution Logs (App. Control)* header. Set this attribute to:
 - Yes This Administrator can view and search execution logs (in the *Log Explorer*) for the objects for which he/she has write permission in the Active Directory.
 - No This Administrator cannot view or search execution logs.

*Compatible**
4. Click on the *Machine Scans (App. Control)* header. Set this attribute to:
 - Yes This Administrator can use the *Scan Explorer* to scan target computers to build lists of approved executable, script and macro files, view the results of scans for objects for which he/she has write permission in the Active Directory, and create new scan templates.
 - No This Administrator cannot use the *Scan Explorer*.

*Compatible**
5. Click on the *Endpoint Maintenance* header. Set this attribute to:
 - Yes This Administrator can issue Endpoint maintenance tickets to user(s)/computers(s). See *Endpoint Maintenance* on page 19 for a complete explanation.



No This Administrator cannot issue Endpoint maintenance tickets.

*Compatible**

6. Click on the *Scheduled Reports* header. Set this attribute to:

Yes This Administrator can create custom reports at pre-scheduled times. See *Schedule tab* on page 85 for a complete explanation.

No This Administrator cannot create custom reports at pre-scheduled times.

*Compatible**

*For all the above options, the default setting is *Compatible*, that is, no restrictions. It is called compatible mode because it is compliant with older versions and useful when upgrading. In compatible mode, there are no restrictions on Administrator roles. For Enterprise Administrators all the attributes appear as *Compatible* — they do not have any restrictions whatsoever.

Chapter 5: Building a white list of authorized files

Sanctuary allows or denies the running of executables, scripts and macros according to your predefined specifications.

Most executable files are identified by their file extensions, for example, .exe, .com, .dll (dynamic link library), .cpl (control panel), .scr (screen-saver), .drv, and .sys (system driver) file extensions normally denote executable files. Sanctuary does not check, or rely on, file name extensions but lets the operating system take care of that. Once the operating system has determined that a file is an executable, Sanctuary then checks the file's signature against its 'white list' of allowed files.

Scripts and macros are more difficult to identify than executables. Sanctuary can only recognize and centrally manage VBScripts and JScripts (.vbs or .js files that are interpreted by the Windows Script Host using cscript.exe and wscript.exe) and Visual Basic scripts (VBA macros) that are embedded in Microsoft Office and other host applications' files.

Sanctuary provides a number of methods that you can use to build a white list of executable files, scripts and macros to authorize. You can:

- > **Import standard file definitions.** This identifies common Microsoft operating system components and applications. Standard file definitions are available on the Sanctuary installation CD, and from our Web site (www.securewave.com).
- > **Select files from your computer directories** and add them to the list of executables that you want to authorize.
- > **Scan each computer** to ascertain which applications, scripts and macros reside on it.
- > **Scan a selected directory of a computer** to identify files to authorize, without unnecessary scanning.
- > **Use the Authorization Wizard** to streamline and automate the scanning process for executables.
- > **Use the FileTool.exe** to scan file locations for executables.



When building a list of executable files (and generating their digital signatures) always use the original media (CD/DVD or downloadable package from the official software vendor) to avoid authorizing executables that have been tampered with or infected.

Sanctuary lets you export a list of file authorization settings from one computer and import these into another computer to update the list of files that are locally authorized to run.

Exporting and importing file authorization settings

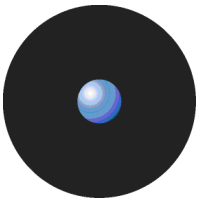
Sanctuary enables you to export a list of file authorization settings, approving a range of executables, scripts and macros, to a file and subsequently import this list onto another computer to synchronize the applications, scripts and macros that can be run on the two computers.

You can also use this feature when a computer is not connected to the network (and cannot be connected for the time being) and you need to change authorizations. The same executable, script and macro authorization rules apply when you import a file of authorizations from the source computer into the target computer.

There is also a special case when you export to a file called 'policies.dat' to install a Sanctuary Client with a set of predefined authorizations. Please consult the *Sanctuary's Setup Guide* for more information.



Files containing exported permissions have a limited usability period of two weeks. After this the file of exported file authorization settings is no longer valid. Contact support if you want to extend the validity of your exported permission files.



To export your file authorization settings from one machine and import them into another:

1. Select the *Export Settings* item from the *Tools* menu (or from the *Control Panel*).
2. Select the name and destination of the settings file in the standard *Save As* Windows dialog. Normally the destination is a network drive or a removable storage device.
3. Go to the client computer where you want to import the permission settings and right-click on the Sanctuary Client Driver icon in the system tray to display a popup menu. The dialog may change depending on your license type and installed programs.

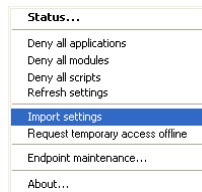


Figure 14: Importing a permission file

4. Select the *Import settings* option.
5. Select the source of the file authorization settings file from the *Import Settings* dialog.

Importing Standard File Definitions

To simplify the building of a white list of executable files, SecureWave provides its clients with a number of ready-calculated *Standard File Definitions* (SFD) files. These contain the hash numbers corresponding to standard executables that are distributed as part of Windows 2000, Windows XP, and Windows 2003 operating systems. Different language versions are available.

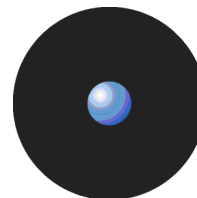
You can use the available Standard File Definitions to simplify the initial setup and maintenance of your Sanctuary system, since they already contain the SHA-1 hash for various operating systems. Standard File Definitions files also include the necessary information to automatically allocate files to predefined File Groups. Standard File Definitions are particularly useful when authorizing product updates such as service packs and 'hot fixes' as they automatically assign the standard hashes to the appropriate File Group.

We recommend that you import Standard File Definitions when you first install your Sanctuary system. For more information, see the Sanctuary's Setup Guide. If, however, the Standard File Definitions are not imported during setup, or you wish to add extra ones later, you must import them manually.

When first installing Sanctuary, a set of predefined File Groups and assignments to user/User Groups are made. You can use these to save time when you logically regroup executables files into file groups:

File Group name	Users assigned
16 Bit Applications	Administrators (group)
Accessories	Administrators (group), Everyone (group)
Administrative Tools	Administrators (group)
Boot files	Local Service (user), LocalSystem (user), Network Service (user)
Communication	Administrators (group)
Control Panel	Administrators (group)
DOS Applications	Administrators (group)
Entertainment	Administrators (group)
Logon files	Everyone (group)
SecureWave support files	Administrators (group), Everyone (group)
Setup	Administrators (group)
Windows Common	Everyone (group)

Table 9. Standard File Definitions



Benefits of using the automatic import option during installation

The automatic import option during installation provides the following benefits:

- > You do not have to scan for basic operating system files or organize them into logical File Groups. SecureWave has already done that for you.
- > You do not have to assign the File Groups to User Groups, as SecureWave has already assigned them to a predefined Administrators group and the Everyone group. This is only done during installation and setup of the SecureWave Application Server.
- > You can be confident that pure versions of the operating system files were used to create the hashes. Using SFDs avoids the risk of accidentally authorizing tampered versions of system files.
- > It is easier to upgrade system files, since Sanctuary recognizes these standard files, and their respective default File Groups, and automatically saves upgraded file definitions in the same locations as the originals.

To manually import Standard File Definitions

If you did not import Standard File Definitions during installation — No problem. You can do it now, if you wish. To manually import Standard File Definitions:

1. Select Import Standard File Definitions from the Tool menu. The Import Standard File Definitions dialog is displayed.

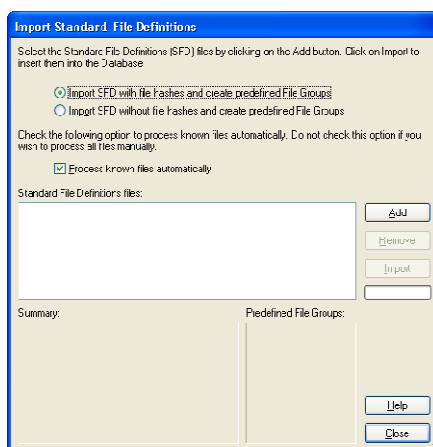

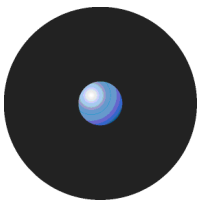


Figure 15. Import Standard File Definitions

2. Click on the ADD button. The dialog box displays available files and folders, with Standard File Definitions having a .SFD extension.
 -  *If you want to import an SFD from our website, www.securewave.com, download this onto a local computer and unzip it.*
3. Navigate to the SFD file(s) you want to import and click OPEN. The file(s) are shown in the ADD window.
4. Repeat steps 2 and 3, if required.
5. Click on the IMPORT button to import the selected Standard File Definitions file(s). Since it can take a few minutes to process these, only choose the Standard File Definitions you actually need.
6. Choose whether you want to import SFDs with or without file hashes by selecting one of the following:
 - > *Import SFD with file hashes and create predefined File Groups: This means that Sanctuary imports ALL files hashes in the predefined File Groups, even those that are seldom or never used by a 'normal' user. If you then proceed to the Database Explorer module, you can see that the database includes signatures of all the executable files, scripts and macros of the SFD file(s). You do not need any extra steps (everything is handled for you). On the other hand, your database includes the signature of all the operating system files, even for those not used. Transmitting this can be problematic, especially if you have slow connections in your network.*



You should not import SFD files for operating systems or programming languages you do not use (or do not plan to use) in your environment.

> *Import SFD without file hashes and create predefined File Groups: The process is similar to the previous one except that no file hashes are imported. Sanctuary does however record the predefined File Groups for each file. When the time comes to scan and assign files from on client machines, Sanctuary uses the imported SFD to suggest 'correct' File Groups. If you choose this option, then once the importation process finishes you have an empty database. You must then scan a newly installed client machine and assign the scanned files to the proposed (or your own) File Groups. The disadvantage of using this option is that you must carry out extra tasks as part of your Sanctuary installation and the system only helps you partially by identifying the file names and proposing File Groups when the time comes to authorize them. The advantage of using this option is that you have a smaller database that contains only the files actually used by your Sanctuary Clients.*

7. Click on the IMPORT button and accept the license agreement (once you have read it and agree to it).
8. When the importing process finishes, click on OK and then click on CLOSE.
9. Assign the created File Groups to users or User Groups, if required. (This step is not required if you imported Standard File Definitions during setup. See *Table 9* on page 34)



When Microsoft produces a new Service Pack or other update for one of its operating systems, SecureWave creates a Standard File Definitions corresponding to it and makes this available to Sanctuary users via our Web site, www.securewave.com. Updated definitions can be imported at any time using the above procedure.



When you install Standard File Definitions, you should be careful to record the hash number corresponding to the logon and boot files. If these are not authorized, the system does not work properly. This is especially important for system updates.



*When installing other Sanctuary products, check that the computer and user/user group 'Execution Blocking' option is set to 'Non-blocking mode'. The setup cannot proceed otherwise. See *Precedence rules for the Execution Blocking option* on page 120 for more information.*

Selecting files to authorize using the Exe Explorer module

You can use the *Exe Explorer* module to create a list of executable files, scripts and macros that you want to authorize. This is the easiest method and does not require a client driver to be installed on all the computers that you want to explore.

Before you use the *Exe Explorer* module, you should set up the default options for this module. These determine the default way it searches computer directories for executable files, scripts and macros and how the results are displayed.

Using the *Exe Explorer* module, you can quickly build lists of files in a single computer directory, or in a directory and all of its sub-directories. If you choose the root directory of a computer, this import process creates a list of all executable files, scripts and macros on the entire computer. This can be slow and it is typically only done when you want to check all the applications installed on a computer.

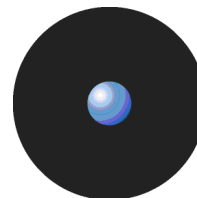
It is best to use a newly configured 'reference' computer to create a list of executable, script and macro files that you want to authorize, so you can be sure that only 'clean' files are authorized. The reference computer does not have to be the same computer on which you are running Sanctuary Management Console. You can browse the network and select any other available machine as your 'reference'.



*Only Sanctuary administrators with the appropriate user access rights can use the Exe Explorer module. See *Chapter 4: Setting up Sanctuary administrators* on page 29 for more information.*




*Although you can manually assign macros and scripts to the white list using the Exe Explorer module, we recommend that you do this using the Log Explorer instead. See *Using the Log Explorer module to authorize unknown files* on page 87.*



An alternative way of selecting files from network directories is to use *FileTool.exe*. This has the advantage that it can be scheduled using the *AT* or *WinAT* command. See *Versatile File Processor* tool on page 127 for more information.

To set up the Exe Explorer default options

1. Click on the *Exe Explorer* icon  located in the *Modules* section of the *Control Panel* of the main window or use the *View→Modules* command.
2. Select *Default Options* from the *Tools* menu (or the *Control Panel*) to display the *Options* dialog.
3. Click on the *Exe Explorer* tab.

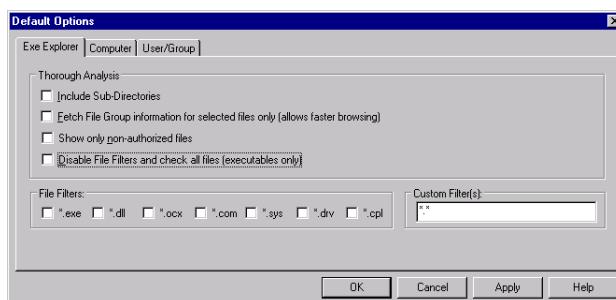


Figure 16. Default options dialog - Exe Explorer options

4. Choose which directories you want to search.

If you want to select files from the named directory and all its sub-directories, check the *Include Sub-Directories* box. If you want to select files from the named directory only (which is faster), make sure it is unchecked.

5. Choose whether you want to display the File Group information for all files or only the selected files.

If you want to display File Group information only for files you select (the faster of the two options), check the *Fetch File Group information for selected files only* box. If you want to show File Group information for all files, make sure it is unchecked.

6. Choose whether you want to display previously authorized files or not.

If you want to filter out previously authorized files and show only the rest (the faster of the two options), check the *Show only non-authorized files* box. If you want to show all files regardless of whether they are authorized or unauthorized, make sure it is unchecked.

7. Choose whether you want the *Exe Explorer* module to check all files or only files with specific extensions to determine whether or not it is an executable, script or macro.

If you only want to search files with specific file extensions, make sure the *Disable File Filters and check all files (executables only)* box is unchecked, and check the boxes in the *File Filters* panel to indicate which types of files to include (as determined by standard file extensions such as *.exe*, *.com*, and so on).



Sanctuary also searches 16-bit programs if you select the file filters options (**.exe* and **.com*).

To search for files with one or more non-standard file extensions, make sure the *Disable File Filters and check all files (executables only)* box is unchecked, and enter the custom extension(s) in the *Custom Filter(s)* field. (When entering several file extensions in this field, separate entries using a semi-colon with no space.)

If you want to check every file (rather than only checking files with specific extensions), check the *Disable File Filters and check all files (executables only)* box. This option is slower than only checking files with specific extensions but it ensures that you do not miss any executable files just because they have non-standard file extensions.

8. Click on the OK button to return to the *Exe Explorer* module.



To select files using the Exe Explorer modules

Once you have set up the default options you want to use for the *Exe Explorer* module you can click on the directory that contains the files that you want to select in the left panel of the *Exe Explorer* window. Executable files, scripts and macros in that directory (and its subdirectories, if appropriate) are displayed in the right panel of the same window.



You can map network drives directly from the console. The 'Explorer →Map Network Drive' command (when the *Exe Explorer* module is active) invokes the standard Windows dialog.

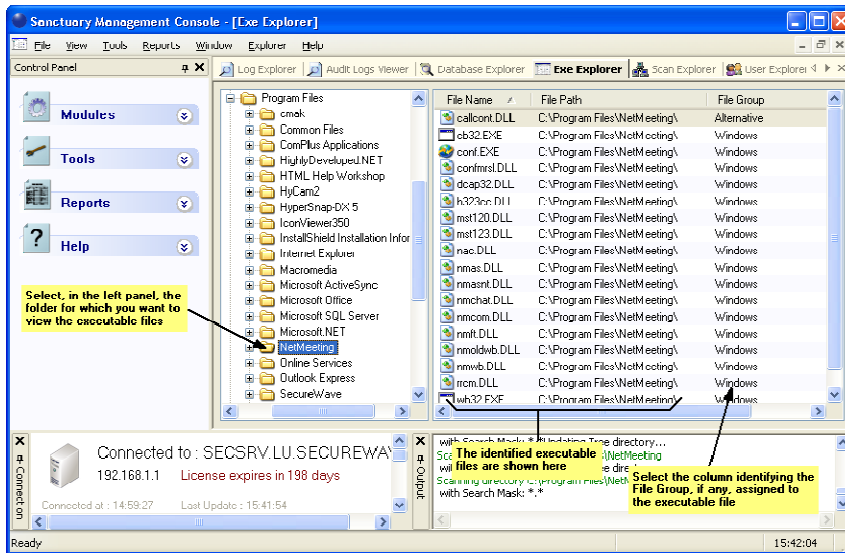


Figure 17. Exe Explorer Module Window

Selecting files using the *Exe Explorer* module may take a few minutes if you have a large system and have selected the more processing-intensive options. The status bar keeps you informed of progress as file details are loaded. A populated *Exe Explorer* screen appears as shown above.

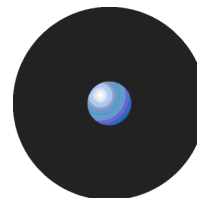


The program does not uncompress archive files (Zip, Cab, RAR, LZH, ARJ, etc.). To do so, use the Authorization Wizard or the *FileTool.exe* tool. See *Using the Authorization Wizard* on page 42 and *Versatile File Processor* tool on page 127 for more information.



You can use the 'Choose columns' option from the right-click menu to select and organize the columns you want to display.

When you have created a list of executables, scripts and macros you are ready to organize them into File Groups and assign these to users and User Groups. See *Chapter 6: Organizing files into File Groups* and *Chapter 8: Granting access using the User Explorer* more details.



Automatically scanning a computer to identify files

The easiest method to identify all installed components of specific software is to automatically scan the computer. The only limitation is that you must first install Sanctuary Client Driver on the machine.

Using the Scan Explorer module

The *Scan Explorer* module scans a target computer running the Sanctuary Client, and builds a detailed list of all the files found on client machines. This is the easiest and quickest way to populate the SecureWave Sanctuary Database from a reference computer, as well as to identify unknown applications.

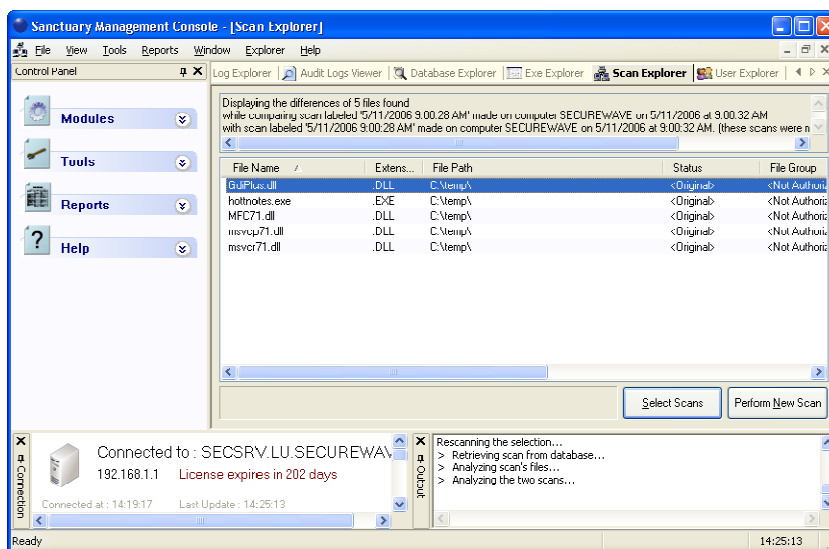


Figure 18. Scan Explorer module main window

You can choose to scan all files on a computer, or you can create a template that tells the system to scan only selected directories, or specific file types (such as *.exe, *.com, *.dll, *.ocx, *.sys, *.drv, *.cpl, *.vbs, *.js), which reduces the scan time required.

You may, for example, want to create a template to identify the changes made when a particular application is installed. If you know that this application installs the following:


- > A group of files in sub-directories of the \Program Files folder.
- > Executable files with extensions .exe and .dll in the WINDOWS directory and SYSTEM32 subdirectory (system root folder).

Then, you could scan for these files by creating a template with the following two rules:

```
Scan all executables matching the pattern
*.exe or *.dll (regardless of case)
in directory
%SYSTEMROOT%
and its subdirectories

Scan all files matching the pattern
* (regardless of case)
in directory
%PROGRAMFILES%
and its subdirectories
```

To create a new template to scan files in a computer

1. Click on the *Scan Explorer* icon  located in the *Modules* section of the *Control Panel* of the main window or use the *View→Modules* command.
2. Click on the PERFORM NEW SCAN button.
3. Click on CREATE NEW TEMPLATE in the upper right of the *Perform New Scan* dialog.

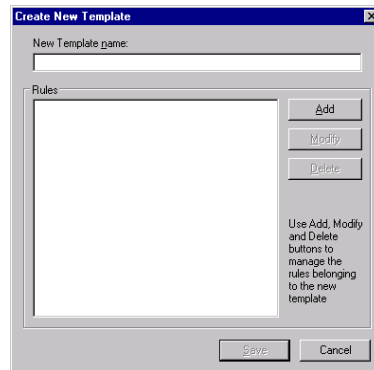


Figure 19. Create New Template dialog

4. Enter the name you want to use for the new template. Choose a meaningful name so you can identify this template again in the future.
5. Click on ADD to display the *New Rule* dialog.

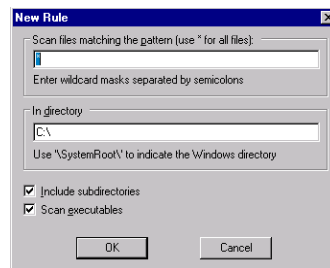


Figure 20. New Rule dialog

6. Complete *New Rule* dialog as follows:
 - > *Scan files matching the pattern* — Specify the name patterns that you want to use to select executables, scripts and macros from client machines. You can use a single asterisk (*) to select all files, an asterisk followed by a dot and extension for specific file types (*.vbs) and/or semi-colons to separate multiple wildcard entries, for example: *.exe;*.hdk;*.dll;*.vbs;*.js.




If you specify wildcard masks — for example, *.com — there is the potential to miss files that do not use the standard file extensions (.exe, .com, .dll, etc.). If this happens the files are not authorized and the application may not work properly, if at all.

- > *In directory* — Enter the path of the directory you want to scan. You can use '\SystemRoot\' (with this capitalization) to indicate the Windows directory.
 - > *Include subdirectories* — Check this box if you also want to scan subdirectories of the directory.
 - > *Scan executables* — Check this box (recommended) if you only want to scan for executable files and ignore all other files. This also searches for 16-bit executables. (If you do not select this, you should use *.exe and *.sys on the matching pattern to search for them.)
7. Click on the OK button.
 8. Click on the SAVE button to keep the template.

When you return to the *Perform New Scan* dialog, the template you have just created is available for selection in the *From Template* drop-down list.

To scan files on a client computer

1. Click on the *Scan Explorer* icon  located in the *Modules* section of the *Control Panel* of the main window or use the *View→Modules* command.



2. Click on the PERFORM NEW SCAN button.

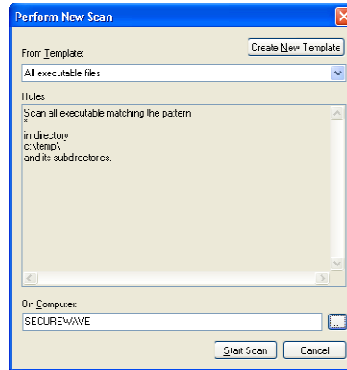


Figure 21. Perform New Scan dialog - template

3. In the *From Template* field, choose a template that selects all files (assuming a template already exists with this mask. See *To create a new template to scan files in a computer on page 39*).

To save time, select a template that only scans the directories you are interested in.

4. Specify the computer you want to scan by clicking on the button to the right of the *On Computer* field and browsing to the appropriate computer in the *Select Computer* window.
5. Click START SCAN to display another *Perform New Scan* dialog.

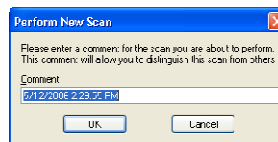


Figure 22. Perform New Scan dialog - comment

6. Enter a name or remark to distinguish this scan in the *Comment* field. Use a descriptive name, especially if you plan to compare two scans afterwards.
7. Click on OK to start the scan.

Sanctuary scans all the files on the computer (or specified directories), calculates hashes for all executables scripts and macros, and adds these new file definitions to the database. The populated *Scan Explorer* display looks similar to this one:

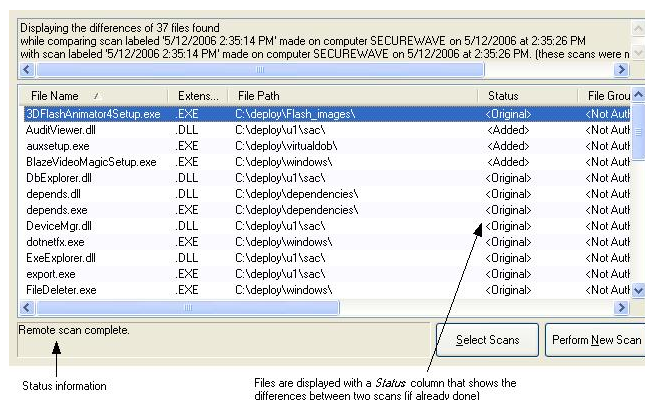
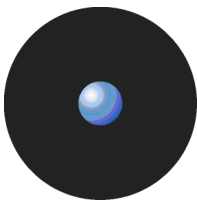


Figure 23. Scan Explorer window after a scan

The lower left panel of the Scan Explorer module window contains important status information.

To compare two scans

1. Perform the scans you want to compare, using the previous procedure. These scans do not necessarily have to be recent ones. In fact, it typically you compare a scan done before installing a new application with another one done after the installation process is complete.



2. Click on the **SELECT SCANS** button or select the *Explorer* → *Select Scans* command from the menu bar at the top of the screen. The following dialog is displayed.

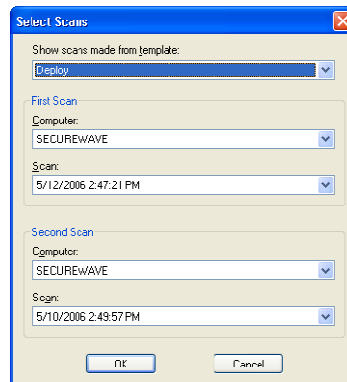


Figure 24. Select Two Scans to Compare

3. In the *Show scans made from template* field, choose the template you used for the scans that you are going to compare.
4. In the *First Scan* section, select the computer and the name of your first scan.
5. In the *Second Scan* section, select the computer and the name of your second scan.
6. Click on the OK button.

The system compares the two scans and displays the results in the *Scan Explorer* window. Each file has a status assigned to it as a result of the comparison as shown in the following table:

Status	Description
Added	The file was added between the first and second scans.
Different	The file has been modified. It has the same filename but a different digital signature. It may be a newer version.
Original	The file remains unchanged from the previous scan.

Table 10. File status when comparing two scans.



It is only meaningful to compare two scans that have been carried out using the same template.

Modifying file authorization

After scanning a computer to identify executables, scripts and macros, or comparing two scans to identify updates, you may want to change your file assignment details. For example:

- > If the purpose of your scan was to identify changes made when installing a new application, you may want to assign the new/modified files to a specific File Group so users can work with the new application or upgrade.
- > If the purpose of your scan was to identify files associated with different applications, you may want to remove them from particular File Groups to prevent further use of the application.

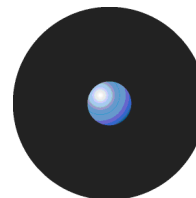
To change the assignment of files to File Groups, right-click on a selected range of files in the *Scan Explorer* list and select the *Assign to file group* or *Remove from File Group* option. For more information, see *Chapter 8: Granting access using the User Explorer* on page 61.

You can use the right-click menu to assign selected files to a File Group, remove them from it, or filter a scan to show only *<Not Authorized>* files. When using this last option, you can revert to the full listing by right-clicking again and selecting *Show all files* from the menu.

Using the Authorization Wizard

The Authorization Wizard utility provides yet another way to:

- > Search for executable files from a given source — such as a computer's hard drive, a network share (UNC path), or a CD/DVD-ROM.




- > Create digital signatures (hashes) for the selected files.
- > Incorporate these digital signatures (SHA-1 hashes) into the SecureWave Sanctuary Database.

The Authorization Wizard can perform these tasks for:

- > Windows operating systems, applications and service packs — even those packaged in ZIP files.
- > Self-extracting ZIP archives.
- > RAR, MSI, and Microsoft CAB files.

True to its name, the Authorization Wizard is easy to use. It guides you through the various stages, gives you advice, and prompts you for information. All you have to do is answer prompts and click NEXT to move to the following step.

 *The Authorization Wizard does not expand setup EXE files and wrongly considers them as a single executable files instead of an auto-extraction file.*

 *The Authorization Wizard does not scan for scripts or macros.*

To authorize executable files using the Authorization Wizard

1. Click on the Windows START button and select *Programs* → *Sanctuary* → *Authorization Wizard*. The Authorization Wizard starts.
2. Read the instructions and click on the NEXT button.
3. At the following dialog, enter the name of a computer running SecureWave Application Server software. You may need to click CHECK SERVER to verify that the required server is connected.



 *If you only leave certain ports open in your firewall, you may need to specify the server TCP port number between square brackets, e.g.: server[1234]. See the Sanctuary's Setup Guide.*



Figure 25. Authorization Wizard

4. Check the *Process known files automatically* box if you want the wizard to insert existing files into the SecureWave Sanctuary Database if they have the same name but different digital signature (hash) as an existing database entry. The wizard also tries to find a suitable File Group for them. Uncheck this option if you want the wizard to identify known files, but allow you to manually process them.
5. Click on the NEXT button.
6. In the next dialog, use the  button to the right of the *Source* field to browse to the root directory where you want to scan for executables and select the temporary directory where the wizard should expand any archives (set of compressed files) found. (Both directories must already exist.)

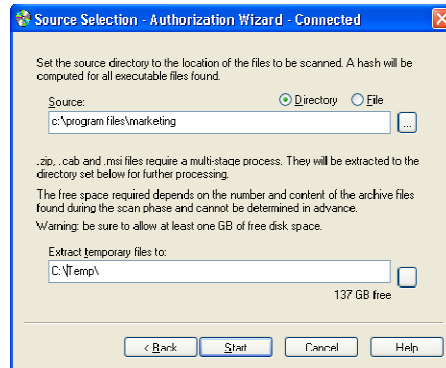
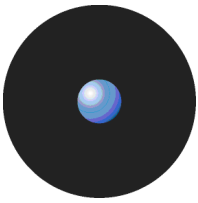


Figure 26. Authorization Wizard: Selecting the Source Directory



The wizard unpacks any archive found in the source directory into the temporary directory. It is important, for this reason, to make sure that your hard disk has enough free space.

7. Click on the **START** button to begin scanning the Source for executables.

The wizard begins searching in the source directory and displays statistics. If you see the *Free space for extraction* fall below 100 MB, you should release some extra disk space.

When the scan is complete, the Authorization Wizard presents a summary showing the number of executables found, as shown in the following example:

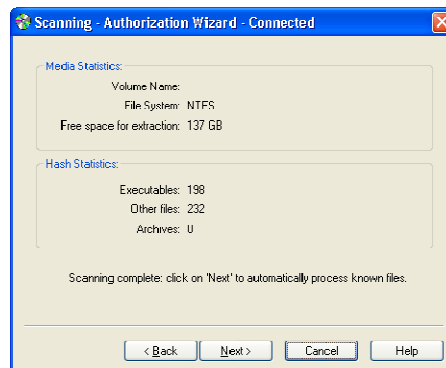


Figure 27. Authorization Wizard: Statistics

8. Click on the **NEXT** button to continue.

If you checked the *Process known files automatically* option in step 4, the wizard processes all executable files and attempts to assign a suitable File Group to each. If a matching filename exists in the database and has been assigned to a particular File Group, the wizard assigns the new file definition to the same File Group.

When the wizard has made all the automatic File Group assignments it can, it presents another summary. This shows how many files were processed, how many were assigned to File Groups, and how many were duplicates of previously assigned files.

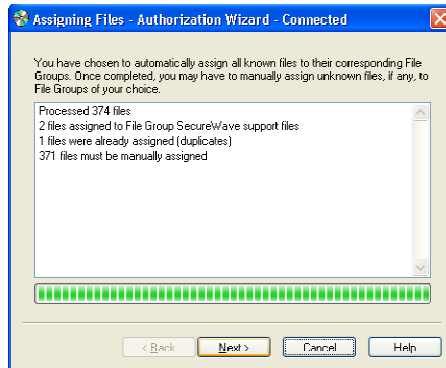


Figure 28. Authorization Wizard: Processing the Files

9. Manually assign File Groups to any remaining files.

The wizard presents a list of files that were not automatically processed either because they did not match existing filenames in the database or because you did not select the *Process known files automatically* option in step 4. You can use this list to directly assign files to File Groups.

To manually assign a File Group, select one or several files (using the Ctrl and/or Shift key) and then click on the *Suggested File Group* drop-down or the FILE GROUPS button to select the appropriate File Group. See *Chapter 6: Organizing files into File Groups* on page 47 for more information.

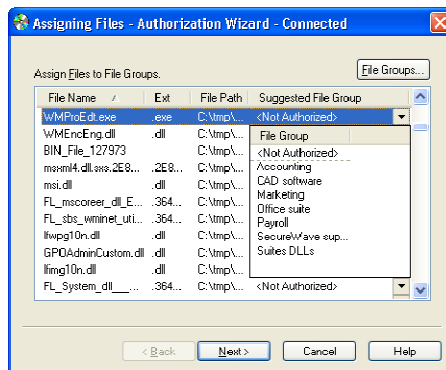


Figure 29. Authorization Wizard: Assigning Files to File Groups

10. Once you finish assigning the files to File Groups, click on the NEXT button to insert the new file definitions into the database.



You may have to update access permissions to enable users/user groups — using the User Explorer module — to run any new applications.


11. Either run the Authorization Wizard again, using a button on its final page, or close the Authorization Wizard.


Chapter 6: Organizing files into File Groups

File Groups simplify the process of administering large numbers of executable, script and macro files and users. Instead of individually authorizing files, you can logically group them to be managed together.

Your File Groups should reflect the way you want to administer Sanctuary. For example, you may want to create an IIS (Internet Information Server) group to associate all network services needed by your Web master when protecting your organization's servers, or a Marketing group to cluster applications used by your marketing department.

File Groups may have child File Groups associated with them. This reflects the way Windows is designed, where applications share common files (libraries of code, data, or resources). If you create a parent-child relationship between File Groups you can update a shared library without recompiling or changing the application itself.

 The use of files in a child File Group can be indirectly authorized through a parent-child relationship.

 Both child and parent File Groups must exist before creating a relationships in the Database Explorer module (in the Groups tab).

Creating and managing File Groups

To create a new File Group

1. Open the *Database Explorer*, *Scan Explorer*, *Log Explorer*, or *Exe Explorer* module. To do this, click the appropriate icon in the *Modules* section of the *Control Panel* or use the *View→Modules* command.
2. Select *Manage File Groups* from the *Explorer* menu. The system displays the corresponding dialog.

Alternatively, if you are working in the *Database Explorer*, *Exe Explorer*, or *Log Explorer* module, you can do this by selecting a file(s), choosing *Assign* from the *Explorer* menu, and clicking on the **FILE GROUPS** button in the *Assign Files to File Groups* dialog. The right-click menu also has the *Assign to File Group* command that opens the same dialog.

3. Click on the **ADD FILE GROUP** button at the top right of the dialog. The system *Add File Group* dialog.

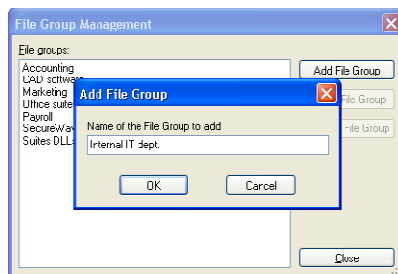
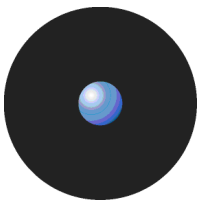


Figure 30. File Group Management

4. Enter the name of a new File Group.
5. Click on the OK button. The new File Group has now been added, and you can now assign files to it.



To delete a File Group

1. Open the *Database Explorer*, *Scan Explorer*, *Log Explorer*, or *Exe Explorer* module. To do this, click the appropriate icon in the *Modules* section of the *Control Panel* or use the *View→Modules* command.
2. Select *Manage File Groups* from the *Explorer* menu. The system displays the corresponding dialog.
3. Select the File Group you want to remove.
4. Click on the DELETE FILE GROUP button. The system displays the *Delete File Group* dialog that outlines the impact of the delete action — which Users, User Groups, and files are affected.
5. If you are confident that you want to continue and delete the File Group, click on OK. The group is removed from the list.



Take care performing this operation — it may prevent some users from running applications they require for their day-to-day work. This is also true when deleting child File Groups since they may authorize the use of related files needed by the parent File Group.

To rename a File Group

1. Open the *Database Explorer*, *Scan Explorer*, *Log Explorer*, or *Exe Explorer* module. To do this, click the appropriate icon in the *Modules* section of the *Control Panel* or use the *View→Modules* command.
2. Select *Manage File Groups* from the *Explorer* menu. The system displays the corresponding dialog.
3. Select the File Group you want to remove.
4. Select the desired File Group and then click the RENAME FILE GROUP button. The system displays the *Rename File Group* dialog.
5. Type the new name of the File Group and click OK. The new File Group name appears in the *File Group Management* dialog.

To create a parent-child relationship between File Groups

Parent-child relationships are created, deleted, or modified using the *Database Explorer* module's *Groups* tab. To do this:

1. Open the *Database Explorer* module by clicking the appropriate icon in the *Modules* section of the *Control Panel* of the main window or using the *View→Modules* command.
2. Select the *Groups* tab. The system displays the corresponding dialog.
3. Select the desired group on the left panel (*File groups*) and assign the relationships by selecting the File Group on the right one (*Relationships*) and using the ADD CHILD, ADD PARENT, or REMOVE buttons. The type changes from *Available* to *Child*, *Parent*, *Child (Indirect)*, or *Parent (Indirect)*.

When creating the relationship you may see the following icons:

Icon	Description
	This File Group is parent of the one selected in the <i>File Groups</i> panel.
	This File Group is child of the one selected in the <i>File Groups</i> panel.
	This File Group is an indirect parent of the one selected in the <i>File Groups</i> panel.
	This File Group is an indirect child of the one selected in the <i>File Groups</i> panel.
	A File Group created by a Sanctuary administrator that can be deleted or renamed
	A File Group created by the program that is blocked and cannot be deleted

Table 11. File Group relationship status icons.



You cannot delete indirect relationships — you must first proceed to the ‘direct’ related *File Group* (left panel) and then continue from there. This is demonstrated in the following examples.

Example 1 — The File Group ‘Accounting’ is the parent of ‘Payroll’, which also has an indirect parent ‘Marketing’:

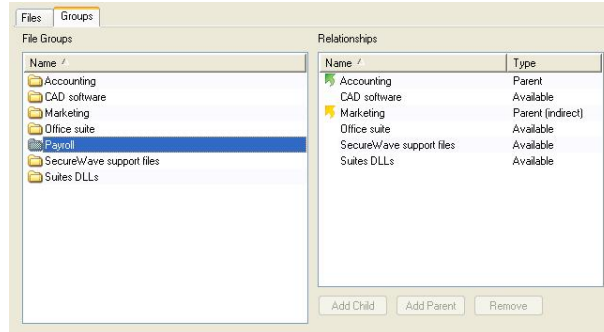


Figure 31. File Group parent relationship

Example 2 — The File Group ‘Accounting’ is the child of ‘Marketing’ who also has an indirect child ‘Payroll’:

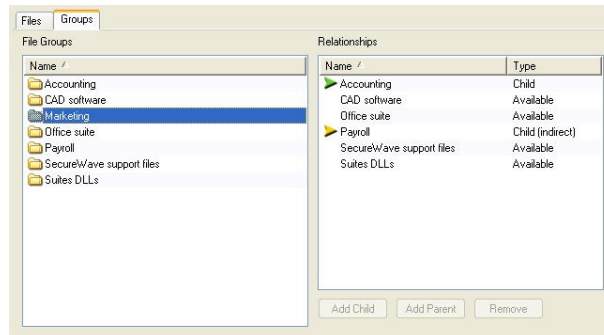


Figure 32. File Group child relationship

This is consequence of the following parent-child assignments:



Figure 33. File Group parent-child relationship

When assigning the File Group ‘Payroll’ to a user (or user group), there is also an indirect assignment because of this relationship:

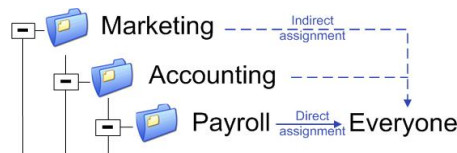
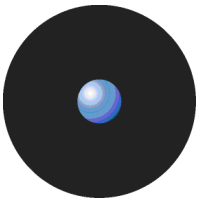


Figure 34. File Group indirect assignment

All the indirect assignments created by defining these relationships are shown in the User Explorer module (File Groups by User tab; Authorized panel). See Direct, indirect, and not authorized File Groups on page 61 (and Figure 43 in the same section).



Assigning executable, script and macro files to File Groups

When you have created the File Groups and any parent-child relationships you want to use, it is time to group executable files, scripts and macros into your File Groups.

To assign files to File Groups

1. Open the *Database Explorer*, *Scan Explorer*, *Log Explorer*, or *Exe Explorer* module. To do this, click the appropriate icon in the *Modules* section of the *Control Panel* or use the *View→Modules* command.

A list of the authorized executable files, scripts and macros, which have been recorded in the SecureWave Sanctuary Database, is shown.

2. Highlight the file, or a range of files, you want to assign to a File Group (using the Ctrl and/or Shift keys).
3. Assign the file(s) to a File group. To do this:

- > Right-click the mouse button and select *Assign to File Group*.

— or —

- > Select *Assign* from the *Explorer* menu while in the *Database Explorer* or *Exe Explorer* module.

— or —

- > Double-click on the filename (if a single file is selected).

The Assign Files to a File Group window is displayed:

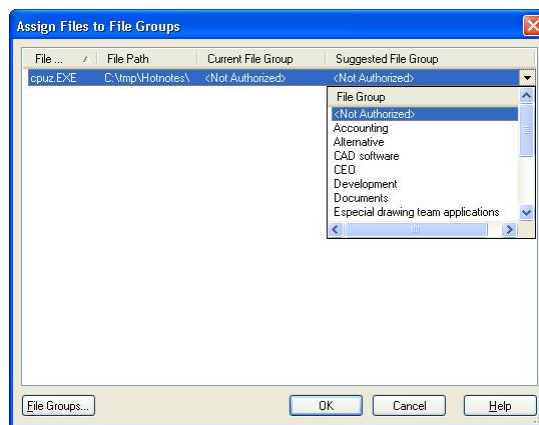


Figure 35: Assign Files to File Groups dialog

The *Current File Group* column shows the group to which the file currently belongs. If a file has not been assigned to a File Group, this column shows *<Not Authorized>*.

The *Suggested File Group* column proposes a File Group based on the filename. If a file with the same name already exists in the database (perhaps a different version of the same application), the system suggests the same File Group to which the earlier file belongs (since you would normally want this to be the same).

4. Select the File Group to which the file or files belong.

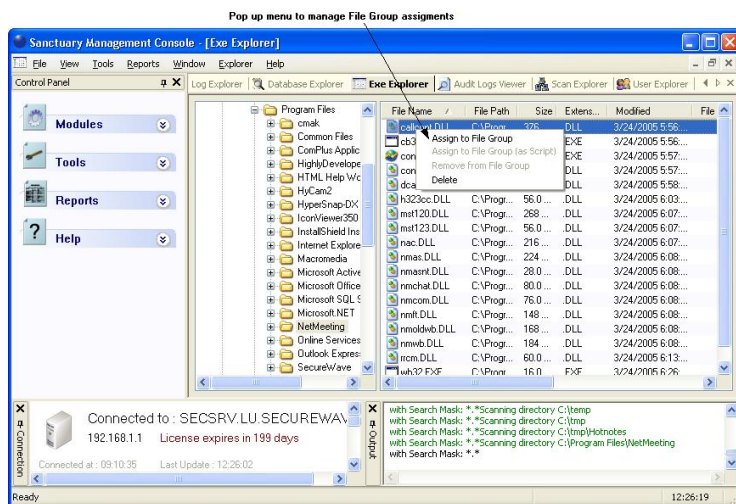
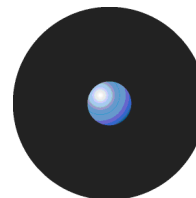




Figure 36. Assigning a File Group using the Exe Explorer module

-  You can assign a scripts or macro to a File Group as a script (as distinct from an executable).
-  You can assign File Groups using the Exe Explorer, Database Explorer, Log Explorer, and Scan Explorer modules.

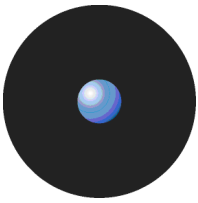
Changing file assignments

Sometimes you need to modify your file lists or file assignments. You typically do this when:

- > New software has been installed on protected servers or computers, and you wish to grant users access to the new applications.
- > Updated versions of existing software have been provided, and you want users to switch to the new versions.
- > An executable file, script or macro has become corrupted or is no longer appropriate, and you want to prevent users from running it.
- > Multiple users are locally authorizing files that are centrally denied, as evidenced from the log files. If, and only if, you are confident that the files can be trusted, you can add them to the SecureWave Sanctuary Database directly from the *Log Explorer* screen. Users will be grateful that they do no longer have to authorize these harmless executables.

To change the File Group to which a file is assigned

1. Open the *Database Explorer*, *Scan Explorer*, *Log Explorer*, or *Exe Explorer* module. To do this, click the appropriate icon in the *Modules* section of the *Control Panel* or use the *View*→*Modules* command
 2. Highlight the file, or range of files, that you want to reassign a File Group to.
 3. Right-click and use the *Assign Files to File Groups* option.
 4. Choose a new File Group for the file(s). To do this:
 - > Click on *OK*, to accept the suggested File Group.
- or —
- > Select the file(s) again, click on the *FILE GROUPS* button (or the *Suggested File Group list icon*) and select a different File Group, if required.
 5. Click on *OK*. The new file assignment details are recorded in the database.



To delete a file from a File Group

1. Open the *Database Explorer*, *Scan Explorer*, *Log Explorer*, or *Exe Explorer* module. To do this, click the appropriate icon in the *Modules* section of the *Control Panel* or use the *View→Modules* command
2. Highlight the file, or range of files, that you want to remove from a File Group.
3. Right-click and use the *Remove from File Group* option.

The system deletes the file and marks the File Group for that entry as <Not Authorized>. You can also explicitly assign the file(s) as <Not Authorized>.

To delete a file from the SecureWave Sanctuary Database

1. Open the *Database Explorer*, *Scan Explorer*, *Log Explorer*, or *Exe Explorer* module. To do this, click the appropriate icon in the *Modules* section of the *Control Panel* or use the *View→Modules* command
2. Highlight the file, or range of files, that you want to delete from the database.
3. Right-click and use the *Delete* option.
4. Click on OK.



You cannot undo this delete operation. If you accidentally delete a file you wanted to keep, you must use the Database Explorer, Scan Explorer, Log Explorer, or Exe Explorer module to generate a new hash for it and add it to the database again.

Viewing file assignments

The *Database Explorer* module displays a list of all the files that have been recorded in the SecureWave Sanctuary Database. For each file the *Database Explorer* module shows the internal system ID, filename, extension, location (path), and the File Group to which the file has been assigned. It also shows any parent-child relationships between File Groups (on the Groups tab).

The following example shows a typical *Database Explorer* listing:

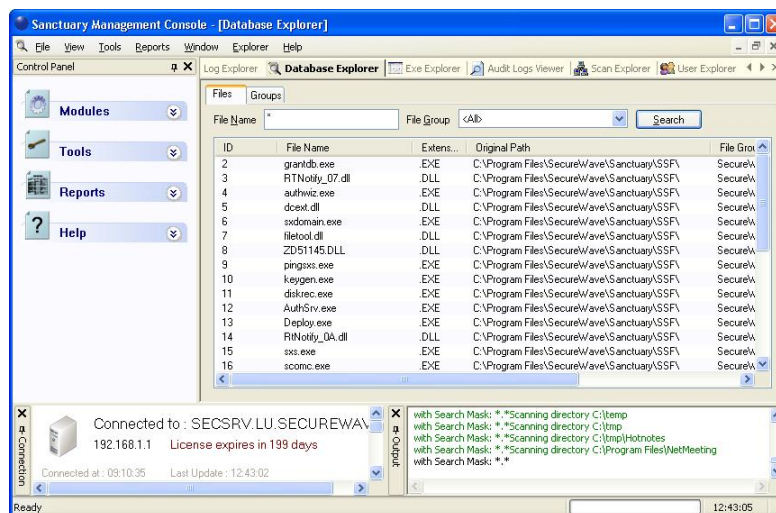


Figure 37. Database Explorer module



The Database Explorer module works in a similar way to the Windows Explorer program.



To sort entries by any attribute, such as filename or File Group

You can click on a column header to sort the file entries by that attribute. (Click again to change the order from ascending to descending, or vice versa).

A small triangle on the header shows the sort order. The ID column shows the internal SecureWave Sanctuary Database ID, for information purposes only.

To display a subset of the files in the database

1. Choose the criteria to refine your query:

File Name Display only filenames that match a given pattern. You can use the standard Windows wildcards ('?' and '*').

File Group Display only the files for a specified File Group or the <Not Authorized> File Group.

2. Click SEARCH to retrieve the files. The system displays files that match your criteria.


You can change the File Group assignment for a file from this display, delete the file from a File Group, or delete the file from the SecureWave Sanctuary Database, using the procedures outlined earlier in this chapter.

Using the Groups tab

You can use the Groups tab to create, modify, or delete parent-child relationships between File Groups. See *To create a parent-child relationship between File Groups* on page 48.

Chapter 7: Authorizing files by location (Path Rules)

Sanctuary identifies allowable files by calculating a unique digital signature ('hash') based on file contents. If the hash does not match the one stored in the system and assigned to the user/machine, the executable cannot run. Normally this is the desired behavior, since malicious programs may change or add executables invalidating their hash.

 *You cannot authorize scripts and macros by file location (Path Rules) — only executable files.*

For a small number of applications, security based on file hashes does not work. For example, some executables are transformed as a natural part of the installation procedure, typically to embed licensing information. Some internal applications may change frequently, yet they are run under the control of trusted users, so you may trust the files.

To allow these sorts of applications to run, Sanctuary solution enables you to authorize executables from a specified location, designated by path. Executable files in the specified directory location are exempted from normal hash checking. They are presumed to be from a trusted source, so they are allowed to run.

To add yet another layer of protection for this type of authorization, you can have the system check the identity of the file's owner — and execute files only from trusted owners.

All these authorization rules are stored on the server and the client so they can be enforced when the machine is disconnected.

Creating, changing, and deleting Path Rules

When creating or modifying a Path Rule you can use the following options:

- > *Ownership Check* — The Path Rule only applies if a user or group is listed as a Trusted Owner and is the proprietor of the executable file. This requires a direct match — group membership is not resolved.
- > *Include subdirectories* — Force the Path Rule to apply to all files in subfolders of the root folder defined in the path field.
- > *Log Execution* — The Path Rule is logged in the log-access-denied logging modes, if this is On (in addition to the log-everything logging mode in which it is logged regardless of this setting). In all cases the Path Rule is logged with the ok-PathRule custom message. Log Execution is On by default, and for existing Path Rules.

To create a new Path Rule that applies to everybody

1. Select *Path Rules* from the *Tools* menu (or from the *Control Panel*). The following dialog appears:

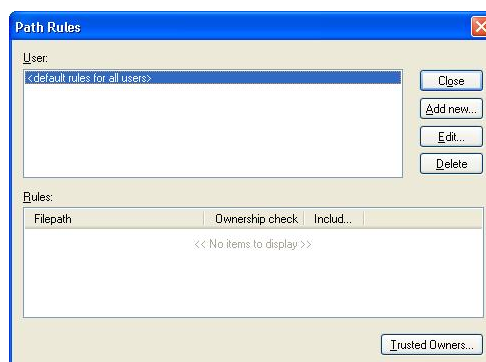
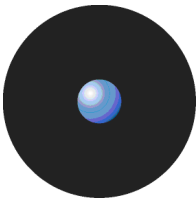


Figure 38. Path Rules dialog



2. Select *<default rules for all users>* and click on **EDIT**. The following dialog appears:

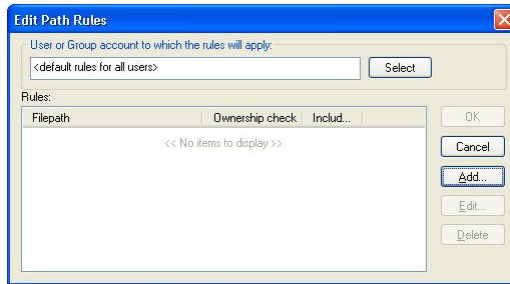


Figure 39. Editing the Path Rules

3. Click on the **ADD** button to insert a new path to the rule.
4. Type the path that identifies the location of the executable file. You can use the system variables %SystemRoot%, %SystemDrive%, and %ProgramFiles%.
5. If you want the rule to apply only to executable files of a Trusted Owner, activate the *Ownership Check*.
6. If you want to traverse all the subfolders beginning from the root, select the *Include subdirectories* option.
7. If you want the Path Rule to be logged in the log-access-denied logging modes (in addition to the log-everything logging mode in which it is logged regardless of this setting), select the *Log execution* option.
8. Click on the **OK** button to close the *Path Rule* dialog.
9. Click on the appropriate button: **ADD** to insert a new path, **OK** to save the rule, **CANCEL** to abandon the operation, **EDIT** to change the selected path for the Path Rule, or **DELETE** to erase the selected path from the Path Rule. The new Path Rule takes effect after an update has been sent to the user's computer.

To create a new Path Rule that applies to a specific user or user group

1. Select *Path Rules* from the *Tools* menu (or from the *Control Panel*) to display the corresponding dialog.
2. Click on the **ADD NEW** button. The following dialog appears:

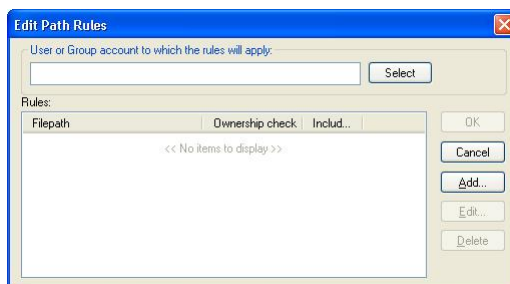
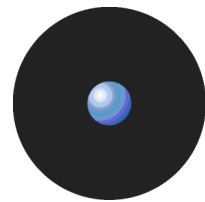


Figure 40. Adding a Path Rule

3. Type the name of a User or User Group to whom the Path Rule will apply, or click on **SELECT** to search for and choose a User or User Group.
4. Type the name for the Path Rule.
5. If you want the rule to apply only to executable files of a Trusted Owner, activate the *Ownership Check*.
6. If you want to traverse all the subfolders beginning from the root, select the *Include subdirectories* option.



7. If you want the Path Rule to be logged in the log-access-denied logging modes (in addition to the log-everything logging mode in which it is logged regardless of this setting), select the *Log execution* option.
8. Click ADD to accept the Path Rule but keep the *Path Rules* dialog open.
9. Click on the OK button to add the Path Rule and close the dialog, or on CANCEL to interrupt the operation.

To modify an existing Path Rule

1. In the *Path Rules* dialog, select the User whose Path Rule you want to modify and then click on the EDIT button. The *Edit Path Rules* dialog appears.
2. Select the Path Rule you want to modify, and click on EDIT. The Path Rule appears on the *Path Rule* dialog.
3. Modify the Path Rule and check/uncheck the *Ownership Check*, *Include subdirectories* and *Log execution* options as appropriate.
4. Once you have finished modifying the Path Rule, click on the OK button.

To delete a single Path Rule for a user or user group

1. In the *Path Rules* dialog, select the User whose Path Rule you want to remove and then click on the EDIT button. The *Edit Path Rules* dialog appears.
2. Select the Path Rule you want to delete from the *Rules* list.
3. Click DELETE and then click on OK.

If a User or Group has only one Path Rule specified, you cannot delete the rule by this method. To remove a single rule, select the User or Group in the *Path Rules* dialog and delete it.

To delete all Path Rules for a user or user group

1. In the *Path Rules* dialog, select the User or Group whose Path Rules you want to delete.
2. Click on the DELETE button.

You cannot delete the *<default rules for all users>* account but you can remove its rules.

Conventions for specifying paths in the rules

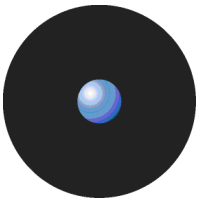
Some special conventions apply to paths in the Path Rules. They allow you to select multiple files in a more convenient way.

Each path name can be up to 900 characters and can consist of the following parts:

- > Root specifier.
- > Path specifier.
- > Filename specifier.

The *root specifier* can be:

- > A Root token:
 - %SystemDrive% — The drive where Windows is installed.
 - %SystemRoot% — The folder where Windows is installed (usually C:\Windows or C:\WINNT).
 - %ProgramFiles% — The Program Files folder for the computer (usually C:\Program Files).
- > A *Drive letter*: any valid drive letter (local drive or mapped network drive).



- > A *Server or computer name*: the UNC name of a machine on the network, such as '\\serverA'.

The *path specifier* is simply the file path relative to the root token. This path name must start and end with a backslash and cannot include wildcards.

The *file specifier* is the file name, with or without wildcards. Allowable wildcards are '*' (asterisk) representing any string of zero or more characters, and '?' (question mark) representing any string of 0 or 1 characters.

Here are some examples of valid path names for a Path Rule:

- > %SystemRoot%\system32*.dll
- > C:\SomeFolder*.*
- > \\serverA\Some Folder\SomeFile.exe



If you specified a non-existing file or directory, the file/directory is not found, but no error or warning message is issued.

Defining and working with Trusted Owners

A fundamental principle of authorization by Path Rules is that the path leads to a trusted source. To add yet another layer of protection for this type of authorization, you can ask the Sanctuary system to explicitly check the ownership of the file — and execute files only owned by trusted owners. You can also adjust Windows NTFS path security properties.

If you activated the *Ownership Check* when setting a Path Rule, the Sanctuary system only permits execution of files owned by an account who is a Trusted Owner. Note that an account not specified explicitly as being a Trusted Owner is not be considered as such, even if this account is a member of a group that is a Trusted Owner.



Trusted Owners are not available for Novell users.

To define or delete a Trusted Owner

1. Select *Path Rules* from the *Tools* menu (or from the *Control Panel*).
2. Click on the TRUSTED OWNERS button in the *Path Rules* dialog. The following dialog appears:

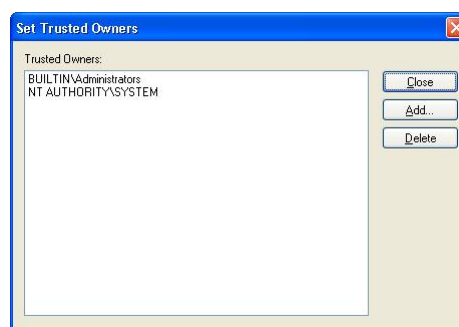


Figure 41. Setting Trusted Owners

3. Click ADD, select the User or Group you want to designate as a Trusted Owner, and click on the OK button.

You can use this same dialog to delete a Trusted Owner by selecting it and clicking on the DELETE button.



Trusted Owner and Path Rule example

As an Administrator, you can create different Path Rules (see *Creating, changing, and deleting Path Rules* on page 55) for different users and combine those with trusted owners to reinforce the effect as illustrated in the following example:

1. The Administrator creates a Path Rule without selecting the *Ownership Check* option (no trusted owner check) to a directory called `c:\marketing\applications*.exe` for a user called Bill (he has neither local nor domain administrative rights).
2. The user (Bill) can now execute all programs in that directory (only the ones with an EXE extension).
3. If the user copies – assuming he has the rights to do so – another EXE file to this already authorized directory (by means of this Path Rule), he/she can run it without any problem. He can also try to copy this file to another directory but it does not run (unless, of course, it belongs to another Path Rule)
4. Since this is not a generally accepted policy, we now add an *Ownership Check* option to the rule and proceed to include Trusted Owners to it. We add the Administrators of the machine (or domain) to the Trusted Owners.

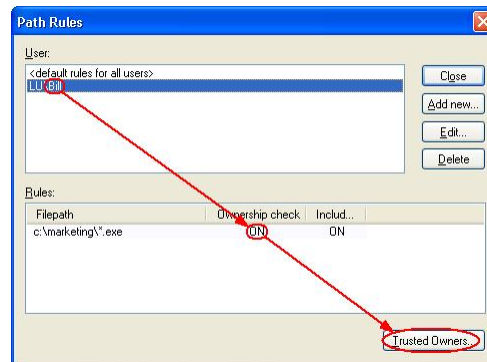


Figure 42. Setting Path Rules with Ownership Checking

5. The situation changed radically from that described in step 3. Bill is not able to run applications that do not belong to the Administrators (unless he himself is an administrator). Only the Administrators can place 'trusted' EXE applications in that directory. If he tries to copy a file to that directory, he becomes the owner — not the administrator — and thus, he cannot run it.



If you are using Sanctuary in a Novell environment, be aware that Path Rules do not work.

Path Rules precedence

When defining Path Rules (*Tools*→*Path Rules* or from the *Control Panel*), you can assign them at different levels:

- > As a default rule for all users.
- > To a specific user group.
- > To a specific user.

When Path Rules are defined at different levels (all users, user group, or user), it is important to understand the resulting policy. For example, you can define a Path Rule that applies to all users and a second one that applies only to a user but have some common files with the first one defined. The general rule is that 'Path Rules are cumulative'.

The next table shows if an application can run or not depending on the defined Path Rule:

Type of Path Rule defined:	If the user is NOT a member of the group	If the user is a member of the group
	Will the application run?	
<i>Default rule for all users</i>	Yes	Yes
<i>For a group</i>	No	Yes
<i>For an specific User</i>	Yes	Yes

Table 12. Resulting permissions when applying Path Rules

Chapter 8: Granting access using the User Explorer

Sanctuary protects your organization's servers and computers by permitting only authorized users to run approved applications, scripts or macros.

A small organization may simply define a standard set of approved applications and grant all users access to the same accepted set of files. However, most organizations differentiate between different types of users, and grant users access only to the applications they need to carry out their specific jobs. For example, you may only want to grant your designated Webmaster access to Web server functions. Similarly, you may only want to grant authorized database administrators access to database servers, or only allow your designated bookkeeper to access your Accounting software. Controlling access to applications by user group or individual user minimizes the risk of your systems being harmed — either accidentally or deliberately.

When you have gathered a list of the executable files, scripts or macros you need to manage, organized these into logical File Groups, and defined users and user groups, the final step you need to carry out to define who can do what is to assign File Groups to users/user groups.

Users and user groups



If you are using Sanctuary Application Control Server Edition, by default your 'users' are server administrators, typically Webmasters, email administrators, database management specialists and other members of the IT team who need to access your organization's critical server's functions. For the purposes of this chapter, and to distinguish them from Sanctuary Administrators, we simply refer to these server administrators as 'users'.

Sanctuary regulates application access by identifying users in the system and checking their access privileges. When a request comes from a user to activate a particular application, script or macro:

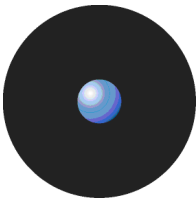
1. The Sanctuary Client Driver checks the digital signature (hash) of the requested file against those in the white list stored locally.
2. If the application is on the white list of approved files, only authorized applications and scripts assigned to a user or a user group from which this user is a member can run on the client. Sanctuary therefore checks next which File Group the requested executable, script or macro is in and whether the user has permission for that File Group.
3. Finally, on the basis of the above, Sanctuary either grants or denies the ability to run the requested executable, script or macro.

Direct, indirect, and not authorized File Groups

Most of the time, specific File Groups are associated with Domain User Groups to minimize management overhead. This means that new group members automatically inherit the right to execute applications assigned to the group.

You can grant permissions to users either directly, or indirectly through a user group. For example, you can assign a right to use an application to a global group. Any member of that global group is then *indirectly authorized through Domain Groups* to use that application.

A user can be a member of several groups of users, in which case he can use all programs, scripts and macros that are authorized for the user groups of which he is a member.



Users can also have indirect assignments granted due to a parent-child relationships. These relationships were set up using the *Database Explorer* module (see *To create a parent-child relationship between File Groups* on page 48).

The following figure shows an example of the *User Explorer* window for a domain user called 'Bill' who has:

- > Two File Groups indirectly authorized because of assignments made to Domain User Groups from which he is a member. These are the Accessories and the Accounting File Groups, shown in the *Indirectly authorized through Domain Groups* panel.
- > Four File Groups directly authorized to him (as shown in the *Authorized* panel). Of these the Microsoft Office and QA File Groups are directly assigned to the user, and the Payroll and Production File Groups are indirectly assigned through parent-child relationships.
- > Several File Groups that are not authorized to him (as shown in the *Not Authorized* panel).

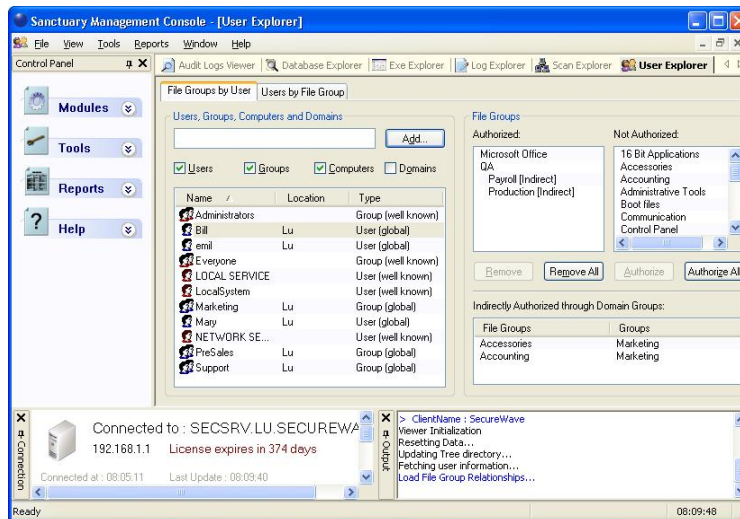


Figure 43. A user having several File Groups indirectly authorized

The Sanctuary system recognizes and embeds 'well-known' groups that are normally found on each of your computers, for example, Administrators, Everyone, Power Users, and Users. These standard groups also apply in a server environment.

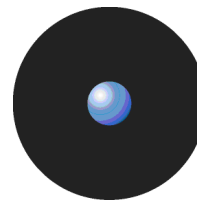


If you give a well-known group or user the permission to execute a file, this right is given to the corresponding account on every computer on your network.



In a default Windows 2000 setup, some of the Global Users and Global Groups are set to be members of the 'well-known' groups (Administrators, Everyone, Power Users, Users). For instance, when a workstation joins a domain, the Domain Administrators group is set by default to be a member of the Administrators group for that workstation. In the User Explorer module, the well-known groups on each workstation get the same set of File Groups authorized. However, it is possible to change which domain users and groups are members of a well-known group on a per-computer basis.

*File Groups authorized to Global Users or Global Groups via the well-known groups **do not appear** in the 'Indirectly Authorized Through Domain Groups' list when you view the authorizations for a Domain User or Domain Group, even though on a per-computer basis, the authorizations may exist.*



LocalSystem

The LocalSystem account is a built-in account used to run services on Windows 2000, XP, 2003 and Vista operating systems. (Vista also uses the built-in LocalService and NetworkService accounts to run services.)

You must grant dedicated accounts such as LocalSystem the right to use the appropriate File Groups containing services. For example, if you create a 'Windows File Group' where you put all operating system executable files (including Windows services that run with the *LocalSystem* account), you should grant LocalSystem the right to use this 'Windows File Group'.



The LocalSystem account and Administrators group are automatically configured in non-blocking mode to simplify day-to-day management issues. You can change this default setting (see Default options for users and user groups on page 111).

Domains

The users, groups, and computers contained in each domain are defined in your respective domain controllers.

You can select the objects (user/groups/computers/domains) to expand and collapse the structure to browse for the user or user group to which you want to grant File Group permissions:

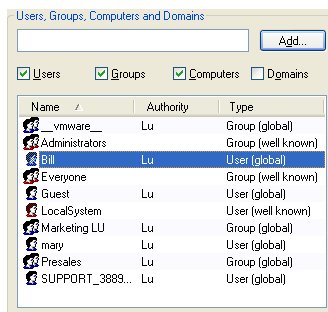


Figure 44. User's tree



Use the 'Synchronize Domain Members' option on the 'Tools' menu (or the Control Panel) to include local users of a computer in the Database, or if you do not see all your users/groups. If you are using a Novell environment, use our synchronization script (described in the Sanctuary's Setup Guide).

Granting users or user groups permission to use designated File Groups is an easy point-and-click process done using the *User Explorer* module. You can either:

> Display a list of users/user groups and bind them to File Groups.

— or —

> Display a list of File Groups and associate them with users and user groups.

Both functions are easily accessible in the *User Explorer* module, and both approaches yield the same result — linking users/user groups with the files they are authorized to execute.


The *User Explorer* module can also be used to assign specific permissions to local users and groups. By default, the SecureWave Sanctuary Database contains only domain users; in order to import local users and groups information, you need to select a computer and right-click on it and select *Synchronize Local Users/Groups* from the context menu. The console prompts you for other credentials if your account does not have the necessary privileges. The context menu also allows you to directly change the User/group options for the selected item.



Assigning File Groups to users/user groups

Users are not allowed to run a program, script and macros (except if the Local Authorization option is activated) unless it has previously been scanned, organized into a File Group, and then assign these File Groups to a user/user group. In this section, we explain you how to perform this last step.

To assign/remove File Groups to/from users

1. Open the *User Explorer* module. To do this, click on the corresponding icon  located in the *Modules* section of the *Control Panel* of the main window or use the *View*→*Modules* command.
2. Click on the *File Groups by User* tab.
3. In the *Users* panel, select a user or user group. The *File Groups* panel shows you the File Groups for which this user/user group already has authorizations, which ones are not authorized, and which are indirectly authorized because the user belongs to a domain group that has authorization.

To add a Group File to the user's *Directly Authorized* list, select it from the *Not Authorized* list and click on the **AUTHORIZE** button.

To revoke a user's access privileges for a File Group, select it from the *Directly Authorized* list and click on the **REMOVE** button.

Even if a user is indirectly authorized for a File Group, you might want to directly authorize it as well, so the user would not be inadvertently affected later if authorization privileges or membership of the group to which he belongs changes.

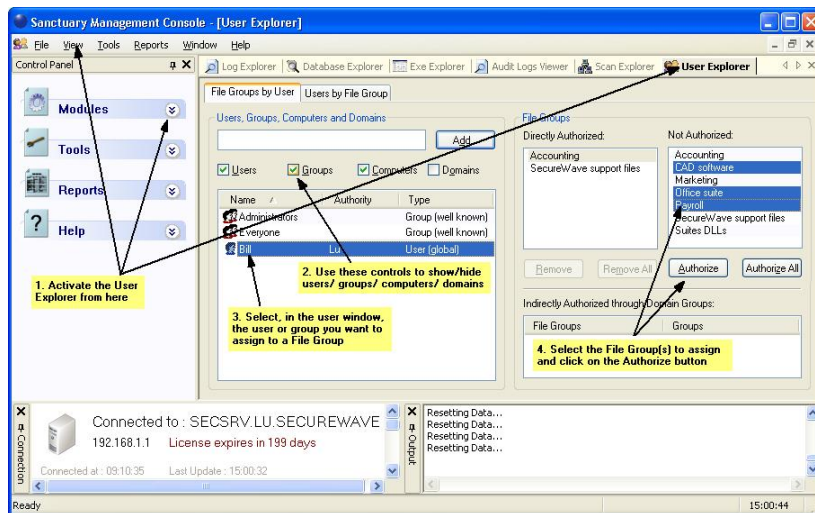


Figure 45. User Explorer Module Window: File Groups by User

4. If you want to make the change immediately, send the updated authorization(s) to affected machines.

To send the new authorization information to all machines, select *Send Updates to All Computers* from the *Tools* menu (or from the *Control Panel*). To push updates to a specific computer, select *Send Updates to <name>* from the *Tools* menu (or the *Control Panel*) and select the computer from there.

If you do not push updates to protected clients, they automatically receive updates at next time they restart or logon.



The 'Indirectly Authorized through Domain Groups' panel does not show Active Directory nested groups.




You can right-click on any user, group, or computer in the 'User Explorer' display to set its Options. For more information, see Chapter 12: Setting Sanctuary system options on page 105.



Assigning users/user groups to File Groups

You may want to assign users/user groups to new File Groups, rather than the other way around. For instance, if you have created a File Group for all the executables in an updated version of an already authorized application. The next step is to grant users the access to the newly created File Group.

To assign/remove users to/from a File Group

1. Open the *User Explorer* module. To do this, click on the corresponding icon  located in the *Modules* section of the *Control Panel* of the main window or use the *View→Modules* command.
2. Click on the *Users by File Group* tab. The system displays a list of File Groups in the left panel and the associated users/groups in the right one.

In the *Associated Users* panel, you find those users who are associated with the selected File Group — that is, which users/groups have privileges to execute files in that File Group.

The underlying authorizations are the same as when viewed in the *File Groups by User* tab. This is just a different way of presenting the same information.

3. Modify the users assigned to a File Group. To do this:
 - > Select one or more user/user group and then click on the **ADD** button to insert them to the File Group.

— or —

- > Select one or more user/user group and then click on the **REMOVE** button to delete them from the File Group.

— or —

- > Click on the **REMOVE ALL** button to delete all users/groups from the File Group.

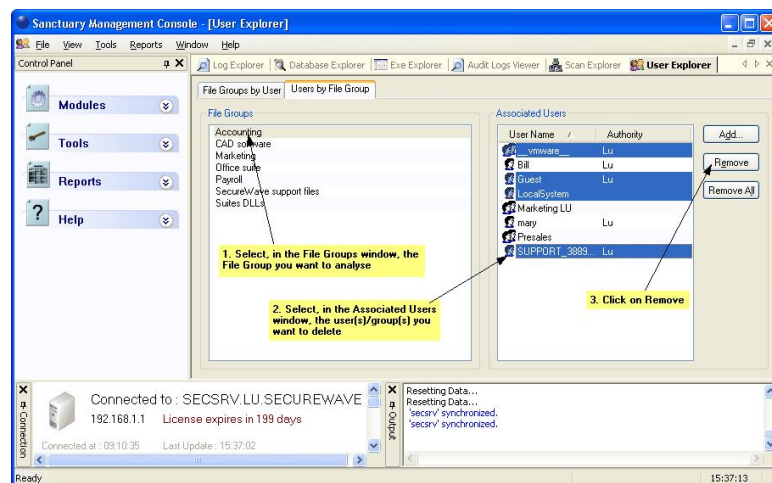


Figure 46. User Explorer Module Window: Users by File Groups

Chapter 9: Monitoring activities using the Log Explorer

Every server or computer under the protection of Sanctuary generates activity logs that record application attempts, denials, and, optionally, authorizations. In addition, they also generate audit logs showing actions carried out by administrators, such as changing user access rights and file group permissions. The information in both these logs is sent to the SecureWave Application Server and can be viewed through the *Log Explorer* module of the Sanctuary Management Console.

If you have appropriate administrative privileges, you can use the *Log Explorer* module to view logs of executable files, scripts and macros:

- > That have been executed or denied by central authorization.
- > That were executed or denied by local authorization.
- > For a designated user, computer, or filename (by matching pattern).

The *Log Explorer* module does more than display this information. From within the log displays you can also:

- > Sort, add criteria, define columns, create templates, and organize information in several ways to suit your needs and those of your company.
- > Monitor the activities of administrators using audit log information.
- > Save the results of querying log entries to a CSV file (comma-separated values).
- > Authorize the use of files that have been denied.

You can use the *Log Explorer* module to generate automatic reports containing either details of granted or denied applications or administrator actions. These can be scheduled to run at regular intervals between specified start and end dates. Templates in the *Log Explorer* module enable you to generate customized reports quickly and easily. They contain the criteria you want to use to select the results in the report. They also contain details of what information is displayed for each result in your report.

Reports can either be generated on demand or you can schedule Sanctuary to generate them in a particular format and deliver them either to a particular shared folder or email recipients. For example, you can specify that you want to receive an email each Monday containing a custom report of the previous week's activities.

The following limitations apply when using the *Log Explorer* module under various user/domain accounts:

Possible configurations	Domain type	Logged user*	Result	Notes
SecureWave Application Server and Sanctuary Management Console are running on the same machine	n/a	Current user	Works properly	
		Other user	Works properly	User has to use either localhost or the local computer name in NetBios format in the Sanctuary Management Console login dialog.
SecureWave Application Server and Sanctuary Management Console are running on different machines	Trusted domain	Current user	Works properly	
		Other user	Works properly	Only if DCOM is configured correctly** (if using Windows XP SP2 or later, Windows 2003 SP1 or SR2, or Vista).
SecureWave Application Server and Sanctuary Management Console are running on different machines	Un-trusted domain	Current user	Would not work	
		Other user	Works properly	Only if DCOM is configured correctly** (if using Windows XP SP2 or later, Windows 2003 SP1 or SR2, or Vista).



* Current User means that you have logged in to Windows and Sanctuary Management Console as the same user. See *Log in as a different user* on page 14.

**A user needs to have both permissions on machine wide DCOM security, and the permissions set in DCOMCNFG to successfully use DCOM. See <http://www.microsoft.com/technet/prodtechnol/winxp/maintain/mangxpsp2/mngsecps.mspx>.

To correctly configure machine-wide DCOM (Group Policy):

1. Run gpedit.msd (*Start → Run*).
2. Go to *Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options*.
3. Double click on '*DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax*' on the right pane, click on '*Edit Security*' and add users and groups who are allowed Local/Remote access.
4. Double click on '*DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax*' on the right pane, click on '*Edit Security*' and add users and groups who will be allowed Local/Remote activation.
5. Close Group Policy Object Editor.
6. Run gpupdate.exe to refresh group policy.

To correctly configure DCOM (dcomcnfg.exe):

1. Run dcomcnfg.exe (*Start → Run*).
2. Select '*Component Services*' and open the '*Computer*' branch.
3. Right-click on the specific computer on the right panel and select '*Properties*'.
4. Select the '*COM Security*' tab, click on '*Edit Limits*' in the '*Launch and Activation Permissions*' panel.
5. Select the user you want to define as the Sanctuary Management Console administrator and activate the '*Remote Activation*' option.
6. Verify that in the '*Access Permissions*' panel the chosen user has '*Remote Access*' activated.


Table 13: Log Explorer module limitations if using other user/domain account



The DCOM settings, as described in the above table must be modified on all machines where the SecureWave Application Server is installed

DCOM does not work across non-trusted domains. This is especially true when using Workgroups. This is a Windows limitation and one possible workaround for this issue is to use the same login/password for the Sanctuary user, Windows user on the SecureWave Application Server (SXS), and Windows user on the Sanctuary Management Console. The Log Explorer module works better when using an account with administrative rights..

Accessing the Log Explorer module

You can access the *Log Explorer* module by clicking on the  icon located on the *Modules* section of the *Control Panel* in the main *Sanctuary Management Console* window.

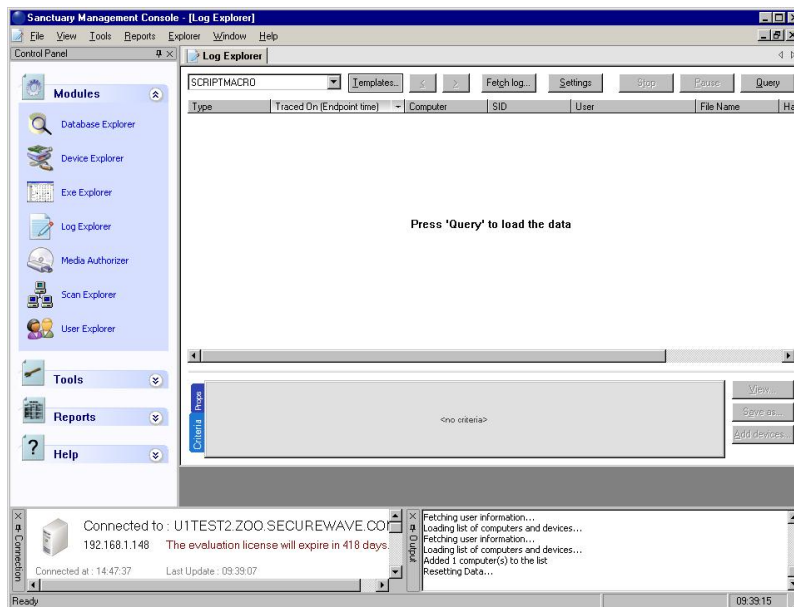
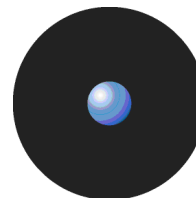


Figure 47: Log Explorer main window





Log Explorer templates

The operation of the *Log Explorer* module is based on templates. These let you generate custom reports containing results that match particular criteria.

As you use the *Log Explorer* module - changing criteria options, column size and order, which columns are displayed in the Results panel (and custom reports), and the whole set of configurable options - you are creating a template. A template is, in this context, a set of rules to use when displaying data in the *Log Explorer* module. Once satisfied with your log report, you can save this template for future use.

You can create your own templates and save them as you progress in your work. Alternatively, you can opt for a simpler approach using predefined templates created by SecureWave.


 *The list of predefined templates may include some that do not apply to the type of license you purchase and, thus, has no use for you.*

 *If you have upgraded from a previous version of Sanctuary your existing templates were stored in the registry (or elsewhere). In this case, when you start the Log Explorer module you can specify how you want to update these. You can migrate some or all of the existing templates stored in the registry, import any that are stored elsewhere, or remove templates from the registry. The Select and edit templates window displays a list showing the templates you can access that have been set up, migrated or imported.*

To use an existing template

1. Choose the template you want to use — created by SecureWave or by you. To do this, either select the template from the list of recently used templates in the top left corner of the *Log Explorer* navigation/control bar, or click on the TEMPLATES button, highlight the template in the list in the Select and edit templates window and click on the SELECT button.
2. Execute the template to create a report that is shown in the main *Log Explorer* window. To do this, click on the QUERY button.

A table of results displays in the main *Log Explorer* window. Each row represents one or more log entries that match your query criteria. For each log entry or group of log entries, the columns represent the display information that chosen for the template.

 *The query only returns results if you have appropriate access rights to view it. See Chapter 4: Setting up Sanctuary administrators on page 29 for more details.*

To create and use a new template

1. Click on the TEMPLATES button in the *Log Explorer* window. The *Select and edit templates* window is displayed.

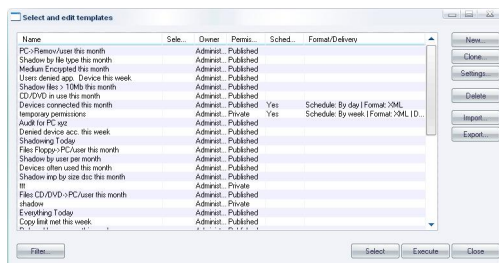


Figure 48: Select and edit templates window

2. Click on the NEW button. The *Templates settings* window is displayed.

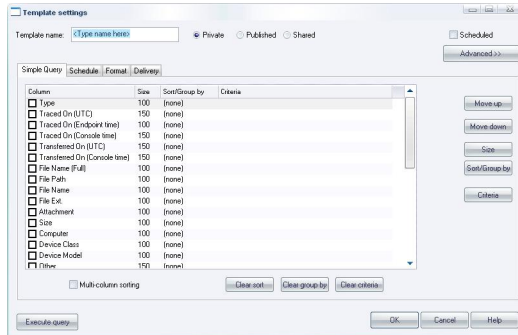
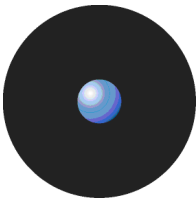




Figure 49: Templates settings window

 If you select the Count Column then the results are automatically grouped.

1. Enter a name for your new template in the *Template name* field.
2. Choose whether you want the new template to be accessible only to yourself and Enterprise administrators (*Private*), to be usable but only editable by the owner and Enterprise Administrators (*Published*), or to be editable by anyone (*Shared*).
3. Specify your query columns and criteria. These determine which log entries are selected as results in the *Log Explorer* report, and the information that is displayed in each.

To select log entries that match certain criteria, select the *Column* to which the criteria apply, by clicking on the appropriate box, clicking  in the *Criteria* column, and specifying what you want to match entry details to. See *Table 17* on page 83 for instructions on how to define query criteria.


You can choose which information to display for each entry, the display size of the columns and how the results are grouped or sorted in particular ways.

For more information about criteria, displaying and sorting results and so on, see *Criteria* on page 82.

7. If you are creating a template for a regularly generated report, specify the schedule, i.e. when the report is automatically produced, the format of the report and the recipients of the report. To do this, complete the fields on the *Schedule*, *Format* and *Delivery* tabs of the *Template settings* window.

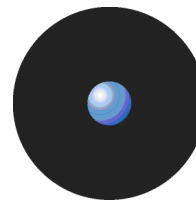
For more information, see *Schedule tab* on page 85.

8. Execute the query. To do this, click on the *QUERY* button in the *Log Explorer* window, or the *EXECUTE* button in the *Template settings* window.

 All fields act interactively: when you change one of them, it does a logical AND with all the others. If, for example, you select a range of traced dates and then a user, the resulting data includes all events for the selected user that occurred between the selected dates.

 The template is stored when you execute the query.

If there are any records that match your query criteria, they appear in the *Results* panel list of the *Log Explorer* window (and your custom reports). The query only returns results if you have appropriate access rights to view it.



Log Explorer window

The main *Log Explorer* window contains the following five main elements:

- > Navigation/Control bar.
- > Column headers.
- > Results panel (the contents of which can be scheduled for sending/storing as a custom report).
- > Criteria/Properties panel.
- > Control button panel.

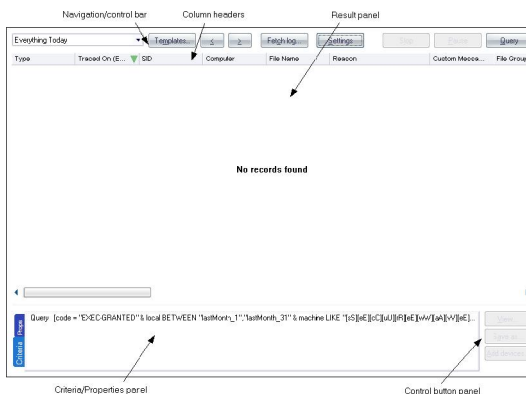


Figure 50: Components of the Log Explorer window

Navigation/Control bar

You can use the button bar on the upper part of the main window to select a template and navigate through or control your results:



Figure 51: Navigation/Control bar

- > Template list — selects a template from your recently used templates list, shown in the drop-down list.



In previous versions of Sanctuary the templates list included all templates created by you or by SecureWave. All templates can be accessed by clicking on the TEMPLATES button.

- > TEMPLATES button — used to create a new template or select an existing one from the list in the Select and edit templates window.
- > ⏪ (Previous) button — navigates to the preceding result list from the ones internally stored, if you are carrying out multiple queries.
- > ⏩ (Next) button — navigates to the following result list, if you are carrying out multiple queries.
- > FETCH LOG button — retrieves logs and shadow files from a computer or a list of computers running the Sanctuary Client Driver. The *Select Computer* window is displayed. See *Forcing the latest log files to upload* on page 87.
- > SETTINGS button — goes directly to the advanced settings dialog for the template you are currently using. Here you can select columns and define criteria. See *Template settings window* on page 80.
- > STOP button — cancels the current query. This is used if you want to interrupt a lengthy sorting operation involving a large number of log entries.
- > PAUSE button — cancels the screen output, with any sorting processes continuing in the background. To resume the screen display, click on this button again.
- > QUERY button — retrieves all log entries that match the criteria defined in the current template.



Column headers

The column headers display the title of the columns. In addition, you can use them to:

- > Sort results — classify the results and display them in a specified depending on the value for the log entry (or log entries) in one or more columns.
- > Show/hide columns — determine what information is displayed for each result in the report.
- > Change the size of the displayed columns — by dragging the column header dividers to the left or right.
- > Change the order in which the columns are displayed — by dragging and dropping the column titles in the column headers.
- > Group log entries — display a single report row corresponding to multiple log entries grouped according to the values in one column.
- > Display computed columns — display calculated values such as a count of the number of log entries in a grouped result, the maximum value, minimum value, sum of values, or average value.



You can make changes to the columns to display different information from the log entries without reexecuting the query.



Any on-the-fly changes you make to the column headers are saved in the template. For example, if you use the column context menu to group the results the next time you run a query using the template the results are automatically grouped.



You can also use the column context menu to access the advanced query settings for the template. For more information about defining complex queries see [Query & Output tab on page 83](#).

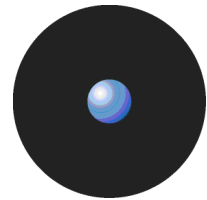
Sorting results

To sort results in an ascending by a value in a particular column, click once on the header — click again to sort in descending order. Click on another heading to change the sorting order to that column. You can see the result as a green arrow in the column's title with the sorting order number. The direction of this arrow shows whether sorting is in ascending or descending order.

If you want to sub classify your results click on the **SETTINGS** button, select the *Multi-column sorting* checkbox, and, in the right-click menu for the relevant Column, select either '*Ascending*' or '*Descending*'. When you save the settings a blue arrow, with the number '2' on it is displayed in the column's title bar. You can set up further sub classifications in the same way.



Figure 52: Column headers showing multiple classifications



Show/hide columns

If you want to show or hide particular columns of log entry information, right-click on the column headers and select/deselect the required column(s) in the context menu respectively.



Figure 53: Columns context menu

The names of the columns in the Columns context menu, shown above, depend on the installed license.

Group log entries

You can group multiple log entries into single report rows according to the values in one or more columns log entries. To do this, select the *Group By* option in the Columns context menu and check the column you want to group your results by. For example, if you check the device type column then all log entries for devices of a particular type are combined into a single result in the report.

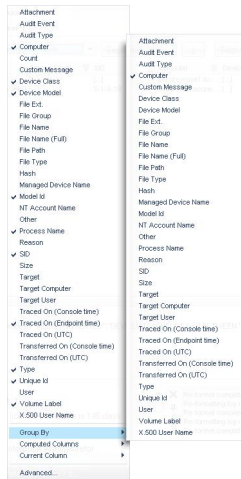


Figure 54: Group By option

A green 'circle' in the column's title shows when a column is used to group results.



Figure 55: Column headers showing grouped results

You can also set up sub groups in the same way. Secondary subgroups are denoted by a blue 'circle' with the number '2' displayed in the column's title bar. You can set up further sub groups in the same way.



Figure 56: Column headers showing sub groups



Computed columns

In addition to the columns corresponding to information stored in the log entries, you can also include computed columns in your report, for example, you can display the number of log entries with a particular value or the average value for the column in a group.

The operations supported by computed columns are:

- > Count — calculates the number of log entries in which a certain type of value exists, for example Count (Device Class) shows how many log entries contain device information. Count (Any) simply shows the total number of log entries.
- > Min, Max — calculates the minimum or maximum value in a column in a given set of results.
- > Sum — (only valid for the file size column) calculates the sum of numerical data.
- > Average — (only valid for the file size column) calculates the numerical average in a given set of results.

 *Not all of these operations work for all columns.*

To set up a computed column, right-click on the column header, highlight the *Computed Columns* option in the Column context menu, highlight the type of calculation you want to carry out in the Computed Columns sub menu, and then select the column that contains the data you want to use to calculate computed values from. For example, the following figure illustrates the selections required to display a column showing the number of devices of each device class.

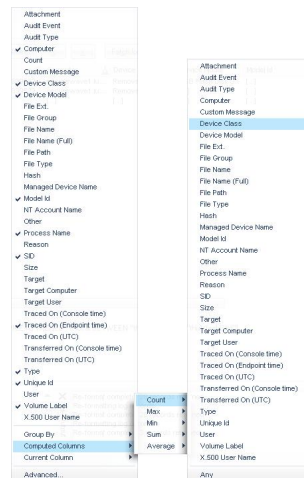


Figure 57: Computed columns

The title of the computed column is displayed in the column header and the calculated values in the Results panel (or custom report).

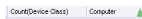


Figure 58: Column headers showing a computed and a sorted column

Clear column settings

If you want to clear the sorting filters and groups, you can either:

- > Proceed to the *Template settings* window. For more information see *Template settings window* on page 80.
- > Change the column settings of the currently selected column. To do this, select the Current Columns option in the Column context menu and select the relevant choices, for example *Unsort* or *Ungroup*.

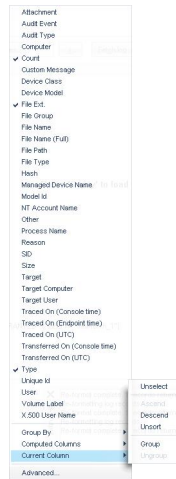



Figure 59: Resetting column headers

Results panel / custom report contents

The Results panel is the main area of the *Log Explorer* window where the results are displayed and classified.

You can, among other things:

- > See which files have been executed or denied by central authorization.
- > Find out which files were executed or denied by local authorization.
- > Check which File Groups were assigned to particular files.

 *The results you see may depend on the role assigned to you by the Enterprise Administrator.*

You can save the information displayed as a CSV file using the **SAVE AS** button of the *Control button* panel (in the bottom right corner of the *Log Explorer* window).

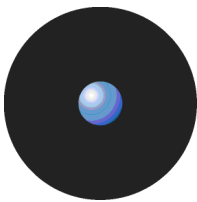
When you generate scheduled custom reports the results, rather than being displayed in the Results panel, are sent to specified email recipients or stored in a specified directory.

Columns in Results panel / custom reports

You can control whether columns of information from log entries are displayed and their size, and position from the *Template settings* window.

Some columns are specific to device logging or shadowing options while others are common to both of them. There are a number of log entry columns that are only applicable when monitoring administrator actions, for example Audit event, Target user, Target computer, and Target.

The following table summarizes the meaning of the log entry information columns:



Column	Description
<i>Audit Event</i>	The nature of the event that triggered the audit log. See <i>Audit events</i> on page 88 for a description of the different audit events that can be recorded.
<i>Audit Type</i>	The type of action the administrator carried out. This can be ' <i>Device Control</i> ' or ' <i>Application Control</i> '.
<i>Computer</i>	The name of the machine where execution was attempted.
<i>Count</i>	This shows how many log entries are hidden in a single row. Alternatively, this may be a computed column of data. A grouping symbol is displayed on the column header.
<i>Custom Message</i>	Indicates why the application is running or not running, for example because it is authorized, because the machine is in non-blocking mode, or because there is a Path Rule authorizing it. See <i>Table 15</i> .
<i>File Ext</i>	The extension of the file.
<i>File Group</i>	The file group to which the executable, script, macro (or file containing a VBA macro) has been assigned. This can also be <Not Authorized>.
<i>File Name</i>	The file whose execution was authorized or denied.
<i>File Name (full)</i>	The full name (including path) of the file whose execution was authorized or denied.
<i>File Path</i>	The path of the file whose execution was authorized or denied.
<i>File Type</i>	Indicates whether the file relates to a script or an application, for example ' <i>Executable</i> ' or ' <i>Script</i> '.
<i>Hash</i>	The digital signature of the file, created by SHA-1 (Secure Hash Algorithm -1). Knowing the hash enables you to differentiate between files with the same name.
<i>NT Account Name</i>	Domain user name of the person who triggered the event, for example ' <i>MARVIN/johns</i> ' or <i>LocalSystem</i> .
<i>Other</i>	This may contain additional information, in the case of an audit event, for example, if an administrator erases a scheduled permission, this may contain its parameters.
<i>Reason</i>	Indicates whether an action was granted or denied. This can have a value of ' <i>NoPermission</i> ', ' <i>Granted</i> ' or ' <i>Denied</i> '.
<i>SID</i>	The Secondary Identifier of the user, for example ' <i>S-1-5-21-647365748-5676349349-7385635473-1645</i> '. This is useful when attributing actions recorded in log files to users who have left your organization.
<i>Target</i>	The device for which the permissions were modified.
<i>Target Computer</i>	Name of the computer that was the target of the administrator action.
<i>Target User</i>	Name of the user or group to which the administrator action was applied.
<i>Traced On (Console time) *</i>	Date the event occurred on the console computer.
<i>Traced On (Endpoint time) *</i>	Date the event occurred on the client computer.
<i>Traced On (UTC)*</i>	Date (Coordinated Universal Time) the event occurred on the client computer.
<i>Transferred On (Console)*</i>	Date the event record was transferred from the client computer to the SecureWave Application Server.
<i>Transferred On (UTC)*</i>	Date (Coordinated Universal Time) the event record was transferred from the client computer to the SecureWave Application Server.
<i>Type</i>	The nature of the event that triggered the log. This can be ' <i>Execution Granted</i> ', ' <i>Execution Denied</i> ', or the type of audit event (see <i>Audit events</i> on page 88).
<i>User</i>	Name of the user who triggered the event, e.g. ' <i>MARVIN/johns</i> '. Also see note after table. For users removed from the Active Directory, this field displays the SID, enabling the person who triggered an event to be identified after they have left your organisation.
<i>X.500 User Name</i>	The username in Lightweight Directory Access Protocol format. This reflects the directory tree in which the user information is stored, for example, the X.500 user name may be ' <i>CN=John Smith, CN=Users, DC=Marvin...</i> '

*Old client drivers provide time in UTC format only leading to incomplete data in these fields

Table 14: Log Explorer module columns



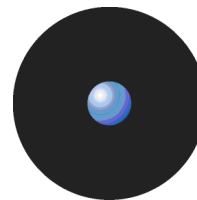
The '*User Name*' column may show the System Identification Number (SID) instead of the resolved user's name in Novell environments when Novell objects are not synchronized. You should first consider running the synchronization script described in detail in the *Sanctuary's Setup Guide*. You can also automate this script's execution for your convenience.



Columns with names starting '*Count*', '*Min*', '*Max*', '*Sum*' and '*Average*' may also be displayed. These contain computed data based on the values in the specified columns. See *Computed columns* on page 74.



Ellipses (...) in the Results panel indicate hidden log entries. For example, if you group a set of results using the value in one column, then the multiple values in some other columns for the results group are shown as [...].



The *Custom Message* field displays one of the following values (which are affected by the system-wide option settings for Execution Blocking and the logging mode):

Custom Message Column Value	Description	Did the file run?
<i>Authorized</i>	This file is known, its digital signature is recorded in the SecureWave Sanctuary Database. If this file has been assigned to a File Group, it is also shown.	Yes
<i>Denied</i>	The file was not allowed to run because it was neither centrally nor locally authorized.	No
<i>Logon</i>	This file was allowed to run because 'Relaxed logon mode' was active (Relaxed logon option). See <i>Relaxed logon</i> on page 113 for more details.	Yes
<i>ok-dllDontCare</i>	The DLL execution was authorized because the Execution Blocking option was set to 'Ask user for *.exe only.'	Yes
<i>ok-hash</i>	The file was executed and this action was logged because the option to Log Everything was set on. This option should only be set for a limited period, or else the system generates an unmanageable amount of data.	Yes
<i>ok-localAuth</i>	This file would have been denied because it is not centrally authorized, but the user was prompted to locally authorize, and he/she allowed execution.	Yes
<i>ok-nonBlocking</i>	If the system had been in blocking mode, this file would have been denied, but it was executed because the NON-BLOCKING option was on.	Yes
<i>ok-nonBlockUser</i>	The file would have been denied based on central authorization, but it was executed because the non-blocking option was on for a user or group of users.	Yes
<i>ok-pathRule</i>	This file was allowed to run because it matched a Path Rule.	Yes

Table 15. Custom Message Field Values

Interpreting results

You can interpret data from the *Log Explorer* window in several ways. The two main reasons for not executing a file, resulting in the value '*Denied*' in the *Custom Message* column, are as follows:

- > The file is unknown or not on the 'white list'. This means that either:
 - The program is not authorized and should remain this way. This is a 'normal' situation where the user is trying to run a non-allowed application.
 - or –
 - That the software has not been yet authorized and should be investigated. If appropriate, you should add it to the 'white list' to conduct your business.

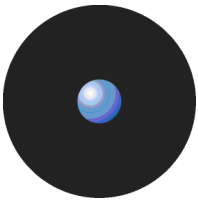


It is dangerous to authorize executables directly from the Log Explorer unless you are absolutely certain that the software can be trusted. A user may try to fool you by renaming an unauthorized application, for example, she could rename an unauthorized file 'notepad.exe' and complain that her notepad is not working. Before you authorize an application, first check the program.

- > The user does not have access to the File Group that the file belongs to. For example, the file may have been scanned and in the 'white list' but may belong to a File Group 'Accessories' which is not accessible to the user. This means that either:
 - This is a 'normal' situation where a user is trying to run a program to which he has no rights.
 - or –
 - The user, or one of the user groups to which he belongs, should be granted access to the appropriate File Group to conduct your business.

When a user has permission to locally authorize files and uses a particular file frequently, it may be worth scanning the file and including it in a special File Group to avoid having several users locally authorizing the same application.

Log entries displaying 'ok-dllDontCare' in the *Custom Message* column are special case of Local Authorization where the user only authorizes the EXE file (using the Execution blocking option 'Ask user for *.exe only') and all DLL are automatically authorized. See *Chapter 12: Setting Sanctuary system options* on page 105.



When you are using the *Log Explorer* module to monitor administrator actions the *Target* field may show a different set of information than that normally received for a File Group. You can see, for example:

- > When a User Access role has been modified, for example from 'Administrator' to 'Enterprise Administrator'.
- > When options were changed.
- > When the name of the authorized files have been changed.

Criteria/Properties panel

The *Criteria/Properties* panel has two tabs. These are:

- > *Props* tab — displays the log entry information corresponding to a selected results row in the Results panel.



Figure 60: Props tab

- > *Criteria* tab — displays the criteria used by the template to select log entry results to show in the Results panel.

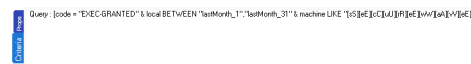


Figure 61: Criteria tab

Control button panel

On the lower right part of the main window, you can find the following control buttons:

- > **VIEW** – Not used if you do not have Sanctuary Device Control installed. See the *Sanctuary Device Control Administrator's Guide* for more details.
- > **SAVE AS** – to save the information in the *Log Explorer Results panel* data as a CSV file.
- > **ADD DEVICES** – Not used if you do not have Sanctuary Device Control installed. See the *Sanctuary Device Control Administrator's Guide* for more details.



Figure 62: Control button bar

Select and edit templates window

The *Select and edit templates* window is used to select, add, edit, import, export and execute templates. To display the *Select and edit templates* window, simply click on the Log Explorer TEMPLATES button.

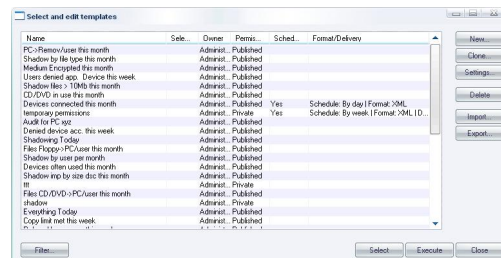
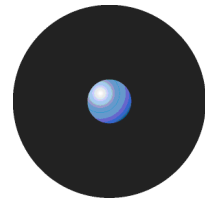





Figure 63: Select and edit templates window



The *Select and edit templates* window contains the following:

- > List of all the existing templates that you can access assuming this list is not filtered — see below). These may be created by yourself, one of your colleagues, or SecureWave. You can select a template and right-click to display a Templates context menu.
 -  The asterisk (*) in the *Selected* column indicates the template that is currently selected. You can either change the settings of this, or another highlighted template. To select a different template, highlight it in the list and click on the *SELECT* button.
 -  The *Permissions* column in the *Select and edit templates* window indicates whether the template can be viewed or changed by people other than the owner. The *Scheduled* and *Format/Delivery* columns indicate whether the template is used to create automatic reports periodically and, if so, who these are emailed to and/or where they are stored.
 -  You can click on the column headers to sort this list, or drag and drop the column titles to reorder the column information.
- > **NEW** button — to create a template (see *To create and use a new template* on page 69).
- > **CLONE** button — to create a new template based on an existing template (with the *Shared* and *Scheduled* flags removed, if these were present in the original template).
- > **SETTINGS** button — go directly to the *Template settings* window for the selected template. Here you can define the criteria used to select results and choose how the results are displayed. For more information see *Template settings window* on page 80.
- > **DELETE** button — to remove a selected template.
- > **IMPORT** button — to import templates in XML format or to import legacy templates (*.tmpl) from the registry.
- > **EXPORT** button — to export the highlighted template to an XML file.
- > **FILTER** button — to choose which templates are displayed in the *Select and edit templates* window. See below.
- > **SELECT** button — to select the highlighted template as the current template and return to the main *Log Explorer* window.
- > **EXECUTE** button — to retrieve all log entries that match the criteria defined in the current template and display these in the *Log Explorer* window.
- > **CLOSE** button — to return to the *Log Explorer* window without changing the current template.

To determine which templates are listed in the *Select and edit templates* window, click on the **FILTER** button, select the appropriate check boxes and click on the **OK** button. Selecting multiple filtering criteria shows a more focused set of templates, i.e. reduces the number of templates that are listed.

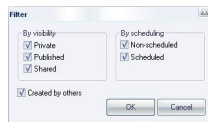


Figure 64: Filter templates dialog

The following template filters can be used:

Checkbox	Used to display...
<i>Private</i>	Templates that are only visible to the owner (and Enterprise Administrators).
<i>Published</i>	Templates that are visible to all Sanctuary Management Console users within your Sanctuary system, but can only be changed by the owner (and Enterprise Administrators).
<i>Shared</i>	Templates that can be seen and changed by all Sanctuary Management Console users within your Sanctuary system.
<i>Non-Scheduled</i>	Templates used to generate ad hoc reports.
<i>Scheduled</i>	Templates that are automatically executed periodically to generate regular reports.



Checkbox	Used to display...
	These are either saved in a shared folder on your Network or emailed to specified recipients.
Created by others	Templates created by other people. This is unchecked, for example, by Enterprise Administrators when they want to display only their own templates.

Table 16: Template Filter checkboxes

When you right-click on the main panel of the *Select and edit templates* window, the Templates context menu is displayed.

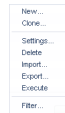


Figure 65: Templates context menu



The options that are available in the Templates context menu depend on whether you have a template highlighted or not when you right-clicked.

You can use the Templates context menu to:

- > Create a new template either from scratch (New) or based on an existing template (Clone).
- > Change the settings of the highlighted template.
- > Delete the highlighted template.
- > Import either templates in XML format or legacy templates (*.tmpl) from the registry.
- > Export the highlighted template to an XML file.
- > Execute the query to retrieve all log entries that match the criteria defined in the current template, and display these in the *Log Explorer* window. This makes the highlighted template the currently selected template.
- > Filter the templates shown in the *Select and edit templates* window.



You can also carry out the same actions on the highlighted template using the following shortcut keys: Insert creates a new template, Delete removes a template, F2 opens the Template settings window, Ctrl+C clones the template, Ctrl+I imports a template, Ctrl+E exports the template, Ctrl+F filters the list of templates, and Ctrl+X executes the highlighted template.

Template settings window

The *Template settings* window is used to define the settings used for a new template, or one highlighted in the *Select and edit templates* window:

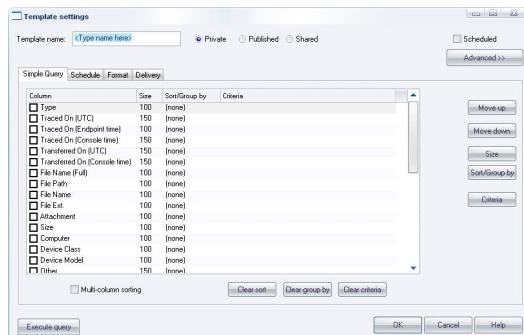
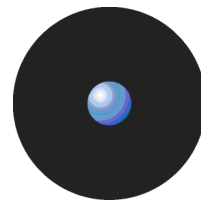


Figure 66: Template settings window – Simple Query tab

You can use the *Template settings* window to do the following:



- > Name of a new template and specify who is allowed to see it and edit it — by selecting one of the *Private*, *Published* or *Shared* options.



Template names are not required to be unique, however we recommend they are to avoid confusion.

- > Choose whether the template is used to generate reports automatically on a periodic basis — by checking the *Scheduled* box.
- > Specify the selection and display settings for the template — using the *Simple Query* tab.
- > Specify complex *selection and display settings for the template* — by clicking on the *ADVANCED* button and using the *Query* and *Output* tab.
- > Schedule the production of periodic reports using the template — using the *Schedule* tab.
- > Define the format of scheduled reports — using the *Format* tab.
- > Choose who you want the reports to be emailed to — using the *Delivery* tab.
- > Execute the query specified by the template and display the results in the main *Log Explorer* window. To do this, click on the EXECUTE QUERY button. (This also makes the template you are editing the currently selected template.)
- > Save the changes made to the template settings — by clicking on the OK button.

Simple Query tab

The *Simple Query* tab is displayed by default when the *Template settings* window opens. You can use it to do the following:

- > Show/hide columns — simply check/uncheck the column names in the Columns list. The column name moves to the top section of the list when you check it.
- > Change the display size of a column — click on the *Size* cell of the row corresponding to the appropriate results column (or highlight the row and click on the *SIZE* button) and type in the size you want. You can also change the size of a column in the main *Log Explorer* window by dragging the column header divider left or right.
- > Sort ascending/descending — click on the *Sort/Group by* cell of the row corresponding to the appropriate results column (or highlight the row and click on the *SORT/GROUP BY* button) and choose either *Ascending* or *Descending* from the drop-down list options. If you want to sort the results of the query by the values in more than one column, check the *Multi-column sorting* box in the lower left of this tab and choose the columns that you want to sort your results by in turn.
- > Group the results according to the value in a particular column — click on the *Sort/Group by* cell of the row corresponding to the appropriate results column (or highlight the row and click on the *SORT/GROUP BY* button) and choose the *Group by* option from the drop-down list. When grouping results, all log entries in the *Log Explorer* Results panel/custom report are 'piled' into single entries corresponding to the unique values in the column.

File Type	Count(Type)	Computer	Traced On (En...
Executable	1
Script	2

Figure 67. Grouping results in the query

In the above image, results are grouped according to their File Type value. The ellipses indicate hidden log entries and the Count column indicates how many log entries have the same File Type.

- > Specify the criteria used to select results to be shown in the report — click on the *Criteria* cell of the row corresponding to the appropriate results column (or highlight the row and click on the *CRITERIA* button) and select the criteria you want to use to select results to display in the main *Log Explorer* Results panel/custom report. For more information about setting criteria, see below.



*If you want to use specify a complex set of selection criteria or display settings click on the *ADVANCED* button and enter information on the *Query* and *Output* tab. For more information see *Query & Output* tab on page 83.*



- > Decide the column display order — using the MOVE UP and MOVE DOWN buttons located on the right of the window.
- > Clear sorts, groups, add or remove criteria, change the size of any column, and execute the query — using the corresponding buttons located on the lower and right part of the window.

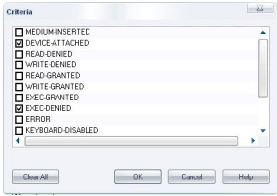
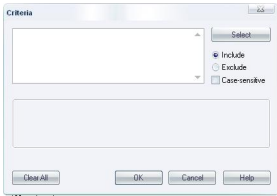
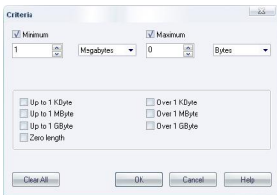
Criteria

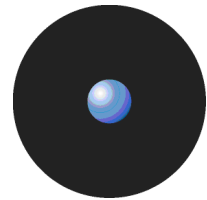
Criteria make it easier to find the result or results you are interested in. Typically the more specific you are with your search criteria, the fewer results are returned, i.e. the Results list in the main *Log Explorer* window is less clogged up with results that are irrelevant to your search.

You specify the criteria you want to use for a particular template using one or more context-dependent *Criteria* dialogs. For example, when you are specifying that a log entry must match one (or more) or a fixed set of values the *Criteria* dialog displays a list of the possible values you may want to match. Alternatively when you are specifying a match to a free text data field the appropriate *Criteria* dialog lets you type in what is needed using wildcards to delimit the criterion, for example, you can say enter 'wind*.*' to search for all files with names starting with 'wind' and with any file extension, or enter 'project.mp?' to search for all files with names starting with 'project.mp' followed by one additional character.

In some *Criteria* dialogs, you can also choose to exclude results that match a criterion. Others contain a SELECT or SEARCH button, for example, where specifying criteria involves matching to one or more particular computers or users.

Various different types of *Criteria* dialogs are explained in the following table:

Criteria Dialog	Description
	<p>Criteria List</p> <p>This form of the <i>Criteria</i> dialog is displayed when log entry fields contain one of a fixed set of values.</p> <p>Check or uncheck the boxes that correspond to the values you are looking for. For example, using the 'Custom Message' column, if you are searching for log entries related to executions that succeeded because the executable was authorized, set the 'ok-Hash' checkbox and clear all others. If you additionally want to see executions that were allowed because of matching Path Rules, set this checkbox as well. The query then returns log entries related to these two types of authorized execution.</p>
	<p>Free-text criteria</p> <p>This form of the <i>Criteria</i> dialog is used to filter the query results based on any text that you type in.</p> <p>Enter the text you want to use to search in the field. You can use wildcards (? to match any single character and * to match any sequence of zero or more characters).</p> <p>If entering several strings, separate them using semicolons (;) to get log entries matching any of the strings specified. You can further specify — using the options on the right of the dialog — whether the search should be case-sensitive, and whether the query should return entries that include or exclude the specified strings.</p> <p>For example, to search all log entries that contain main executables run by users, enter '*.exe' (without the quotes). To additionally return results concerning XP Service Pack Message DLLs (xpsp1res.dll, xpsp2res.dll...), enter '*.exe;xpsp?res.dll' (without quotes).</p>
	<p>Size criteria</p> <p>This form of the <i>Criteria</i> dialog is only meaningful if you also use Sanctuary Device Control. It shows event logs for shadow files based on their size.</p> <p>The query returns log entries concerning files with the size specified in the 'minimum' and 'maximum' values. Alternatively, you can select one of the predefined common sizes by clicking the corresponding checkboxes.</p>



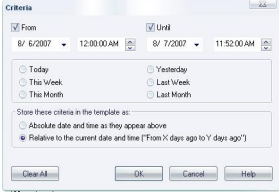
Criteria Dialog	Description
	<p>Time criteria</p> <p>This form of the <i>Criteria</i> dialog is used to search for log entries that were produced, or uploaded to the server, at a certain date/time.</p> <p>You can enter any period into the 'From' and 'Until' controls, or click one of the commonly used time range settings. You can further specify how these time criteria are stored in the template (this influences they are interpreted when you execute the query).</p> <p>If you chose to save your settings as absolute values, there are considered as unconditional parameters. For example, a query for log entries between May 21st 2007 and May 23rd 2007 returns the log entries produced between these two dates.</p> <p>If, on the other hand, you select to store the values as relative ones, the values are converted to a comparative time relative to the current date and time. For example, if on May 23rd 2007 at 10h00 you query for entries generated after May 23rd 2007 9:00, and select 'relative time', the criterion is stored as 'return all entries generated in the last hour'. If you run this query again on June 12th 2007 at 11h30, you get log entries generated during the last hour, i.e. after June 12th 2007 10h30.</p>

Table 17: How to use the available criteria dialogs

Once you have set up the criteria used in your template, these are displayed in the *Criterion* column of the *Template settings* window after closing the *Criteria* dialog and clicking on the QUERY button (or by clicking on the EXECUTE button of the *Template settings* window).

Column	Size	SortGroup by	Criteria
<input checked="" type="checkbox"/> Type	100	(none)	MEDIUM-INSERTED-DEVICE-ATTACHED
<input checked="" type="checkbox"/> Traced On (Endpoint time)	100	Descending	Entries generated this week
<input checked="" type="checkbox"/> Computer	30	(none)	SECUREWAVE1
<input checked="" type="checkbox"/> Device Class	100	(none)	DVD/CD Drives;Floppy Disk Drives;Imaging Devices
<input checked="" type="checkbox"/> ModelId	150	(none)	
<input checked="" type="checkbox"/> Volume Label	100	(none)	
<input checked="" type="checkbox"/> Traced On (Console time)	150	(none)	From 8/1/2007 to 8/7/2007 11:56:52 AM
<input checked="" type="checkbox"/> Size	100	(none)	At least 1Megabytes
<input checked="" type="checkbox"/> User	150	(none)	
<input type="checkbox"/> SID	100	(none)	
<input type="checkbox"/> Process Name	150	(none)	
<input type="checkbox"/> Unique Id	150	(none)	
<input type="checkbox"/> Device Model	100	(none)	
<input type="checkbox"/> Traced On (UTC)	150	(none)	
<input type="checkbox"/> Transferred On (UTC)	150	(none)	
<input type="checkbox"/> Transferred On (Console time)	150	(none)	

Figure 68: Example of criteria settings

Query & Output tab

The *Query & Output* tab is displayed when you click on the ADVANCED button on the *Template settings* window. You can use it to carry out the same actions as a simple query, but with more complex criteria and specifications.

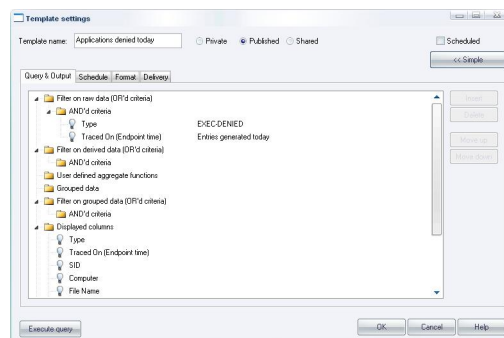
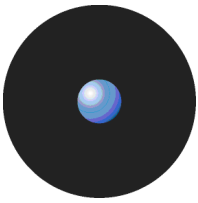


Figure 69: Query & Output tab

In the *Query & Output* tab you enter complex queries using Tree control. The tree representing the query has seven top-level nodes. These are used to:

- > *'Filter on the raw data'* — specify the criteria, based on information actually in the log entries, used to select results to be included in reports generated using the template. For example, if you specify an *'AND'd criteria'* of *Type* and the criteria *ADDED FILE* the report includes events when a user has added a file to the system.
- > *'Filter on derived data'* — specify the criteria, based on information derived from the Sanctuary Management Console, used to select results to be included in reports. For example, you can specify an *'AND'd criteria'* of *Traced On (Console time)* or *User*.



- > 'Display user defined aggregate functions' — such as the sum, minimum, maximum, or average of values contained in the log entries.
- > 'Group the data' — to produce a single result corresponding to multiple log entries with the same value for a particular field. You can, for example, group log entries by *Type* or *Traced On (UTC)* date.
- > 'Filter on grouped data' — determine whether the report generated using the template only displays results where the values for the computed columns match specified criteria.
- > Display columns — determine which columns are displayed and their order.
- > Sort the data — determine the order in which rows of results are displayed.




You can normally switch back to the Simple query tab by clicking on the SIMPLE button. This is not possible when you have defined a complex query that cannot be represented correctly in the Simple Query tab. In this case, the SIMPLE button is disabled.

The INSERT button adds a new node into the highlighted node of the tree. If the nodes in the group cannot be reordered then the new node is positioned below any existing nodes.

When nodes representing columns are highlighted a set of controls is displayed to its right. These can be used to select columns, criteria, and so on.

To set up and use a complex query:

1. Click on the ADVANCED button in the *Template settings* window.
2. Choose the criteria you want to use to select results.

To add each criterion, click on the 'AND'd criteria' node of the top-level node 'Filter on raw data (OR'd criteria)', click on the INSERT button and select the column and the criteria you want to use (using the drop-down list and the Criteria dialog opened when you click on the  button). Repeat for derived data by setting up criteria under the top-level node 'Filter on derived data (OR'd criteria)'.



You can also use shortcut keys: Insert creates a new clause or term, Delete removes a clause or term, Ctrl+Up or Ctrl+Down move a clause up or down respectively, and Ctrl+1, Ctrl+2, Ctrl+3 edit the first, second or third control for the highlighted clause.

3. Select computed information you want to display, if required. For example, you may want to display a count, an average value or a maximum value for a column when you have grouped results. These computed information columns are named C1, C2, and so on. (They may be selected in step 5.)

To add each computed column, click on the top-level node 'User defined aggregate functions', click on the INSERT button and select the column and the calculated function you want to use (using the drop-down list).

4. Define how you want your results grouped, if appropriate. To add each result grouping, click on the top-level node 'Grouped data', click on the INSERT button and select the column you want to group results by (using the drop-down list). You can group results by the values in several columns.
5. Specify that the values in your computed columns match particular criteria, if required. For example, you may only want to include results in your report where the value of a computed field exceeds a particular value.

To specify criteria based on the computed column values, click on the 'AND'd criteria' node of the top-level node 'Filter on grouped data (OR'd criteria)', click on the INSERT button, select the computed column and criteria you want to use, and enter an appropriate value.

6. Choose the columns of information you want to display and their ordering.

To select each column you want to display, click on the top-level node 'Displayed columns', click on the INSERT button and select the column (using the drop-down list).

You can reorder the displayed columns by clicking on the MOVE UP and MOVE DOWN buttons.

7. Specify how you want to sort the results in the report. To add a level of sorting, click on the top-level node Sorting, click on the INSERT button and select the column you want to sort by and how you want this sorted (using the drop-down lists). You can sort results using several columns.
8. Click on the EXECUTE QUERY button to close the *Template settings* window and execute the query.



Schedule tab

The *Schedule* tab is used to define the following:

- > Start and end dates between which reports are automatically generated using this template.
- > How often the report is generated and the pattern for its production. For example, you can choose for it to be produced on a daily basis, every so many hours, on a weekly basis (on chosen days) or on a monthly basis.



In order for the information in this tab to have an effect the Scheduled checkbox in the top right corner of the Template settings window must be checked.

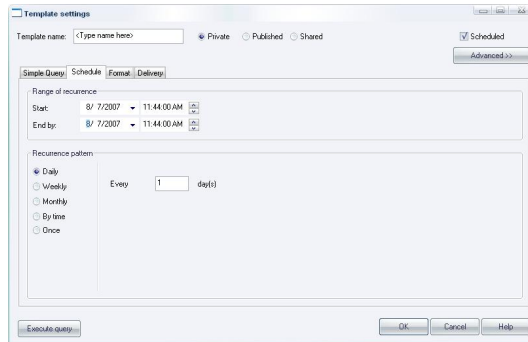


Figure 70: Schedule tab

Format tab

The *Format* tab is used for reports that are sent or written to shared folders. You can define the following:

- > Text contained in the body of an email — by typing in a *Description*.
- > The format of the output file and the appropriate output file extension. The format of the report can use XML, Comma Separated Value (CSV) or HTML (for emails).
- > The email address from which the report appears to come.

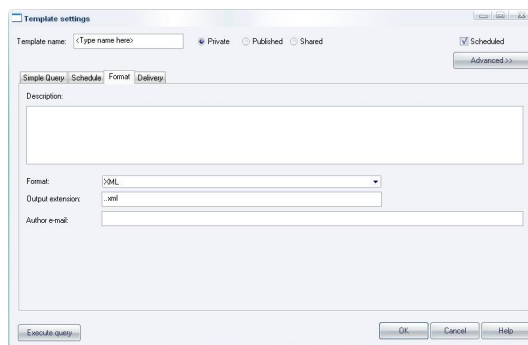


Figure 71: Format tab



Delivery tab

The *Delivery* tab is used to define how and where reports are sent via email or where they are saved in a shared folder on your network.

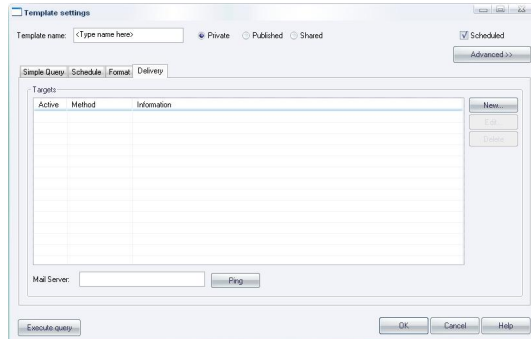


Figure 72: Delivery tab

The Active status determines whether the specified email recipient is sent the report or whether the report is sent to the specified shared folder. The *Method* of delivery is either 'Share' or 'E-mail' indicating whether the report is saved to a shared folder on the network or emailed to 'To' and 'Cc' recipients specified in the *Information* column.

The *Mail Server* must be specified for emailed reports. Its connection status can be checked by 'pinging' it.



You can also use the following shortcut keys: Insert creates a new target, Delete removes a target, F2 edits a target.



You must be careful when setting email delivery options. If not correctly set, all report can end up in the junk-email folder.



The chosen email server should accept anonymous connections or the report delivery option may not work properly.

To set up a new target:

1. Click on the NEW button to the right of the *Delivery* tab. The *Edit target* dialog is displayed.

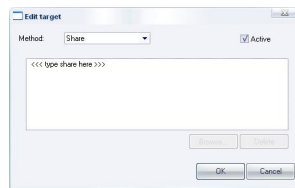


Figure 73: Edit target dialog

2. If you want to save the scheduled reports in a shared folder on your network, select the *Method* 'Share', click on the field below, click on the BROWSE button and select the shared folder.



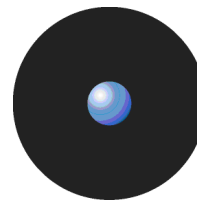
Alternatively you can use the *Ctrl+B* shortcut key to browse for a folder.

3. If you want to send the scheduled report as an email, select the *Method* 'E-mail' and specify the 'to' and 'Cc' recipients in the resulting *Edit target* dialog.



Figure 74: Edit target dialog (E-mail)

4. Click on the OK button.



Using the Log Explorer module to authorize unknown files

You can use the *Log Explorer* module to show Local Authorization decisions made by users, to override denials from central authorization. This may reveal certain executables, scripts and macros that are needed by users to complete their work. These files should be included in the white list.

If a user is complaining that he needs certain executables, scripts and macros to do his daily work, you can check which files the user has attempted to use and decide whether to authorize them or not. If you are absolutely certain that the files can be trusted, you can authorize them directly from the *Log Explorer* module.

To authorize a new executable, script or macro from the Log Explorer module

1. Right-click on a file, or range of files, in the *Log Explorer* window. The system displays the *Assign Files to File Groups* dialog.
2. From the drop-down list associated with the *Suggested File Group* column, select the *File Group* to which the new file(s) should be added.




Be careful when authorizing files directly from the Log Explorer module. There is no guarantee that they are not infected with a virus or that the end user has not attempted to run a rogue application under another name. For maximum security, it is best only to authorize applications from trusted sources using the Log Explorer module.

Forcing the latest log files to upload

Sanctuary-protected clients upload their log information to the SecureWave Application Server at the time specified in the system options. However, you may need to view up-to-the-minute log information to help you quickly troubleshoot application problems or to verify that authorizations have been set correctly for new software.

To force the immediate retrieval of the latest logs from any client, you can:

1. Activate the *Log Explorer* module, if it is not already open. To do this, click on the *Log Explorer* icon  located in the *Modules* section of the *Control Panel* or use the *View→Modules* command.
2. Click on the **FETCH LOG** button or select *Fetch Log* from the *Explorer* menu. The system prompts you to specify the machine from which you want to fetch all logs present on the client. You can only fetch logs from the computers that have the Sanctuary Client Driver installed.

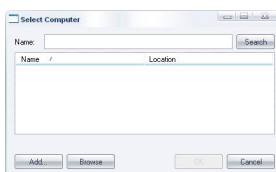


Figure 75. Fetching New Logs

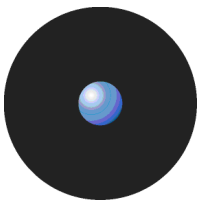
3. Select the target machine from the drop-down list and click OK.



You may need to wait half a minute before the latest logs are available when using 'Fetch log'. When the log entries are retrieved from the client machine they are processed by the server, put into a database insertion queue and inserted in a batch. The time between retrieving the log entries from the client and the latest logs becoming available depends on the queue size and the database availability at the time of upload.





When you use the 'Fetch Log' functionality to retrieve the latest logs from client computers, the logs are appended to the server log insertion queue. They are processed by the server, put into a database insertion queue and inserted in a batch. This means that the data is not immediately available after the log has been uploaded. The whole 'Fetch Log' can take about half a minute (depending on the queue size and the database availability at the time of upload).




Viewing administrator activity

In addition to using the *Log Explorer* module to monitor executables and other files, you can also use it to monitor the actions of your administrators including changes made to files, File Groups, and the assignment of resources to users and user groups.

 *In previous versions of Sanctuary this was done using the Audit Log Viewer module. The functionality of this module has now been incorporated into the Log Explorer module and the Audit Log Viewer module no longer exists.*

 *Sanctuary Device Control Enterprise Administrators have access to all audits. When running under a Windows Active Directory based domain, the Sanctuary Administrator is only shown audits of computers and users he/she is allowed to manage. You can use *Ctrlacx.vbs*, explained in Sanctuary's Setup Guide, to create, view, or modify control rights in the active directory.*

To view audit information about the actions carried out by administrators:

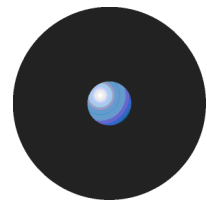
1. Click on the *Log Explorer* icon  located in the *Modules* section of the *Control Panel* or use the *View→Modules* command. The system opens the *Log Explorer* window.
2. Select (or amend, if required) the template that you want to use to generate a report showing the administrator activity.
3. Execute the system administrator activity query. To do this, click on the *QUERY* button in the *Log Explorer* window (or the *EXECUTE* button in the *Template settings* window). The system displays a list of audit events showing, for example, all changes made to permissions between specified dates.

Audit events

Audit events describe the actions performed by administrators.

Audit events	Description
ADDED FILE	A file (includes the name, path, and ID) was added to the database.
ADDED FILE GROUP	The File Group's name and ID were added to the database.
ASSIGNED FILE TO FILE GROUP	This file (includes the name, path, and ID) was added to this File Group.
AUTHORIZED USER	This user/user group was granted the right to use this File Group, shown by the name and ID.
AUTOMATIC USER ACCESS UPGRADE	This administrator was implicitly defined as an Enterprise Administrator, because none other was identified.
DELETED DEFAULT OPTION	Whenever a default option that applies to all the machines is deleted (in the <i>Tools→Default Options</i> menu), the option and the user/machine are traced.
DELETED EVERYONE OPTION	An action that affects all users is removed.
DELETED FILE GROUP	This File Group was erased.
DELETED OPTION	Whenever an option specific to a machine is deleted, the option and the user/machine are traced.
MODIFY USER ACCESS	When changes are made to the Sanctuary Administrator's roles, the user and role are logged.
PURGED DB AND FILE STORAGE	This action is recorded every time maintenance is performed on the system.
REMOVED FILE	This file (includes the file name and File Group) was deleted from the database.
RENAMED FILE GROUP	This file was renamed.
SET DEFAULT OPTION	A default option is one that applies to all the machines. Whenever a change is done by the administrator to one of these options (by using the <i>Tools→Default Options</i> menu), the option being changed and the user/machine are traced.
SET EVERYONE OPTION	An action is set that affects all users.
SET OPTION	This action is traced whenever a change to the system options is made, the option, user/machine are logged.
SET USER/MACHINE OPTION	A change was made to this option for this machine or user.
UNASSIGNED FILE FROM FILE GROUP	This unassigned file was removed from this File Group.
UNASSIGNED FILE TO FILE GROUP	This unassigned file was added to this File Group.
UNAUTHORIZED USER	This user's permission to use the named File Group was revoked.

Table 18. Audit events



Generating reports of system status and settings

In addition to online audit trails of application execution and administrator activity, you can generate reports of authorization information, system settings, and online machines.

For more information about reports, see *Chapter 11: Generating Sanctuary reports* on page 97.

Chapter 10: Managing files using the Database Explorer

The SecureWave Sanctuary Database serves as the central repository of authorization information, such as:

- > The white list of approved executable files, scripts and macros.
- > Digital signatures ('hashes') that uniquely identify the approved files.
- > File Groups.
- > File Groups parent-child relationships.
- > Authorized users and user groups.

The SecureWave Sanctuary Database is created using Microsoft SQL Server 2000/2005, SQL Server 2005 Express Edition, or the Microsoft Database Engine (MSDE). For organizations with fewer than approximately 200 users, SQL Server 2005 Express Edition is sufficient. Larger organizations use the Microsoft SQL Server.



There are inherent limitations when using SQL Server 2005 Express Edition (for example, 4 GB database limit). See the Sanctuary's Setup Guide.


The *Database Explorer* module of the Sanctuary Application Control Suite is the primary tool for viewing and managing database records. Using it you can:

- > View database records.
- > Perform routine database maintenance.
- > Back up the SecureWave Sanctuary Database.
- > Remove old execution logs and machine scans.

Viewing database records

The *Database Explorer* module displays a list of the executable, script and macro files for which digital signatures (hashes) are found in the SecureWave Sanctuary Database — and the File Groups to which they are assigned.

Using the Database Explorer module

To open the *Database Explorer* module, click on the *Database Explorer* icon  located in the *Modules* section of the *Control Panel* (or use the *View→Modules* command). The system displays the *Database Explorer* window, as shown in the following figure.



If your database includes a very large number of files, there may be a slight delay before this list appears when you click on SEARCH.



The Database Explorer module works in a similar way to the Windows Explorer program.

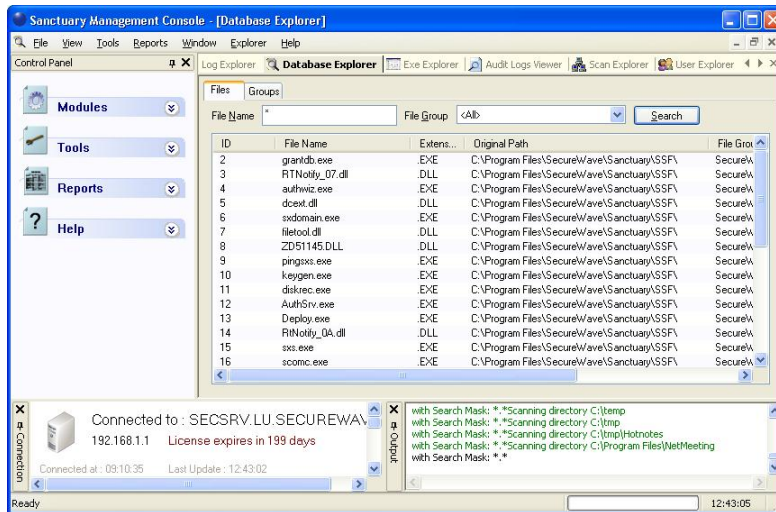


Figure 76. Database Explorer Module

To sort entries by any attribute, such as filename or File Group

You can click on a column header to sort the file entries by that attribute. (Click on it again to change the order from ascending to descending, or vice versa).

A small triangle on the header shows the sort order. The ID column shows the internal SecureWave Sanctuary Database identifier, for information purposes only.

To expand the display to show/hide other columns

You can right-click on the header row of the *Database Explorer* main window and add/remove column(s).



Figure 77. Selecting columns to display in the Database Explorer Module

If you wish to organize columns of information, select the *Choose Columns* option of the right-click menu. The *Choose Columns* dialog is displayed, from where you can select and classify all available report columns. You can change the width of each individual column using the *Width of selected column (in Pixels)* field at the bottom of the dialog.

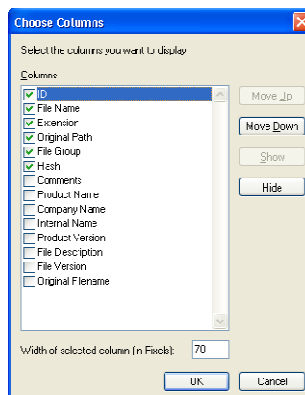
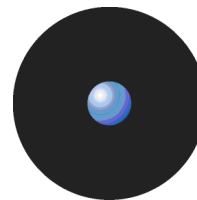


Figure 78. Choose Columns dialog



To save this list as a CSV file

To save the list of database records as a CSV file (comma-separated values), select the *File Save As* option from the *File* menu. You can then import the resulting information into a third party reporting tool.

Synchronizing Sanctuary accounts with Microsoft and/or Novell accounts

Sanctuary stores a copy of user/administrator and computer accounts in its database. From time to time, you will want to explicitly synchronize this information with the domain controller. Since permissions are usually applied to groups, you only need to do this rarely.

If you are using the program in a Novell environment, you should run the Synchronization Script. Please check the *Sanctuary's Setup Guide* for further information.

To synchronize domain members

1. Select *Synchronize Domain Members* option from the *Tools* menu (or from the *Control Panel*). The system displays the following dialog:



Figure 79. Synchronizing Domains

2. Type in the name of the domain that you want to be synchronized.
3. Click on the OK button. The system updates its reference list of users and groups from the domain.



If you enter a machine name (rather than a domain name), and the machine is a domain controller, then the particular domain controller is used for synchronization. This is useful when the replication between domain controllers is slow and you cannot wait for user account information to replicate between them all.



*Windows XP's Simple File Sharing feature sometimes interferes with the synchronization process. If you have problems, turn this option off and try again. To switch it off, open Windows Explorer on the target machine, select *Tools* → *Folder Options*, display the *View* tab, and uncheck the *Simple File Sharing* option.*



You can synchronize local users/groups of one or more machines in a domain. This feature is used to enforce policies on a local user despite being in a domain.

SXDomain command-line tool

The SXDomain command-line tool provides an alternative method for updating the SecureWave Sanctuary Database with changes in the domains, users, groups, and workstations within your network.

Novell's synchronization script

If you are using Sanctuary Application Control Suite in a Novell environment, you should periodically run our synchronization script. This can be done manually (provided there are not too many changes in your eDirectory structure) or automatically using scheduler software. See details in the *Sanctuary's Setup Guide*.



To synchronize user/account information from a workgroup (not a domain)

If Sanctuary is protecting servers or computers in a workgroup, there is no domain controller from which the Synchronize Domain function can get a list of users. In this case, you must add servers or computers in the workgroup individually.

1. Select the *Synchronize Domain members* option in the *Tools* menu (or the *Control Panel*). The *Synchronize Domain* dialog is displayed.
2. Enter the name of the computer you want to add.
3. Click on the DIFFERENT USER NAME button to display the *Connect As...* dialog:

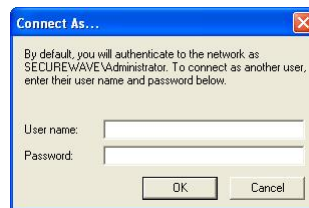


Figure 80. Connecting as a different User

4. Enter the user name (including server's name) and password for the local administrator of the machine you want to add.
5. Click on OK twice (to confirm both dialogs). The computer is added to the SecureWave Sanctuary Database and you can assign privileges to its local users.

Performing database maintenance

Backing up the SecureWave Sanctuary Database

You can find detailed information on how to back-up SecureWave Application Server files and hash keys information in the *Sanctuary's Setup Guide*.

Removing old database records

After you have been using Sanctuary for a while, your database will have accumulated a large number of activity logs, scan results, shadow files and key recovery information. Older records take up unnecessary database space and may no longer be needed for your daily operations. If this is the case, you can periodically clean up the database by removing obsolete records. Do not forget to make a backup of your information before doing this.

To delete old database records

1. Select the *Database Maintenance* option from the *Tools* menu (or from the *Control Panel*).
2. In the *Database Maintenance* dialog, check the type of database content you want to delete.

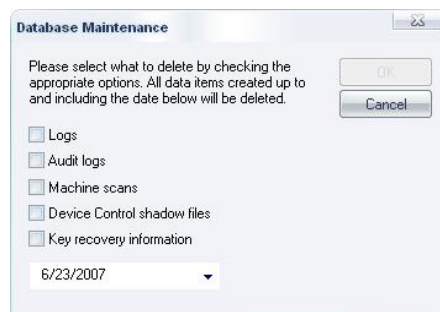
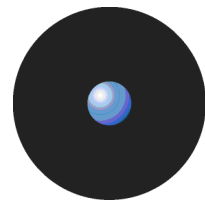



Figure 81. Database Maintenance





You can select the following:

- > *Execution logs* — Deletes all execution logs before the specified date.
 - > *Audit logs* — Deletes all logs of administrator activities before the specified date.
 - > *Machine scans* — Deletes the results of all scans before the specified date. This process does not delete scan templates (which define how scans are performed) only scan results.
 - > *Device Control Shadow Files* — This option is not available if you are not running Sanctuary Device Control.
 - > *Key Recovery information* — Deletes all records of recovered passwords for decentralized encrypted media before the specified date. This option is not available if you are not running Sanctuary Device Control.
3. Enter the cut-off date. The default date is one month earlier than the current system date. To do this, click on the arrow to the right of the date field and select a data from the calendar.

 *The format used for the date, i.e. mm/dd/yyyy or dd/mm/yyyy, where yyyy represents the year, mm the month, and dd the day of the month, depends on how you configure Sanctuary's Regional Settings.*

4. The system deletes the requested content from SecureWave Sanctuary Database tables and the SecureWave Application Server data file directory.

 *Check you have sufficient free space on the computer for the system to generate the transaction logs that accompany database maintenance. If you get an error message due to insufficient space, you can retry the process selecting a shorter time period.*

 *The database clean-up process cannot be undone. Be sure to make a backup before proceeding.*

Removing obsolete computer connections records

SecureWave Application Servers keep a record of machines connected within your organization in an online table. This is updated each time a user logs on to, or unlocks, a computer.

Occasionally a machine is removed from your organization's networks without notifying the system that it is no longer available. In this case, orphan entries are left in the online connection table. These can affect the performance of the *Send Updates to All Computers* function, which sends fresh hash lists to all computers within your organization.

The good news is that you do not have to worry about this. Sanctuary automatically removes the database record corresponding to any machine that has not responded to three successive connection requests, from the online table.

To manually remove obsolete computer connections records, use the *Purge Online Table* option from the *Tools* menu (or *Control Panel*).

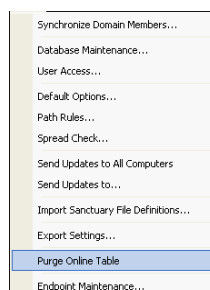


Figure 82. Purging the online computers table

Chapter 11: Generating Sanctuary reports

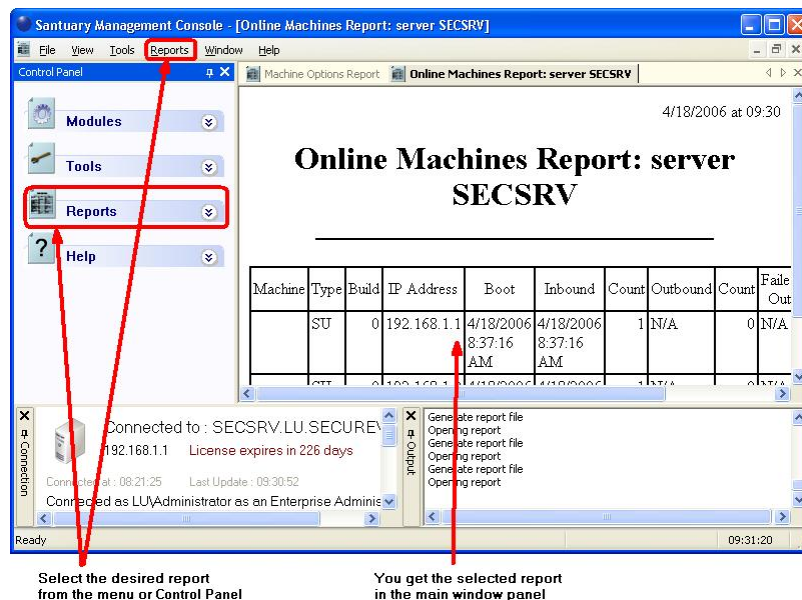
You can easily generate HTML reports that can be viewed, saved, or printed from within any Sanctuary module, for example, the *Exe Explorer* or *Scan Explorer* module.

To generate a report simply click on the *Reports* menu, or the *Reports* module, and choose one of the following options:

- > **File Groups by User** — This generates a report of File Groups for the user or User Group you specify.
- > **Users by File Group** — This creates a report of users for all File Groups defined in the system.
- > **User Options** — This produces a report of current user option settings, such as those that determine what activities are logged and whether users are prompted to locally authorize denied executables, scripts and macros.
- > **Machine Options** — This generates a report of current machine option settings, such as when log files are uploaded to the SecureWave Application Server.
- > **Online Machines** — This creates a report that shows which machines are currently online and able to receive updated authorization information for the connected SecureWave Application Server.



In addition to the standard reports that are available through the Reports menu, you can define your own criteria for selecting log entries and producing reports using the Log Explorer module. For more information see Chapter 9: Monitoring activities using the Log Explorer on page 67.

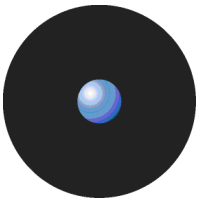



Select the desired report from the menu or Control Panel


You get the selected report in the main window panel

Figure 83. To generate a report

The reports generated using the Reports module are HTML files, viewed in an internal window. You can save these reports and view them using Internet Explorer or any other Web browser. Reports can also be printed, copied, converted, and modified as required. They are provisionally created and saved in the Report folder located in your temporary directory, %TEMP%.



 Once the output is displayed, you can use the *File* → *Save as* or *Print* command to create a backup of it. You can access the same right-click menu used for a Web page in Microsoft Internet Explorer.

 The format used for dates, i.e. *mm/dd/yyyy* or *dd/mm/yyyy*, where *yyyy* represents the year, *mm* the month, and *dd* the day of the month, on the *Regional and Language settings* in the *Control Panel* of your Windows operating system. Consult *Help on Windows* for more information.

File Groups by User

The *File Groups by User* option is used to generate a report showing the File Groups assigned to each user or a specific user. To generate this report:

1. Select the *File Group by User* option from the *Reports* menu (or the *Control Panel*).
2. In the *Select Domain User or Group* dialog, select one or more users.

An example of the User report is shown below:

25/05/07 at 19:08

User Report

1. secure\Bill
(Domain User)
Direct File Groups Authorization

- Accounting*
- Office suite*
- Payroll*
- QA*

File Groups Authorized via *Marketing Users*

- Pre Sales Planning*
- Pert charts*

Figure 84. File Groups by User report



Users by File Group

The *User by File Groups* option in the *Reports* menu (or the *Control Panel*) is used to generate a report showing the users assigned to each File Group defined in your Sanctuary system. This shows the users both directly assigned to the File Group and those indirectly assigned to it because they are members of a particular user group.

An example of the File Groups report is shown below:

25/05/07 at 16:09

File Groups Report

1. Marketing

Marketing LU	(Domain Group)
Marty	(Domain User)
Presales	(Domain Group)
Administrators	(Well-Known Group)

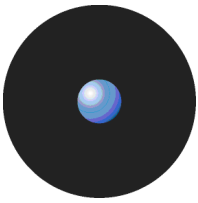
2. 16 bit Applications

>>> No user within your administration scope is associated with this **File Group** <<<

3. TrackRecord

>>> No user within your administration scope is associated with this **File Group** <<<

Figure 85. Users by File Group report



User Options

The *User Options* option in the *Reports* menu (or the *Control Panel*) is used to generate a report showing the Sanctuary option settings for the current user. These options determine, for example, what activities are logged and whether users are prompted to locally authorize denied executables, scripts and macros.

An example of the User Options report is shown below:

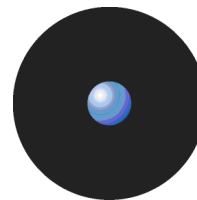
25/05/07 at 16:10

User Options Report

Option	User / Group	Setting
Execution Blocking	default	(*) Blocking mode
	Administrator	Non-blocking mode
	LocalSystem	Non-blocking mode
Execution Eventlog	default	(*) No events logged
Execution Log	default	(*) Log access denied
Execution Notification	default	(*) No Notifications
Execution Notification Text	default	(*) Please contact your system administrator
Macro and Script protection	default	(*) Disabled
Relaxed logon	default	(*) Disabled
Relaxed logon time	default	(*) 600

Figure 86. User Options report

An asterisk (*) indicates that the options has not been configured and takes the default value.



Machine Options

The *Machine Options* option in the *Reports* menu (or the *Control Panel*) is used to generate a report showing the Sanctuary option settings for the current computer. These options determine, for example, when log files are uploaded to the SecureWave Application Server.

An example of the Machine Options report is shown below:

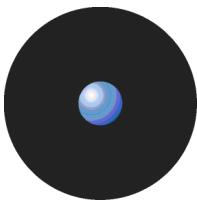
25/05/07 at 16:11

Machine Options Report

Option	Machine	Setting
Client Hardening	default	(*) Disabled
Sanctuary Status	default	Show All
eDirectory Translation	default	(*) Enabled
Execution Blocking	default	Non-blocking mode
Execution Eventlog	default	(*) No events logged
Execution Notification	default	Access-denied
Execution Log	default	(*) Log access denied
Local authorization	default	(*) Enabled
Log upload interval	default	(*) 180
Log Upload Threshold	default	(*) 10000
Log upload time	default	(*) 05:00
Log upload delay	default	(*) 3600
Server address	default	(*)

Figure 87. Machine Options report

An asterisk (*) indicates that the options has not been configured and takes the default value. The *default* value in the *Machine* column means that this option is configured for all computers.



Online Machines

The *Online Machines* option in the *Reports* menu (or the *Control Panel*) is used to generate a report showing all machines that are online, and able to receive updated authorization information for the connected SecureWave Application Server, when the report is generated.

This report is useful when troubleshooting: If a particular machine is not in the list, it does not receive updates through the *Send updates to all* command. If a particular machine is in the list but its *Failed Out* counter is not zero, this indicates that there may be a communication problem, configuration error, networking problem, network timeout that is not configured, or a similar problem.



The machines listed in this report depend on the Active Directory delegation rights of the administrator who generates this report.

An example of the Online Machine report is shown below:

25/05/07 at 16:12

Online Machines Report: server APPSERV1

Machine	Type	Build	IP Address	Boot	Inbound	Count	Outbound	Count	Failed Out	Count	Consecutive
Company	SN	0	192.168.1.15	N/A	2006-08-10 13:35:45 PM	1	2006-08-10 14:49:01 PM	16	N/A	0	0
Marketing	SU	0	127.0.0.1	2006-08-10 15:00:15 PM	2006-08-10 15:00:31 PM	6	2006-08-10 16:21:47 PM	3	2006-08-10 16:36:31 PM	2	2
Sales	SX	0	192.168.1.10	2006-08-10 09:00:15 AM	2006-08-10 14:00:30 PM	9	2006-08-10 14:21:15 PM	4	N/A	0	0

Figure 88. Online Machines report

The information in each column of the Online Machines report is explained in the following table:

Column	Description
<i>Machine</i>	The computer's name. A machine that is not listed in this table does not receive updates when using the <i>Send Updates to All Computers</i> or <i>Send Updates to</i> command in the <i>Tools</i> menu. The table updates when the client machine reboots or logs.
<i>Type</i>	The type of client driver installed on the client computer. This is one of the following: SN for Sanctuary Client Driver version 3.1 or older, SX for Sanctuary Client Driver version 2.1, or SU for Sanctuary Client Driver version 3.2 or later.
<i>Build</i>	Always zero.
<i>IP Address</i>	The IP address of the computer.
<i>Boot</i>	The date and time the SecureWave Application Server last received a boot notification from the client machine. 'N/A' indicates that the SecureWave Application Server did not receive a boot notification but did receive a logon or unlock notification. This notification applies for machines that could not contact a SecureWave Application Server at boot up.
<i>Inbound</i>	The date and time the SecureWave Application Server last accepted a connection from the client computer.
<i>Count</i>	The number of <i>inbound</i> connections accepted from the client computer by the SecureWave Application Server.
<i>Outbound</i>	The date and time of the last connection initiated from the SecureWave Application Server towards the client computer.
<i>Count</i>	The number of <i>outbound</i> connections that the SecureWave Application Server initiated with the client computer.
<i>Failed out</i>	The date and time of the last unsuccessful connection between the SecureWave Application Server and the client computer.
<i>Count</i>	The total number of <i>failed out</i> connections that occurred between the SecureWave Application Server and the client computer. This number increases in the case of poor connections between the client and the server, or when there is a high load on the server side.
<i>Consecutive</i>	The number of consecutive connections that failed between the SecureWave Application Server and the client computer. After four unsuccessful connection tries, the client machine is considered as being offline and automatically removed from the online table.

Table 19. Columns of the 'Online Machines' Report



Server Settings Report

Use this report to see how your SecureWave Application Server(s) is set providing you with invaluable configuration and troubleshooting info. To generate this report, select *Server Settings Options* from the *Reports* menu (or from the *Control Panel*). Please refer to *Sanctuary's Setup Guide* for more details on the meaning of each option.

An example of the Server Settings report is shown below:

25/05/07 at 16:14

Server Settings Report

Setting	Machine	Setting
CommVer	secsrv.lu.company	2
	secsrv1.lu.company	3
DataFileDirectory	secsrv.lu.company	\\lu\DataFileDirectory
	secsrv1.lu.company	\\lu1\DataFileDirectory1
DBConnectionCount	secsrv.lu.company	20
	secsrv1.lu.company	30
DBConnectionString	secsrv.lu.company	Provider=sqloledb; Data source=SECSRVSQLEXPRESS; Initial Catalog=sx; Trusted_Connection=yes
	secsrv1.lu.company	Provider=sqloledb; Data source=SECSRVCOMPANY; Initial Catalog=sx; Trusted_Connection=yes
DBConnectionTimeout	secsrv.lu.company	(*) 5
	secsrv1.lu.company	(*) 5
Log file name	secsrv.lu.company	Sxs.log
	secsrv1.lu.company	Sxs.log
Log to Console	secsrv.lu.company	No
	secsrv1.lu.company	No
Log to dbwin	secsrv.lu.company	No
	secsrv1.lu.company	No
Log to file	secsrv.lu.company	No
	secsrv1.lu.company	No
MaxRPCCalls	secsrv.lu.company	(*) 50
	secsrv1.lu.company	(*) 50
MaxSockets	secsrv.lu.company	5000
	secsrv1.lu.company	5000
Port	secsrv.lu.company	65129
	secsrv1.lu.company	65129
Protocols	secsrv.lu.company	(*) ncacn_ip_tcp
	secsrv1.lu.company	(*) ncacn_ip_tcp
RegProtectionLevel	secsrv.lu.company	6
	secsrv1.lu.company	6
SecureInterSXS	secsrv.lu.company	No
	secsrv1.lu.company	No
SecureCertSerial	secsrv.lu.company	(*)
	secsrv1.lu.company	(*)
ServerName	secsrv.lu.company	(*)
	secsrv1.lu.company	(*)
SndPort	secsrv.lu.company	33115
	secsrv1.lu.company	33115
SxdConnectAttempts	secsrv.lu.company	(*) 10
	secsrv1.lu.company	(*) 10
SxdConnectDelayBeforeRetray	secsrv.lu.company	(*) 500
	secsrv1.lu.company	(*) 500
SxdConnectTimeoutMsec	secsrv.lu.company	5000
	secsrv1.lu.company	5000
SxdPort	secsrv.lu.company	33115



	secsrv1.lu.company	33115
TLSCertFriendlyName	secsrv.lu.company	Lux Server
	secsrv1.lu.company	USA Server
TLSCertID	secsrv.lu.company	611CF237000000000002
	secsrv1.lu.company	711DE216000000000011
TLSCertIssuer	secsrv.lu.company	DC=company, DC=LU, CN=Company
	secsrv1.lu.company	DC=company, DC=LU, CN=Company
TLSCertName	secsrv.lu.company	CN=secsrv.lu.company
	secsrv1.lu.company	CN=secsrv.lu.company
TLSCertMaxSockets	secsrv.lu.company	5000
	secsrv1.lu.company	5000
TLSPort	secsrv.lu.company	65229
	secsrv1.lu.company	65229

Figure 89: SecureWave Application Server Options report

Chapter 12: Setting Sanctuary system options

Sanctuary is a highly flexible application. If you have appropriate administrative privileges, you can customize many aspects of the global system operations, such as:

- > What types of events are logged and how.
- > What type of notification users receive.
- > Under what conditions users can locally authorize unknown applications (if at all).

This chapter describes how to set or modify the following options:

- > Default options for all computers protected by the Sanctuary Application Control Suite.
- > Default options for all users protected by the Sanctuary Application Control Suite.
- > Options that override global options for specific computers, users, or User Groups.

Since options can be set in several ways, the Sanctuary system uses a hierarchical logic to determine which option settings apply. At the end of this chapter, you can find information about *Determining which option setting takes precedence* (see page 115).



Details of how to set up default options for the Exe Explorer module are explained in To set up the Exe Explorer default options on page 37.



Older versions of Sanctuary Application Control Suite lose the Notification Text set in the User Tab of the Options dialog during an upgrade. You must retype them in the corresponding option fields.

Options set in old Sanctuary versions

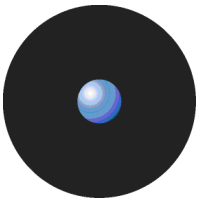
A number of default options have been renamed or changed since Sanctuary Application Control Suite version 3.x and earlier. For more information see the readme file located in your installation CD.

The following table summarizes the changes made to the Sanctuary default options:

New name	Old name (version 3.x or previous)
<i>eDirectory Translation</i>	**
<i>Endpoint Status</i>	<i>Device Control Status Window, Sanctuary Status</i>
<i>Execution Blocking</i>	<i>Blocking Mode</i>
<i>Execution Eventlog</i>	<i>Eventlog Mode</i>
<i>Execution Log</i>	<i>Log Mode</i>
<i>Execution Notification</i>	<i>Notification Mode</i>
<i>Log Upload Threshold</i>	<i>Max Log Lines Before Log Upload</i>
<i>Server Address</i>	<i>SecureWave Application Server Address</i>
*	<i>Notification Text</i>
*	<i>Server Connect Timeout</i>
*	<i>Server Connect Failure Lockout</i>

Where * indicates an option that has been discontinued and ** indicates a new option.

Table 20: Option name comparison



Default options

You customize Sanctuary using the *Default Options* option in the *Tools* menu (or the *Control Panel*). This lets you change some aspects of the program's behavior and the way protected clients and computers interact with your Sanctuary solution.

If you change a default option, the client computers that are protected by Sanctuary need to be updated with the changes.

To change default option settings

1. Select *Default Options* from the *Tools* menu (or the *Control Panel*).
2. Select the appropriate tab depending whether you want to change a default option for protected clients or users/User Groups. You can either click on:

> *Computer tab* — To change the default options that govern how servers or computers under the protection of Sanctuary interact with the Sanctuary system.

— or —

> *User/Group tab* — To change the default options that govern certain aspects of how users and User Groups interact with the Sanctuary system.



The default option settings specified in the *Computer* tab apply to all machines under the protection of Sanctuary, unless they are explicitly overridden for a particular machine.



The default option settings specified in the *Users/Group* tab apply to all users under the protection of Sanctuary, unless they are explicitly overridden for a particular user or User Group.

3. Highlight the option for which you want to change the default settings, in the *Option* list box (on the left-hand side).
4. Uncheck the *Default setting* box in the *Option Value* panel.



The label to the right of the *Default Setting* checkbox is the current value that is being used by default for the option, for example, if the *Local Authorization* option is enabled by default the checkbox is labelled *Enabled*.



The settings for each default option are explained later in this chapter, where the Sanctuary default setting for each is also indicated. Where the predefined defaults are still in use star symbols, ★, are displayed in the *Current Value* column of the *Option* list box.

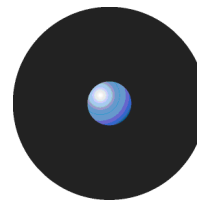
5. Select the required value for the option from the drop-down list of option values.
6. Enter a message to be displayed to the user, if required.
7. Save the amended option value as the default value. You can either

> Click on *OK* to save the setting and close the *Default Options* dialog.

— or —

> Click on *APPLY* to save the setting without closing the dialog. You can then repeat steps 2 to 7 to change other default option settings.

Once you have made all the required changes to the default option settings, you need to send the updated information to protected clients. To do this, select either the *Send Updates to All Computers* or *Send Updates to* option in the *Tools* menu (or the *Control Panel*).



Default options for protected servers and computers

You can set global options that govern certain aspects of how protected clients interact with the Sanctuary system. These settings apply to all servers or computers under the protection of Sanctuary.

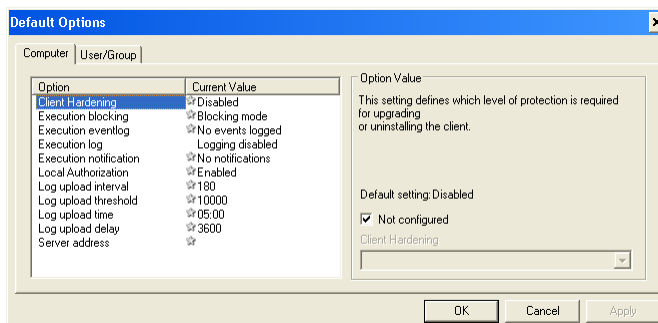


Figure 90. Default Options - Computer

The tab label in the *Default Options* dialog is simply *Computer* indicating that the options are not specific to a particular machine, but are the defaults for all of them. If you do not override these default options for a specific computer, they are applied to all machines in SecureWave Sanctuary Database.

A description of all computer options, default settings, and available values for each selection is given in the following sections.

Client Hardening

The *Client Hardening* option controls if a user with administrative privileges on a machine can uninstall the Sanctuary Client Driver or not, and also whether a user can delete shadow files or log entries. When the client driver starts, it generates a 15-byte random value used for protection purposes. This key — which we call Salt — is used to guarantee that the machines are uniquely identified.

You can choose from these settings:

- > *Disabled* — (default value) Sanctuary Client Driver protection mechanism is deactivated.
- > *Basic* — Client driver protection mechanism is enabled and can be deactivated with a signed ticket.
- > *Extended* — Client driver protection mechanism is enabled and can be deactivated with a signed ticket but the administrator must include a valid salt value.

Use the *Endpoint Maintenance* command to send maintenance ‘tickets’ to selected computers/users (see *Endpoint Maintenance* on page 19 for more information).

The Client Hardening feature fully protects all Sanctuary Client Driver executables, DLLs, registry keys, and the %Windows%/sxddata folder (temporary repository used by the client driver) from user with administration rights. It also prevents shadow files and log entries from being deleted.



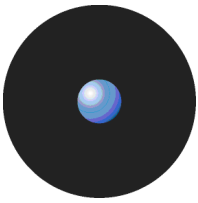
You must disable client hardening before you can run a ‘check disk’ (*chkdsk*) in a client machine.



When you have set the client hardening option to ‘Extended’ and you want to create a relaxation ticket with a salt for a given machine, if the client machine is running a different operating system than the administrator’s machine, the user specified must be ‘Administrators’. This limitation is caused by file ownership changes when files are copied to the ticket directory under these operating systems.



Windows Vista restore points, if enabled, can revert the Sanctuary Client Driver protected files, registry keys, and directories to previous states.



eDirectory translation

The *eDirectory translation* option is only effective in machine where a Novell client is also installed. The possible settings are:

- > *Enabled* — (default value) The eDirectory account information is shown along with the Windows account information to use them for permission definitions.
- > *Disabled* — eDirectory account information is not shown, only Windows accounts are shown to use them for permission definitions.

Endpoint status

The *Endpoint status* option allows you to select whether the Sanctuary Client Driver icon is displayed in the system tray of the client computer and control what is shown in the client's Status - Sanctuary Device Control window. The possible settings are:

- > *Do not Show* — The Sanctuary Client Driver icon is not displayed.
- > *Show All* — (default value) The Sanctuary Client Driver icon is displayed. All information is shown to the client user.
- > *Show All without Shadow* — The Sanctuary Client Driver icon is displayed. All information except shadowing details can be viewed.
- > *Show Allowed* — The Sanctuary Client Driver icon is displayed. Only the information about the devices allowed for the client can be viewed.
- > *Show Allowed without Shadow* — The Sanctuary Client Driver icon is displayed. Only the information about the devices allowed for the client can be viewed. There is no information shown about shadowing details.



When the option is set to 'Show Allowed' or 'Show Allowed without shadow', the user can only see the devices for which she, or the group she belongs to, has permission to see.

Execution blocking

The *Execution blocking* option determines whether or not to block execution of unauthorized executable files, scripts and macros according to the user or the user groups to which the user belongs. The available settings are:

- > *Blocking mode* — (default value) Files that are not centrally authorized do not run. There is no local authorization.
- > *Non-blocking mode* — Files that are not authorized can be run. This is useful for testing, configuration purposes, and installing new software.

See *Precedence rules for the Execution Blocking option* on page 120 for details of the Execution Blocking value that should be used in the case of different values having been set for different users/user groups and the computer.



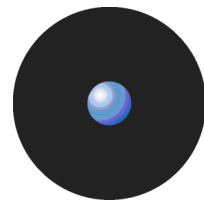
When Sanctuary is installed, the LocalSystem account and Administrators group are automatically set up in non-blocking mode to simplify day-to-day management issues.



Non-blocking mode does not apply to scripts and macros – only executables.



The 'Execution blocking' option works in combination with central authorization using digital signatures (the white list of approved executables, scripts and macros), local authorization and, in the case of scripts or macros, the 'Macro and Script protection' option, to either grant or deny authorization for a particular executable file, script or macro.



Execution eventlog

The *Execution Eventlog* option determines which execution events are reported to the Windows Event Log.

The possible settings are:

- > *No events logged* — (default value) Do not create a log entry when an execution file access is denied.
- > *Access-denied logged* — Create a log if file execution is denied.
- > *Non-blocked access-denied* — Log unauthorized file executions, such as when the system is configured in non-blocking mode and a user runs a file that is not centrally authorized.


 *This option is only included for backward compatibility.*

Execution log

The *Execution log* option determines which execution events are reported to the SecureWave Application Server log.

You can choose from these settings:

- > *Log everything* — Log every access to an executable file, script and macro.

 *This setting generates a large amount of data. Some Windows DLLs can be loaded several times a second. This setting should only be used for testing purposes and for short periods.*

- > *Log access denied* — (default value) Log every denied access to an executable file, script and macro.
- > *Logging disabled* — Do not keep a log.

Execution notification

The *Execution notification* option determines whether the user is notified of Sanctuary allow/deny execution decisions.

You can choose from these settings:

- > *No notifications* — (default value) Do not notify the user of system actions.
- > *Access-denied* — Notify the user when a file execution is denied.
- > *Non-blocked access-denied* — Notify the user when the system is in *Non-Blocking Mode* (see *Execution blocking* on page 108) and tries to run a file that is not centrally unauthorized.

If you select *Access-denied* or *Non-blocked access-denied*, you can also type the desired message to display.


Local Authorization

You can use the *Local Authorization* option to determine whether to permit local authorization of unknown files after prompting the user.

You can choose between:

- > *Disabled* — Files that are not centrally authorized do not run. There is no local authorization.
- > *Enabled* — (default value) Files that are not authorized can be run if the user *Execution Blocking* option is set either to *Ask user for *.exe only* or to *Ask user always* and the user clicks on the AUTHORIZE button of the corresponding authorization dialog.

For more information on local authorization see *Local authorization of executables, scripts and macros* on page 25.

 *In order to permit local authorization of executables, scripts and macros the 'Local Authorization', 'Execution blocking' and 'Macro and Script protection' options must have the required values.*



For a user to be asked if they want to authorize or deny an executable, script or macro, the file must be assigned to a File Group **and** the user must be assigned permission to use files in that File Group (either explicitly as a user, or through membership of a User Group).



Sanctuary contains a spread check mechanism to prevent the malicious spread of locally authorized files. If Sanctuary detects that an unknown executable, script or macro has been locally authorized too many times within the defined period, it disables the local authorization capability and the executable.

Log upload interval

The *Log upload interval* option defines the time, in seconds that log entries are collected before being uploaded to the SecureWave Application Server. The Sanctuary Client Driver accumulates the log entries during this period; once uploaded, the next log entry triggers the interval again (default of 3 min.). The default value of 180 seconds applies when this option is not configured. Select this option and type any valid numerical value (in seconds) in the field.

Log upload threshold

The *Log upload threshold* option defines how many log entries are gathered before being automatically uploaded to the SecureWave Application Server. The default value of 10,000 lines applies when this option is not configured. Select this option and type any valid numerical value (# of lines) in the field.

Log upload time

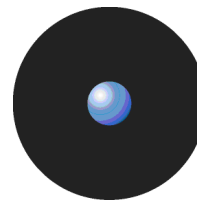
The *Log upload time* option determines the hour when log entries are uploaded to the SecureWave Application Server, if the other log upload thresholds have not already been reached. The default value of 05:00, 5AM, applies when this option is not configured. Select this option and type any valid numerical value (24-hour clock format; HH:mm) in the field.

Log upload delay

The *Log upload delay* option defines a random upper limit value, in seconds, to wait before uploading log files. It is use to alleviate network and server congestion when there are simultaneous uploads. A random value between zero and 3600 seconds — 1 hour — applies when this option is not configured. Select this option and type any valid numerical value (in seconds) in the field.

Server address

The *Server address* option defines the SecureWave Application Server's IP address or fully qualified name. If you have more than one, separate them by using commas. The default IP value defined during the installation applies when this option is not configured. Select this option and type any valid IP address (n.n.n.n) in the field. You can specify several addresses by separating them using a comma. To specify a port on that server, add it to the end of the IP address after a colon (n.n.n.n:nnnn).



Default options for users and user groups

The default options for users and groups govern certain aspects of how users and User Groups interact with the Sanctuary system. These settings apply to all users under the protection of Sanctuary.

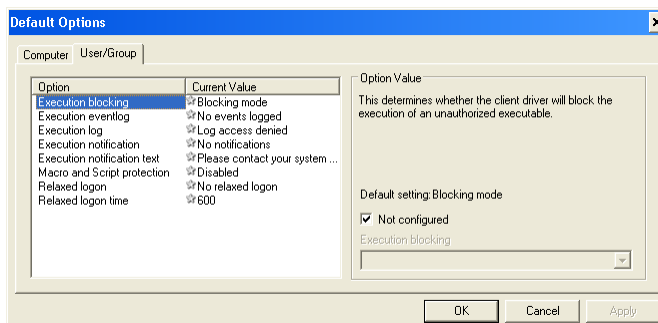


Figure 91. Default User/Group Options

Typically, any changes made to the default options for users and groups are automatically downloaded whenever a client connects to the network.

Execution blocking

The *Execution blocking* option determines whether or not to block execution of unauthorized executable files, scripts and macros according to the user or the user groups to which the user belongs. The available settings are:

- > *Blocking mode* — (default value) Files that are not centrally authorized do not run. There is no local authorization except for the Administrators and LocalSystem account.
- > *Non-blocking mode* — Files that are not authorized can be run. This is useful for testing, configuration purposes, and installing new software.
- > *Ask user for *.exe only* — Prompt the user to explicitly authorize any file with an .exe extension for which a hash is not found in the SecureWave Sanctuary Database. In this case a user can locally authorize the main executable, without needing to authorize all necessary external elements, and each additional module needed.
- > *Ask user always* — Prompt the user to explicitly authorize any file for which a hash is not found in the SecureWave Sanctuary Database. The user must locally authorize the main executable and control the loading of each additional module or ActiveX.

If you select the *Ask user for *.exe only* or *Ask user always*, you can also type the desired message to display.

See *Precedence rules for the Execution Blocking option* on page 120 for details of the Execution Blocking value that should be used in the case of different values having been set for different users/user groups and the computer.



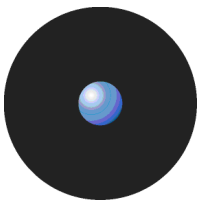
When Sanctuary is installed, the LocalSystem account and Administrators group are automatically set up in non-blocking mode to simplify day-to-day management issues.



Non-blocking mode does not apply to scripts and macros – only executables.



The 'Execution blocking' option works in combination with central authorization using digital signatures (the white list of approved executables, scripts and macros), local authorization and, in the case of scripts or macros, the 'Macro and Script protection' option, to either grant or deny authorization for a particular executable file, script or macro.



Execution eventlog

The *Execution eventlog* option determines what execution events are reported to the Windows Event Log.

You can select among these values:


- > *No events logged* — (default value) Do not log execution system events.
- > *Access-denied logged* — Log when file execution is denied.
- > *Non-blocked access-denied* — Log unauthorized file executions, such as files that would have been otherwise denied if *Blocking Mode* was active (see *Execution blocking* on page 111).

 *This option is only included for backward compatibility.*

Execution log

The *Execution log* option determines what execution events are reported to the SecureWave Application Server log.

You can select among these settings:

- > *Log everything* — Log every access — execution denial — to an executable file.
 *This setting generates a large amount of data. Some Windows DLLs can be loaded several times a second. This setting should only be used for testing purposes and for short periods.*
- > *Log access denied* — Log every denied access to an executable file.
- > *Logging disabled* — (default value) Do not keep a log.

Execution notification

The *Execution notification* option determines whether the user is notified of Sanctuary decisions or not.


You can choose from these settings:


- > *No notifications* — (default value) Do not notify the user. The user always receives an 'Access Denied' or similar message from Windows — there is no way of suppressing this message.
- > *Access-denied* — Notify the user when execution is denied.
- > *Non-blocked access-denied* — Notify the user when the system is in non-blocking mode or in Blocking Mode (see *Execution blocking* on page 111) and runs an unauthorized file.

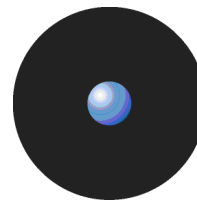
If you select *Access-denied* or *Non-blocked access-denied*, you can also type the desired message to display.

Macro and Script protection

The *Macro and Script protection* option determines whether scripts and macros can run or not.

 *If a user creates or records a new macro in Microsoft Office (i.e. not loading it from a file), the macro is not intercepted and the user can run it without notification.*

 *The 'Macro and Script protection' option works in combination with the option 'Execution blocking' (this must be in 'Non-blocking' mode), central authorization using digital signatures (the white list of approved executables, scripts and macros) and local authorization of executables, scripts and macros to either grant or deny authorization for a particular executable file, script or macro.*



You can select the following values from the pull-down list:

> *Disabled* (default value) No script or macro protection is applied. All VBScripts, JScripts, and macros run, irrespective of whether they are on the white list or not.

> *Ask User* Either:

If a particular VBScript, JScript, or macro is in the white list (*and* authorized by the user having been assigned the File Group that contains the script or macro, or being a member of a User Group which has been assigned to the File Group), or if it has been locally authorized on the same computer, then it automatically runs.

— or —

- If a particular VBScript, JScript, or macro is not in the white list (*or* is in the white list but its File Group is neither assigned to the user or a User Group that they belong to), and has not been locally authorized on the same computer, then Sanctuary gives the local user the authority to determine whether it executes on the computer he is using or not.

> *Deny All* VBScripts, JScripts, or macros that are in the white list (*and* authorized by the user having been assigned the File Group that contains the script or macro, or being a member of a User Group which has been assigned to the File Group) run, but not others.

Relaxed logon

The *Relaxed logon* option allows the user to run logon scripts without having to authorize them. This setting permits to run the files that would otherwise be blocked during the logon process.

You can select between:

> *Disabled* — (default value) No delay occurs before blocking is activated. Unauthorized files cannot even run during logon.

> *Enabled* — A delay occurs before blocking is activated. Unauthorized files can execute during logon.



Change this registry key on each client computer if you want to prevent logon scripts from running asynchronously:

HKML\Software\Microsoft\Windows NT\CurrentVersion\winlogon

The RunLogonScriptSync key should be set as a REG_DWORD with a value of 1.

By doing this, users cannot run unauthorized files by double-clicking their icon on the desktop while an asynchronous logon script is running in the background during a 'Relaxed Logon'.

However, you should note that it is still possible to start applications from the NEW TASK button in the 'Applications' tab of the 'Task Manager'.

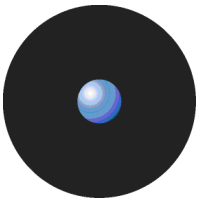
Relaxed logon time

The *Relaxed logon time* option defines the length of time, in seconds, of the 'Relaxed logon time' grace period. The default value of 600 ms applies when this option is not configured. Specify your own value when configuring the option.

Blocking can also be activated at the end of the logon script by running the endlogon.exe command. 'Endlogon.exe' activates blocking immediately, even if the relaxed logon time has not yet expired. The 'endlogon.exe' program forms part of Sanctuary installation.




The relaxed logon time option does not apply to scripts and macros – only executables.



Options that apply to specific machines or specific users

The default option settings you defined in the *Computer* tab of the *Default Options* dialog boxes apply to all computers being protected by Sanctuary. Similarly the default option settings you defined in the *User/Group* tab apply to all uses or users who belong to all User Groups. You can however override these default settings for specific computers, or specific users/User Groups.

To override default option settings

1. Open the *User Explorer* module. To do this, click on the  icon located in the *Modules* section of the *Control Panel* (or use the *View→Modules* command).
2. Select the *File Groups by User* tab.
3. Right-click on any computer, user, or user group in the list and select *Options* in the context menu.

The system displays an *Options* dialog box that is similar to the global *Default Options* dialog box except that it contains options for the specific computer, user, or user group.



These option settings apply only to the selected machine, user or user group. In this case, they take precedence over the global default option settings. For more information about orders of precedence see later in this chapter.

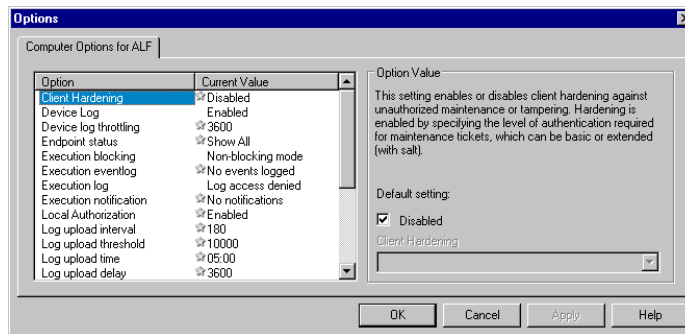


Figure 92. Options - for a specific computer

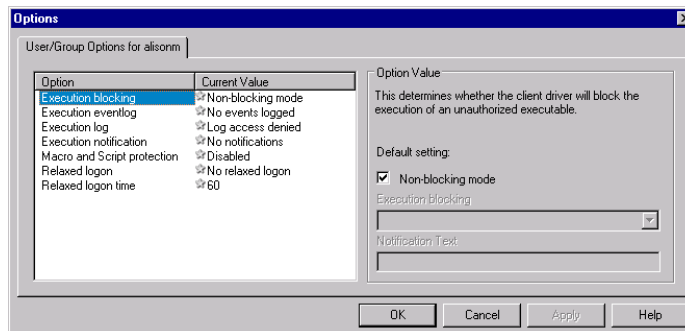


Figure 93. Options - for a specific user

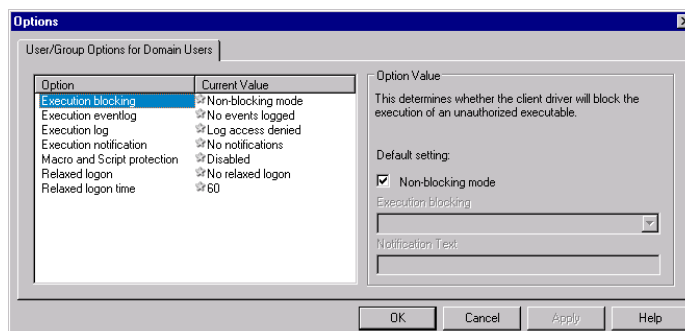
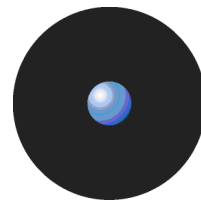


Figure 94. Options - for a specific user group



4. Highlight the option for which you want to override the default settings, in the *Option* list box.
5. Uncheck the *Default setting* box in the *Option Value* panel.



The label to the right of the Default Setting checkbox is the current value that is being used by default for the option, for example, if the Local Authorization option is enabled by default the checkbox is labelled Enabled.



The settings for each default option are explained earlier in this chapter, where the Sanctuary default setting for each is also indicated. Where the predefined defaults are still in use star symbols, ☆, are displayed in the Current Value column of the Option list box.

6. Select the required value for the option from the drop-down list of option values.
7. Enter a message to be displayed to the user, if required.
8. Save the amended option value. You can either

> Click on OK to save the setting and close the Options dialog.

— or —

> Click on APPLY to save the setting without closing the dialog. You can then repeat steps 4 to 8 to override other default option settings for the specific computer, user, or user group.

Determining which option setting takes precedence

For some options, it is possible to have different settings at the user level, group level, machine level, or global level. When these values are different, a logical decision hierarchy determines which setting takes effect.

Precedence rules for computer options

For the options that apply to computers (rather than for users/user groups), the order of precedence is as follows:

1. If a value is set for the specific computer, that value is in force and supersedes all other option settings.
2. If no value is explicitly set for the computer, global *Default Option* setting in the *Computer* tab applies.
3. If no global *Default Option* setting is defined for this option, the predefined Sanctuary system default settings apply. See *Default options for protected servers and computers* on page 107 for more information.

The following flowchart shows the process corresponding to computer precedence rules:

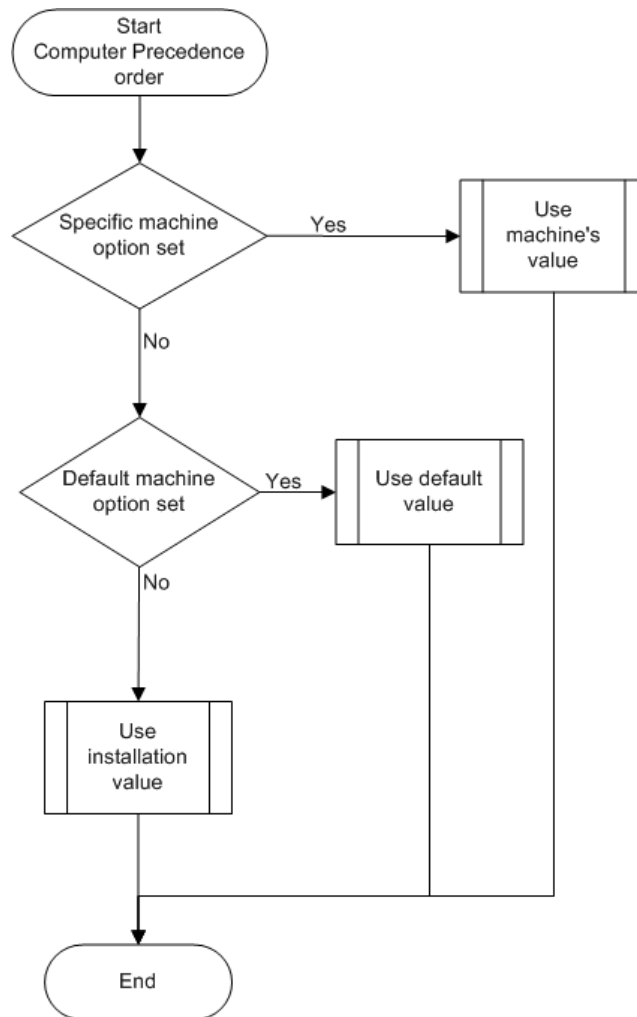
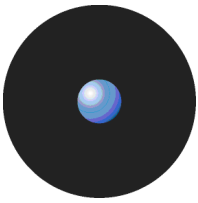


Figure 95. Computer Precedence Process

Precedence rules for user and user group options

For most options that apply to users and groups, the order of precedence is as follows:

1. If a value is set for the specific user, that value is in force and supersedes all other option settings.
2. If no value is explicitly set for the user, but a value is set for the user group to which that user belongs, the group option setting applies.
3. If the user belongs to several user groups that have different option settings, the highest precedence option setting applies (see Table 21).
4. If no value is set for the user or any user groups to which the user belongs, the global *Default Option* settings in the *User/Group* tab apply.
5. If no global *Default Option* is set in the *User/Group* tab, the predefined Sanctuary system default settings apply. See *Default options for users and user groups* on page 111 for more information.

The following flowchart shows the process corresponding to users/groups precedence rules:

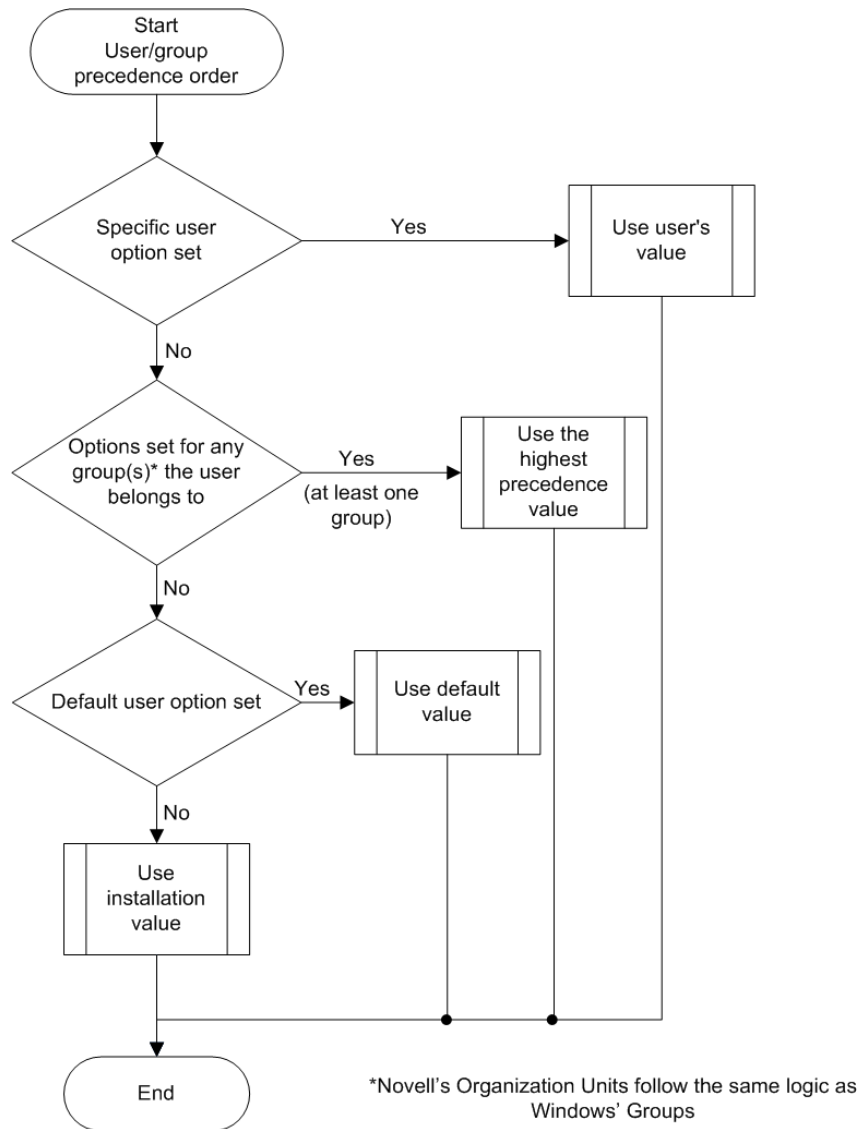


Figure 96. Users/Groups Precedence Process

The precedence used to determine which option setting is used in the case where a user belongs to multiple user groups which have different values of the same option, depends on a predefined value precedence. The value precedence for various options is shown in the following table:

*In the following table the option value with the **higher** number takes precedence, i.e. for the Execution Blocking option the value 'Always ask user' (3) has a precedence than 'Ask user for *.exe' only (2), 'Non-blocking' (1), and 'Blocking' (0).*

Although the numbers associated with the precedence are not shown in Sanctuary the option values are listed in the drop-down list in the right panel of the Default Options and Options dialog in this order.



Option	Value precedence
<i>Execution Log</i>	0. Log everything 1. Log access denied 2. Logging disabled
<i>Execution Blocking</i>	0. Blocking mode 1. Non-blocking mode 2. Ask user for *.exe only 3. Ask user always
<i>Execution Notification</i>	0. No notifications 1. Access-denied 2. Non-blocked access-denied
<i>Execution Eventlog</i>	0. No events logged 1. Access-denied logged 2. Non-blocked access-denied
<i>Macro and Script protection</i>	0. Disabled 1. Ask User 2. Deny all

Table 21: The precedence of option values



The *User Options* and *Machine Options* reports present a summary of all options defined in the system. See *User Options* on page 100 and *Machine Options* on page 101 respectively.



If the *Local Authorization* option is disabled, the 'Ask user for *.exe only' or 'Ask user always' values are ignored.

Precedence rules for options with both computer and user/user group values

Some options can be set not only at a global level and at a level that is specific to a particular computer, user or user group, but also they may be set *both* using *Computer* and the *User/Group* tabs. For the *Execution eventlog*, *Execution log* and *Execution notification* options that are governed by computer *and* user/user group options, the priority is as follows:

1. Options explicitly set for a specific user (these settings take precedence over all others).
2. Options explicitly set for a user group to which the user belongs. If the user belongs to several groups that have different option settings, the highest precedence option setting applies (see Table 21).
3. Global settings from the *User/Group* tab of the *Default Options* dialog.
4. Options explicitly set for the machine that the user is using.
5. Global default settings from the *Computer* tab of the *Default Options* dialog.
6. Predefined Sanctuary system default settings.

The following flowchart shows the process corresponding to computer *and* user/user group precedence rules:

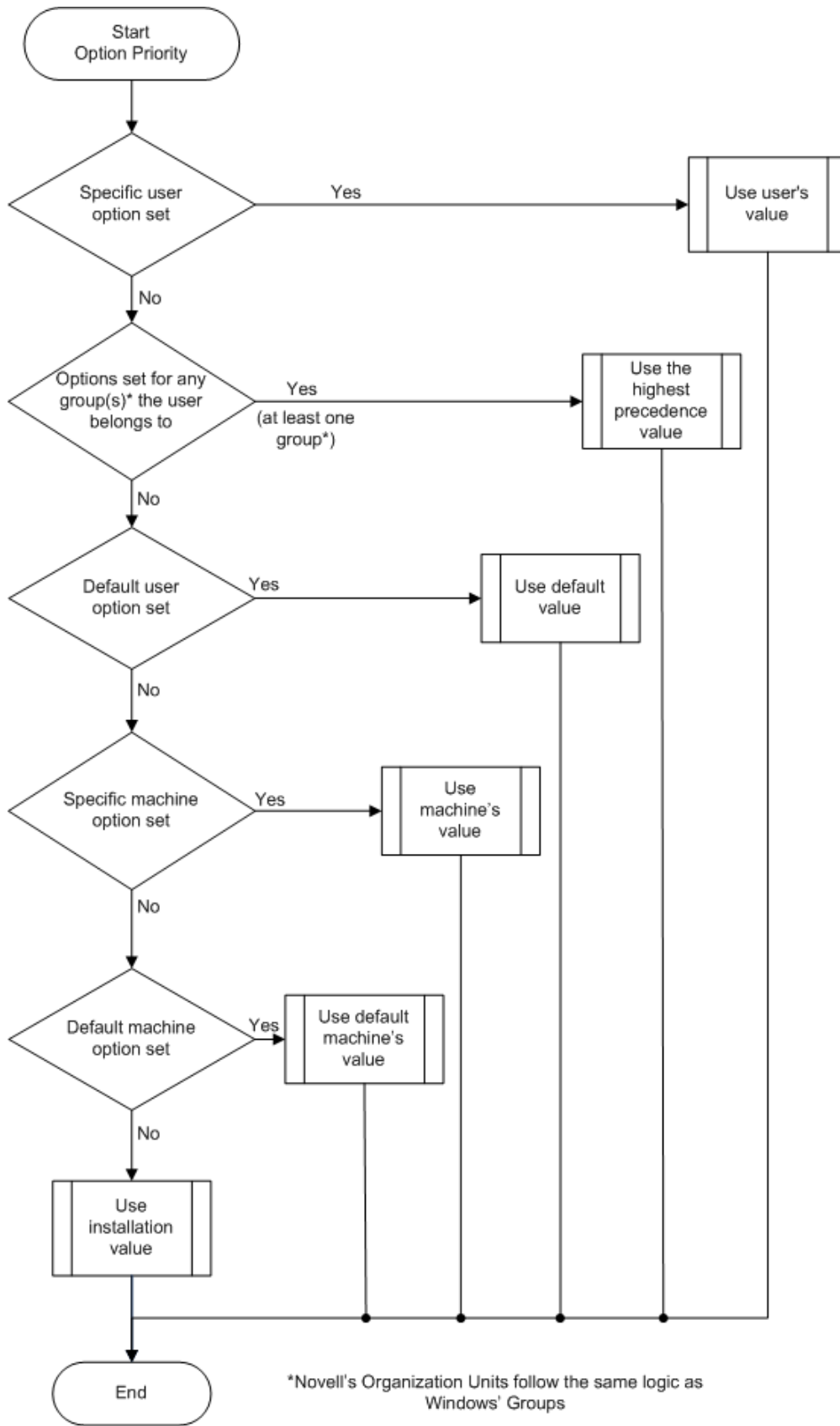


Figure 97. Computer and user/user group precedence process



Precedence rules for the Execution Blocking option

The *Execution Blocking* option follows a special rule pattern:

1. If the User option is set to *Non-Blocking*, then it is used.
2. Otherwise, if at least one group to which the user is a member is set to *Non-Blocking*, then the non-blocking mode is used.
3. Otherwise, if a default value in the *Default Users/Groups Options* dialog is set to *Non-Blocking*, then it is used.
4. Otherwise, if the Machine Option is set, it is used.
5. If no value is set for the machine, then the default option is applied as set in the *Default Machines Options* dialog.
6. If no default machine option is set, then the installation default (*Execution Blocking*) is applied.

The following flowchart shows the process corresponding to Execution Blocking precedence rules:

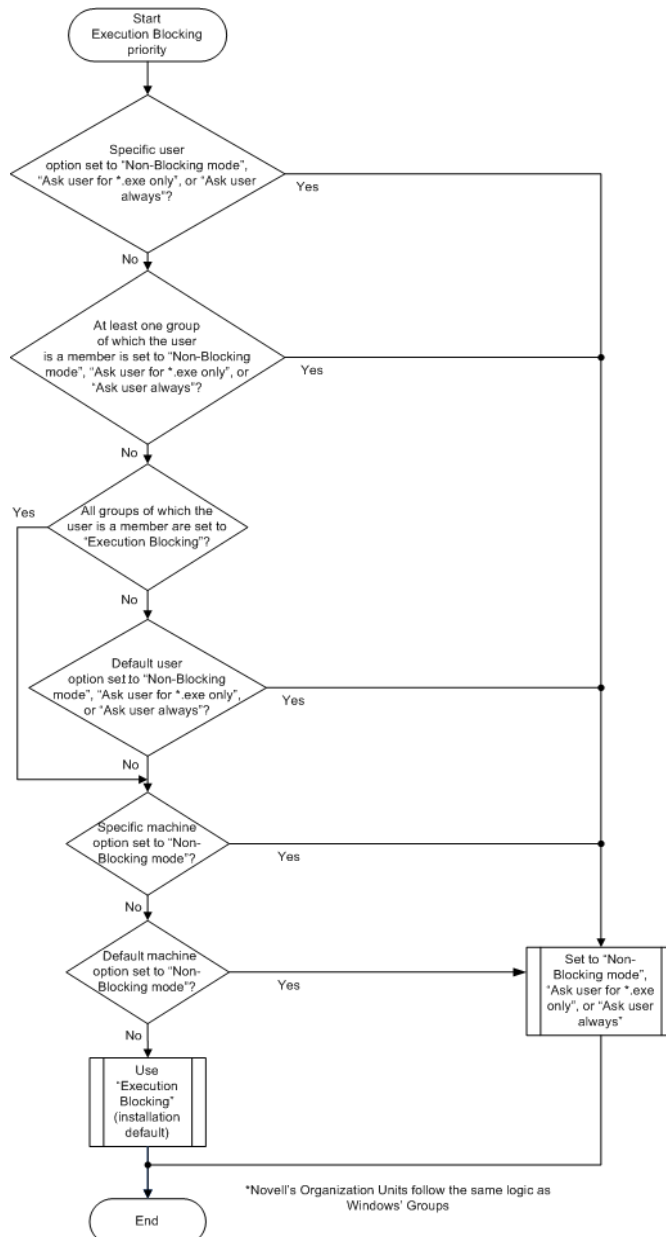
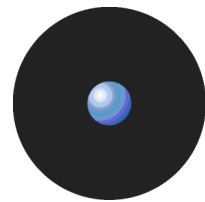


Figure 98. Execution blocking precedence process



If the Local Authorization option is disabled altogether — either via global system settings or because the Spread Check mechanism is enacted to stop self-propagating code — all applications that are not included list of authorized files are blocked, regardless of the values of the Execution Blocking option.

Examples of the precedence of Execution Blocking options

In the following examples of the precedence of Execution Blocking options, the user Bill is a member of the domain groups Marketing, Sales, and Domain Users.

- > The *Execution Blocking* option for the group Marketing is set to 'Ask user for *.exe only' and the user option for Bill is set to 'Non-Blocking'. Bill is in non-blocking mode. A specific user option takes precedence over a group option.
- > The *Execution Blocking* option for the group Marketing is set to 'Ask user for *.exe only', the option for Domain Users is set to 'Ask user always', and the option for Sales is set to 'Non-Blocking'. If no other options are set, Bill is in 'Ask user always' mode. All options are set at the group level: the 'Ask user always' value is applied as it has the highest precedence (i.e. corresponding to the *lowest* value precedence number for the *Execution Blocking* option in Table 21).
- > You have set Bill's computer specific option to 'Non-blocking'. Nevertheless, Bill sees the local authorization dialog every time he tries to execute an unauthorized application. It means that:
 - > *The Local Authorization option has an 'Enabled' value either for the computer Bill is working on, or in Computer tab of the Default Options dialog (i.e. as the global default option).*

— and —

 - > *The Local Authorization option has not been disabled because the Spread Check mechanism is enacted to stop self-propagating code.*

— and —

 - > *An 'Ask user for *.exe only' or 'Ask user always' value has been chosen for the Execution Blocking option either for Bill, one of the groups of which he is a member, or in the Default Options dialog (i.e. as the global default option).*

A user/user group option always takes precedence over a computer specific option.

- > The *Execution Blocking* option for the group Marketing is set to 'Ask user for *.exe only' and the option for Sales is set to 'Non-Blocking'. If no other options are set, Bill is in 'Ask user for *.exe only' mode. If the 'Local Authorization' option is disabled by the spread check mechanism, then Bill is in 'non-blocking' mode. When the Local Authorization is disabled, the 'Ask user for *.exe only' and 'Ask user always' options are ignored!

Informing client computers of changes

Whenever you make a change to the Sanctuary options, File Groups, the assignment of File Groups to users and so on, you can notify the client computers immediately that something has changed rather than waiting for the next log time a user logs on.

To update all computers, click on the *Send Updates to All Computers* option in the *Tools* menu (or the *Control Panel*). You can also send updates to a specific computer using the *User Explorer* window, right-clicking on the name of the computer and selecting the *Send Updates to: <name>* option from the context menu.

Any computer that is switched off, or disconnected from the network, receives the updates the next time it is booted up. Alternatively, you can export them to a file and import them on the computer you want to update. See *Exporting* on page 33 for more information.

Chapter 13: Windows Updates and other tools

This chapter described three useful tools:

- > Authorization Service Tool (AuthSrv.exe) — used to monitor changes made to Microsoft applications and operating systems when they are updated.
- > Versatile File Processor tool (FileTool.exe) — used to scan files in specific locations. See *Versatile File Processor tool*, on page 127.
- > File Import/Export Tool (Fimpex.exe) — the command-line tool that lets you export and import hashes and File Groups to/from the SecureWave Sanctuary Database. See *File Import/Export Tool* on page 130.

Authorization Service Tool

This section provides you with useful information about the Authorization Service Tool.

Microsoft Software Update Services and Windows Server Update Services

Microsoft's Software Update Services (SUS) assists Microsoft Windows administrators with the distribution of security fixes and critical update releases provided by Microsoft. Running SUS is equivalent to running a Windows Update service from inside your own network.

SUS is used to distribute official updates to Microsoft Windows 2000, Microsoft Windows XP and Microsoft 2003 computers, including servers and desktops.



SUS does not support Vista.

Windows Server Update Services (WSUS, previously SUS v2.0) is a new version of SUS. WSUS supports updating Windows operating systems as well as all Microsoft corporate software.

What does the Authorization Service Tool do?

You can use *Authorization Service Tool* (AuthSrv.exe) to monitor changes on the approved and synchronized files done by SUS or WSUS, and process them, when needed, using the *Versatile File Processor Tool* (FileTool.exe).

The aim of this process is to update computer without any administration effort. All Microsoft Authorized updates and fixes are automatically authorized, their hash numbers created, and the Sanctuary database updated. Once installed, you should not worry about the security of your Microsoft updates again! (There is, however, sometimes a need to fine-tune the Authorization Service Tool's features manually.)

To use Authorization Service Tool you need:




- > SUS or WSUS installed on your machine.
- > A mail server and an e-mail account, depending on your selected options.

In addition, WSUS requires the following (depending on the configuration of your machine):

- > Microsoft Internet Information Services (IIS) 5.0.
- > Microsoft .NET Framework pack.
- > Background Intelligent Transfer Services (BITS) 2.0. This lets you download updates in the background using available network bandwidth.
- > SQL Server 2000/2005, MSDE 2000, or SQL Server 2005 Express Edition.



Authorization Service Tool can trigger a full SUS directories scan when it is unable to determine the new approved files. It monitors SUS ('history-sync.xml' and 'history-approve.xml') and WSUS logs to trigger the *Versatile File Processor* tool on the new files.

-  *If the registry configuration is not valid (for example it has invalid paths, etc.), Authorization Service Tool will not run.*
-  *Do not use network drive mapping with the Authorization Service Tool — only Universal Naming Convention (UNC) names. Drive maps are assigned per logon session and the Authorization Service Tool runs in a different one from where the mapping was originally created.*
-  *The Authorization Service Tool does not support Express Installation files. See the Sanctuary's Setup Guide for instruction on how to configure the WSUS service.*

The following diagram summarizes the behavior of Authorization Service Tool:

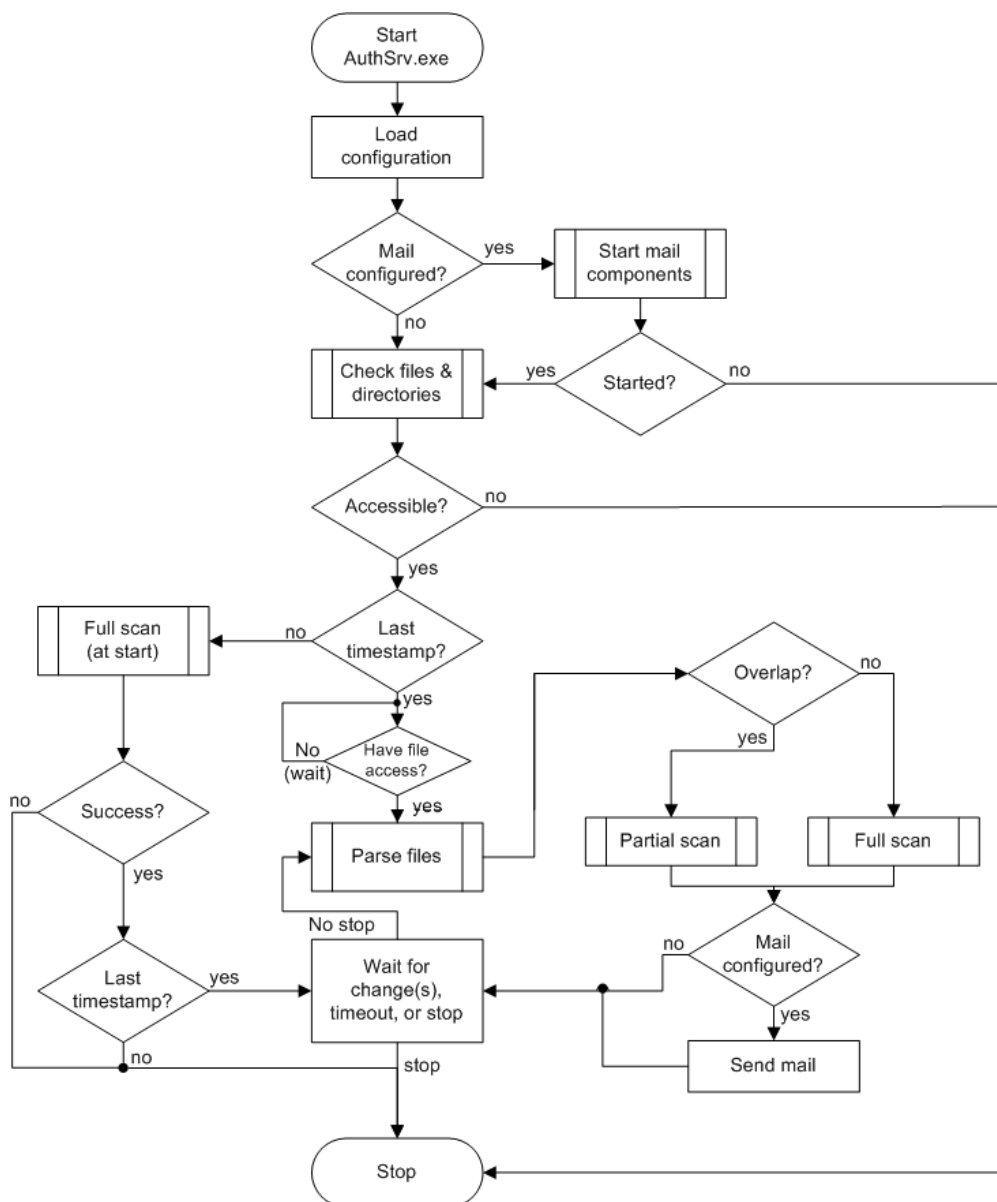
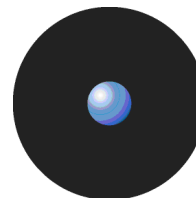


Figure 99. Flowchart to describe the Authorization Service Tool process



The rectangular block marked as *Wait for change(s), Timeout, or stop* forms the main loop of the Authorization Service Tool. The process only exits only when there is a problem, no changes, or a stop signal. When you run this tool, it searches for new updates in the defined directory, C:\Microsoft\updated files by default.

Each time an update is released, Authorization Service Tool locates and scans the update files and creates an XML log file in an installation folder, typically %PROGRAMFILES%\SecureWave\Sanctuary\Authorization Service.

Installing the Authorization Service tool

You install the Authorization Service Tool using a setup wizard. See the Sanctuary's Setup Guide for details.

If you did not activate the *Do not automatically start the Authorization Service when Setup is finished* option, the program starts once the installation ends.

Authorization Service Tool then waits until one of the following occurs:

- > A change is made in the default update folder, by WSUS.
- > The administrator approves the updates in the SUS console.
- > An hour has passed.

Once installed and loaded, you can authorize update files. A screen similar to the example below is displayed when you choose the *Microsoft Update Files* option in the *Database Explorer* module:

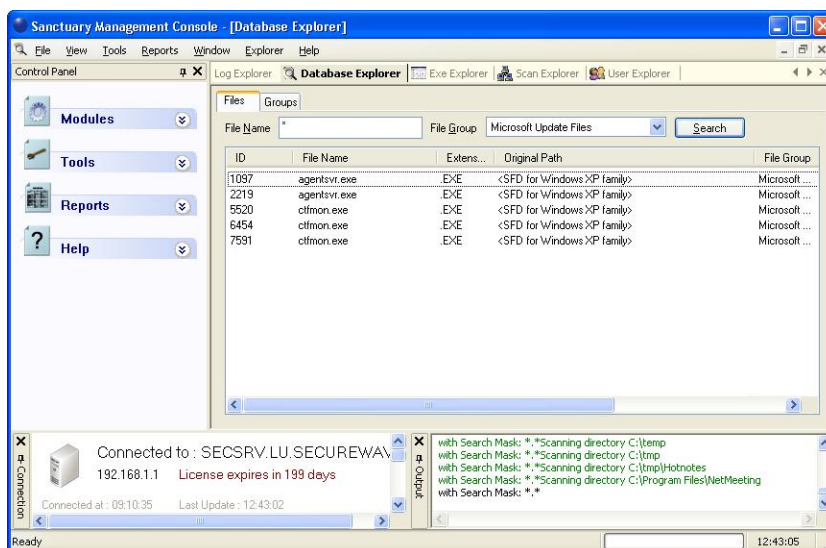


Figure 100: Sanctuary's initial scan

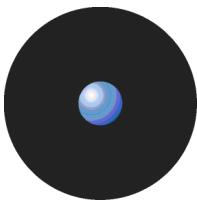
Configuring the Authorization Service tool

You normally configure Authorization Service Tool during setup. Subsequent modification can either be made using the setup wizard, or by directly modifying the appropriate Windows registry key.

Authorization Service Tool does not support Outlook Express or Internet Information Server (IIS) as clients for sending email messages. If there is already an account in these types of clients, the SMTP IP address is transferred directly to the Authorization Service Tool configuration. The 'LoadConfiguration' registry key parameter is always set to '3'.

To modify Authorization Service Tool parameters using the setup wizard

1. Run the setup wizard (located on your Sanctuary CD). The first screen informs you that the product is already installed.
2. Click on the NEXT button. The second screens allows you to modify the installation.
3. Select the *Modify* option and click on NEXT.



4. Change the server's address and port in the third screen.
5. Finish the modification process.

To manually modify the Authorization Service Tool parameters

If you wish to fine tune the Authorization Service Tool's parameters, you can manually modify it directly using the following Windows registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AuthSrvHlpr\Parameters

The following table as a guide when adding or changing parameters:

Parameter	Type	Description	Default value
Standard Parameters			
HistoryDirectory	REG_SZ	Absolute directory path to 'history-sync.xml' and 'history-approve.xml'.	
SUSContentDirectory	REG_SZ	Absolute directory path where SUS files are located.	
WSUSContentDirectory	REG_SZ	Absolute directory path where WSUS files are located. If you are using SUS, you must define HistoryDirectory and SUSContentDirectory. If you are using WSUS, you must define this entry. If you define both entries, the program uses WSUSContentDirectory.	
OutputDirectory	REG_SZ	Directory path where output XML reports are located.	
VerboseReport	REG_SZ	Yes Verbose report mode No Normal report mode.	'No'
SXSServer	REG_SZ	Name or IP address of the SecureWave Application Server.	
Mail Parameters			
SendMail	REG_SZ	If enabled ('yes'), the service sends an email at the end of a scan. This email includes the command line and the xml report attached.	'No'
SendMailFrom	REG_SZ	Email address of the sender.	
SendMailTo	REG_SZ	Email address of the addressee.	
LoadConfiguration	REG_SZ	-1 Collaboration Data Object (CDO) mail objects try to load the user's Outlook or IIS Mail configuration. 1 CDO mail objects try to load the user's IIS Mail configuration. 2 CDO mail objects try to load the user's Outlook configuration. 3 Use CDO mail objects.	3
SMTPServer	REG_SZ	SMTP server name or IP address.	
SMTPServerPort	REG_SZ	SMTP Server Port.	25
UserName	REG_SZ	Username if SMTP requests login.	
Password	REG_SZ	Password if SMTP requests login. We suggest using IIS or Outlook mail configuration to avoid having plain text password in Windows registry.	
AuthenticateLevel	REG_SZ	0 none 1 basic 2 NTLM	1
UseSSL	REG_SZ	Use Secure Socket Layer (SSL) communication between the mail client and the SMTP server.	'No'
Since mail configuration may not be straightforward and needs some tuning, you can set these parameters using a script: e.g., create a text file with .reg extension containing: REGEDIT [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AuthSrvHlpr] 'UserName'='TheAdministrator'			
Advanced Parameters			
CmdLineExecutable	REG_SZ	Allow an absolute path configuration of the Versatile File Processor. This is normally located in the Authorization Service Tool installation directory.	'FileTool.exe'
CmdLineGlobalParams	REG_SZ	Using -v and C:\temp as values: '-v'c:\temp\FileTool <date and time>.xml'	Depends on OutputDirectory & VerboseReport
CmdLineBlockParams	REG_SZ	Allow user to setup assignment mode, group name(s), filters, etc. in FileTool.exe command line parameters.	-a1 'Microsoft Update Files'**
Log file name	REG_SZ	Gives the name of the log file written if 'Log to file' is true.	Depends on 'Log to file' value
Log to file	REG_SZ	If 'yes' or '1', sends debug messages to the log file (see the Log file name entry).	'No'
** If you use -a1, all new update files are assigned to this group and, as a result, you maybe changing File Group authorizations that already exit in the database. To keep the files' original File Group, use the -a0 parameter. See Table 23.			

Table 22. Authorization Service Tool configuration parameters

For example, the following key setting:

'log to file' = 1; 'log file name'='c:\temp'

means create a log file and place it in the c:\temp directory.



Versatile File Processor tool

The Versatile File Processor tool is used to scan files in specific locations. It supersedes AddFiles.exe. It consists of two parts:

- > A DLL (filetool.dll) that provides the underlying functionality. This is used by other SecureWave tools, for example, the Authorization Service Tool.
- > A command line executable, filetool.exe (which uses the DLL).

Versatile File Processor tool can work in two modes:

- > **Online** — In the online mode, it scans file locations (that must be specified) and connects to a SecureWave Application Server to assign the files. It can assign files automatically, using SecureWave Application Server suggestions, if configured. It connects, by default, to the local SecureWave Application Server, using the identity of the current user. These defaults can be overridden using the command line options `-s <server>` and `-u <user> <password>`. After the assignment, and if the `-p` option is specified, the tool can request SecureWave Application Server to notify all the clients (drivers).
- > **Offline** — In the offline mode, it produces scan files. Even though the scan files have exactly the same format as the scan files produced by the driver, these cannot be used directly. Offline mode requires an output file name only if using the `-o <scan>` option. File assignment cannot be performed in offline mode. The resulting file can be copied to the SecureWave Application Server drive to compare with other scanned files.



The Versatile File Processor tool can scan files contained in archives files (cab, zip, rar, ace, jar, cx from PatchLink). However, some CAB archives do not have a standard cabinet structure despite having a .cab extension and it may not be possible to correctly scan their contents.

Command line parameters

If you execute the Versatile File Processor Tool without parameters, it displays a help output:

Parameter	Description
Usage: filetool [-s<server>] [-u user password] [-o <scan>] [-d#] [-f <n> <m>] [-v <report>] [-r <report>] [-i <block> [<block> ...] [-p <block>: target [target ...] [-e <mask>] [-c#] [-a# <FileGroup>] [-x#]	
-s	SecureWave Application Server server (default is this machine).
-u	User/password to connect to SecureWave Application Server (default: current user).
-o	Offline mode, generate a scan.
-d0	Delta mode off*.
-d1	Delta mode on, avoid rescanning files already scanned.
-d2	Delta mode on, clear the list then memorize files already scanned.
-f	Access failure; retry <n> times with a least <m> sec. in between.
-v	Verbose report; generate an xml report.
-r	Report; generate an xml report, errors only.
-i	Ignore archive contents.
target	File or directory to scan. To avoid recursive scan on directory, terminate with \\ (e.g., C:\temp\). The target may also be one of these keywords in brackets: [drives] all hard drives. [media] all removable media. [all] all hard drives and removable media.
-e	An optional wildcard mask, e.g., '*.ex?' (default: '*').
-c0	File group creation, use only existing groups.
-c1	File group creation, create if necessary*.
-a0	Keep existing assignment, auto-assign new files, assign rest to group*. Accepts a list of groups <FileGroup1>;<FileGroup2>;...;<FileGroupN>. Multiple groups are used to disambiguate suggestions via the first-match policy. The last group terminates the disambiguation process unconditionally.
-a1	Keep existing assignment, assign new files to group.
-a2	Assign existing and new files to group.
-x0	Process all files. This is risky since this option scans files even if they are not executables (*.txt, *.doc, etc.).
-x1	Only process executables (16 and 32 bits) *.
-x2	Only process executables with a valid digital signature.
-p	Push updates to all online clients.
*The default options.	

Table 23: FileTool.exe command line parameters

The command line parameters have three sections: mode parameters, global options, and file blocks.



Usage notes

Delta mode

The delta mode (`-d` command line parameter) is useful when FileTool.exe is used to process ever-growing file collections, such as those produced by Windows update components. In this mode, FileTool.exe simply inspects files that were not there since the last run. The `-d1` option loads the list of previously scanned files, `-d2` clears the list (thus resetting the delta mode); both options store the list of scanned files upon exit. The `-d0` option (default value) disables delta-mode operations.

Retry logic

FileTool.exe has a retry logic used in case a file cannot be opened. It repeats the file open operation five times (default value), waiting five seconds before each try. These parameters can be changed using the `-f <n> <m>` option.

Reports

The Versatile File Processor tool can generate an XML report. This includes the options, any errors encountered, and, in the verbose mode, file assignments. Use the `-r` option for a standard report and `-v` for a verbose one.

Archive files

If you specify the `-i` option, archives and self-extracted executables are not unpacked.

When archive content is allowed, FileTool.exe can process ZIP, CAB, and MSI archives. Additionally, InstallShield archives are supported if you have ZD50149.DLL and ZD51145.DLL in your system; ACE archives if UnAceV2.dll can be found; and RAR archives if UnRar.dll is present. We do not ship these files due to copyright restrictions. You can download them directly from Internet.

File block

A file block is a list of one or more targets and options associated with a list.

Targets are simply file locations specified with the `target` command line option. They can specify individual files, directories, and special locations. Files and directories are specified by path, for example: `C:\temp`, `C:\temp\app.exe`. Directories are scanned with their subdirectories. If you do not want to process subdirectories, terminate the target directory with a double backslash, e.g., `C:\temp\`. There are three special locations: `[drives]`= all hard drives, `[media]`= all removable media, and `[all]`= a combination of the two.

You can limit the target file scan using a filter of one or more wildcard masks. E.g., `-e *.dll;*.ocx` only scan `.dll` and `.ocx` files.

A further restriction is based on the actual file type. By default, only executables are considered in the scan process. Because certain MS-DOS executable files cannot be identified as executable, you can use the `-x0` option to scan all files (subject to the target and wildcard restrictions).

All other file block options apply only to the online mode.

The file assignments obey the `-a#` option:

```
> -a0 <FileGroup1>;<FileGroup2>;...;<FileGroupN>
```

If the file is known, the assignment is not changed.

If the file is unknown, and no group is suggested, the file is assigned to the `<Not authorized>` File Group.

If the file is unknown, and only one group is suggested, the file is assigned to that File Group.

If the file is unknown, and two or more groups are suggested, the file is assigned to the first one that matches or, if no counterpart is found, to the last one (`<FileGroupN>`).

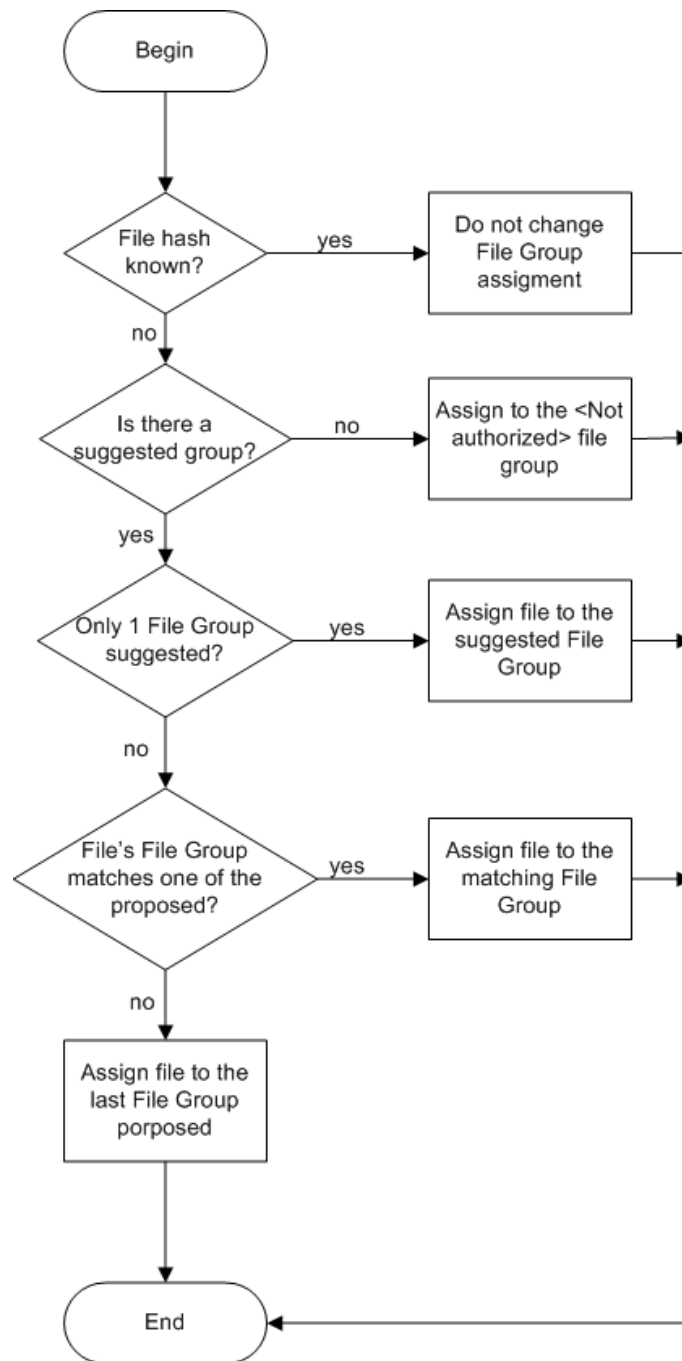


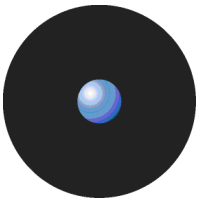
Figure 101: FileTool's File Group assignments

- > `-a1 <FileGroup>` assigns unknown files to `<FileGroup>`. If the file is known, the assignment is not changed.
- > `-a2 <FileGroup>` always assigns files to `<FileGroup>`, even those already assigned to other groups. If `<FileGroup>` is empty, using `"` (single quotation marks) for the group name, known files are removed from their groups.

By default, any non-existent group specified in the `-a#` options are created, which may be prevented using the `-c0` option. This is useful as a precaution against typing errors.



*Always specify the correct options or you risk creating hashes for unusable files (e.g. *.doc, *.txt). You can avoid this by specifying the file extensions or by using the `-x0` option carefully.*



The information on the file blocks is included in the report, one option tag per each file block. The following attributes are included in the report:

Attribute	Description
<i>Mask</i>	Empty by default, set with <code>-e</code> .
<i>Files</i>	'Executables' by default, set to 'all' with <code>-x0</code> .
<i>Name</i>	'...' matches the group(s) specified with <code>-a0</code> , <code>-a1</code> or <code>-a2</code> .
<i>Assignmentpolicy</i>	'Auto' for , 'standard' for , 'overwrite' for <code>-a2</code> .
<i>Creation</i>	'Yes' by default, 'no' when <code>-c</code> is used.

Table 24. FileTool.exe File Block Report Options

Examples

Scan files in path `c:\test`, recursively, with no mask, scanning all executables, use the group 'test' for assignment, do an automatic assignment of the files found, and create the group if not found.

```
filetool.exe C:\test -a0 test
```

Scan all executables on all drives, auto-assign, and allocate all non-assigned files automatically to testGroup:

```
filetool.exe -r report.xml [drives] -a0 testGroup
```

Scan `c:\temp` without subdirectories, un-assign all found executables, and then notify all online client drivers:

```
FileTool.exe c:\temp\ -a2 "" -p
```

If we combine the two previous examples, we get:

```
FileTool.exe -r report.xml [drives] -a0 testGroup c:\temp\ -a2 "" -p
```

Connect to the SecureWave Application Server located on this machine using the current user credentials, avoid rescanning files already scanned, scan all files (including archives) in the `to_scan_directory` of drive C recursively pushing the updates to all on-line machines and keeping existing File Group assignments.

```
C:\"program files"\SecureWave\Sanctuary\sxstools\filetool.exe -d1
c:\to_scan_directory -p
```

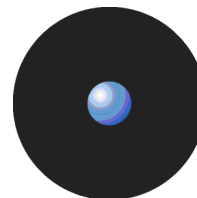
File Import/Export Tool

The File Import/Export Tool (Fimpex.exe) is a command-line tool that allows you to import and export hashes and File Groups to/from the SecureWave Sanctuary Database locally or remotely. It is used when updating from another Sanctuary system or to simply fill-up the database with already defined File Groups and hashes. This tool is installed when deploying the Sanctuary Application Control Suite.

Command line parameters

If you execute the File Import/Export Tool without parameters, it displays a help output.

Parameter	Description
usage: fimpex [-s <server>] [-d <database>] [-k -r] [-o -a] [-u <usr> <pw>] [-g <group>] [-g <group2> ...] [-m <SrcGroup> <DstGroup>] [-m <SrcGroup> <DstGroup> ...] {-e -i} <file>	
<code>-s</code>	Database Server. The default is the local machine.
<code>-u</code>	User/password to be used for an un-trusted connection. If not used, a trusted connection is attempted.
<code>-d</code>	Database name.
<code>-g**</code>	Defines a File Group to be exported. If not used, all hashes and File Groups are exported. This switch can be repeated as needed to define several File Groups. It is ignored during an import.
<code>-k*</code>	Keeps File Group associations for existing hashes (default value).
<code>-r*</code>	Replaces File Group associations for existing hashes.
<code>-o*</code>	Obliterate mode (default). Before a File Group is imported, all its member files are deleted.
<code>-a*</code>	Amend mode. File Group members files are not deleted during the importation.
<code>-m*</code>	Maps the contents of the File Group SrcGroup (input) to DstGroup (database). The DstGroup File Group must exist in the database before importing.
<code>-e</code>	Export the files and File Group tables.
<code>-i</code>	Import the files and File Group tables.
<code><file></code>	Data file name. On import, all File Groups and file hashes in this file are copied into the database. On export, all selected File Groups and hashes are written to this file. HOWEVER, if the file name contains '#' or '\$' (export



Parameter	Description
	only), then each exported file group gets its own data file; '\$' in the file name is replaced by the File Group name, and '#' is replaced with the internal ID number of the File Group. Example: if you have a File Group 'Office' with ID 101 and a File Group 'Games' with ID 303, using the data file name 'fimpex.#-\$.dat' generates 'fimpex.101-Office.dat' and 'fimpex.303-Games.dat'. Any character not allowed in file names is replaced with an underscore (_).
	* These switches are only used when importing.
	** Only used when exporting.

Table 25: FileTool.exe command line parameters

Usage notes

On import, fimpex overwrites existing hashes and/or File Group if they conflict with imported data. See `-r`, `-k`, `-o`, and `-a` parameters for details.

Examples

Export the SX database on the local computer to a file named 'fimpex.dat':

```
fimpex -e fimpex.dat
```

Import a file named 'fimpex.dat' into the SX database of the local computer:

```
fimpex -i fimpex.dat
```

Export the 'accessories' File Group from the local SX database to a file named 'fimpex.dat':

```
fimpex -g accessories -e fimpex.dat
```

Export the 'accessories' and 'Windows Common' File Groups from the local SX database to a file named 'fimpex.dat':

```
fimpex -g accessories -g "Windows Common" -e fimpex.dat
```

Import the 'fimpex.dat' file into the SX database located on the 'My_database_server' server:

```
fimpex -s My_database_server -i fimpex.dat
```

Import hashes from the 'fimpex.dat' file. File hashes that were assigned to the File Group 'groupA' during the export of the source database are now assigned to 'groupB' in the target database during import:

```
fimpex -m groupA groupB -i fimpex.dat
```

Note that the File Group 'groupB' must already exist in the target database. The File Group 'groupA' does not need to exist in the target database. If the File Group 'groupA' exists in the target database, you should set the `-r` option. In this case, all files assigned to File Group 'groupA' are deleted and assigned to 'groupB':

```
fimpex -r -m groupA groupB -i fimpex.dat
```

```
fimpex -r -i fimpex.dat
```

This imports the 'fimpex.dat' file in the local SX database and replaces the File Group associations for the existing hashes.

Chapter 14: Inspecting your endpoints and authorizing software

The 'Discover' procedure

When first installing Sanctuary Application Control Suite (Sanctuary Application Control Custom Edition, Sanctuary Application Control Terminal Services Edition, and Sanctuary Application Control Server Edition) the authorization lists are empty — you only have the ones corresponding to the operating system imported using the Import Wizard or during the SecureWave Application Server installation process. Your first job is to 'discover' and assign the existing files to File Groups and then to different users and user groups. This procedure is carried out in three phases:

1. Inspect the hard disk(s), installation CD/DVD, or specific directories recognizing executables and files forming part of an application.
2. Assign the files found in step 1 to File Groups.
3. Assign the File Groups to users/groups.

There are several forms of doing this exploring procedure as stated further down in this chapter.

 You can find the latest OS and common application Standard File Definitions on our Web site.

Once the files are detected, there are different ways of 'pushing' the Sanctuary permissions to all your client machines. We propose two different forms of doing this job in this document, as described in the next sections.

When you have many users in your organization, it pays to do first some planning. It is a better idea to assign users beforehand to user groups grouped by application. This simplifies the assignation process by assigning File Groups to groups of users instead of assigning them to each individual user.

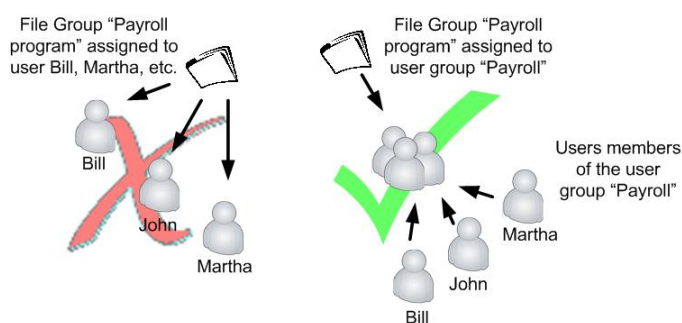


Figure 102: Assign File Groups to user groups instead to individual users

Although there are different ways of finding and authorizing applications, we propose two general ones:

1. A granular, precise, control approach where each application is linked to one corresponding File Group, which in turn is assigned to the required user(s)/group(s).
2. A global, pragmatic protection, schema where you do not care much about control granularity. The objective of this method is a quick control of all your installed applications. You create very few File Groups — one in extreme cases — and then assign them to the required user(s)/group(s).



If you select one or the other method, this does not mean that you cannot change your mind afterwards and switch from one to the other at your convenience. For example, you can begin with a global approach and then, when the program introduction is over, you know your way around, and feel more confident, change to a more granular control.

No matter which method you use, we divide each process in two general parts:

- > Discover and assign present applications.
- > Discover and assign future applications and installations.

In the first of them, we deal with all the programs already installed on your network machines that need to be processed, assigned to File Groups, and related to users/user groups.

The second relates to all the future installations and to those programs that constantly change due to updates or patches (for example, the operating system and antivirus programs). As they form a special case, Sanctuary has dedicated tools to deal with them.

The following diagram resumes these different strategies:

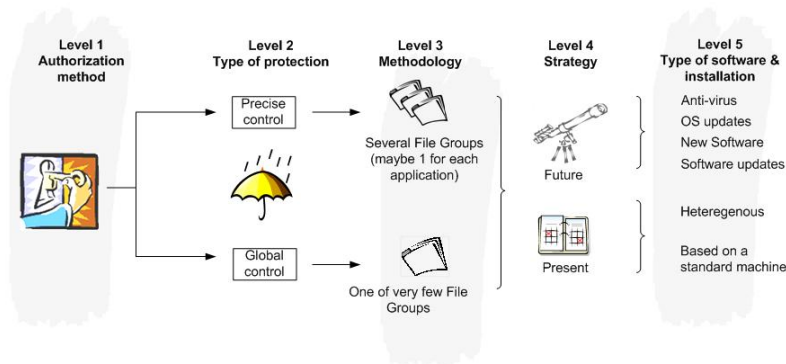


Figure 103: Authorization strategies

Exact match: 'High-control foundation'

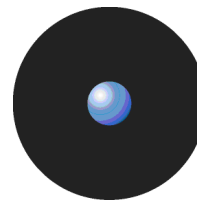
The Exact match: 'High-control foundation' procedure guarantees, basically, that all feasible software installed in your network is assigned to a precise and, in the best-case, different File Group. This allows a fine-tuning installation where every application is recognized as an entity. With several thousand possible files on a computer, this could include a large amount of resulting components. The price to pay for this accuracy is a higher initialization time defining the File Groups and assigning them to your users/user groups.

Procedure

We divide this procedure in two stages:

1. Authorizing your present installation.
2. Maintaining the work done in the previous step. This includes future operating system updates and patches, software updates, daily changing programs (for example antivirus), and new program installations.

We analyze each step in the following sections.



Authorizing your present installation

The first step when ‘discovering’ your installed applications consists on deciding whether you are working on a homogeneous environment where all machines have similar, consistent, applications, or a widely heterogeneous one.

If working in a homogeneous environment you can always use a ‘typical’ installation machine with all the normally used software available at the company. The best way to identify, classify, and finally authorize the software is to:

1. Install a ‘typical’, clean, machine with the operating system used by the most part of your clients and all user applications installed. If you did not import the corresponding OS SFD files when first installing your Sanctuary Application Control Suite, you can do it now from the *Tools* → *Import Standard File Definitions* command. This process creates all necessary File Groups that you can later assign to your users and automatically suggests the right *File Group* for all your OS files.



When importing the SFD files, you should consider using the ‘Import SFD without the hashes and create predefined File Groups’ (see Figure 104) since the processed files might not correspond exactly to the signature of those installed in other machines.

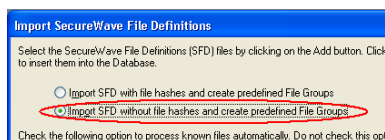


Figure 104: Importing Standard File Definitions files without hashes

2. Define a complete scan for this machine (a simple ‘*Scan all the disk*’ template scan is enough here), create new *File Groups* (use a meaningful name) corresponding to all applications (based upon file location) and proceed to assign new files to these *File Groups* and then to your users/user groups.

Once the process ends — or as you go along — you can assign the *File Groups* to their respective user groups or, if necessary, single users — using the *User Explorer* module.

This method has the clear advantage of uniquely identifying which files belong to which software. You have a great level of granularity. If you do an update, you only scan those files that are different and assign the resulting ones to the previously created *File Group* for that software.



Do not authorize directly from the Log Explorer module. If necessary, use the source CD/File Server for this.

Pros and cons

Pros

- > High precision.
- > Each individual feasible file, including DLLs, is assigned precisely.
- > Works well as a basic protection against unknown malware and unauthorized applications.
- > Creates differentiation among diverse authorized applications and user groups.
- > When updating software, you only explore the differences and directly assign them to your previously created File Group.

Cons

- > The initial setup time to complete the process depends on how many different application you use on your organization.



Pragmatically: 'Average foundation'

If the previous method of control is too cumbersome for your company, you can opt for a more practical 'one fits all' approach. When using this procedure, it cannot be guaranteed that each individual file among thousands possible available can be matched with its correct application. However, the advantage of this method is, as opposite to the previous one, its reduced setup time.

Procedure

As with the 'High-control foundation' method, we divide this procedure in two stages:

1. Authorizing your present installation
2. Maintaining the work done in the previous step. This includes future operating system updates and patches, software updates, daily changing programs (for example antivirus), and new program installations

We analyze each step in the following sections.

Authorizing your present installation

The first step when 'discovering' your installed applications consists on deciding if you are working on a homogeneous environment where all machines have similar, consistent applications, or a widely heterogeneous one.

If working in a homogeneous environment you can always use a 'typical' installation machine with all the normally used software available at the company. The best way to identify, classify, and finally authorize the software is to:

1. Install a 'typical', clean, machine with the operating system used by the most part of your clients and all user applications installed. If you did not import the corresponding OS SFD files when first installing your Sanctuary Application Control Suite, you can do it now from the *Tools* → *Import Standard File Definitions* command. This process creates all necessary File Groups that you can later assign to your users and automatically suggests the right *File Group* for all your OS files.



When importing the SFD files, you should consider using the 'Import SFD without the hashes and create predefined File Groups' (see Figure 104) since the processed files might not correspond exactly to the signature of those installed in other machines.

2. Define a complete scan for this machine (a simple 'Scan all the disk' template scan is enough here), create a single — or as few as possible — new *File Group* (use a meaningful name). You can use this *File Group* for all your non-authorized files.
3. Proceed to assign all non-authorized files (selecting them all) to this *File Group* and then to your users/user groups — using the *User Explorer* module.

This method has the clear advantage of an almost negligible setup time. You do not have a great level of granularity. If you do an update, you only scan the files that are different and assign the resulting ones to the previously created, general, *File Group*.

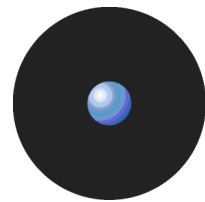


Do not authorize directly from the Log Explorer module. If necessary, use the source CD/File Server for this.

Pros and cons

Pros

- > The fastest assigning method you can use. The initial setup time to complete the process does not depend on how many applications you use on your organization.
- > You have a basic protection against unknown malware and unauthorized applications.
- > When updating software, you only explore the differences and directly assign them to one, general, *File Group*.



Cons

- > No possibly differentiation between authorized applications.
- > Each user uses the same File Group assignment.
- > Users can run all applications even if they do not require some of them (a secretary may have a CAD program authorization installed in her computer).
- > Does not have differentiation among diverse authorized applications and user groups.

Maintenance phase

There are often OS patches, SP, and updates; new software installations; frequently changing programs, etc. to authorize. As these are common tasks in a network — even in an isolated machine — SecureWave provides different tools to address each situation individually as explained in the following sub-sections.

Frequently changing programs

Some engines must be updated almost daily, as it is the case of antivirus, antispam, or antispymware programs, while other receive periodic upgrades or updates.

If these engines are automatically updated on your machines, you trust the source of the files, and have confidence on these update mechanisms; the general rule to follow is to define a *Path Rule* instead of individually authorizing program's files using *File Groups*. You can combine *Path Rules* with *Trusted Ownership* verification to complete the schema. Please consult the Administrator's Guide for more information. With a precise Path Rule and Trusted Ownership you can be sure that only the updated programs can modify the engine.

Operating system updates and patches

Operating systems, as with the programs explained in the previous subsection, are also a special case subject to continual updates and upgrades. Microsoft provides Windows Server Update Services (WSUS) as a tool to download, approve, and manage the distribution of Windows Operating System and Corporate Software updates and releases to all computers in your network. You can use *Authorization Service Tool* to monitor and authorize these changes and create updates (using Microsoft's SUS or WSUS) providing a 'zero' administration effort. Please consult the Administrator's Guide for more information.

New software installations

All kind of networks are subject, more or less, to periodic new software installations. These installations can be started from three general locations:

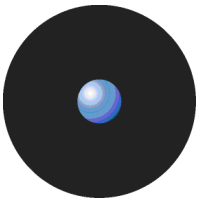
- > From a centralized file server repository.
- > Directly on the PC by means of a CD/DVD.
- > Using Microsoft Systems Management Server (SMS) packages.

No matter the stock method, you can always use the Authorization Wizard to find and authorize the new program files. As an alternative, you can use a scan and log analysis on the lab computer where you test your deployments.

Software updates

Software updates fall into one of the previously described categories. They can modify only a few files in the computer or be a radically new program by itself.

Depending on the type of update and from where you are going to install the software, you can use one of the methods described in the previous subsections (using the *Scan Explorer* module, the *Log Explorer* module, or the Authorization Wizard).



Changing from a test to a production environment

Once all machines scanned and authorized is time to change some options to go from a testing environment — where you get to know the program, scan the machines, create File Groups and assign them, and authorize all your programs — to a production one — where you take control over what is used or not.

To help you ease this change, follow these steps:

1. In order to install and authorize programs you must first change the *Blocking mode* to *Non-blocking* (*Tools* → *Default Options* of the management console). You should change it back to *Blocking mode* when this task is finished.
2. You should also change the *Log Mode* option to *Logging Disable* (same dialog as for the previous step) so that you do not saturate your database server with a log of everything that the users run.
3. Change the *Log Mode* option to *Log Everything* or *Log access denied* for a few machines and watch carefully their logs to be sure that everything is working properly as specified in the next step.
4. Monitor the machines chosen in step 3 looking for boot files, user's applications, and antivirus updates. If they are marked as *<not authorized>* in the *Log Explorer* module you should proceed to approve them but ONLY from the original source.
5. When all log activity comes back to 'normal' and all necessary files have been authorized, change back to *Logging Disable* and *Blocking mode*.



It is important that you authorize all software before deploying it.

Identifying DLL dependencies

What are DLLs?

Dynamic Link Libraries or DLLs, are a set of prefabricated components that other programs can use to carry out common tasks needed for their inner workings. They provide diverse functionalities related to such unconnected jobs as creating a window in a certain position, to returning cryptographically information, or simple database operations. They were designed to help programmers in their every-day programming job and to have a common body of useful routines that can be updated by a single source (mainly Microsoft) and used by different vendors.

In essence, DLLs are also executable programs, but cannot be run independently. They form a 'programmer's toolkits' that can be used by other running programs — including other DLLs. Rather than re-inventing the wheel, a programmer uses a DLL containing optimized code for the task at hand.

They can be classified as:

- > Shared or common — used by many programs.
- > Proprietary — used by one specific program or software publisher.

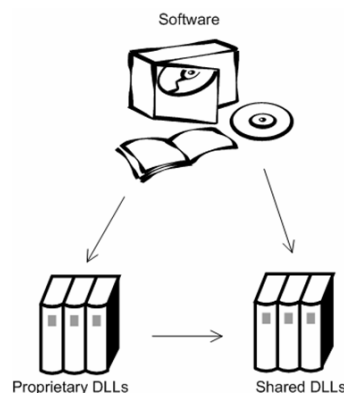


Figure 105: DLL relations



What are dependencies?

A dependency is the degree to which each program module depends on other to do its work. When one program depends of another, both of them should be installed and authorized in order to work together. The first step on doing this is to identify such dependencies.

Applications can load DLL in several different ways:

- > *Implicitly loaded* — The DLLs that are listed in a program's EXE Import Table. This table is consulted before loading the program to resolve DLL references.
- > *Dynamically loaded* — DLLs loaded explicitly by the application at run time.
- > DLLs loaded as dependencies of other: DLLs that use others DLLs.

How are DLLs dependencies identified?

With the earliest versions of Windows, Microsoft designated a specific directory for the storage place of common DLLs. Proprietary DLLs were supposed to be installed in the program's own folder. The release of a new and improved version of a DLL was intended to replace obsolete ones assuring backward compatible. There is normally only one copy of a shared DLL on the system available to all applications that need it.

Windows operating system allows only one copy of a specific DLL to be in memory at any one time. It remains there until no longer needed. The problem arises when different programs need different versions of DLLs with dissimilar functionalities located in different directories. You must guarantee that the newest version is always available and that it is authorized.

You can trace DLL dependencies using a variety of tools although some of them might not give you all the required information or provide the needed functionality. In the case of 16-bit applications, the enumerating process is more involved. The first of them is 'Depends.exe' that you can find included on the Visual C++ CD or on Dependency Walker's web site. It lists the DLLs that an application or another DLL needs. While this tool does a good job identifying some kind of DLLs, they are useless with COM objects or when dynamically loading certain DLLs.

One way to identify dynamically loaded DLLs is by using the free software found on SysInternals Web site. Other freeware and shareware tools can suit your needs.

How to integrate dependencies with Sanctuary

Once these dependencies identified, you can proceed to associate the application to the related files. As explained in the first section of this chapter, these files can be proprietary —easy to identify and classify — or shared — more difficult to categorize since they also belong to other programs and may already be authorized. The best way to 'discover' these files, is to install the software in a test machine with all existing files previously identified and assigned to their respective File Groups or, at least, to a general one. When exploring anew the machine, all the 'unknown' files are, obviously, the new installed ones. They do not show common relations.

Once more, if you are using a third party software, as explained in *How are DLLs dependencies identified?* on page 139, you can uniquely identify and assign all required files to the corresponding application File Group.

Glossary

ACL

Access Control List. A list that keeps the permissions that each user or group has to a specific system object. Each object has a unique security attribute that identifies which users have access to it.

ADSI

Active Directory Service Interface. Previously known as OLE Directory Services, ADSI makes it easy to create directory management applications using high-level tools such as Basic, Java, or C/C++ without having to worry about the underlying differences between the dissimilar namespaces.

AES

Advanced Encryption Standard. A symmetric key encryption technique that is replacing the commonly used DES standard. It is the result of a worldwide call for submissions of encryption algorithms issued by NIST in 1997 and completed in 2000.

CAB

File extension for **cabinet** files, which are multiple files compressed into one and extractable with the extract.exe utility. Such files are frequently found on Microsoft software distribution disks.

Client Computer

The computers on your network that has the Sanctuary Client Driver installed.

CSV

Comma Separated Value. A file format that allows easy data table retrieval into a variety of applications. It is often used to exchange data between disparate applications. The file format has become a pseudo standard throughout the industry, even among non-Microsoft platforms. Common examples of applications that use this format are spreadsheets and databases. You can also see and edit these files using an ASCII text editor (Notepad, Word, WordPad, Excel, etc.).

DCOM

Distributed Component Object Model. A set of Microsoft concepts and interfaces built into Windows operating system in which client program objects can request services from server program objects on other computers in a network. The first versions of DCOM were exploited to introduce worms and Trojans into networks. Windows XP SP2 and Windows Server 2003 SP1 and later include many changes that enhanced security. Although these resolved problems present in earlier versions of Windows, they also changed some DCOM properties that must be fine-tuned.

Delegation

The act of assign responsibilities for management and administration of a portion of the resources or items used in a shared computing environment to another user, group, or organization.

Dependencies

Additional executable files (.exe, .dll, or others) required by executable files to run properly.

Dependencies are split into two categories: *static dependencies*, which are files, declared explicitly in the executable file as being required, and *dynamic dependencies*, which are additional files an executable may require at runtime.

**DN**

Distinguish Name. A name that uniquely identifies an object in the Directory Information Tree.

Executable Program

A computer program that is ready to run. The term usually applies to a compiled program translated into computer code in a format that can be loaded in memory and executed by a computer's processor.

Exploit

A piece of software that takes advantage of a bug, glitch or vulnerability, leading to privilege escalation (exploit a bug) or denial of service (loss of user's services) on a computer system.

File Group

Organizational groups used to cluster authorized executable, script and macro files. Files must be assigned to 'File Groups' before users can be granted permission to use them. You can choose to assign files to 'File Groups' from various modules throughout the Sanctuary Application Control Suite, e.g. by double-clicking on a file in the *Database Explorer*, *Exe Explorer*, *Log Explorer* or *Scan Explorer* module.

GUID

Global Unique Identifier. This number is generated when the NDS object is created. It is simply an object's NDS attribute. In order to ensure data consistency, Novell eDirectory implements a globally unique ID (GUID) for all objects within the directory. The total number of unique keys (2128 or 3.4028 x 1038) is so large that the possibility of using the same number twice is nearly zero.

Hash

A complex digital signature calculated by Sanctuary Application Control Suite to uniquely identify each executable, script and macro file that can be run. The hash is calculated using the SHA-1 algorithm that takes into account the entire contents of the file.

iFolder

A Novell client that runs on Windows-based computers. It allows a user to work on his files anywhere —online or offline. iFolder integrates encryption and file synchronization services.

MAPI

Messaging Application Programming Interface enables Windows applications to access a variety of messaging systems.

MDAC

Microsoft Data Access Components. Required by Windows computers to connect to SQL Server or MSDE databases.

MSDE

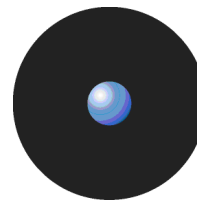
Microsoft Data Engine (also known as Microsoft SQL Server Desktop Engine), is a SQL Server compatible database server, suitable for small and medium size organizations. MSDE databases can subsequently be migrated to SQL Server 2000/2005. SQL Server 2005 Express Edition now supersedes MSDE.

NDAP

Novell Directory Access Protocol. The NDAP component gives Windows applications full access to the Novell eDirectory and administration capabilities for NetWare servers, and volumes.

NDS

Novell's eDirectory previously called *Novell Directory Services*. eDirectory is a hierarchical, object oriented database that represents all the assets in an organization in a logical tree. Assets can include users, positions, servers, workstations, applications, printers, services, groups, etc.



NICI

Novell International Cryptographic Infrastructure. NICI is a base set of cryptographic services available for Novell. NICI provides an API set that offers a consistent interface for application developers to use and deploy cryptography within their applications.

OU

Organizational Units. A part of the Active Directory (AD) structure inherited from Novell's NDS structure. Within Novell's NDS/eDirectory there are three classes of objects in the NDS database: Roots, Containers, and Leafs. There are three supported types of container objects: Country (C=), Organizations (O=), and Organizational Units (OU=).

Private Key

One of two keys used in public key encryption. The sender uses the private key to create a unique electronic number that can be read by anyone possessing the corresponding public key. This verifies that the message is truly from the sender.

Public Key

One of two keys in public key encryption. The user releases this key to the public, who can use it for encrypting messages to be sent to the user and for decrypting the user's digital signature.

RPC

A **Remote Procedure Call** is a protocol that allows a computer program running on one host to run a subroutine on another host. RPC is used to implement the client-server model of distributed computing.

RSA Encryption

In 1977, Ron Rivest, Adi Shamir, and Len Adleman developed the public key encryption scheme that is now known as RSA, after their initials. The method uses modular exponentiation, which can be performed efficiently by a computer, even when the module and exponent are hundreds of digits long.

SFD

SecureWave provides a number of pre-computed file hashes for most versions of suites and Windows Operating Systems, in several languages, and for all the available Service Packs. The file hashes are referred to as *Standard File Definitions* or SFD. They are installed during the setup, but you can import them as soon as SecureWave releases new ones. You can find the latest ones on our Web site.

SHA-1

Secure Hash Algorithm 1, as defined in the Federal Information Processing Standards Publication 180-1. This algorithm produces a one-way 160-bit hash that can be used for a variety of applications including authentication and cryptography.

SID

Security identifier, a security feature of Windows NT and 2000 operating systems. The SID is a unique name (alphanumeric character string) used to identify an object, such as a user or a group of users in a network.

Windows grants or denies access and privileges to resources based on an ACL (**Access Control List**), which uses a SID to uniquely identify users and their group memberships. When a user requests access to a resource, the user's SID is verified by the ACL to determine if the user, or the group he belongs to, is allowed to perform that action.

SQL

Structured, Query Language, a language used to construct database queries.

SUS

Software Update Services is a tool provided by Microsoft to assist Windows administrators with the distribution of security fixes and critical update releases.

**SecureWave Application Server**

The main component of all Sanctuary's products. Beside calculating hashes, authorizing applications and devices, it serves as a bridge between the database and the client.

TCP/IP

Transmission Control Protocol/Internet Protocol. The protocol used by the client computers to communicate with the SecureWave Application Servers.

VBScript

A scripting language created by Microsoft embedded in many applications used in Windows. Although it allows for powerful interoperability and functionality, it also creates a great deal of security risks unless it is tightly controlled.

Vulnerability

A weakness or other kind of opening in a system, usually caused by a bug or other design flaw.

Well-Known Security Identifiers

A security identifier (SID) is a unique value used to identify a security principal or security group. The values of certain SIDs remain constant across all installations of Windows systems and for this reason are termed well-known SIDs. Everybody, Local, Guest, Domain Guest, etc. are some examples of SIDs.

WMI

Windows Management Instrumentation. WMI is a standard technology to access management information in an enterprise environment. WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components. You can use WMI to automate administrative tasks in an enterprise environment. WMI improves administrative control by allowing administrators to correlate data and events from multiple sources and vendors on a local or enterprise basis. It is used as a complement to ADSI.

WSUS

Windows Server Update Services (previously SUS v2.0) is a new version of Software Update Services (SUS).

Index of Figures

Figure 1. Connecting to the SecureWave Application Server	14
Figure 2. Connection and Output window	15
Figure 3. The main screen	15
Figure 4. License status warning	16
Figure 5. Docked Control panel	16
Figure 6. Docked window.....	16
Figure 7. Floating Control panel.....	16
Figure 8. Floating windows	17
Figure 9. Minimized windows	17
Figure 10. Endpoint Maintenance	20
Figure 11: Local authorization dialog	26
Figure 12. Spread Check dialog.....	27
Figure 13. User Access Manager dialog	29
Figure 14: Importing a permission file	34
Figure 15. Import Standard File Definitions	35
Figure 16. Default options dialog - Exe Explorer options	37
Figure 17. Exe Explorer Module Window	38
Figure 18. Scan Explorer module main window	39
Figure 19. Create New Template dialog.....	40
Figure 20. New Rule dialog.....	40
Figure 21. Perform New Scan dialog - template.....	41
Figure 22. Perform New Scan dialog - comment.....	41
Figure 23. Scan Explorer window after a scan	41
Figure 24. Select Two Scans to Compare.....	42
Figure 25. Authorization Wizard.....	43
Figure 26. Authorization Wizard: Selecting the Source Directory	44
Figure 27. Authorization Wizard: Statistics.....	44
Figure 28. Authorization Wizard: Processing the Files	45
Figure 29. Authorization Wizard: Assigning Files to File Groups	45
Figure 30. File Group Management	47
Figure 31. File Group parent relationship.....	49
Figure 32. File Group child relationship.....	49
Figure 33. File Group parent-child relationship.....	49
Figure 34. File Group indirect assignment.....	49
Figure 35: Assign Files to File Groups dialog.....	50
Figure 36. Assigning a File Group using the Exe Explorer module.....	51
Figure 37. Database Explorer module.....	52
Figure 38. Path Rules dialog.....	55
Figure 39. Editing the Path Rules	56

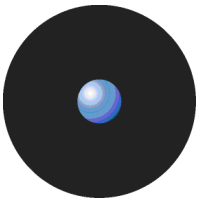


Figure 40. Adding a Path Rule	56
Figure 41. Setting Trusted Owners.....	58
Figure 42. Setting Path Rules with Ownership Checking.....	59
Figure 43. A user having several File Groups indirectly authorized	62
Figure 44. User's tree.....	63
Figure 45. User Explorer Module Window: File Groups by User	64
Figure 46. User Explorer Module Window: Users by File Groups	65
Figure 47: Log Explorer main window	68
Figure 48: Select and edit templates window	69
Figure 49: Templates settings window	70
Figure 50: Components of the Log Explorer window	71
Figure 51: Navigation/Control bar.....	71
Figure 52: Column headers showing multiple classifications	72
Figure 53: Columns context menu.....	73
Figure 54: Group By option	73
Figure 55: Column headers showing grouped results.....	73
Figure 56: Column headers showing sub groups.....	73
Figure 57: Computed columns	74
Figure 58: Column headers showing a computed and a sorted column.....	74
Figure 59: Resetting column headers.....	75
Figure 60: Props tab	78
Figure 61: Criteria tab	78
Figure 62: Control button bar	78
Figure 63: Select and edit templates window	78
Figure 64: Filter templates dialog	79
Figure 65: Templates context menu	80
Figure 66: Template settings window – Simple Query tab	80
Figure 67. Grouping results in the query	81
Figure 68: Example of criteria settings	83
Figure 69: Query & Output tab	83
Figure 70: Schedule tab.....	85
Figure 71: Format tab.....	85
Figure 72: Delivery tab.....	86
Figure 73: Edit target dialog	86
Figure 74: Edit target dialog (E-mail).....	86
Figure 75. Fetching New Logs	87
Figure 76. Database Explorer Module.....	92
Figure 77. Selecting columns to display in the Database Explorer Module	92
Figure 78. Choose Columns dialog	92
Figure 79. Synchronizing Domains.....	93
Figure 80. Connecting as a different User	94
Figure 81. Database Maintenance	94
Figure 82. Purging the online computers table	95
Figure 83. To generate a report	97
Figure 84. File Groups by User report	98
Figure 85. Users by File Group report	99
Figure 86. User Options report.....	100
Figure 87. Machine Options report.....	101

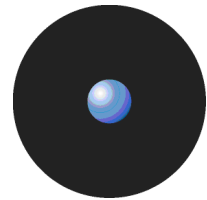


Figure 88. Online Machines report.....102

Figure 89: SecureWave Application Server Options report104

Figure 90. Default Options - Computer107

Figure 91. Default User/Group Options.....111

Figure 92. Options - for a specific computer.....114

Figure 93. Options - for a specific user114

Figure 94. Options - for a specific user group114

Figure 95. Computer Precedence Process116

Figure 96. Users/Groups Precedence Process117

Figure 97. Computer *and* user/user group precedence process.....119

Figure 98. Execution blocking precedence process120

Figure 99. Flowchart to describe the Authorization Service Tool process.....124

Figure 100: Sanctuary's initial scan.....125

Figure 101: FileTool's File Group assignments129

Figure 102: Assign File Groups to user groups instead to individual users.....133

Figure 103: Authorization strategies.....134

Figure 104: Importing Standard File Definitions files without hashes.....135

Figure 105: DLL relations.....138

Index of Tables

Table 1. The System Modules	18
Table 2. The File Menu	18
Table 3. The View Menu	18
Table 4. The Tools Menu	19
Table 5. The Reports Menu	21
Table 6. The Explorer Menu	21
Table 7: The Window menu items.....	22
Table 8. The Help Menu	22
Table 9. Standard File Definitions	34
Table 10. File status when comparing two scans.	42
Table 11. File Group relationship status icons.....	48
Table 12. Resulting permissions when applying Path Rules	59
Table 13: Log Explorer module limitations if using other user/domain account.....	68
Table 14: Log Explorer module columns	76
Table 15. Custom Message Field Values.....	77
Table 16: Template Filter checkboxes	80
Table 17: How to use the available criteria dialogs.....	83
Table 18. Audit events	88
Table 19. Columns of the 'Online Machines' Report.....	102
Table 20: Option name comparison	105
Table 21: The precedence of option values	118
Table 22. Authorization Service Tool configuration parameters.....	126
Table 23: FileTool.exe command line parameters.....	127
Table 24. FileTool.exe File Block Report Options	130
Table 25: FileTool.exe command line parameters.....	131

Index

A

Access denied, 77
Access values, 77
ACL, 141
Active directory, 88
Active Directory Service Interface, 141
Administrator, 29, 88
ADSI, 141
Advanced Encryption Standard, 141
Advanced queries, 83
AES, 141
Anti-virus, 9
Applications
 Allow, 10
Access permissions, 61
Audit events, 76, 88
 Added media, 88
 Change device group, 88
 Deleted default option, 88
 Deleted option, 88
 Modify user access role, 88
 Purged DB and file storage, 88
 Removed media, 88
 Set default option, 88
 Set option, 88
Audit logs, 75
Authorization Service tool, 123
 Configuration, 125
Authorization strategies, 23
Authorization Wizard, 42
 Add executables to the database, 43
Authorized, 77
AuthSrv.exe, 123

B

BITS, 123
Black list, 9
Block user, 77
Building a list of executables, 33

C

CAB, 141
Calculated values, 74
Central authorization, 24
 By file location, 25
Change file assignments, 51
Choose columns, 38
CIM, 144
Client computer, 106, 108, 141
Client Hardening, 19

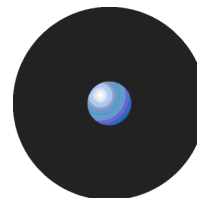
Client ticket, 19
 Create, 20
 Rules, 20
Column headers, 72
Common Information Model, 144
Compare two templates' scans, 41
Computed columns, 74
Contact details, 7
Conventions, 6
Create template, 39
Criteria, 78, 82
Criteria dialog, 82
CSV, 141
ctrlacx.vbs, 88
Custom reports, 69, 83

D

Database, 63, 93
 Backup, 94
 Delete file, 52
 maintenance, 94
Database Explorer, 91
Default options
 Groups, 111
 Protected servers, 107
 Users, 111
Delegation, 141
Delete
 Old logs, 94
Denied, 77
Dependencies, 139, 141
Device control status window, 105
Discover
 Exact match, 134
 Procedure, 133
DLL, 138
 Definition, 138
 Dependencies, 138
 Dependencies definition, 139
 Identifying dependencies, 139
DN, 142
Domain, 62, 63
 Administrators, 62
Don'tCare, 77

E

Endpoint Maintenance, 19, 107
Enterprise administrator, 29
Exe Explorer, 36
Executable
 Files, 9, 63, 141
 Program, 142



- Viruses, 9
- Exploit, 142
- Explorer menu, 21

F

- File Groups, 10, 18, 62, 142
 - Assign executables, 50
 - Assign to users, 64
 - Change file assignment, 51
 - Create, 47
 - Delete, 48
 - Remove file, 52
 - Rename, 48
- File Import/Export tool, 130
- File menu, 18
- FileTool.exe, 127
 - Archive files, 128
 - Command line parameters, 127
 - Delta mode, 128
 - File block, 128
 - Report options, 128
 - Retry logic, 128
 - Usage examples, 130
 - Versatile File Processor tool, 127
- Fimpex.exe, 130
 - Command line parameters, 130
 - Examples, 131
 - Usage notes, 131
- Format custom reports, 85

G

- Global Users, 62
- Grouping log entries, 73
- GUID, 142

H

- Hash, 24, 77, 142
- Help menu, 22

I

- Identify executable files, 39
- iFolder, 142
- Indirectly authorized through Domain Groups, 61
- Informing client computers, 121
- Internal structure, 9

L

- Local authorization, 25, 77
 - Allow, 25
 - Delete list, 27
- Local users, 63
- LocalSystem, 63
- Log entries, 78
- Log entry fields, 75
- Log Explorer, 68, 71
 - Authorize unknown files, 87
 - Force latest log, 87
 - Interpreting, 77
- Logon, 77

M

- MAPI, 142
- MDAC, 142
- Microsoft Data Access Components, 142
- Microsoft Software Update Services, 123
- Monitor system activity, 67
- MSDE, 142

N

- Navigation/Control bar, 71
- NDAP, 142
- NDS, 142
- NICI, 143
- Non blocking option*, 77

O

- Options
 - Changes, 105
 - Client hardening, 107
 - Device control status window*, 105
 - eDirectory translation, 108
 - Execution blocking, 108, 111
 - Execution eventlog, 109, 112
 - Execution log, 109, 112
 - Execution notification, 109, 112
 - For specific machines, 114
 - Local authorization, 109
 - Log upload delay, 110
 - Log upload interval, 110
 - Log upload threshold, 110
 - Log upload time, 110
 - Macro and script protection, 112
 - Relaxed logon, 113
 - Relaxed logon time, 113
 - Sanctuary status, 108
 - Server address, 110
 - Settings, precedence, 115
- Organizing files, 47
- OU, 143
- Ownership Check, 55

P

- Path rule, 77
 - Create, 55
 - Delete, 57
 - Delete all, 57
 - For a specific user or use group, 56
 - Modify, 57
 - Pathname conventions, 57
 - Precedence, 59
- Private key, 143
- Public key, 143

Q

- Queries
 - Complex, 83
 - Simple, 81

R

- Recursive, 55
- Remove



- Old scans, 94
- Reports, 69, 97
 - File groups by user, 98
 - Machine options, 101
 - Menu, 21, 103
 - Online machines, 102
 - Server Settings, 103
 - User options, 100
 - Users by file group, 99
- Root specifier, 57
- RPC, 143
- RSA
 - Definition, 143
- S**
- Salt, 19
- SAM, 14
- Sanctuary Management Console
 - Connection window, 15
 - Control panel, 15
 - Main page panel, 15
 - Menu, 15
 - Modules, 18
 - Output window, 16
 - Status bar, 16
- Sanctuary Management Console, 13, 14, 15
- Sanctuary status, 108
- Scan
 - A computer, 39
 - Automatic, 39
 - Pragmatic approach, 136
- Scan Explorer, 39
- Scheduled custom reports, 85
- Search
 - Executable files 16 bit, 37
- SecureWave Application Server, 14, 18, 144
- SecureWave Sanctuary Database, 91
- Sending updates, 28
 - Send updates to a specific computer, 106
 - Send updates to all computers, 106
- Server administrators, 29
- SFD, 143
 - Automatically imported, 35
 - Manually imported, 35
- SHA-1, 142, 143
- Show/hide columns, 73
- SID, 76, 143
- Software Unlicensed, 9
- Sorting results, 72
- Spread Check, 121
- SQL, 143
 - Server, 142
- Standard File Definitions, 143
- SUS, 123, 143
- SX Domain command-line tool, 93
- Synchronize
 - Domain, 19
 - Domain members, 93
- System
 - Options, 105
- System Administrator
 - Full management privileges, 29
 - Restricted access privileges, 30
- T**
- Target, 76
- TCP/IP, 144
- Technical support, 7
- Templates, 69, 83
 - Adding, 69
 - Columns, 75
 - Filtering, 79
 - Queries, 81
 - Select and edit templates, 78
 - Settings, 80
 - Using, 69
- TLS, 12
- Tools
 - Menu, 19, 63
- Traced, 76
- Trojans, 9
- Trusted owners, 58
- Typefaces, 6
- U**
- Unlicensed software, 9
- User Explorer, 62, 64
- User groups, 61
 - define, 61
- Users, 9, 61, 63, 93
- V**
- VBScript, 144
- View
 - File assignments, 52
 - Menu, 18
- Viruses, 9
- Vulnerability, 144
- W**
- Well-known
 - Groups, 62
 - Security Identifiers, 144
- White list, 9
- Window menu, 22
- Windows
 - Management Instrumentation, 144
 - Server Update Services, 123
- WMI, 144
- Workstation, 62
- Worms, 9
- WSUS, 123, 144