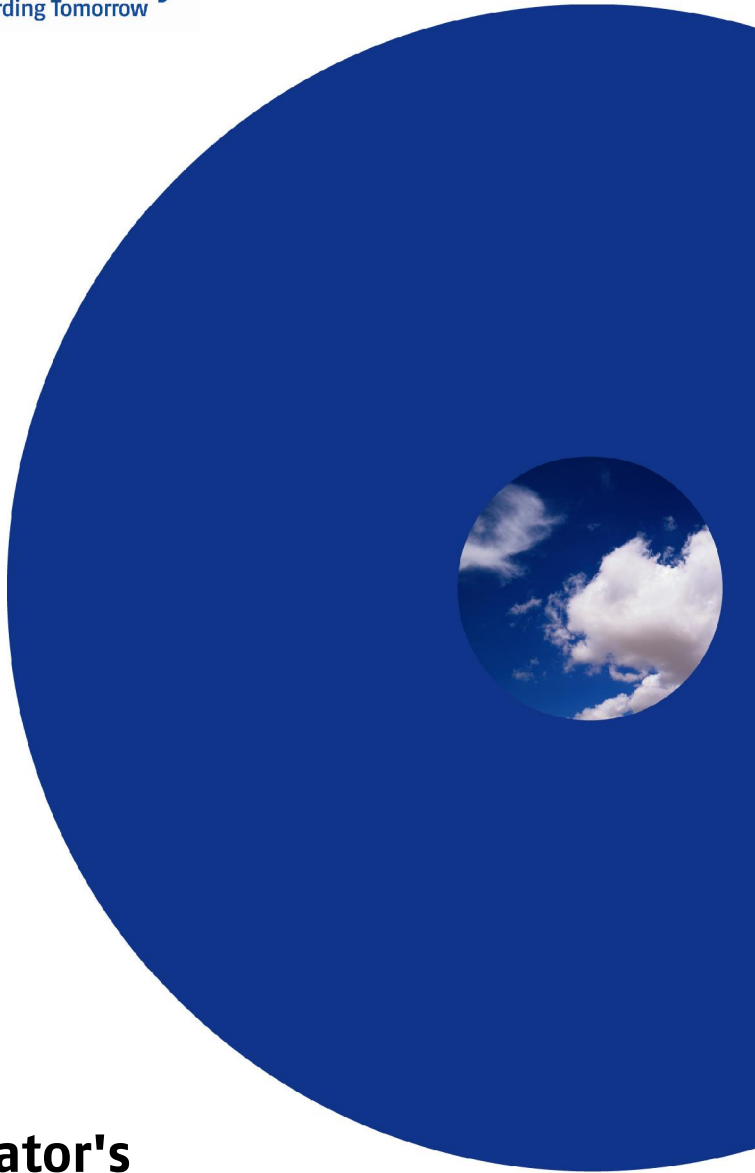




SecureWave
Sanctuary[®]
Safeguarding Tomorrow



Administrator's Guide

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SecureWave claims copyright in this program and documentation as an unpublished work, revisions of which were first licensed on the date indicated in the foregoing notice.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 2000–2006© SecureWave S.A.
All rights reserved.

Trademarks

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

SecureWave
Atrium Business Park
23-ZA Bourmicht
L-8070 Bertrange
Luxembourg

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

You can contact our technical support team by calling:

+352 265 364 300 (International),
1-877-713-8600 (US Toll Free),
0-800-012-1869 (UK Toll Free)

or by sending an email to support@securewave.com

Published on: October 2006

Sanctuary Application Control Suite Administrator's Guide v4.0.0



Contents

Introducing Sanctuary Application Control Suite	7
A complete portfolio of security solutions	7
About this Guide	8
Conventions used in this guide	9
Typographical conventions	9
Symbol conventions	9
Keyboard conventions	10
For more information	10
To contact us	11
For people who do not read user manuals.....	12
Chapter 1: Understanding the program advantages and internal structure	13
Welcome to Sanctuary.....	13
Benefits of the 'white list' approach	14
How does the system know which applications to allow?.....	14
What do you gain using Sanctuary?.....	15
Overview of system architecture and connectivity.....	18
The SecureWave Sanctuary Database	19
The SecureWave Application Server	19
The Sanctuary Client.....	19
The Sanctuary Management Console.....	20
Administration Tools	21
How does the Sanctuary solution work	21
Before you activate the Sanctuary solution	21
When a computer signs on to the network	22
When a machine asks to run an application	22
If the application is on the approved list.....	22
If application access is denied	22
If a computer is taken off the network	23
Chapter 2: Working with Sanctuary	25
New features & differences from previous version	25
Working with the Sanctuary system.....	26
Starting up the Sanctuary Management Console.....	27
To start up the management console of your Sanctuary application.....	27
To connect to the SecureWave Application Server	27
Log in as a different user.....	28
The Sanctuary Management Console.....	29
Controlling your workspace.....	30
Sanctuary modules, menus and tools	33
The File menu.....	33
The View menu	34
The Window menu	34
The Tools menu.....	34



- Endpoint Maintenance 36
- The Reports menu 38
- The Explorer menu 38
- The Help menu 39
- The six system modules 39
- Chapter 3: An overview of authorization strategies 41**
 - Central authorization by digital signature (hash) 42
 - Central authorization by file location (path) 43
 - Authorization for Windows scripts and macros 43
 - To centrally allow or deny authorization for *all* scripts and macros 44
 - To grant local users authority to allow or deny scripts and macros 44
 - Local authorization 45
 - If 'local authorization' is allowed 45
 - To prevent Users or User Groups from performing local authorization 46
 - To enable users to locally authorize applications not listed in the Sanctuary system 46
 - To prevent the malicious spread of locally authorized files 46
 - Sending updated authorization information to computers 47
 - To push updates to all computers protected by Sanctuary 47
 - To push updates to a designated computer 48
 - If you do not push updates to computers 48
- Chapter 4: Setting up a Sanctuary system administrator 49**
 - Overview -- Types of administrators 49
 - How to set up a Sanctuary system administrator 49
 - To define a system administrator with full management privileges 50
 - To define a system administrator with restricted access privileges 51
 - To define access privileges to specific functions and modules 51
- Chapter 5: Building a list of executable files to be managed 53**
 - Export file permissions 54
 - Importing standard file definitions from SecureWave 55
 - If you chose the automatic import option during installation 56
 - If you did not import standard file definitions during installation 56
 - Selecting executable files from network directories 59
 - Using the EXE Explorer module (no client driver required) 59
 - Automatically scanning a computer to identify executable files 59
 - Using the Scan Explorer module (requires a client driver) 60
 - Using the Authorization Wizard 66
 - To add executables to the Sanctuary database using the Authorization Wizard 67
- Chapter 6: Organizing files into File Groups 71**
 - Creating and managing File Groups 71
 - To create a new File Group 71
 - To delete a File Group 72
 - To rename a File Group 73
 - To create a parent-child relationship between File Groups 73
 - Assigning executable files to File Groups 76
 - To assign files to File Groups 76
 - Changing file assignments 78



To change the File Group to which a file is assigned	78
To remove a file from a File Group	78
To delete a file from the Sanctuary database altogether	79
Viewing file assignments	79
To sort entries by any attribute, such as filename or File Group	80
To display just a subset of all files in the database	80
Using the Groups tab	80
Chapter 7: Authorizing software by location (Path Rules)	81
Creating, changing, and deleting Path Rules	81
To create a new Path Rule that applies to everybody	82
To create a new Path Rule that applies to a specific user or user group	83
To modify an existing Path Rule	84
To delete a single Path Rule for a user or user group	84
To delete all Path Rules for a user or user group	84
Conventions for specifying paths in the rules	85
Defining and working with Trusted Owners	86
To define or delete a Trusted Owner	86
Trusted Owner and Path Rule example	87
Path Rules precedence	88
Chapter 8: Assigning access permissions to users and groups; the User Explorer	89
Assigning File Groups to users/user groups	90
To assign/remove File Groups to/from users	90
Assigning users/user groups to File Groups	92
To assign/remove users to/from a File Group	92
Users and user groups	93
Direct, indirect, and not authorized File Groups	94
Chapter 9: Monitoring system activity; the Log Explorer	97
Monitoring logs of application activity on your protected clients	98
Basic operation	99
To use an already defined template:	99
Managing templates	100
The Log Explorer window in detail	101
Navigation/Control bar	102
Column Headers	103
Results window	108
Criteria/Properties panel	108
Control buttons panel	108
Sorting and applying criteria to specific fields	109
Available columns	110
Interpreting the Log Explorer data	111
Using the Log Explorer to authorize unknown files	112
Forcing an upload of the latest log files	112
Saving application execution logs to a CSV (comma-separated values) file	113



Chapter 10: Monitoring Sanctuary system administrator activities; the Audit Logs Viewer	115
To view system administrator activity	116
Search options	116
Actions	119
Generating reports of system status and settings.....	122
Chapter 11: Sanctuary's database; the Database Explorer	123
Viewing database records	123
To activate the Database Explorer module	124
Performing routine database maintenance	126
Synchronizing Sanctuary accounts with Microsoft accounts	126
Backing up the Sanctuary database.....	128
Removing old execution logs and machine scans	128
To delete all execution logs and scan results before a given date	128
Removing old audit logs of Sanctuary administrator activity	129
Audit log files	129
To remove old audit logs of Sanctuary administrator activity.....	130
Removing obsolete records of computer connections.....	131
Chapter 12: Generating reports of Sanctuary records and settings	133
File Groups by User.....	135
Users by File Group.....	136
User Options	137
Machine Options.....	138
Online Machines.....	139
Chapter 13: Setting system options; using the Exe Explorer.....	141
Changes from previous versions	142
Setting default options for the Exe Explorer module.....	142
To build a list of executable files from a computer directory	143
To search for specific executable files extensions.....	143
To have the system check every file to determine if it is an executable.....	144
Setting default options.....	146
To set an option	146
Setting default options for protected clients.....	146
Individual options	147
Setting default options for users and groups	151
To set default options for protected users and groups	151
Individual options	152
Setting options that apply to specific machines or users.....	156
Determining which option setting takes precedence	156
Computer options	156
User and group options.....	158
Computer, user, and group options.....	161
Informing client computers of changes	165
Chapter 14: Windows Updates	167
Sanctuary Authorization Service Tool	167



- What is the Microsoft Software Update Services (SUS)? 167
- What is the Windows Server Update Services (WSUS)? 167
- What is the Sanctuary Authorization Service tool?..... 167
- Installing the Authorization Service tool..... 170
- Sanctuary Authorization Service tool configuration 171
- Versatile File Processor tool 174
 - FileTool.exe command line parameters..... 175
 - Versatile File Processor tool usage notes..... 176
 - FileTool.exe usage examples 178
- Chapter 15: Best practices for Sanctuary security 179**
 - Sanctuary in an organization-wide strategy..... 179
 - Setting up your new Sanctuary solution 179
 - Routine system administration 180
 - Verifying new software 181
 - To verify the performance of new software on a client 181
 - Assigning File Groups to user groups instead of users 181
 - Tips for maximum security..... 182
 - Preventing Local Authorization 182
 - Preventing 'Relaxed logon' 183
- Chapter 16: Troubleshooting your Sanctuary solution 185**
- Glossary 189**
- Index of Figures..... 195**
- Index of Tables 199**
- Index 201**



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 will 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.

- > Sanctuary Standard Edition enables you to define a group of files that can be run on the organization's computers. Nothing else will run.
- > Our Sanctuary Application Control Suite, can be any of the following programs:
 1. Sanctuary Custom Edition lets you create multiple File Groups and User Groups, so you can control application execution at a more granular level.
 2. Sanctuary Terminal Services extends application control to Citrix or Microsoft Terminal Services environments, which share applications among multiple users.
 3. Sanctuary Server Edition delivers application control to protect the 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.

About this Guide

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

- > *Chapter 1: Understanding the program advantages and internal structure*, provides a high-level overview of the solution, how it works and benefits your organization.
- > *Chapter 2: Working with Sanctuary*, 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 a Sanctuary system administrator*, tells how to set up two types of system administrators—with full or limited privileges.
- > *Chapter 5: Building a list of executable files to be managed*, describes four ways to load definitions of allowable files 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 software by location (Path Rules)*, describes the process of using pathname rather than digital signature to define allowable files.
- > *Chapter 8: Assigning access permissions to users and groups*, describes two key ways to give users privileges to use executable files.
- > *Chapter 9: Monitoring system activity*, describes the logs of application-execution activity.
- > *Chapter 10: Monitoring Sanctuary system administrator activities*, explains how to verify the log of the system administrator activities.
- > *Chapter 11: Sanctuary's database*, describes the database in full as well as those routine housekeeping functions such as system cleanup and backup.
- > *Chapter 12: Generating reports of Sanctuary records and settings*, describes the HTML reports that can be easily created by the system.



- > *Chapter 13: Setting system options; using the Exe Explorer*, describes the various options that govern system operation at user, machine, group, or global levels.
- > *Chapter 14: Windows Updates*, explains how you can use Sanctuary with the technologies provided with Windows.
- > *Chapter 15: Best practices for Sanctuary security*, outlines recommended procedures for using Sanctuary in the context of a total security strategy.
- > *Chapter 16: Troubleshooting your Sanctuary solution*, provides straightforward answers to issues you may encounter while using the program.
- > The *Glossary* and indexes (*Index of Figures*, *Index of Tables*, and *Index*) provide quick access to specific terms or topics.

Conventions used in this guide




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: <http://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 USA.

You can contact our technical support team by calling:

+352 265 364 300 (International),
1-877-713-8600 (US Toll Free),
0-800-012-1869 (UK Toll Free)

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

Alternatively, you can write to customer support at:

SecureWave Support
Atrium Business Park
23-ZA Bourmicht
L-8070 Bertrange
Luxembourg



For people who do not read user manuals

If you are a busy person, you surely do not have the time to read user manuals completely. We do not blame you. You need your work done in the most efficient and quick way.

Although Sanctuary is a powerful tool, its inner workings are deceptively simple. The program can be up and running in almost no time. To help you get the most of it, we have prepared a brief first part introduction material. You can get the essential information by focusing on the following:

- > *Chapter 1: Understanding the program advantages and internal structure* and *Chapter 2: Working with Sanctuary* (pages 13 & 25). You find here:

- An overview of how the solution differs from anti-virus and intrusion-detection systems on the market

- A quick description of how the program works

- The internal workings and structure of the system

- A brief view, description, and functionality of Sanctuary main components

- An introduction to the menu's commands

- > *Chapter 15: Best practices for Sanctuary security* (page 179) is a must-read. This chapter summarizes the key processes that a well-informed system administrator will follow to get the most value from the Sanctuary solution. This chapter also touches on how the Sanctuary solution fits into best practices for an organization's overall security strategy.

The rest of the chapters are always there as a reference, when you are ready to use specific system functions. And, of course, online help is only a click away.

So, welcome to Sanctuary.



Chapter 1: Understanding the program advantages and internal structure

This chapter introduces the powerful new Sanctuary and explains how it benefits your organization. You will discover:

- > How this solution fundamentally differs from most anti-virus and intrusion-detection systems on the market today
- > How the Sanctuary approach 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 solution and what each contributes to the security strategy
- > What happens behind the scenes to make Sanctuary such a powerful, effective, yet easy-to-use solution
- > How to navigate through the different screens and options

Welcome to Sanctuary

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 your crucial servers or computers... rest easy. Now you have Sanctuary.

Sanctuary 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 will work, period. That means no matter how inventive and evolved some new malicious code might be, it simply will not run. You are protected.

Using Sanctuary 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 works exactly the opposite way as 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 that are allowed to run.

Benefits of the 'white list' approach

Most security and anti-virus products on the market operate on 'black lists' of files that are *not* allowed to run. In contrast, Sanctuary security operates on 'white lists' of files that *are* allowed to run. This innovative approach offers several significant benefits:

- > 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 will 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 will 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 of protection covering your organization's servers & computers.

How does the system know which applications to allow?

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

1. Build a list of executable files that you want to manage.

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

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



4. Organize those 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.

5. Link users with their allowed File Groups.

Having defined File Groups, Users, and User Groups, you can now specify not only which applications can be used, but by whom. Applications are centrally authorized once and then are immediately available to be used by all authorized users.

Sanctuary does not check the file extension to determine if the file should be verified or not as this is performed by the Operating System. Once a file has been deemed to be an executable file and that the file has been loaded in memory for execution – but before any execution takes place – then, and only then, Sanctuary checks the entire file to determine if the file can be run or not.

If you are using Sanctuary Server Edition, the solution protects your organization's servers and, by nature, your 'users' are system administrators. For 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, or other inappropriate applications—whether loaded deliberately or accidentally.

What do you gain using Sanctuary?

We have already described the benefits of a white-list approach versus the typical blacklist approach. Looking further, Sanctuary offers a wide range of features and benefits:

> Strong file identification

Sanctuary works by examining each executable 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 the executable 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 will 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 will 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 '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 computer 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. 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 automatically disables 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 VBScript, Microsoft Office VBA, and Jscript. 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

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.

Rest easy. You have Sanctuary.



Overview of system architecture and connectivity

A Sanctuary solution includes the following four main components:

- > One *SecureWave Sanctuary Database Server (SX)*
- > One or more *SecureWave Application Server (SXS)* with one or more *Data File Directory (DFD)* and one, shared if needed, *Audit File Directory (AFD)*
- > The *Sanctuary Client Driver (SK)*
- > Administrative tools – especially the *Sanctuary Management Console (Sanctuary Management Console)*

The following diagram shows these relations:

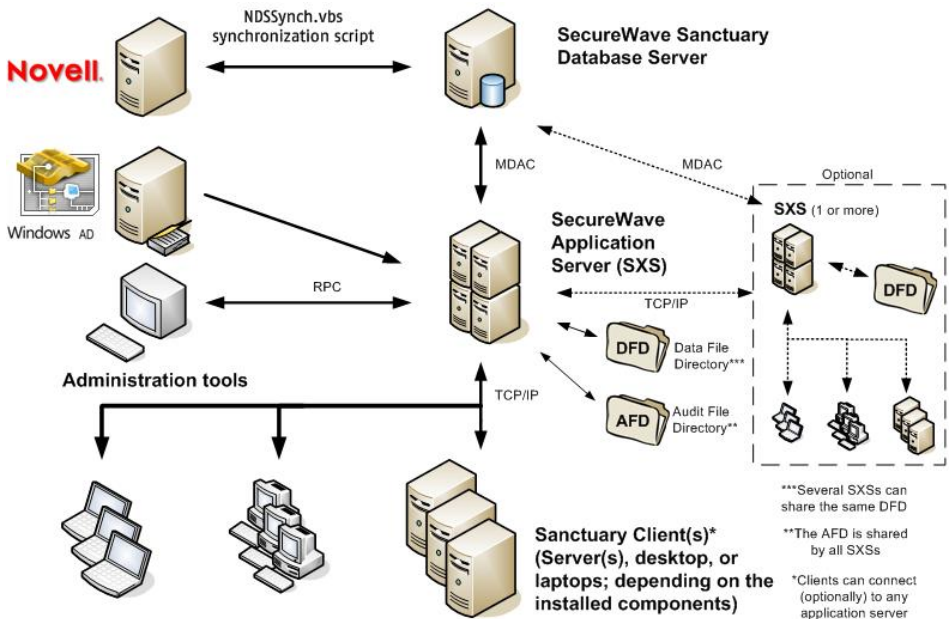


Figure 1: Sanctuary components



We explain each of these components in the following sections.

The SecureWave Sanctuary Database

Sanctuary's database serves as the central repository of authorization information, such as lists of executable files, the digital signatures ('hashes') that uniquely identify those files, File Groups, and authorized users and User Groups.

This database is built on the Microsoft SQL Server 2000/2005, 2005 Express Edition, or Microsoft Database Engine (MSDE) 2000. For organizations with fewer than 200 users, the MSDE 2000 or SQL Server 2005 Express Edition is sufficient. Larger organizations need to use Microsoft SQL Server.

The SecureWave Application Server

Each Sanctuary installation requires at least one SecureWave Application Server. It has a related *Data File Directory* – contained or not on the same machine) – to store log information. All servers can optionally write to the same, shared, directory or you can opt for having different ones for each server (see *Figure 1*). The SecureWave Application Server (SXS) communicates between the SecureWave Sanctuary Database and the protected servers or computers. Each Sanctuary installation needs one, common, Audit File Directory (AFD) where all audit and history files are stored.

The SecureWave Application Server component runs as a Windows Service under any domain user account capable of reading Domain users/groups/computers accounts from the Domain Controller. It performs the following functions:

- > Gets the latest information about access privileges from the database and stores it in its cache
- > Signs, compress, and passes this access information to servers & computers, where it is also stored locally
- > Saves a log if an application access is denied.

The Sanctuary Client

The Sanctuary Client Driver is installed on each server & computer you want to protect. This client component runs as a kernel driver on Windows XP/2000/2003 and provides the following functions:

- > Calculates the digital signature ('hash') of files loaded for execution
- > Checks that hash against the locally stored authorization list



- > Ensures that only authorized executable files can run
- > Bans and logs any attempts to run unauthorized files
- > Optionally, permits local authorization of a denied file
- > Generates log records of all application access attempts – approved and denied. The *Log Access Denied* option is enable by default
- > The communication component of the client, SCC, which runs as a service, sends log data that can be viewed via the management console.

The administrator can also ask the user to show the "salt" value used to do endpoint maintenance when the computer is not connected to the network and this value cannot be obtained by alternative methods. See *Endpoint Maintenance* on page 36 for more info.

The Sanctuary Management Console

The Sanctuary Management Console (SMC) provides the administrative interface to the SecureWave Application Server. This interface – that can be installed on one or more computers – is used to configure the solution and perform a range of day-to-day administrative tasks, such as:

- > Building lists of executable files to be managed
- > Organizing those executable files into logical File Groups
- > Defining Administrator roles
- > Assigning File Groups to users and User Groups
- > Managing and maintaining the authorization database
- > Monitoring system activity logs and option settings
- > Getting all kind of useful reports.

The console and application server are linked through the RPC level 6 protocol (fully encrypted messages). The unique architecture of the Sanctuary solution generates minimal network traffic, so you do not need high-speed connections.

Each protected server & computer client maintains its own local authorization copy, so routine application requests do not have to traverse the network. Only log files and periodic differential updates are sent to them.



Administration Tools

When you install the management console, you also install other tools to manage the system:

- > The *Client Deployment Tool*: to install the Sanctuary Client in your protected computers & servers. It uses standard MSI technology and can also be used to find out which computers already have the client and its status. See a complete description in the *Setup Guide*
- > The *Authorization Wizard*: to identify those files copied to computers by installation routines, and to incorporate them into the Database. The source can be either the original CD/DVD-ROM or the files held on the target system hard drive. See a complete description in *Using the Authorization Wizard* on page 66
- > The *Sanctuary Authorization Service Tool* to monitor changes and create updates (using Microsoft's SUS or WSUS). See a complete description in *Chapter 14: Windows Updates* on page 167
- > The *Versatile File Processor Tool* used with the Sanctuary Authorization Service Tool or independently to scan files). See a complete description in *Versatile File Processor tool* on page 174
- > The *Key Pair Generation*: to create a unique set of private and public keys. See a complete description in the *Setup Guide*
- > The *SXDomain* command-line domain synchronization tool: to inform the Database of the changes done to the domains, users, groups, and workstations within your network. See a complete description in the *Setup Guide*

How does the Sanctuary solution work

Here is a high-level summary of the behind-the-scenes workings of this powerful yet easy-to-use security solution.

Before you activate the Sanctuary solution

- > You gathered a list of executable files that are allowed to run. The system uses a special algorithm to calculate a unique digital signature for each file called a 'Hash'.
- > You organized these file definitions into logical groups (File Groups), and specified which users/User Groups may run these executable files.



This information is maintained in the SecureWave Sanctuary Database.

When a computer signs on to the network

The SecureWave Application Server:

- > Reads the Security ID (SID) of the machine or account
- > Gets the latest authorizations from the central Sanctuary database (only if its cache is empty or if permissions changed)
- > Signs this information for secure transmission across your LAN or WAN and to avoid tampering, compress it, and selects only those parts that changed
- > Automatically downloads this authorization information to the requesting user/machine

This authorization information is then stored locally in a secure location on the client's hard disk, where it cannot be tampered with.

When a machine asks to run an application

The Windows operating system checks the file extension to determine if it is registered as an executable. Once Windows has determined that it is an executable file (for example, those files with .exe or .dll extension), Sanctuary takes action.

The system checks the entire file at a binary level to calculate a 20-octets hash code, checks it against the list of pre-approved hashes from authorized applications, and determines whether the file can be run. This verification is transparent to the user and virtually instantaneous.

If the application is on the approved list

The application starts up with no user intervention required. Sanctuary, optionally, logs the successful application access. This feature is not activated by default.

If application access is denied

Sanctuary sends a denial notification to the user and logs the incident. If the local machine has been configured to allow optional override, the user may choose to assume the risk of activating a denied application. This action will be logged as well.



If a computer is taken off the network

Sanctuary is designed to protect computers at all times from running unauthorized programs. The same control and protection is provided to your users even when they are disconnected from the network, e.g. laptops that are taken off the network. Once a list of hashes has been downloaded, the local copy is used until it is reconnected to the network and able to receive automatic updates once again. The local copy is kept in an inaccessible folder and available even when disconnected from the network.

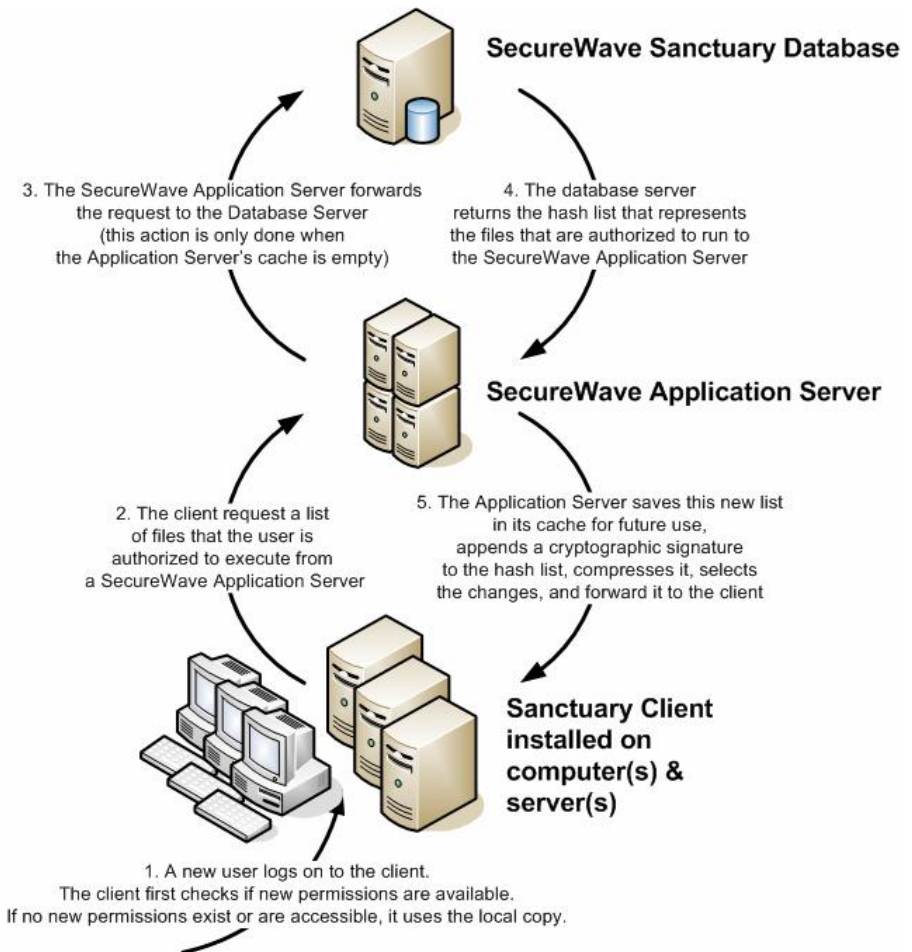


Figure 2: How the Sanctuary solution works



Chapter 2: Working with Sanctuary

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

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

New features & differences from previous version

If you are upgrading from a previous version of Sanctuary it may be useful for you to know about the changes made and the new features. Please consult the readme file located on your Sanctuary CD for a full and detailed list of changes. The following table summarizes them:

<i>Category</i>	<i>Feature</i>
Management ease	File groups can now be classified inside other File Groups. This helps clarify those cases where some files are used by several applications and, thus, create indirect authorizations.
New design	The management console has been completely redesigned.
Unified Management Console	Each one of the programs that form our Sanctuary Application Control Suite previously required an independent console component. We have designed a unified console component that now works with our entire software suite, depending on those modules that you have purchased.
Advanced administrative protection	More control of who can uninstall/modify the client driver.
Differential updates	Instead of sending a complete authorization list, the application server now sends only those permissions that changed.
Unified Logging	All our products now share the same log.
Upload and Storage Enhancements	You can now have several 'data file directories' (DFD, see <i>Figure 1</i>) defined and spread over your network to be used by the SecureWave Application Server(s). The previous limitation of all servers using the same, single, shared, DFD has been removed. Now it is possible for each server to use its own, distinct, one. This improves performance in multi-server installations as each server can be configured to store its data files in a location that is physically closer, or reachable through a high-speed network connection. It also helps spread disk load, as each defined directory only contains part of the files. Note that: <ul style="list-style-type: none">- It is still possible for more than one server to use the same DFD- All servers can still access all data files; it does not matter if only one or multiple directories are used. When a server does not find a file in its



<i>Category</i>	<i>Feature</i>
	defined directory, it requests a copy from a server having access to it. There is also an extra, unique and common, Audit File Directory (AFD). This is the place where all audit and history files are stored.
More client localizations	The client is now available in several other languages beside English, French, German, and Spanish.
Option changes	Computer and user/group options have changed. Some of them include an optional message text to inform the user why the program will not run.

Table 1. New Features & Differences from Previous Versions

...and many, many more features. Please see the *Readme.txt* file located on your CD installation disk for a full list of features and changes.

Working with the Sanctuary 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–styled screen displays, you can easily perform the following tasks:

- > Build a list of executable files that you wish to allow
- > Define authorizations for those executable files (applications)
- > Organize files into File Groups and manage those File Groups. You can also create a parent–son relationship easing the task of classifying all those 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 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.

To start up the management console of your Sanctuary application

1. Click the Windows **START** button and select **PROGRAMS** → **SANCTUARY** → **SANCTUARY MANAGEMENT CONSOLE**.
2. The system displays a *Connect to SXS Server* dialog box:



Figure 3. Connecting to the SXS Server

To connect to the SecureWave Application Server

When you initially launch the Sanctuary Management Console, you need to connect to a SecureWave Application Server.

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 have to append the port number to the server name as in this example:

secsrv.secure.com[1234]



Please refer to the description of the registry key settings of the Application Server in the 'Setup Guide' for more details on how to configure the server to use a fixed port.



When the 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. Please see 'Appendix E' in the '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 the next section.

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 a Sanctuary system administrator* on page 49.

Log in as a different user

If you choose to click on the *Login as* option, instead of using your credentials – default way to establish a connection – 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. DOMAIN\ADMIN).

By default, the system establishes the connection using your 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.

Once the connection established, the user's credentials are shown in the *Connection Window* while the output window show the license details – if you do not see these windows, select the VIEW → CONNECTION and/or VIEW → OUTPUT command:

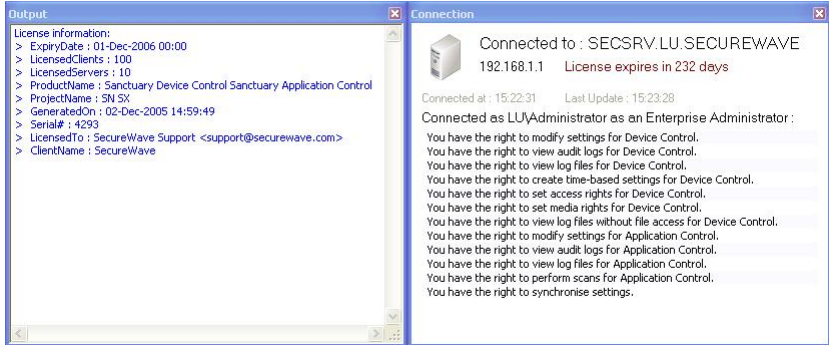


Figure 4. Connection & Output window

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.

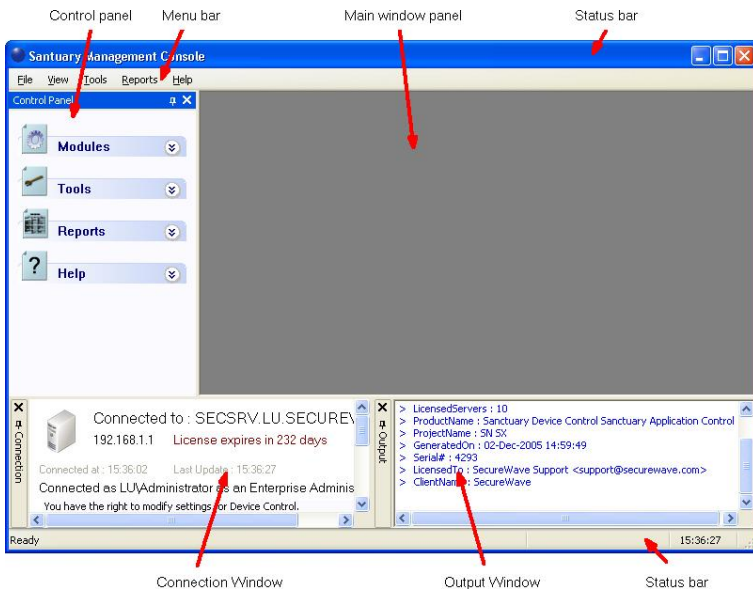


Figure 5. The main screen



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+PA to get an HTML Online Machine report.

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, it stays open – arranges in stacked tabs – until explicitly closed. You can use the *Window* command of the menu bar to organize your workspace.

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 *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 *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 *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.

Once a day, when starting the management console, you get the following screen informing you of your license status:

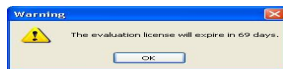





Figure 6. License status warning

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

Use the Pin icon  to “pin down” – Park (the icon changes to  – or “float” () the *Control Panel*, *Connection*, or *Output* window. 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 7. Docked Control Panel



Figure 8. 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:

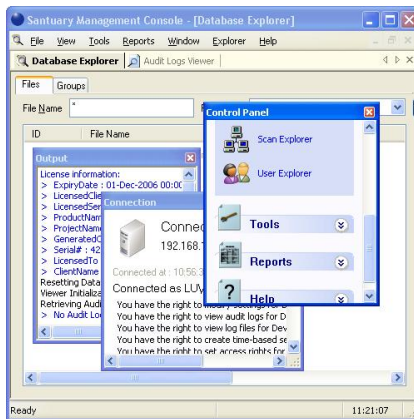


Figure 9. Floating Control Panel

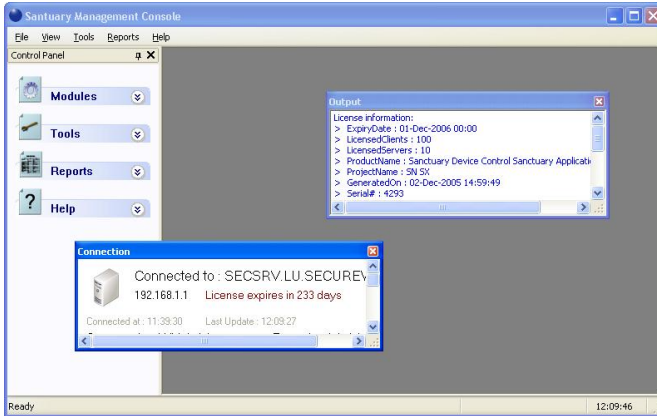


Figure 10. Floating windows

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 those opened module's windows in a tile, cascade, or iconize mode. Each window can also be close, maximize, or iconize independently as needed. If several modules are already open (as shown in *Figure 9*), 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.

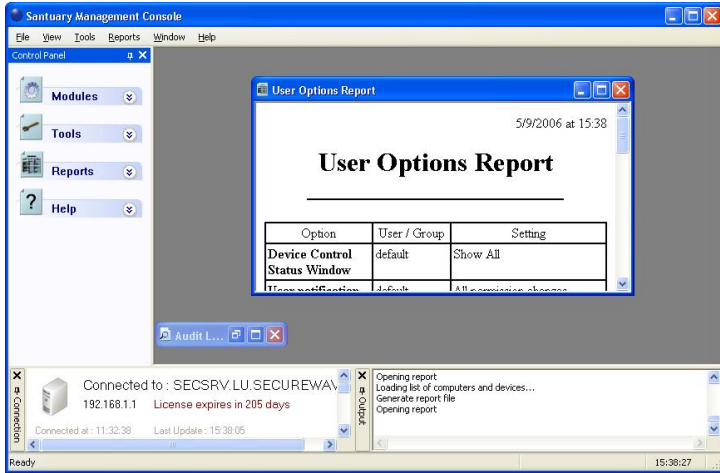


Figure 11. Minimized windows

Sanctuary modules, menus and tools

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

The File menu

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

<i>Use this option</i>	<i>To</i>
Connect	Communicate with another SecureWave Application Server in other server or/a different user name in order to carry out administrative tasks.
Disconnect	Detach from the current server SecureWave Application Server. You need to do this in order to reconnect using a different user or server.
Save As	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.
Print	Print the active report window. You get the standard Internet Explorer print dialog where you can choose the printer and select several printer options.
Exit	Exit from the Sanctuary Management Console application. Note that this command does not stop the Sanctuary Application Server, just your administrative session.

Table 2. The File Menu



The View menu

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

<i>Use this option</i>	<i>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

The Window menu

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

<i>Menu</i>	<i>Description</i>
<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.
<i>Arrange Icons</i>	Position your iconize windows in orderly rows.

Table 4: The Window menu items

The Tools menu

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

<i>Use this option</i>	<i>To</i>	<i>See page</i>
Synchronize Domain Members	Update the database with the current list of users and groups of a domain or machine.	126
Database Maintenance	Delete log files and items generated from a database scan created before a specified date.	123
User Access	Define Sanctuary Device Control Enterprise Administrators and Sanctuary Device Control Administrators. It will allow you to restrict the right to set permissions, view the audit log or the shadowing information.	49
Default Options	Change the option settings.	141
Path Rules	Use path locations and file 'owners' to define which applications can run.	81
Spread Check	Prevent the spread of self-propagating code by disabling suspicious executables that have been locally authorized on too	45



<i>Use this option</i>	<i>To</i>	<i>See page</i>
	many computers.	
Send Updates to All Computers	Dispatch the latest changes to all computers in the SecureWave Application Server(s) online table(s). Changes can be sent in synchronous or asynchronous mode	47
Send Updates to	Transmit updates to one or more selected computers.	47
Import SecureWave File Definitions	Import files and their hash definitions for any server platforms supported by the Sanctuary solution (Windows 2000/XP/2003). When you initially install Sanctuary, you can also install some file definitions. You can find new ones on our Web site: www.securewave.com .	55
Export Settings	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.	54
Purge Online Table	SecureWave Application Servers keep 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 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.	131
Endpoint Maintenance	Create and save maintenance "tickets" for computers/computer groups allowing protected files and/or registries to be modified. See next section for an explanation.	36 & 146

Table 5. 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 its Security Identifier (SID) but not its 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 process to synchronize depends on whether the protected computers are on 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 – we call it Salt – is used to guarantee that only authorized process/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 *Setting default options* on page 146). If the "Extended" or "Basic" value is used, the client protection mechanism can only be deactivated using the endpoint maintenance. The generated "ticket" can be saved and transported to the client computer(s) by any available means (shared directory, email, or removable device).



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's icon – located on the system bar – and selecting 'Endpoint Maintenance' from the contextual menu.

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).
2. The time options are only valid to accept the corresponding maintenance ticket. Once the ticket is accepted, there is no time limit for it. To deactivate the ticket you will need to 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 will appear on the audit log. You can review them by using the Audit Logs Viewer module (see *Chapter 10: Monitoring Sanctuary system administrator activities; the Audit Logs Viewer* on page 115)



To create and save maintenance “tickets” for endpoint machines/users

1. Select the **TOOLS** → **ENDPOINT MAINTENANCE** item from the menu bar (or from the Control Panel).
2. Choose the salt value – this depends on which *Hardening* option is set. Use the **QUERY** button to obtain the value directly from the client computer. Use the right click contextual menu of Sanctuary client's icon when the machine is not connected to the network.
3. Select the period.
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**.

The screenshot shows the 'Endpoint Maintenance' dialog box. It has a title bar with the text 'Endpoint Maintenance' and a close button. The dialog is divided into several sections: 'Salt' with radio buttons for 'Without' and 'With' (selected), a text field containing '8UH7R-N5T5K-J0M37-YAY95-Z7GTA', and a 'Query...' button; 'Validity Period' with radio buttons for 'From Now' and 'Until (now+1hour)' (selected), and 'From'/'Until' date and time pickers; 'Targets' with text fields for 'Computer(s)' and 'Users(s)', and 'Computers...' and 'Users...' buttons; and 'Comments' with a large text area. At the bottom are 'Save...' and 'Close' buttons.

Figure 12. 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 *Setup Guide* for a description of the registry keys. As previously explained, this ticket also depends of the *Client Hardening* option value.



The Reports menu

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

<i>Use this option</i>	<i>To</i>	<i>See page</i>
File Groups by User	Select one or more Users and/or Groups and generate a report of the File Groups they may use.	135
Users by File Group	Select one or more File Groups and generate a report of the Users and Groups given access to them.	136
User Options	Display all the user options defined in the system.	137
Machine Options	Display all the computer options defined in the system.	138
Online Machines	Show all machines currently recognized by the SecureWave Application Server that you are connected to.	139

Table 6. The Reports Menu

The Explorer menu

The *Explorer* menu (on the menu bar) changes depending on the module you are using.

<i>Use this option</i>	<i>To</i>
In the Audit Logs Viewer module	
Clear all filters	Clean the searching info fields.
In the Database Explorer module	
Assign	Change the File Group to which a file is assigned.
Manage file groups	Add, rename and delete a File Group. See page 71 for more details.
In the EXE Explorer module	
Map Network Drive	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.
Disconnect Network Drive	Remove the letter assignation from any shared resource on a network. This is the opposite operation than that done with the <i>Map Network Drive</i> command.
Assign	Change the File Group to which a file is assigned.
Manage File Groups	Add, rename, and delete a File Group. See page 71 for more details.
In the Log Explorer module	
Fetch log	Obtain the latest log from a client computer. See page 112 for details.
Assign	Change the File Group to which a file is assigned.
Manage File Groups	Add, rename, and delete a File Group. See page 71 for more details.
In the Scan Explorer module	
Perform scan	Scan a computer to identify executable files that need to be authorized.
Select scans	Choose the two scans you want to compare.



<i>Use this option</i>	<i>To</i>
Assign	Change the File Group to which a file is assigned.
Manage File Groups	Add, rename, and delete a File Group. See page 71 for more details.
In the User Explorer module	
<i>No options are available in the Explorer menu for this module.</i>	

Table 7. The Explorer Menu

The Help menu

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

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

Table 8. The Help Menu

The six system 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>Use this module</i>	<i>To</i>	<i>See page</i>
Audit Logs Viewer 	View logs of the administrators actions.	115
Database Explorer 	View the list of executable files that have been entered into the Sanctuary database and manage file assignment details.	123
EXE Explorer 	Build a list of executable files that are allowed to run, assigning these files to File Groups.	59
Log Explorer 	View logs of applications that have been run, those to which access was denied, or those locally authorized after denial.	97
Scan Explorer 	Scan a computer or domain to identify executable files that need to be authorized, and assign those files to a File Group.	60
User Explorer 	Align users or User Groups with File Groups, to grant them permission to use the files in those File Groups.	89

Table 9. 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 71.

You will find detail information about how to use these modules in the following chapters.



Chapter 3: An overview of authorization strategies

Sanctuary protects your organization's servers and computers by permitting only authorized applications to run. The system supports several approaches to authorization:

- > Centrally managed by digital signature. This is the primary method for securing your servers and computers against all unwanted executables – known and unknown. The organization centrally manages the authorization by establishing what is specifically approved, and by default denying everything else.
- > Managed by file location (path). This alternative method enables you to control executable files for which hash definitions are not useful or applicable. This is used to handle exceptions, for example, auto-changing executable files. You can also design a Trusted Owner to reinforce security.
- > Centrally or locally managed for scripts and macros. VBScripts script files and Office VBA macros are files that can be run on a Windows system, but they are not Win32 executables in the strict sense of the word. You can centrally determine that all scripts and macros are denied, or you can lean on local users' discretion to allow/deny/authorize programs.
- > Locally controlled by provisional override. You can choose to grant users limited right to authorize additional executables—unknown files that they may need to use for their work.

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



Central authorization by digital signature (hash)

This is the primary method for authorizing executable files – the most powerful and all encompassing. A central administrator defines which users and User Groups can use which files throughout the organization.

Central authorization generally addresses all the applications used to manage and maintain the organization's servers, such as the operating system itself, and those specific business applications.

Central authorization is based on the following steps:

1. Build a list of executable files 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, Log Explorer, or Versatile File Processor Tool.
2. Create a unique digital signature of each approved executable. Whichever method is used to identify executable files, the Sanctuary solution examines the binary contents of the files, calculates a 20 character alphanumeric digital signature (or 'hash') for each one, and records this information in a central repository. The list of centrally authorized applications is the list of all the programs that you trust and that you specifically want your users/user groups to be able to use at any time.
3. Organize approved executables files into File Groups. An authorized Sanctuary system administrator can assign the files "hashed" in step 2 to File Groups, such as 'Windows Operating System', to simplify administration of related and/or interdependent files.
4. Associate File Groups with users/user groups. An authorized Sanctuary system administrator designates which users and/or user groups can use these File Groups. Thereafter, users will only be able to activate the applications for which they have privileges to use.

For convenience and ease of use, Sanctuary provides several methods for setting up and maintaining central authorization: from the *Database Explorer*, *EXE Explorer*, *Log Explorer*, *Scan Explorer*, and using the Authorization Wizard, FileTool.exe, or AuthSrv.exe tools.

5. Download authorization information to protect your machines. Digital signatures for approved files are downloaded to the user's machine and stored in a secure location on their local hard drive. The solution



references this locally stored authorization list whenever the user (or a server administrator) or the machine requests the launching of an executable file.



It is particularly important to centrally authorize the operating system files and driver files (video card user interface such as `atiptaxx.exe`, for example) that must run before logon is completed. Users would not be able to locally authorize them because they execute before the user logon completes.

Central authorization by file location (path)

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

This type of authorization is set up through the *Path Rules* item of the *Tools* menu (or from the Control Panel). Please see *Chapter 7: Authorizing software by location (Path Rules)* on page 87 for more information.

Authorization for Windows scripts and macros

Windows scripts and macros — such as VB script files, Office VBA macros, Windows Script files, and Java scripts — interpreted on Windows systems even though they are not Win32 executables. Since they are not recognizable as executable files by Windows (they do not have `.exe` or `.com` extensions, for example), they would not be picked up by a Sanctuary scan and added to the authorization database.

By default, Sanctuary allows all scripts and macros to run. However, you can determine centrally that all scripts and macros are all denied, all permitted, or give local users discretion to allow or deny them.



To centrally allow or deny authorization for *all* scripts and macros

1. Select *Default Options* from the *Tools* menu (or from the *Control Panel*).
2. In the *Default Options* dialog, select the *User/Group* tab.
3. Select *Macro and Script Protection*.
4. Uncheck the *Not configured* box so you can enter a value other than the system default.
5. Select *Deny All* from the drop-down list. This option setting prevents execution of all scripts and macros.

The client can revert this setting through the context-sensitive menu of the Sanctuary Tray icon.

To grant local users authority to allow or deny scripts and macros

Set the *Macro and Scripts protection* option, in the *Default Options* dialog, to *Ask User* mode. When the Sanctuary system intercepts a script execution, the user is presented with a screen that offers the following choices:

Deny Prevent the execution, as the source of the script or macro is not fully trusted.

Deny all Prevent execution of this and future scripts and macros.

Authorize Allow the script or macro to execute for this one time and one computer only. Once authorized, this prompt does not appear again.



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



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

By default, Sanctuary does not permit users to perform local authorization (override a denial based on centrally maintained authorization information). However, you may wish to allow users to locally authorize applications, if it is necessary for their productivity, such as to run a special one time executable.



This 'Local Authorization' does not applies to those files that already form part of a 'File Group' that is not assigned to the user who is trying to authorize the file.

If 'local authorization' is allowed

If 'local authorization' is permitted, the process follows these steps:

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

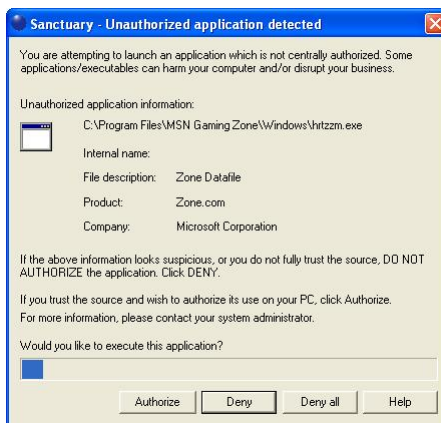


Figure 13: Local authorization screen

3. Within the alert dialog, the user can then choose to authorize the application, deny it, or deny all unknown applications. If the user does not respond within the time-out period (two minutes is the default), the dialog automatically disappears and the file is denied.



4. Whether the executable is authorized or denied, the Sanctuary system logs the action.
5. If the same application is locally authorized on a certain number of machines in a defined period, Sanctuary regards this as suspicious self-propagation program and disables the application (not those already running) and local authorization capabilities in general, using the *Spread Check* feature – if activated.

To prevent Users or User Groups from performing local authorization

- > Disable the *Local Authorization* option globally. See *Chapter 13: Setting system options* on page 141 for more details.
- > An individual user can essentially mimic this function by clicking on the DENY ALL button when prompted to authorize an unknown application. The client can revert this setting through the contextual menu of the Sanctuary Tray icon.

To enable users to locally authorize applications not listed in the Sanctuary system

- > Set the *Local Authorization* option to *Enable* (the default setting).
- > Configure the *Execution Blocking* option to either *Ask user for *.exe only* or *Ask user always*.

See *Chapter 13: Setting system options* on page 141 for more details.

To prevent the malicious spread of locally authorized files

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

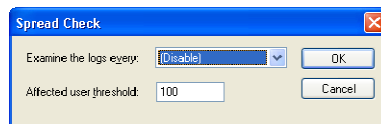


Figure 14. Spread Check Dialog

2. Select how frequently the system should check activity logs for suspicious propagation of locally authorized files – every 5 minutes, 15 minutes, etc.



3. Enter the number of users you consider being the threshold of suspicion. It is set to one hundred by default.
4. Click OK.

Now, if the system detects that an unknown executable has been locally authorized on the designated number of servers or computers (100, in this example) within the defined period, Sanctuary immediately disables the executable and the local authorization capability. This will not disable the already running authorized executables. Self-propagating viruses and worms are stopped in their tracks. Once the administrator has investigated the reason why the spread check triggered, and possibly clean-up the machine, local authorization can be turned back on.



If you have more than one SecureWave Application Server on your network, verify that only one of them is doing the 'Spread Checking'. If this is not done, the other servers can default to 'Execution Blocking' and activate the 'Spread Checking' feature.

Sending updated authorization information to computers

When you change any system setting – options, parameters, file authorizations, etc. – you will want to distribute these changes to servers and computers protected by the Sanctuary system.


To push updates to all computers protected by Sanctuary

Select *Send Updates to All Computers* from the *Tools* menu (or from the *Control Panel*). Updates are distributed to all clients in the SecureWave Application Server(s) online table(s). This works by sending an update signal to all clients and the clients responding to it by contacting the SecureWave Application Server and getting the new hashes.

If you click on the Yes button, the program may take a lot of time sending updates since this process is done synchronously; the *SecureWave Management Console* has to wait for the *SecureWave Application Server* to finish sending the updates to all machines in the online table. If, on the other hand, you choose No, then the process is done asynchronously and the *SecureWave Management Console* does not wait for the *SecureWave Application Server* to finish. You will be able to continue working while the update is done in the background.



To push updates to a designated computer

1. Activate the *User Explorer* module (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. 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 from the *Control Panel*).
 2. Choose the desired computer from the *Select Computer* dialog.
 3. Click on the OK button to close the dialog and send the updates.

If you do not push updates to computers

They will automatically be downloaded whenever a server or computer logs on to the network.



Chapter 4: Setting up a Sanctuary system administrator

Overview – Types of 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 files, setting and changing authorizations, and viewing logs of system activity:

The 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 system *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.

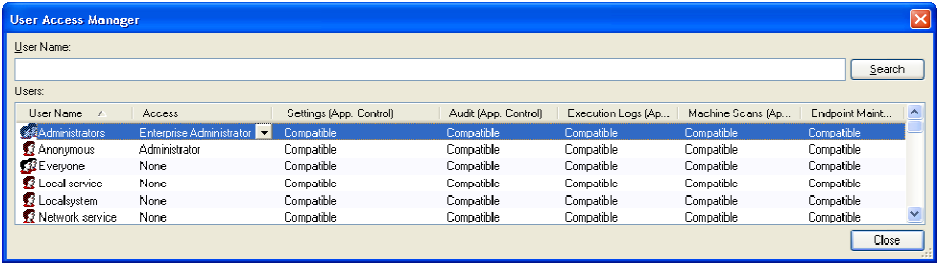



Figure 15. User Access Manager Dialog

2. Enter a user name in the *User Name* field.
3. Click 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 the *Access* column and set that user as an *Enterprise Administrator*. This user will now have rights to connect to the SecureWave Application Server to manage any object (users, groups, computers, default options, SecureWave 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 will 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 will now have 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 the *Audit (App.Control)* header. Set this attribute to:

Yes This Administrator can view and search audit logs of system activity.

No This Administrator cannot view or search audit logs.

*Compatible**

3. Click 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 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 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 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 36 for a complete explanation.

No This Administrator cannot issue Endpoint maintenance tickets.

*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 list of executable files to be managed

Sanctuary allows or denies the running of executable files according to your predefined specifications. Most executable files are identified by their extensions. Extension such as .exe, .com, .dll (for dynamic link libraries), .cpl (for control panel files), .scr (for screen-savers), .drv, and .sys (for system drivers) are sometimes synonyms of 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 will take over and check the file's signature against the list of allowed files.

Sanctuary provides several methods for building a list of executable files to authorize. You can:

- > Import standard file definitions from SecureWave, which address common Microsoft operating system components and applications. You get a set of these files in the installation CD but you can also find the latest ones on our Web site
- > Select files from computer directories to add to the application list
- > Scan a computer to generate a list of the applications residing on that machine
- > Scan a selected directory of a computer to identify files without unnecessary scanning
- > Use the Authorization Wizard to streamline and automate the process
- > Use the FileTool.exe to scan file locations



To avoid authorizing tampered or infected executables, you should always use the original media (CD/DVD or downloadable package from the official software vendor) when building a list of executable files and generating digital signatures.



Export file permissions

With this feature, you can export a group of carefully crafted authorizations for a range of programs to a file and then import them onto a computer to synchronize it.

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 rules will apply when you import them into the target computer.

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

To export your settings:

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

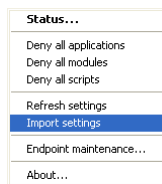


Figure 16: Importing a permission file

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



Importing standard file definitions from SecureWave

SecureWave makes available to its clients a number of pre-computed file hashes for Windows 2000, Windows XP, and Windows 2003 versions. These hashes are referred to as *SecureWave File Definitions* or *SFD* files. The purpose of these files is to simplify Sanctuary initial setup and maintenance since such lists already contain the SHA-1 hash for various operating systems. SecureWave File Definitions files also include the necessary information to allocate automatically files to predefined File Groups. File definitions are particularly useful when authorizing product updates such as service packs and hot fixes as they can assign them automatically to the corresponding File Group.

The recommended process is to import SecureWave File Definitions during the installation. You can find more information in the Setup Guide. However, if the SecureWave File Definitions are not imported during setup, or you wish to add additional ones later, you must import them manually.

When first installing the program, a set of predefined file groups and assignments are made. You can use them to save you time when you logically regroup executables files into file groups:

<i>File Group Name</i>	<i>Users assigned</i>
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 10. SecureWave File Definitions (SFD).



If you chose the automatic import option during installation

You will enjoy several advantages:

- > You will not have to take the time to scan basic operating system files or organize them into logical File Groups. SecureWave has already done that for you.
- > You will not have to assign those 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 the setup of SecureWave Application Server.
- > You can be sure that pure versions of the operating system files were used to create the hashes. There is no chance of accidentally authorizing tampered versions of system files.
- > Your life will be easier when system files are upgraded, since the system recognizes these standard files – and their respective default File Groups – automatically saving upgraded file definitions in the same locations.

If you did not import standard file definitions during installation

No problem. You can do it now, if you wish:

1. Select *Import SecureWave File Definitions* from the *Tool* menu. The corresponding dialog opens.
2. Click **ADD** and the dialog box will display available files and folders. SecureWave File Definitions have a *.SFD* extension.
3. Navigate to the *.SFD* file(s) you wish to import, and click **OPEN**. The file now appears in the **ADD** window.
4. Click on the **ADD** button to select more files to import or on **IMPORT** to import the selected file(s). Since it can take a few minutes to process the SecureWave File Definitions, choose only the ones you will actually need.
5. Select between importing SFD with or without file hashes:

Import SFD with file hashes and create predefined File Groups: The program imports ALL files hashes in the predefined File Groups, even those that are not used or seldom 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 of the selected SFD file. The advantage here is that you do not need any extra step, everything is handled for you. On the other hand, your database includes the signature of all the OS files, even for those not used. Transmitting this can be problematic, especially if you have slow lines in your network.



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

Import SFD without the file hashes and create predefined File Groups: The process is similar to the previous option, but no file hashes are imported. However, the program memorizes the suggested predefined File Groups for each file. When the time comes to scan and assign files found on client machines, the program will propose the 'correct' File Group. If you select this option, once the importation process finishes you will have an 'empty' database. Your second step is to scan a 'newly installed' client machine and then assign these scanned files to the proposed (or your own) File Groups. The disadvantage here is that you need extra steps to accomplish the task and the system only helps you partially by identifying the file's names and proposing File groups when the time comes to authorize them. On the other hand, you have a small database that contains only those files used by your clients.

6. Click on the **IMPORT** button and accept the license agreement.
7. Once the importing process finishes, click **OK** and then **CLOSE**.
8. Assign the created file groups to users or User Groups. (Note that this step is automatic if you imported SecureWave File Definitions during setup. See *Table 10* on page 55)

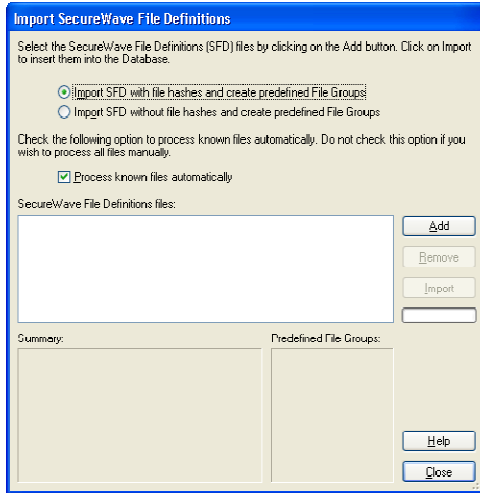


Figure 17. Import SecureWave File Definitions (SFD)

- ✎ *When Microsoft produces a new Service Pack or other update for one of its operating systems, SecureWave will create the equivalent SFD file. These files are available at our Web site: www.securewave.com. These updated definitions can be imported at any time using the previously outlined steps.*
- ✎ *When you install the file definitions, you should take care of the logon and boot files. If these are not authorized, the system will not work properly. This is especially important when doing system updates.*
- ✎ *When installing other products of our suite, check that the computer and user/group 'Execution Blocking' option is set to 'Non-blocking mode'. If this is not done, the setup cannot proceed. See Chapter 13: Setting system options on page 141 for more information.*



Selecting executable files from network directories

You can use the Exe Explorer module to create a list of executable files to authorize. This is the easiest method and does not require a client driver installed in the machine you are going to explore.

Using the EXE Explorer module (no client driver required)

From 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 on the entire computer. This process can be slow and it is typically done when you want to recognize all the applications installed on a computer.

It is best to use a newly configured 'reference' computer to carry out this task, so you can be sure that only 'clean' files are authorized for execution. This reference computer does not have to be the one running the management application. You have the option to browse the network and select any other available machine for this task.

The FileTool.exe is another alternative for doing this same job with the advantage that it can be scheduled using the AT or WinAT command.

✍ Note that you must have authorization to use the EXE Explorer module. Please refer to Chapter 4: Setting up a Sanctuary system administrator on page 49 for more information.

✍ This process would not open CAB or MSI files. You need to use the 'Authorization Wizard' for this. Please see Using the Authorization Wizard on page 66 for more details.

Automatically scanning a computer to identify executable files

This is the easiest method to identify all installed components of specific software. The only limitation is that you must first install Sanctuary client on the machine.



Using the Scan Explorer module (requires a client driver)

The Scan Explorer module scans a target computer, which has the client previously installed, and builds a detailed list of all files found. This is the easiest and quickest way to populate the Sanctuary database from a reference computer, as well as to identify unknown applications.

You can 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 (*.exe, *.com, *.dll, *.ocx, *.sys, *.drv, *.cpl), which reduces the scan time required.

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

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

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

```
Scan all executables matching the pattern
*.exe or *.dll (without regard to case)
in directory
%SYSTEMROOT%
and its subdirectories
```

```
Scan all files matching the pattern
* (without regard to case)
in directory
%PROGRAMFILES%
and its subdirectories
```

See *To create a new template to scan executable files in a computer on page 61* for details on how to create a template.

The following illustration shows the Scan Explorer module main window:

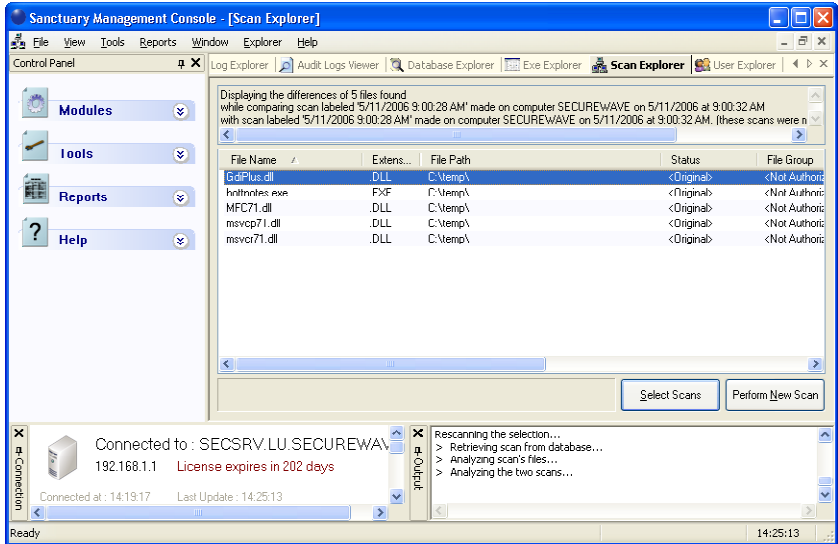


Figure 18. Scan Explorer module main window

To create a new template to scan executable files in a computer

1. Click 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 to open its dialog.
3. Click on **CREATE NEW TEMPLATE** in the upper right part of the dialog. The following dialog opens:

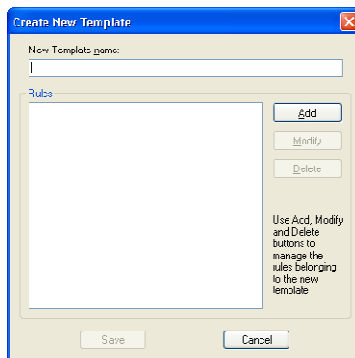


Figure 19. Create New Template Dialog



4. Enter a name to represent the new template. Choose a meaningful name so you can identify and use this template again in the future.
5. Click on **ADD** to display the *New Rules* dialog. Complete this dialog as follows:

Scan files matching the pattern

Use a single asterisk (*) for all files.

Use an asterisk with a dot and extension for specific file types (*.exe)

Use semi-colons to separate multiple wildcard entries. (For example: *.exe;*.hdk;*.dll)



*If you specify wildcard masks – for example, *.com –, there is the potential to miss any file that does not use the standard file extensions (.exe, .com, .dll, etc.). Such files, if missed, are not authorized and therefore the application they are part of will not work properly (or not at all).*

In directory

Enter the path of the directory you want to scan.

Use '^SystemRoot\' with this capitalization to indicate the Windows directory.

Include subdirectories

Check this box if you also want to scan subdirectories within the specified directory.

Scan executables

Activate this option if you only want to scan for executable files and ignore all others (recommended). This will also do a 16 bits executable search. If you do not activate it, you should use *.exe and *.sys on the matching pattern to search for them.

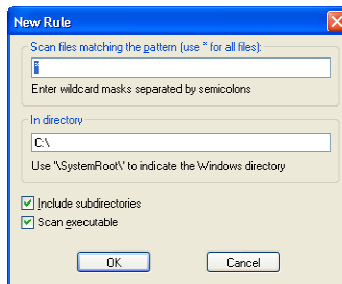



Figure 20. Insert New Path Rule Dialog

6. Click on the **OK** button and then on **SAVE** 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 all files on a computer to identify executable files

1. Click 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. The following dialog opens:

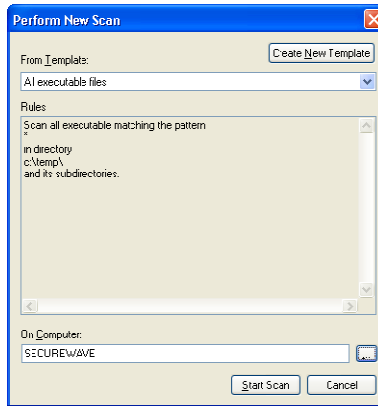


Figure 21. Perform New Scan Dialog

3. In the *From Template* field, choose all files (we are supposing that you already created a template with that mask. See *To create a new template to scan executable files in a computer on page 61*).
4. Choose the computer you want to scan.
5. Click **START SCAN** to display another *Perform New Scan* dialog.
6. In the *Comment* field, enter a name or remark to distinguish this scan. Use a descriptive name, especially if you plan to compare two scans afterwards.

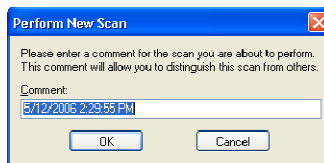
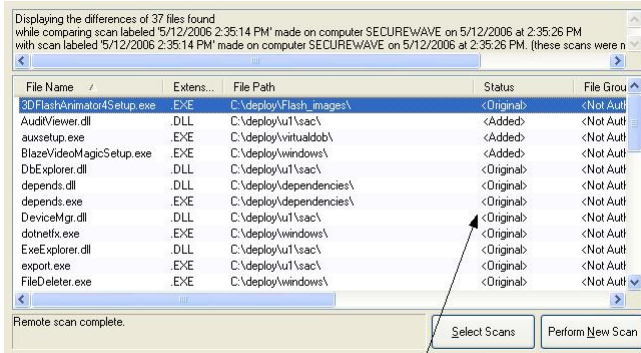


Figure 22. Perform New Scan: Comment



7. Click OK to start the scan. Sanctuary scans all the files on the computer, calculates hashes for all executables, and adds these new file definitions to the database. The populated *Scan Explorer* display will look similar to this one:



Files are displayed with a *Status* column that shows the differences between two scans (if already done)

Figure 23. Scan Explorer window after a scan

To save time by scanning just selected directories on a computer

1. Click the *Scan Explorer* icon from the Management sidebar.
2. Click on the PERFORM NEW SCAN button to open its dialog.
3. In the *From Template* field, choose a template from the drop-down list. The definition of that template is displayed in the *Rules* area of the dialog. Choose from the available templates the one that specifies the filename extensions and/or directories you want to scan.
4. Choose the computer you want to scan.
5. Click on the START SCAN button to display the *Comment* dialog. If you wish, enter a comment that defines this scan. Use a descriptive name, especially if you plan to compare two scans afterwards.
6. Click OK to start the scan.

To compare the differences between two scans

1. Perform the scans you want to compare, following the previously outlined steps. These scans do not necessarily have to be recent ones. In fact, it would be typical to perform one before installing new



software and another one after the installation process is complete – and then compare them.

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

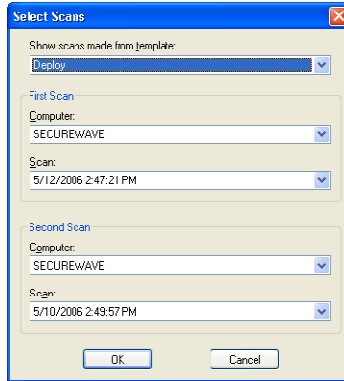


Figure 24. Select Two Scans to Compare

3. In the *Show scans made from template* field, choose the one used for the scans that you are going to compare. This is why you need to be specific with the scan name.
4. In the *First Scan* section fields, select the computer and scan of the first one of them.
5. In the *Second Scan* section fields, select the computer and scan of the second one.
6. Click on the OK button. The system compares the two scans and displays the result 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:

<i>Status</i>	<i>Description</i>
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 11. File status when comparing to scans.



It is only meaningful to compare two scans that have been done with the same template.



Modifying file authorization

After scanning a computer to identify executable files – 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 new files and file changes made when installing a new application, you may want to assign the new and modified files to the appropriate File Group so your users can work with the new application or upgrade.
- > If the intention of your scan was to identify different applications files, you may want to remove them from File Groups to prevent further use of the application.

To modify 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, refer to *Chapter 8: Assigning access permissions to users and groups* on page 89.

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



A scan does not open CAB or MSI files. You should use the Authorization Wizard for this. See next section.

Using the Authorization Wizard

The Authorization Wizard utility provides yet another method for:

- > Searching for executable files from a given source – such as a computer's hard drive, a network share (UNC path), or a CD/DVD-ROM
- > Creating digital signatures (hashes) for those files
- > Incorporating those digital signatures into the 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.

To add executables to the Sanctuary database using the Authorization Wizard

1. Click the Windows START button and select PROGRAMS → SANCTUARY → AUTHORIZATION WIZARD. The Authorization Wizard starts.
2. Read the instructions and click NEXT to begin.
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 the connection to the required server.



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]. Please refer to Appendix E of the Setup Manual.

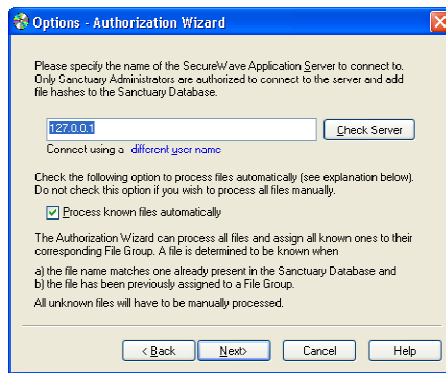


Figure 25. Authorization Wizard

4. Check the *Process known files automatically* option to have the wizard insert files into the SecureWave Sanctuary database if they are already there with the same name but different digital signature (hash). The wizard will also try to find a suitable File Group for them. Deactivate the option if you want the wizard to identify known files but allow you to manually process them.



- At the next dialog, select the root directory where you want to scan for executable files and select the temporary directory where the wizard should expand any archives (set of compressed files) found. Both directories should already exist. You can browse for them using the ellipsis button located next to the field.

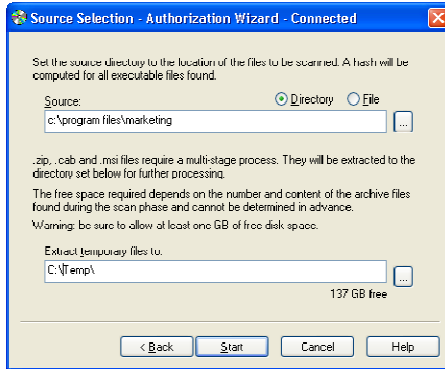


Figure 26. Authorization Wizard: Selecting the Source Directory



The wizard will unpack 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 sufficient free space.

- Click **START** to begin scanning the source directory for executable files. The wizard will begin searching in the source directory displaying statistics on the number of executables found. You should release some disk space if you see the *Free space for extraction* disk space field fall below 100 MB.

When the scan is completed, the wizard presents a summary, as shown below.

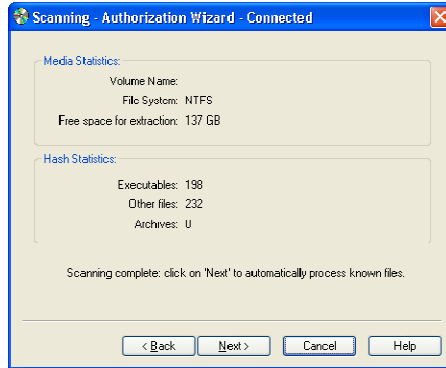


Figure 27. Authorization Wizard: Media Statistics

7. Click NEXT to continue.
8. If you previously checked the *Process known files automatically* option, the wizard processes all executable files found and tries to determine a suitable File Group for each one of them. That is, if a matching filename exists in the database and has been assigned to a File Group, the wizard assigns this file definition to the same File Group. You may need to manually assign unknown files, if any.

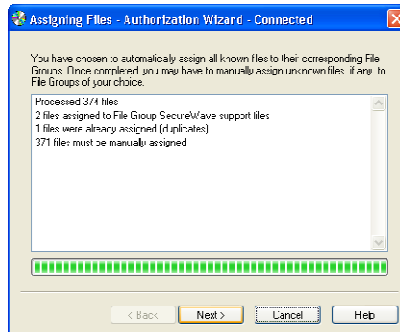


Figure 28. Authorization Wizard: Processing the Files

9. When this task is completed, the wizard presents another summary of activity – how many files were processed, how many were assigned to File Groups, and how many were duplicates of previously assigned files.
10. The wizard either presents a list of files that were not automatically processed because they did not match existing filenames in the database or because you did not activate the *Process known files automatically* option. You can use this list to directly assign files to File

Groups. Select one or several files using the CTRL and/or SHIFT key and then click on the *Suggested File Group* field button list or use the FILE GROUPS button to define new File Groups. See next chapter for complete details.

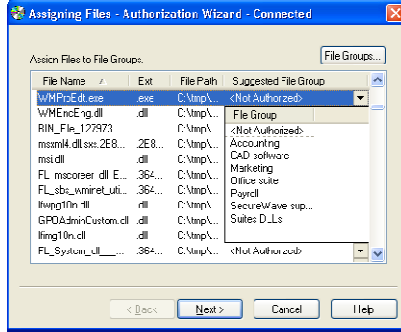


Figure 29. Authorization Wizard: Assigning Files to File Groups

- Once you finish assigning the files to File Groups, click on NEXT to insert the new definitions into the database. Note that you may have to update access permissions to enable users/user groups – using the *User Explorer* module – to run these new applications. You can choose to run again the wizard in the final screen.



Chapter 6: Organizing files into File Groups

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

You may set up File Groups to reflect the way you want to administer the solution. For example, you might create an IIS (Internet Information Server) group to associate together all network services needed by your Web master when protecting servers in your organization or a Marketing group to cluster all software needed by your marketing personal.

File groups can have child File Groups assigned to them. This is sometimes necessary because, by the way Windows is designed, many applications use common files (libraries) containing code, data, or resources, in any combination, to do their work. This allows changing shared library version or coding without the need to recompile or change the application itself. By creating a parent-child relationship, you can indirectly authorize the use of these File Groups. Child File Groups have to exist before creating these relationships in the *Database Explorer* module (in the *Groups* tab).

Creating and managing File Groups

To create a new File Group

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

If you are working in the *Database Explorer*, *Exe Explorer*, or *Log Explorer* module, you could also select a file(s), choose *Assign* from the *Explorer* menu, and then click 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 the ADD FILE GROUP button at the top right of the dialog. The system displays the corresponding dialog.

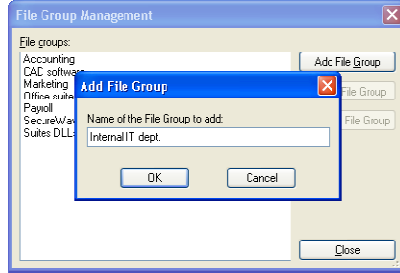


Figure 30. File Group Management

4. Type the name of a new File Group to add, and click OK. The new File Group has now been added, and you can now assign files to it.

To delete a File Group

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

If you are working in the *Database Explorer*, *Exe Explorer*, or *Log Explorer* module, you could also select a file(s), choose *Assign* from the *Explorer* menu, and then click 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. Select the desired File Group and then click 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.
4. If you are confident that you want to delete the File Group, click OK. The group is removed from the list.



Perform this operation with care, as some users may no longer be able to execute some needed applications assigned to them. 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 either the *Database Explorer*, *Scan Explorer*, *Log Explorer*, or *Exe Explorer* module (click the appropriate icon in the Modules section of the *Control Panel* of the main window or use the *View→Modules* command).
2. Select *Manage File Groups* from the *Explorer* menu. The system displays the corresponding dialog.

If you are working in the *Database Explorer*, *Exe Explorer*, or *Log Explorer* module, you could also select a file(s), choose *Assign* from the *Explorer* menu, and then click 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. Select the desired File Group and then click the RENAME FILE GROUP button. The system displays the *Rename File Group* dialog.
4. Type the new name of the File Group and click OK. The new File Group name will appear in the *File Group Management* dialog.

To create a parent-child relationship between File Groups

The parent-child relationship can only be created, deleted, or modified in the *Database Explorer* module using the *Groups* tab.

1. Open the *Database Explorer* 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:

<i>Icon</i>	<i>Description</i>
	This File Group is parent of the one selected in the File Groups panel.
	This File Group is child of the one selected in the File Groups panel.
	This File Group is an indirect parent of the one selected in the File Groups panel.
	This File Group is an indirect child of the one selected in the File Groups 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 12. 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.

The following to examples help clarify these situations.

In this first example, the File Group "Accounting" is the parent of "Payroll" which also has an indirect parent "Marketing":

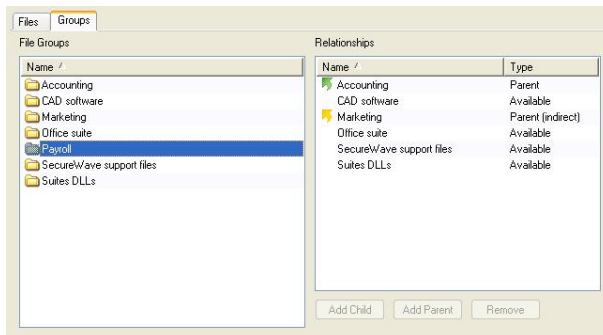


Figure 31. File Group parent relationship

In this second example (related to the first one), "Accounting" is child of "Marketing" who also has an indirect child "Payroll":

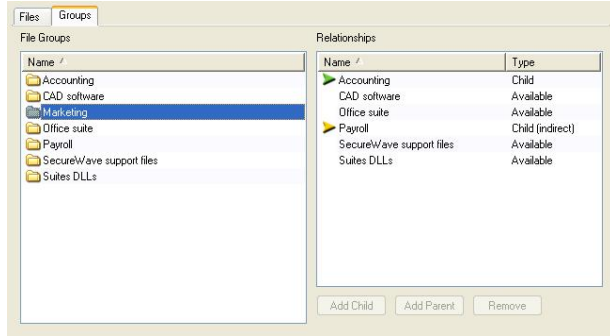


Figure 32. File group child relationship

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



Assigning executable files to File Groups

Now that you have created the File Groups – and eventually their parent-child relationships – you want to use, it is time to group executable files into those File Groups.

To assign files to File Groups

1. Activate either the *Database Explorer*, *Scan Explorer*, *Log Explorer*, or *Exe Explorer* module (click the appropriate icon in the Modules section of the *Control Panel* of the main window or use the *View→Modules* command). The system displays a list of executable files that have been recorded in the Sanctuary database.
2. Select (highlight) the file or a range of files you want to assign to a File Group by using the CTRL and/or SHIFT keys.
3. Right-click the mouse button and select ASSIGN TO FILE GROUP

– or –

Select *Assign* from the *Explorer* menu while in the *Database Explorer* or in the *EXE Explorer* module,

– or –

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

The *Assign Files to a File Group* window appears.

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

The *Suggested File Group* column proposes a File Group based on the filename. If a file with the same name already appears in the database (perhaps a different version of the same application), the system suggests the same File Group to which the earlier file belongs – typically a very appropriate choice.

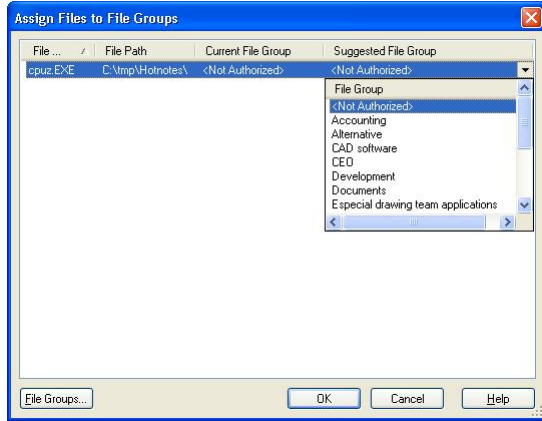


Figure 35: Assigning files to file groups

4. Select the File Group to which these files belong.

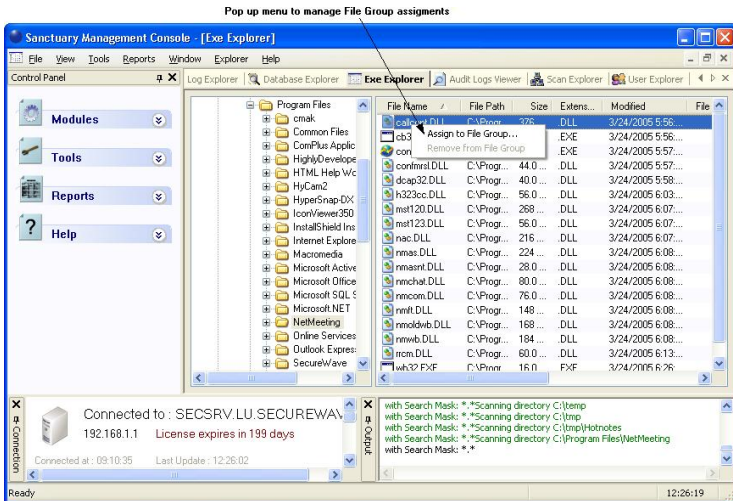


Figure 36. Assigning a File Group from the EXE Explorer module



You can perform the same action on files displayed in the Exe Explorer, Database Explorer, Log Explorer, or Scan Explorer module.



Changing file assignments

You may want to modify your file lists or file assignments under any of the following conditions:

- > 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 newer versions.
- > An executable file has proven to be corrupted or otherwise inappropriate, and you want to prevent users from activating it.
- > Multiple users are being required to locally authorize files that are centrally denied. This activity will be evident from log files, which show which files are being denied and then locally authorized. If, and only if, you are confident that the files can be trusted, you can add them to the Sanctuary database directly from the Log Explorer screen – not the preferred method. Users will be grateful that they do not have to authorize these harmless executables.

To change the File Group to which a file is assigned

1. In the *Database Explorer*, *Scan Explorer*, *Log Explorer*, or *Exe Explorer* module, select the file or range of files to reassign.
2. Right-click on the selected file(s) and use the *Assign Files to File Groups* command to display the corresponding dialog.
3. To accept the suggested File Group click OK. To choose a different one, select once more the file(s), click the FILE GROUPS button or the *Suggested File Group* list icon and select it.
4. Click OK. The new file assignment details are recorded in the database.


To remove a file from a File Group

1. In the *Database Explorer*, *Scan Explorer*, *Log Explorer*, or *Exe Explorer* module, select the file or a range of files to remove from a File Group.
2. Right click and select *Remove from File Group*. 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 Sanctuary database altogether

1. In the *Database Explorer* screen, select the file or range of files you want to delete.
2. Right click and select *Delete* from the pop-up dialog box. Click OK.

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

Viewing file assignments

The *Database Explorer* module shows all the files that have been recorded in the Sanctuary database—their internal system ID, filename, extension, location (path), and the File Group to which they have been assigned. It also shows the parent-child relationship (if any; using the Groups tab) for all defined File Groups.

Here is a typical Database Explorer listing:

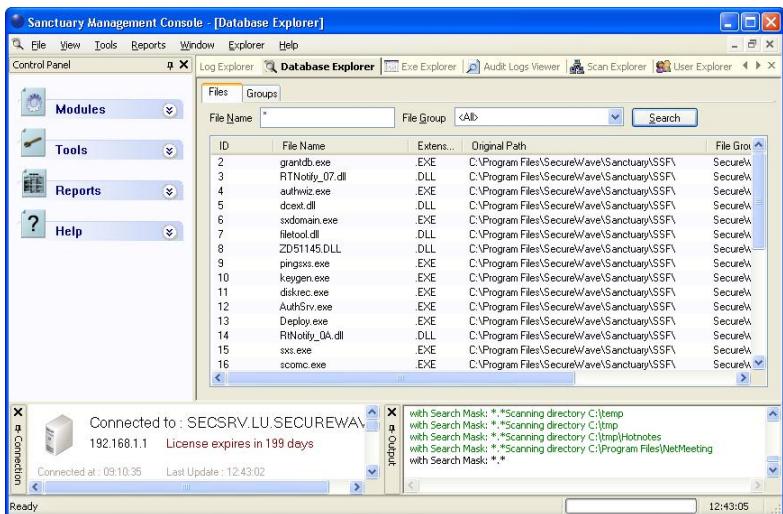


Figure 37. The Database Explorer Module

This module works just like a typical Windows Explorer program.



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

Click any column header to sort the 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 is the internal Sanctuary database ID, for information purposes only.

To display just a subset of all 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.

From this display, you can change the File Group assignment for a file, delete the file from a File Group, or delete the file from the Sanctuary database, using the steps described earlier in this chapter.

Using the Groups tab

The Groups tab is used to create, modify, or delete parent-child relationships between File Groups. For a complete description, please refer see *To create a parent-child relationship between File Groups* on page 73.



Chapter 7: Authorizing software 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 will not run. Normally this is the desired behavior, since malicious programs may change or add executables invalidating their Hash.

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:

Recursive: force the path rule to apply to all files in subfolders of the root folder defined in the path field.

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.



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:

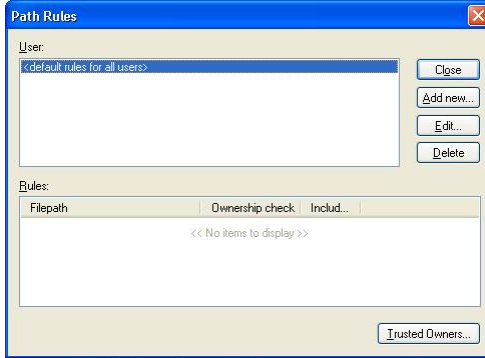


Figure 38. The Path Rules Dialog

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

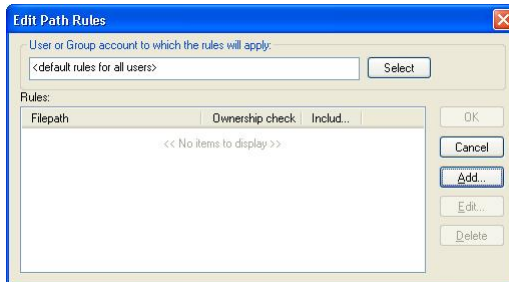


Figure 39. Editing the Path Rules

3. Click 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*. If you want to traverse all the subfolders beginning from the root, select the *Include subdirectories* option.
6. Click on the *OK* button to close the *Path Rule* dialog.



7. Click 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:

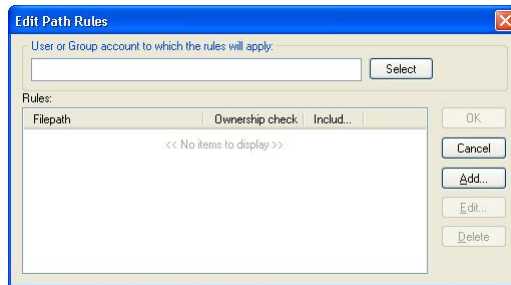


Figure 40. Adding a Path Rule

3. Type the name of a User or User Group to whom the path rule will apply, or click **SELECT** to search for and choose a User or User Group.
4. Type the name for the path rule. If you want the rule to apply only to executable files of a Trusted Owner, activate the *Ownership Check*. If you want to traverse all the subfolders beginning from the root, select the *Include subdirectories* option.
5. Click **ADD** to accept the path rule but keep the *Path Rules* dialog open. 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 or uncheck the *Include subdirectories* and *Ownership Check* options as appropriate.
4. Once you finish 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 **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 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 will not be 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 from 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 will only permit execution of files owned by an account who is a Trusted Owner. Note that an account not specified explicitly as being a Trusted Owner will not be consider as such, even if this account is 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 the TRUSTED OWNERS button in the *Path Rules* dialog. The following dialog appears:

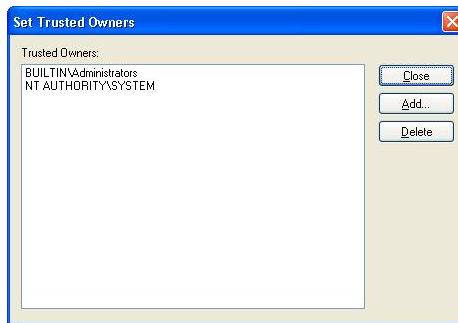


Figure 41. Setting Trusted Owners

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 87) 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 will 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.

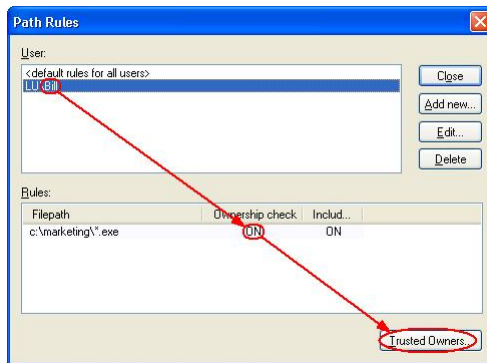


Figure 42. Setting Path Rules with Ownership Checking

5. The situation changed radically from that described in step 3. Bill will not be 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 will run or not depending on the defined Path Rule:

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

Table 13. Resulting permissions when applying Path Rules



Chapter 8: Assigning access permissions to users and groups; the User Explorer

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

A small organization might simply define a standard set of approved applications and grant all users access to this accepted set. However, most organizations will want to differentiate between diverse types of users, and grant users access only to the applications they need to do their jobs.

For example, you might want to grant access to the Web server functions only to your designated Webmaster. Similarly, you might grant access to database servers only to authorized database administrators or Accountable software only to your designated bookkeeper. This control strategy minimizes the chance that systems would be exposed to harm – either accidental or deliberate.

If you have already gathered a list of executable files that will be managed, organized those files into logical File Groups, and defined users and user groups, now you are ready to connect the dots. It is time to assign File Groups to users/user groups, to define who can do what.



Sanctuary Server Edition manages servers, so by default, your 'users' will be server administrators. For the purposes of this chapter – and to differentiate them from Sanctuary system administrators – we will refer to these server administrators simply as 'users.'

Granting users permission to use designated File Groups is an easy point-and-click process done in 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/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 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 will prompt 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

Your users will not be allowed to run a program (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 (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.

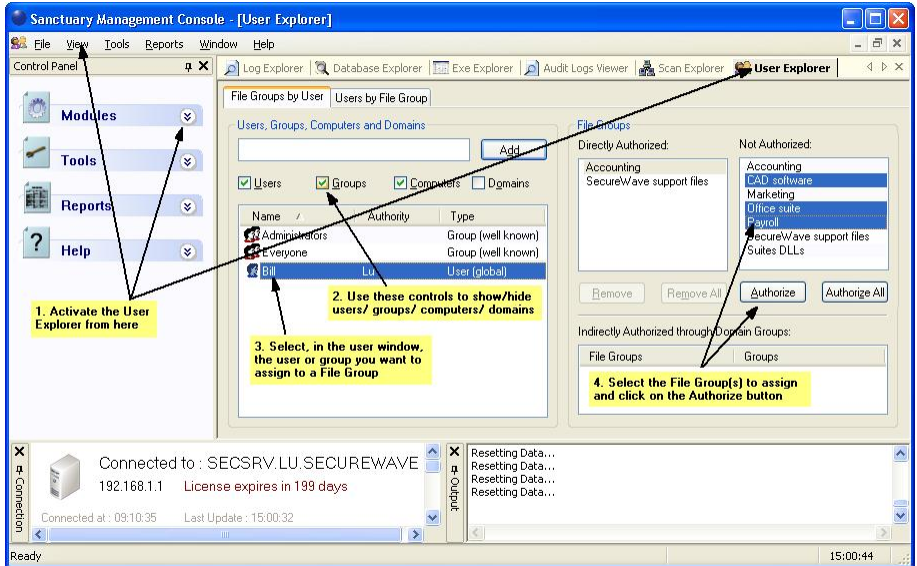


Figure 43. The User Explorer Module Window: File Groups by User

4. If you want to activate 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 from the *Control Panel*) and select the computer from there.

If you do not push updates to protected clients, they will automatically receive updates at next 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 13: Setting system options on page 141.



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, you may 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 (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 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. 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.

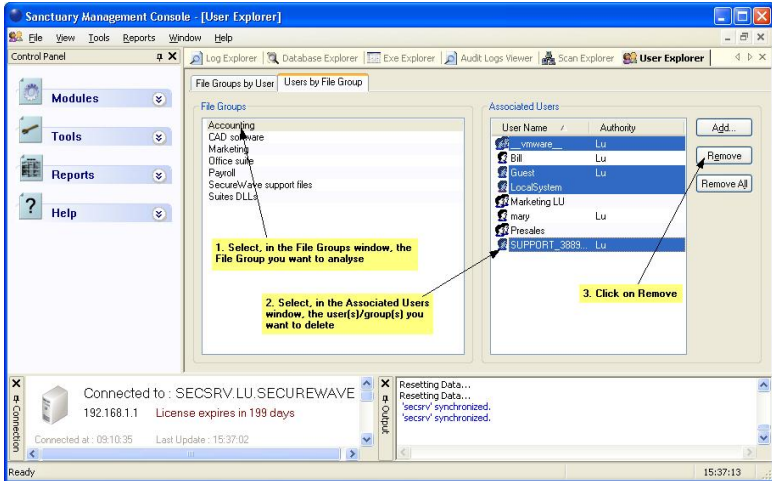


Figure 44. The User Explorer Module Window: Users by File Groups

Users and user groups



If you are using Sanctuary Server Edition, normally your 'users' are server administrators rather than end users. Typical users are your Webmasters, email administrators, and database management specialists – members of the IT team who need access to the organization critical server's functions. In this section, we will refer to them as 'users', although they are not IT end users in the typical sense of the word.

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

- > The Sanctuary client driver checks the digital signature of the requested application against those approved ones stored locally.
- > If the application is on the approved list, then the program runs. Only authorized applications assigned to a user or a user group from which this user is a member can run on the client.
- > Finally, the software grants or denies the ability to run the application.

The following section describes the process of setting up users and user groups File Group authorizations.



You can also find other useful information in these sections:

- > *Chapter 5: Building a list of executable files to be managed* on page 53, describes several key ways to populate the database of approved applications.
- > *Assigning File Groups to users*, in this chapter, describes the process of linking approved files and approved users to establish a robust security strategy.

Direct, indirect, and not authorized File Groups

Most of the time, File Groups are associated to Domain User Groups to minimize management overhead. New group members automatically inherit the right to execute applications assigned to the group.

Permissions may be granted 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. That user can use all programs that are authorized for the user groups of which he is a member.

The following image shows an example of the domain user 'Bill' having two File Groups indirectly authorized because of assignments made to Domain User Groups from which he is member, several not authorized, and four File Groups directly authorized to him.

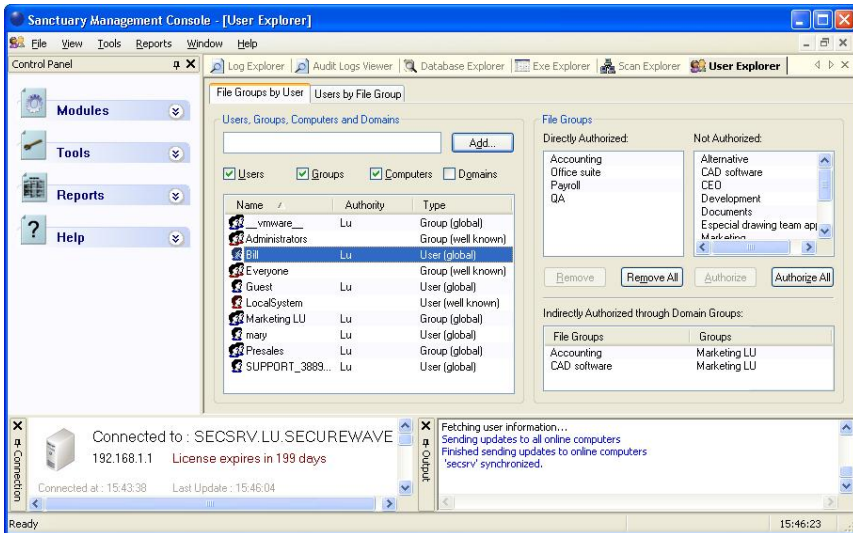


Figure 45. A user having several File Groups indirectly authorized



The Sanctuary system recognizes and embeds the 'well-known' groups that are normally found on each of your computers: 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 each 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

This is a built-in account that is used to run services on Windows 2000, XP, and 2003 operating systems. Services run under dedicated accounts like LocalSystem. You must grant these accounts the right to use the corresponding File Groups. 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 preset in non-blocking mode to simplify day-to-day management issues. You can change this default setting. See Setting default options for users and groups on page 151.

Domains

These are the users, groups, and computers contained in each domain, as 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:

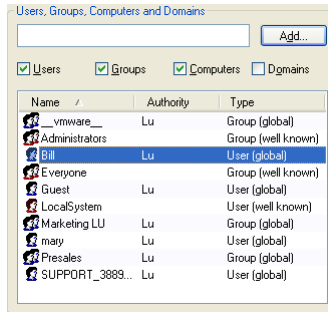


Figure 46. User's tree



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



Chapter 9: Monitoring system activity; the Log Explorer

Every server or computer under the protection of Sanctuary generates activity logs that record application attempts, denials, and, optionally, authorizations. This information 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:

- > 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:

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

You should be aware of the following limitations while using the Log Explorer module under other user/domain account:

<i>Possible configurations</i>	<i>Domain type</i>	<i>Logged user*</i>	<i>Result</i>	<i>Notes</i>
SXS & SMC are running on the same machine	n/a	Current user	Works properly	If SXS and SMC are running on un-trusted domains, the configuration may not work
		Other user	Would not work	DCOM error when using the Log Explorer module
SXS & SMC 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 or




<i>Possible configurations</i>	<i>Domain type</i>	<i>Logged user*</i>	<i>Result</i>	<i>Notes</i>
				Windows 2003 SP1 or SR2)
SXS & SMC are running on different machines	Un-trusted domain	Current user	Would not work	
		Other user	Would not work	
*Current User = the same user that logged to Windows is the one that logs to SMC. See <i>Log in as a different user</i> on page 28.				
To correctly configure DCOM: <ol style="list-style-type: none"> 1. Run dcomcnfg.exe (Start → Run) 2. Select 'Component Services' and open the 'Computer' branch 3. Right click on the desired 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 SMC administrator and activate the 'Remote Activation' option. 6. Verify that in the 'Access Permissions' panel the chosen user has 'Remote Access' activated. 				

Table 14: Limitations while using the Log Explorer module under other user/domain account

Monitoring logs of application activity on your protected clients

The Log Explorer module of the Sanctuary management console provides a powerful way of monitoring system activity for designated users, computers, and other parameters.

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

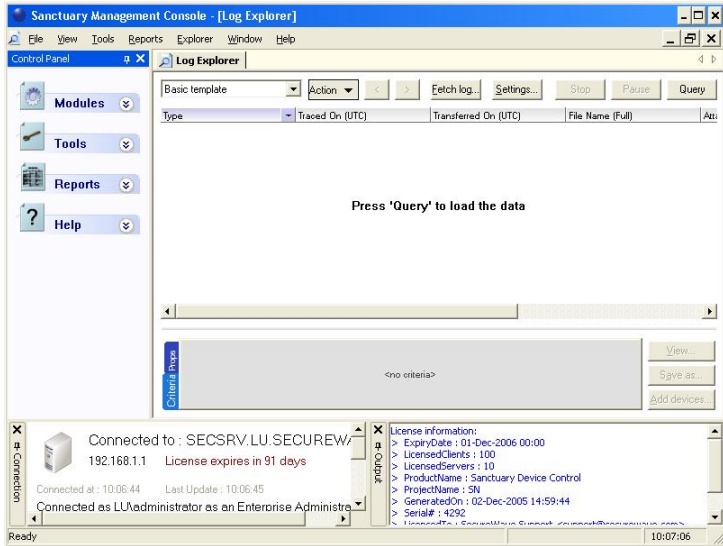


Figure 47. The Log Explorer main window

Basic operation

The operation of the *Log Explorer* module is based on templates. Although you can fully configure this module and its related templates, you can opt for a simpler approach using our predefined templates. You can, of course, create your own and save them as you progress in your work.



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

To use an already defined template:

1. Select a predefined template – created by SecureWave or by you – from the template list located in the upper left corner of the *Log Explorer* main window.
2. Click on the QUERY button.



Managing templates

What is a template

As you work in the *Log Explorer* changing criteria options, column size and order, which columns must be show in the window, 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 always save this template for future use. Your templates can be reloaded, saved with another name, renamed, deleted, imported, and exported as needed.

To create a template

Click on the ACTION button and select *New* from the list. You will see the template name change to New (o)* indicating that this is a new template and it has not been saved. After changing the required options, click once more on the ACTION button and select *Save As* from the list. Do not choose to save your template if you want to freely modify filters and other parameters without overwriting your original one.

You can see that a template needs to be saved when there is an asterisk [*] by its name in the template list.

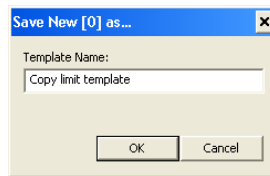


Figure 48. Saving your new template

To delete, save with another name, rename, import, and export a template

Once a template is created, you can delete, save with another name, rename, reload, import, and export it as needed. All this is done directly using the ACTIONS button and the corresponding command from the list. To use these commands (except Import), you must first select the template from the Template list.

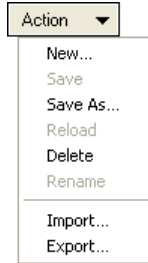


Figure 49. Managing your templates

- > New – to create a template as explained in the previous subsection
- > Save – to save your on-going work in a template
- > Save As – to save your template with a new name or used when creating a new template
- > Delete – to erase a previously created and selected template
- > Rename – to change the name of the active template
- > Export – to save to disk your template – to later import it or to make a backup copy
- > Import – to recover from disk a previously exported template. The imported template becomes the active one
- > Reload – Reopen the original template (only available when the template changes)

The Log Explorer window in detail

The main Log Explorer window is divided in 5 main sections:

- > A Navigation/Control button bar
- > The Column Headers
- > The Results window
- > The Criteria/Properties panel
- > A Control button panel

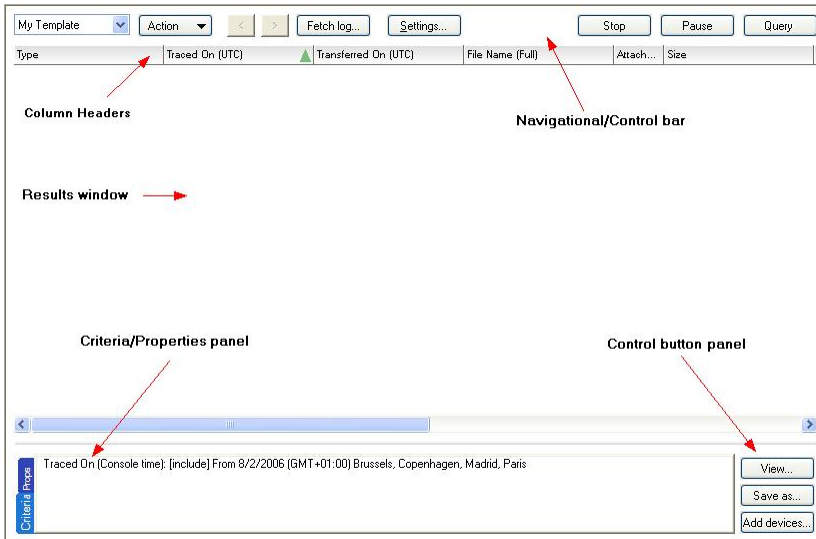


Figure 50. Components of the Log Explorer window

Navigation/Control bar

You can use the button bar on the upper part of the main window to navigate/control your results:



Figure 51. Navigation/Control bar

- > Template list – select a template from those created by you or by SecureWave. If you see an asterisk by the name [*], it means that the template needs to be saved since you recently modified a search or classifying parameter
- > Action – used to manage your templates (save, create, delete, rename, reload, export, or import a template). See *To delete, save with another name, rename, import, and export a template* on page 100
- > Previous – navigate to the preceding result list from the ones internally stored
- > Next – navigate to the subsequent result list from the ones internally stored
- > Fetch log – retrieve all client's logs (and shadow files if using Sanctuary Device Control)
- > Settings – go directly to the advanced settings dialog where you can select columns and define criteria



- > Stop – cancels the current query, usually when you want to interrupt a long classifying operation – involving a large number of log entries
- > Pause – cancels the screen output but the classifying process continues in the background. Click again on this button to continue the screen display
- > Query – recuperates all log entries corresponding to defined criteria

Column Headers

The column headers, besides being used as a title of the chosen column, can also be used to classify results. To sort ascending by a 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.

If you want to sub classify using another column, click once (or twice for descending order) on the column of the main criteria and then Ctrl-click once (or twice for descending order) in the secondary criteria column. You can see the result as a blue arrow in the column's title:

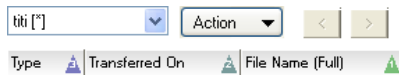


Figure 52. Column Headers

If you want to show/hide some columns, right click on the 'Column Headers'. You get a pop up menu from where you can hide/show the required column(s).



Figure 53. Show/hide columns



The options shown in *Figure 53* may be different depending on the installed license. If you want to clear the sorting filters, proceed to the *Settings* dialog as described in the next section.

The Settings dialog

If you want to access the detailed settings options, right click on the column header and choose *Advanced* from the menu or click directly on the blue arrow that appears when you place the mouse over the header. You can also click on **SETTINGS** button in the Navigational/Control bar:



Figure 54. How to open the Settings dialog

In all cases, the *Settings* dialog opens:

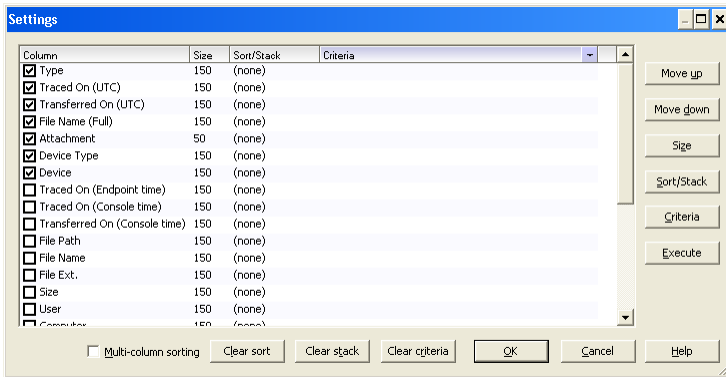


Figure 55. Settings dialog

In this dialog, you can:

- > Show/hide columns – simply check/uncheck the desired one(s)
- > Change the display size of a column – select the desired field, place the cursor over the size column, click, and change the size directly. You can also do it from the main window by dragging the heading divider
- > Sort ascending/descending and by several criteria – click on the sort/stack column and choose among the available options. If you want to do a multi-column sorting, select another classification from the Sort/stack column. You



can sort using several columns by selecting first the *Multi-column sorting* option located on the lower left part of the dialog

- > Stack by any field by clicking on the Sort/Stack column and selecting the *Stacked* option. When selecting a stack, all log entries in the main result window will be 'pile' in single entries. You can also add a total by selecting the Count column

Custom Message	Count	File Name (Full)
	75	[...]
ok-Hash	3096	[...]
ok-nonBlocking	2101	[...]
ok-nonBlockUser	668	[...]
Sanctuary has denied acces...	2	[...]
USB keys are forbidden in y...	4	[...]
You are not allowed to acce...	23	[...]

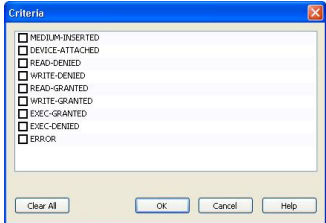
Figure 56. Stacking the query

In the previous image, the Custom Message is stacked and you can see the ellipsis indicating hidden log entries and the count column indicating how many entries are present.

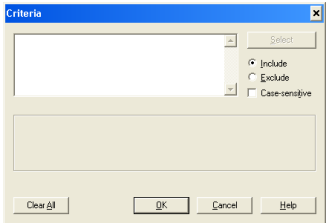
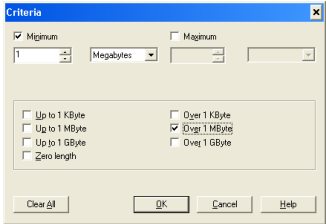
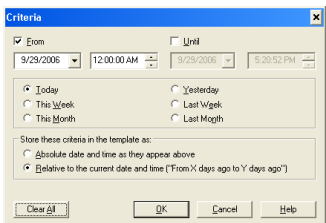
- > Decide the column displaying order – using the MOVE UP and MOVE DOWN buttons located on the right part of the dialog
- > Clear sorts, stacks, add or remove criteria, change the size of any column, and execute the query – using the corresponding buttons located on the lower and right part of the dialog
- > Allow multi-column sorting – as controlled with the *Sort/Stack* column option

Criteria are used to avoid clogging your result list with unnecessary data or to classify it in a more useful way to facilitate analysis.

Criteria dialogs are context dependent as shown in the following table:

Criteria Dialog	Description
	<p>Criteria List</p> <p>Dialog box displayed when log entry fields can only have a fixed set of values.</p> <p>Check or uncheck the boxes that correspond to the values you are looking for.</p> <p>Examples: (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</p>



<i>Criteria Dialog</i>	<i>Description</i>
	<p>because of matching path rules, set this checkbox as well and the query will return log entries related to these two types of authorized execution.</p>
	<p>Free-text criteria</p> <p>This dialog is used to filter the query results based on any text that you type in.</p> <p>Enter the text you want to search in the field. You are allowed to use wildcards (? to match any single character and * to match any sequence of zero or more characters). If entering several strings, separate them by using semicolons (;) to get log entries matching any of the strings specified. You can further specify – by using the corresponding controls on the right part of the dialog – if the search should be case-sensitive, and whether the query should return entries that include or exclude the entered strings.</p> <p>Examples: to search all log entries that contain main executables run by users, enter "*.exe" (without the quotes). To additionally get 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 dialog – only meaningful if you also use Sanctuary Device Control – is used to show event logs for shadow files based on their size.</p> <p>The query will return log entries concerning files with the size specified manually in the "minimum" and "maximum" controls. You can alternatively use one of the predefined commonly used sizes by clicking the corresponding checkboxes.</p>
	<p>Time criteria</p> <p>This 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 manually into the "from" and "until" controls, or click one of the most commonly used time ranges settings. You can further specify how these time criteria are stored in the template; this has an influence on how the time criteria you specify will be interpreted if you execute again this query.</p> <p>If you select to save your settings as absolute values,</p>



<i>Criteria Dialog</i>	<i>Description</i>
	<p>there are considered as unconditional parameters. As an example, a query for all log entries produced between May 21st 2006 and May 23rd 2006 will always return the log entries produced between these two dates.</p> <p>If, on the other hand, you select to store the values as relative ones, those values will be converted to a comparative time span relative to the current date and time.</p> <p>For example, if on May 23rd 2006 at 10:00 you query for entries generated after May 23rd 2006 9:00, and select "relative time", the criterion will be stored as "return all entries generated in the last hour". If you run again this query on June 12th 2006 at 11h30, you will get all entries generated during the last hour, i.e. after June 12th 2006 10h30.</p> <p>If you set the criteria to be stored as relative time and select one of the predefined periods, they are reevaluated each time you run again the query. For example, if on May 23rd 2006 you query for all entries generated "last month", you will get all entries generated between April 1st and April 30th. If you set this criteria to be stored as relative time and run the query on August 17th, you will get all entries generated between July 1st and July 31st.</p>

Table 15: How to use the available criteria dialogs

Some of them contain predefined values – you only choose the required options from a list. Others are free context dialogs where you can type in what is needed using wildcards to delimit the criterion. For example, if you are using the "File Name" column criterion, you can directly type `wind*.*` to search for all files matching this pattern (beginning with 'wind' and with any extension).

In some of these dialogs, you can also choose to include or exclude those entries matching a criterion while others have a **SELECT OR SEARCH** button (for example, those of the computer or user fields).

Once a criterion set, you can see it in the *Criterion/Properties* panel after closing the dialog and clicking on the **QUERY** button (or by directly clicking on the **EXECUTE** button of the Settings dialog).



Column	Size	Sort/Stack	Criteria
<input checked="" type="checkbox"/> Type	150	(none)	
<input checked="" type="checkbox"/> Traced On (UTC)	150	(none)	
<input checked="" type="checkbox"/> Transferred On	150	(none)	From 5/10/2006 10:42:44 AM (GMT+01:00) Brussels, Copen...
<input checked="" type="checkbox"/> File Name (Full)	150	(none)	win*. *
<input checked="" type="checkbox"/> Attachment	50	(none)	
<input checked="" type="checkbox"/> Size	150	1st, Descending	>1000
<input checked="" type="checkbox"/> User	150	Stacked	LU\Bill
<input checked="" type="checkbox"/> Computer	150	(none)	
<input checked="" type="checkbox"/> Device Type	150	(none)	
<input checked="" type="checkbox"/> Device	150	(none)	
<input type="checkbox"/> Traced On (Endpo...	150	(none)	
<input type="checkbox"/> Traced On (Console)	150	(none)	
<input type="checkbox"/> File Path	150	(none)	
<input type="checkbox"/> File Name	150	(none)	
<input type="checkbox"/> File Ext.	150	(none)	
...

Figure 57. Example of filter settings

Results window

This is the main area of the *Log Explorer* window where the results are displayed and classified. You can save this data as a CSV file using the **SAVE AS** button of the *Control button bar*.

Criteria/Properties panel

This window has the double functionality of showing you the applied data criteria and the properties for those chosen registers of the main window.



Figure 58. Filter/Properties window

Control buttons panel

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

- > View – Not used if you do not have Sanctuary Device Control. See the Sanctuary Device Control Administrator Guide for more details.
- > Save as – to save the *Main Result Window* data as a CSV file
- > Add devices – Not used if you do not have Sanctuary Device Control. See the Sanctuary Device Control Administrator Guide for more details.

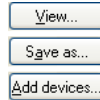


Figure 59. Control button bar

Sorting and applying criteria to specific fields

You can use the *Settings* dialog (see *The Settings dialog* on page 104) to:

- > Define criteria for the Query (and execute it)
- > Set display option like which columns are displayed, the sorting order, stacking process, etc.
- > Change column order and size

On the Result Window 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
- > Which File Groups were assigned to which files

You may or may not see some of these entries. This depends on the role assigned to you by the Enterprise Administrator.

For instructions on how to define a query, see *Table 15* on page 107.

When you have selected all columns, close the *Settings* dialog and click the **QUERY** button or click directly on **EXECUTE**. The resulting log entries are shown.



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 will be all event for that user that occurred between the selected dates.

If there are any records that match your query criteria, they appear in the results window list. Query will only return results if you have the corresponding access rights (see *How to set up a Sanctuary system administrator* on page 49).



Available columns

You can control the visibility, size, and position of a column from the *Settings* dialog. Right click on any heading or click on the blue arrow shown in the right end of the column title available when you place the mouse over that zone.

The following table summarizes the column meaning:

<i>Column</i>	<i>Description</i>
Access	Show the status of the file as defined on <i>Table 17</i> .
Computer	The name of the machine where execution was attempted.
Count	If stacking is active, shows how many log entries are hidden.
File Ext	The extension of the file.
File Group	The file group to which the file has been assigned. Can also be <Not Authorized>.
File Name	The file whose execution was authorized or denied.
File Name (full)	Contains the full name (including path) of the file whose execution was authorized or denied.
File Path	The path of the file whose execution was authorized or denied.
Hash	The digital signature of the file, created by SHA-1 (Secure Hash Algorithm -1). Knowing the hash enables you to differentiate files with the same name.
Traced On	The date and time the file execution attempt was traced.
Transferred On	The date and time the log file was transferred to the SecureWave Application Server.
Type	The nature of the event that triggered the log – Execution Granted or Execution Denied.
User name	The name of the user who attempted to execute the file.

Table 16: Log Explorer module column meaning

The Access field will show any of the following values, which are affected by system-wide option settings for Execution Blocking and logging mode:

<i>Value in the Access Field</i>	<i>Description</i>	<i>The file ran?</i>
Authorized	This file is known, its digital signature is recorded in the Sanctuary database. If this file has been assigned to a File Group, it is also shown.	Yes
Denied	The file was not allowed to run because it was neither centrally nor locally authorized.	No
Logon	This file was allowed to run because 'Relaxed logon mode' was active (Relaxed logon option). See <i>Individual options</i> on page 147 for more details.	Yes
ok-dllDontCare	The DLL execution was authorized because the Execution Blocking option was set to 'Ask user for *.exe only.'	Yes
ok-hash	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
ok-localAuth	This file would have been denied because it is not centrally	Yes



<i>Value in the Access Field</i>	<i>Description</i>	<i>The file ran?</i>
	authorized, but the user was prompted to locally authorize, and he/she allowed execution.	
ok-nonBlocking	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
ok-nonBlockUser	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
ok-pathRule	This file was allowed to run because it matched a Path Rule.	Yes

Table 17. Possible Access Field Values

Interpreting the Log Explorer data

You can interpret data from the Log Explorer window in several ways. Regarding those marked as Denied on the Access column, there are two common cases to refuse file execution:

- > The file is unknown and, hence, it is not authorized. It has never been scanned, does not exist on the 'white list' and, if it is a recurring file, you should investigate further the origin. The two possible scenarios of unauthorized applications are:
 - 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.
 - The software has not been authorized and should be, to conduct your business.

It is inherently dangerous to authorize executables directly from the Log Explorer unless you are sure that the software can be trusted – a user can try to fool you by renaming an unauthorized application. As an example, a user renames an unauthorized file as 'notepad.exe' and then complains that his notepad is not working. Check first the program.

- > If the column *File Group* is different from <Not Authorized>, the file has been scanned and it is known, in the 'white list', and belongs to a File Group, for example, Accessories. The user simply has no access to that File Group. In this case there are also two different scenarios:
 - This is a 'normal' situation. A user is trying to run a program to which he has no rights.
 - The user must be able to use this file and this situation should be corrected giving the user, or one of the groups he belongs to, access to the corresponding File Group.



Local authorization deserves special attention. Does the user use this file frequently? Maybe you should scan the file and include it on a special File Group to avoid having several users locally authorizing the application.

The log entries displaying ok-dllDontCare are special case of 'Local Authorization' where the user only authorizes the EXE file (Ask user for *.exe only) and all DLL are automatically authorized. See *Chapter 13: Setting system options; using the Exe Explorer* on page 141.

Using the Log Explorer to authorize unknown files

You can query the Log Explorer to show all authorization decisions made by users to override denials from central authorization. The results of this query may reveal that certain executables are frequently needed by users to complete their work. They should be included in the Sanctuary database to be centrally authorized. If a user is complaining that he needs certain executables to do his daily work, you can see here those used by this user and decide to authorize them or not.

If you are confident that the files can be trusted, you can authorize them directly from the Log Explorer module. You do not have to use other module to do this.

To authorize a new executable from the Log Explorer module

1. Select a file or range of files in the *Log Explorer* display.
2. Right click the mouse button. The system displays the *Assign Files to File Groups* dialog.
3. From the pull-down list located on 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'. 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 to authorize applications only from trusted sources.

Forcing an upload of the latest log files

At the time specified in the system options, protected clients upload their log information to the SecureWave Application Server. However, you may need to view recent log information. This information can 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


1. Activate the *Log Explorer* module, if it is not already open. Click on the Log Explorer icon  located in the Modules section of the *Control Panel* of the main window or use the *View→Modules* command.
2. Select *Fetch Log* from the *Explorer* menu or use the *FETCH LOG* button of the dialog. 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 those computers that have the Sanctuary client installed.



Figure 60. Fetching New Logs

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


Saving application execution logs to a CSV (comma-separated values) file

You can save your logs to this file format and then recover them with other CSV editing or viewing tools, for example, Excel, WordPad, etc.



Chapter 10: Monitoring Sanctuary system administrator activities; the Audit Logs Viewer

Sanctuary keeps a full audit trail of all activities carried out by its administrators. You can view records of changes made to files, File Groups, and assignment of those resources to users and User Groups. If you have appropriate administrative privileges, you can use the *Audit Logs Viewer* module of the Sanctuary management console to monitor this activity.

You can access the *Audit Logs Viewer* by clicking on the  icon located on the *Modules* section of the *Control Panel* of the main window.

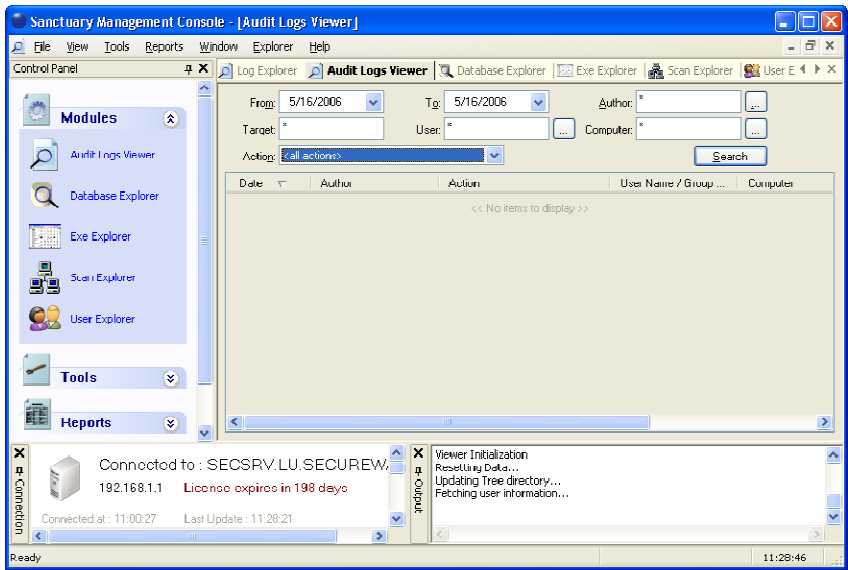



Figure 61. The Audit Logs Viewer Module



If the 'Audit (Application Control)' access of the Sanctuary Management Console Administrator User Access is set to 'No', the currently logged-in administrator is not able to see or use the Audit Logs Viewer module. Please refer to Chapter 4: Setting up a Sanctuary system administrator on page 49 for more details.



To view system administrator activity

1. Click on the *Audit Logs Viewer* icon  located in the Modules section of the *Control Panel* of the main window or use the *View→Modules* command. The system opens an empty *Audit Logs Viewer* screen.
2. Enter the dates in the *From* and *To* fields, and click on the *SEARCH* button. The system displays a list of all changes made to permissions between those dates. If you do not enter dates, the system displays today's changes.



If you have the full administrative rights of a Sanctuary Enterprise Administrator, you can view all logs. If you have the restricted privileges of a Sanctuary Administrator (and your network runs under a domain where Active Directory delegation is used – using Windows 2000/2003 Active Directory), you can view logs for the clients and users in your span of control.

Search options

There are several options you can use to search information in the Audit Log. They are found on the upper panel in the right side of the *Audit Logs Viewer* window.

You can do a search by Date, Author, Target, User name, Computer, or/and Action using as many criteria as you want or need.

The first of these possible searches is the *Date* search. You can directly type the dates in the *FROM* and *To* boxes, and then click the *SEARCH* button. A list of all the changes made to permissions between those dates is displayed. You can alternatively click on the down arrow to show a calendar where you can pick the dates graphically:

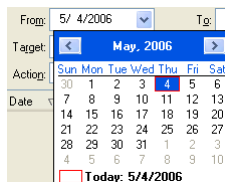


Figure 62. Using the calendar pull-down to select a search date



Sanctuary Application Control Enterprise Administrators have access to all audits. When running under a Windows Active Directory based domain, the Sanctuary Application Control Administrator will be only shown audits of computers and users he is allowed to manage.

The second way of searching is by using the author's name. The Author, in this context, is the Administrator that authorize a file. You can type the name (including wildcards *,?) in the *Author* field or click on the ellipsis (...) button at one side of the field to get a search dialog:



Figure 63. Using the Author field to do a search

You can choose the user directly from this dialog or use the SEARCH button located to the right of the *Name* field.

The *Target* search field lets you search by the different File Groups, Path rules, and files available in the system. You can type wildcards (*, ?) to limit the search. Using this field not only can you search by File Groups, but also by User access, option names, and authorized files.


When using the *Target* field you get a different set of information than that normally received for a File Group. You can get, for example:

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



If you want to know who changed an option and when, type the option or part of it (using wildcards, for example, block to get all "Execution Blocking" changes) on the Target field.*



With the *User* search field, you can quickly find all authorization changes done by an Administrator for a particular user. As an example, you want to find out what authorizations were granted to the user 'Bill', you can type b* in the user field. As with almost all the other fields, you can use wildcards (*, ?) in the user name specification. You can use the ellipsis  button to do a quick user name search.

With the *Computer* search field, you can do searches to monitor the changes done in certain computers. The names defined here are the same ones used in the *Computer Name* tag of the Windows' *System Properties* dialog. Since file authorizations are done at the user/user group level, this column has no use for application control.

You can alternatively choose the action to list in the *Action* field. Click on the arrow to show a list of all available options:

- <all actions>
- ADDED FILE
- ADDED FILE GROUP
- ASSIGNED FILE TO FILE GROUP
- AUTHORIZED USER
- AUTOMATIC USER ACCESS UPGRADE
- DELETED DEFAULT OPTION
- DELETED FILE GROUP
- DELETED OPTION
- MODIFY USER ACCESS
- PURGED DB AND FILE STORAGE
- REMOVED FILE
- RENAMED FILE GROUP
- SET DEFAULT OPTION
- SET OPTION
- UNASSIGNED FILE FROM FILE GROUP
- UNASSIGNED FILE TO FILE GROUP
- UNAUTHORIZED USER

Figure 64. Using the Action Field to do a search




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 dates and then an action, the resulting data will be the Boolean combination of the dates plus the action.



Actions

Once you have the search list shown, you can do the following actions:

- > Change the size of the displaying field to suit your needs. You must place the cursor in the dividing trace and wait until the mouse cursor changes into a double head arrow: 
- > Sort the list in any order by clicking on any of the column headers. Click once to sort ascending, twice to get a descending order

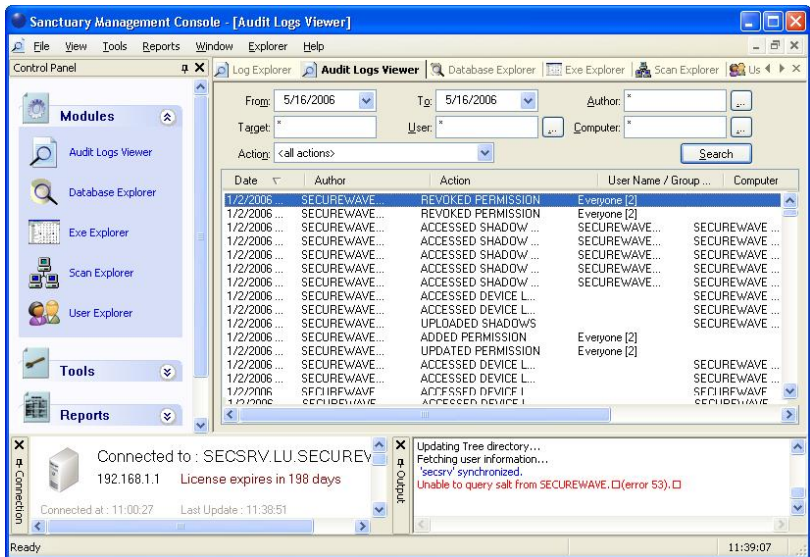


Figure 65. Using the sorting facilities of the Audit Logs Viewer Module

- > You can right-click on any field of any item, and choose to filter on that item, restricting the displayed list to those items that match the filter. If you have applied a filter, then right clicking again allows you to remove the filter

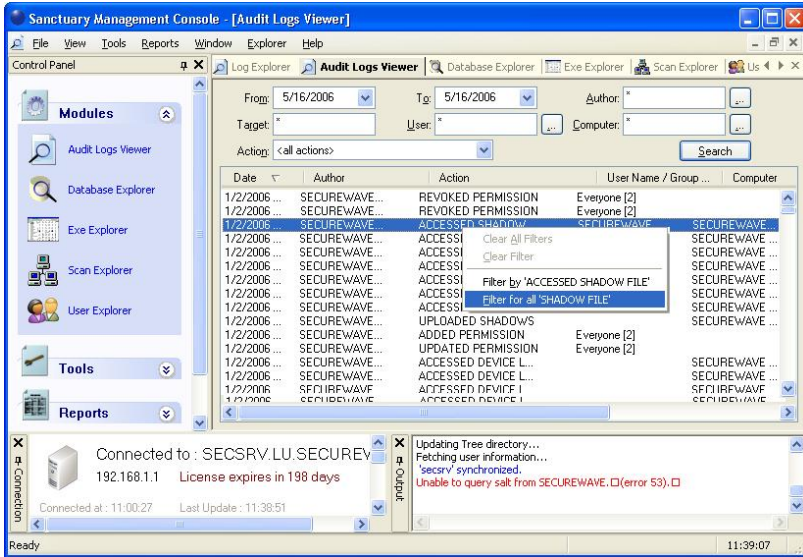


Figure 66. Filtering actions in the Audit Logs Viewer Module

Notice that the pop-up menu changes depending where the cursor is located. If, for example, you have the cursor on the *Everyone* word on the *User Name/User Computer* field, the filter is:



Figure 67. A filtering pop-up dialog example

This is different from the pop-up window you see when the cursor is located on the *Action* field in the option *Accessed Shadow Action*.

You can clear all filters by using the contextual menu or the *Explorer* → *Clear all Filters* command.



The *Audit Logs Viewer* displays the following columns:

<i>Column</i>	<i>Description</i>	
Date	Informs you of the date when the administrator did the action. This field is always present.	
Author	Contains who created the action. This field is always present.	
User name/group	Name of the user or user group to which the action was applied.	
Computer	Computer name of the machine that was the target of the action, if any. It is empty if a modification was made to the 'default setting'. Contains the name of the computer in case a computer-specific action was done.	
Target	File, group, path rule, file group, etc.	
Information	Additional information related to the corresponding register (if applicable). This field shows more details in some cases. For example, if a Sanctuary Administrator erases an authorization, its parameters are included here.	
Action	A code describing the action performed by the administrator. This field is always present. Actions may be:	
	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	
	Deleted File Group	This File Group was erased.
	Deleted Option	This option was removed for the specified user or machine.
	Modify User Access	A change was made to this user's role.
	Purged DB and File Storage	This routine database maintenance was performed.
	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 Tools → Default Options menu or from the Control Panel), the option being changed and the user/machine are traced
	Set Option	This option was created for the specified user or machine.
Set User/Machine Option	A change was made to this option for this machine or user.	



<i>Column</i>	<i>Description</i>	
	Unassigned File from File Group	This file was removed from this File Group.
	Unassigned File to File Group	
	Unauthorized User	This user's permission to use the named File Group was revoked.

Table 18. Audit Logs Viewer Result Information

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 12: Generating reports of Sanctuary records and settings* on page 133.



Chapter 11: Sanctuary's database; the Database Explorer

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

- > The lists of executable files
- > The digital signatures ('hashes') that uniquely identify those files
- > The File Groups
- > The authorized users and user groups
- > File Groups parent-child relationships

This database is created on the Microsoft SQL Server 2000/2005, SQL Server 2005 Express Edition, or on the Microsoft Database Engine (MSDE). For organizations with fewer than 200 users, the SQL Server 2005 Express Edition is sufficient. Larger organizations will want to use the Microsoft SQL Server. Please note that there are inherent limitations when using SQL Server 2005 Express Edition (for example, 4 GB database limit) specified in the Setup Guide.

The Database Explorer module of the Sanctuary Management Console is the primary tool for viewing and managing database records.

This chapter describes the following database management functions:


- > Viewing database records
- > Performing routine database maintenance
- > Backing up the Sanctuary database
- > Removing old execution logs and machine scans

Viewing database records

The Database Explorer module displays a list of the executable files for which digital signatures are found in the Sanctuary database – and the File Groups to which they have been assigned.



To activate the Database Explorer module

Click the *Database Explorer* icon  located in the Modules section of the *Control Panel* of the main window or use the *View→Modules* command. The system displays the Database Explorer screen, as seen in the following image. If your database includes a very large number of executable files, there may be a slight delay before this list appears when you click on SEARCH.

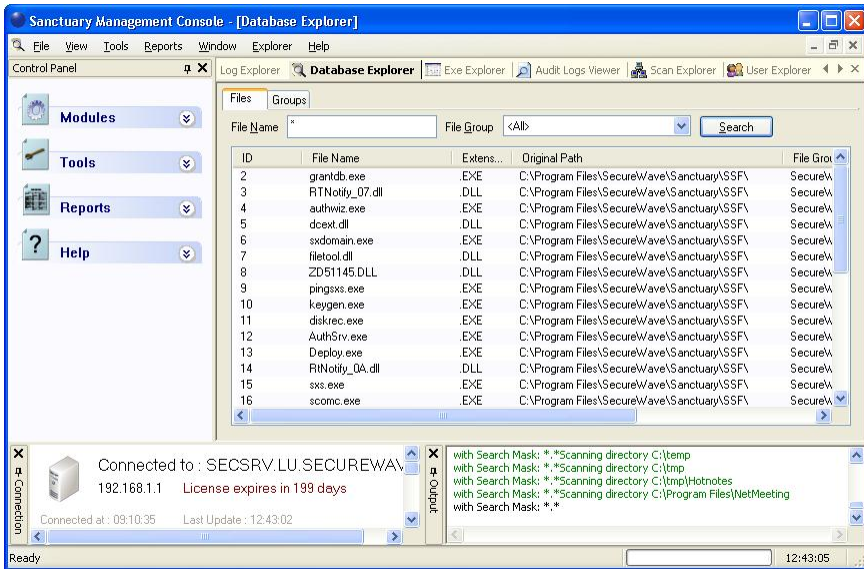


Figure 68. The Database Explorer Module

This display works just like any familiar Windows Explorer display.

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

Click any column header to sort the 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 is the internal Sanctuary database identifier, and it is shown only for information purposes.



To expand the display to show/hide other columns

Right click on the header row of the *Database Explorer* main window and add/remove the desired column(s).



Figure 69. Selecting columns to show in the Database Explorer Module

If you wish to organize them, click on the *Choose Columns* item. The *Choose Columns* dialog appears from where you can select and classify all available report columns. You can also change the width of each individual column here using the provided field located at the bottom of the dialog.

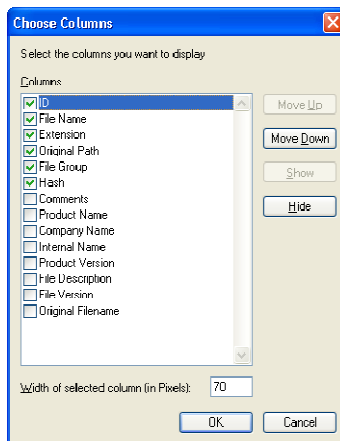


Figure 70. The Choose Columns dialog

To save this list as a CSV file (comma-separated values)

Select the *File Save As* item from the *File* menu. This option is useful to import the resulting information into third party reporting tools.



Performing routine database maintenance

Synchronizing Sanctuary accounts with Microsoft 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 seldom need to perform this function. If you are using the program in a Novell environment, you should run our Synchronization Script. Please check the *Setup Guide* for further information.


To synchronize domain members


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




Figure 71. Synchronizing Domains

2. Type in the name of the domain to be synchronized and click on the OK button. The system will update its reference list of users and groups from the domain.

 *! If you enter a machine name (not a domain name), and the machine is a domain controller, this particular domain controller is used for synchronization. This feature can be useful when the replication between various domain controllers is slow and you cannot wait for user account information to replicate between all of them.*

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

 *You can also synchronize local users/groups of one or more machines in a domain. Use this feature 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 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. You can run this script manually from time to time (if there are not too many changes in your eDirectory structure) or automatically using scheduler software. See details in the *Setup Guide* and help file.

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 would add servers or computers in the workgroup individually.

1. Select *Synchronize Domain members* from the *Tools* menu (or from the *Control Panel*). The system displays the *Synchronize Domain* dialog.
2. Type the name of the computer you want to add.
3. Click on the DIFFERENT USER NAME button to display the following dialog:



Figure 72. Connecting as a Different User

4. Type in the user name (including server's name) and password for the local administrator of the machine you want to add.
5. Click OK twice to confirm both dialogs. The computer has now been added to the database, and you can assign privileges to its local users.



Backing up the Sanctuary database

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

Removing old execution logs and machine scans

As time passes, the database can accumulate a large number of activity logs and scan results. Older versions of these records consume unnecessary database space and may not be needed for your daily operations. You can periodically clean up the database by removing obsolete logs and scans. Do not forget to make a backup of your information before proceeding.

To delete all execution logs and scan results before a given date

1. Select *Database Maintenance* 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 – execution logs or machine scans.
 - Execution logs. Delete all execution logs before the specified date.
 - Machine scans. Delete the results of all scans before the specified date. This process cannot delete scan templates, which define how scans are performed, only scan results.
 - Device Control Shadow Files. This option is not available if you do not own a license for Sanctuary Device Control.
3. Enter the cut-off date in 'yyyy-mm-dd' format. Note that the default date is one month less than the system date.



The date format depends on your 'Regional Settings' configuration.

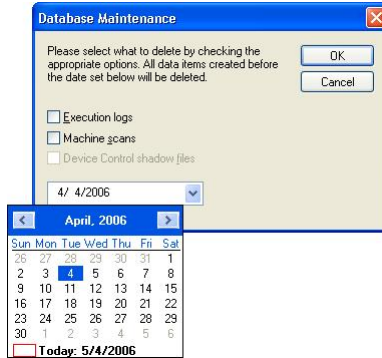


Figure 73. Database Maintenance

4. The system deletes the requested content from Sanctuary database tables and the SecureWave Application Server data file directory (see *Removing old audit logs of Sanctuary administrator activity* on page 129 for the location of this directory).



Make sure 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 period.



*This process does not purge audit logs of Sanctuary administrator activity. Those files can be manually removed if necessary. You can find them in the history subfolder of the DataFileDirectory. For more information, please see *Removing old audit logs of Sanctuary administrator activity* later in this chapter.*



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

Removing old audit logs of Sanctuary administrator activity

Audit log files

The system keeps a register of all actions in audit log files stored on the hard disk of the SecureWave Application Server. These files are defined on the



'DataFileDirectory' registry key of each SecureWave Application Server (if several data file directories are defined) located at:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sxs\Parameters\  
'DataFileDirectory'
```

The audit log files follow the naming convention, 'History SX (yyyy-mm-dd).log,' where *yyyy* represents the year, *mm* the month, and *dd* the day of the month.

These files are created in this location as the user works with the system. You can clean or remove those audit log files following the procedures outlined in the following sections.

To remove old audit logs of Sanctuary administrator activity

To delete the unnecessary audit log files from your system, you must eliminate them manually from the history sub-folder as defined on the 'DataFileDirectory' registry key (see previous section).



Do not forget to make a back up of these files if you wish to keep the information.

You can remove the history files one at a time or use Windows File Search function to remove all 'History SX *.log' files before a specified date. You should do this for every data file directory defined in your system.



Removing obsolete records of computer connections

SecureWave Application Servers keep a record of connected machines in an online table that is updated every time a user logs onto or unlocks a computer. Sometimes, machines are disconnected without notifying the system that they are not available anymore. In this case, orphan entries are left in the online connection table. This unnecessary data can affect the performance of the *Send Updates to All Computers* function, which conveys fresh hash lists throughout your organization.

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

If you need to do a manual update to have the most recent information, use the *Purge Online Table* item from the *Tools* menu (or Control Panel).

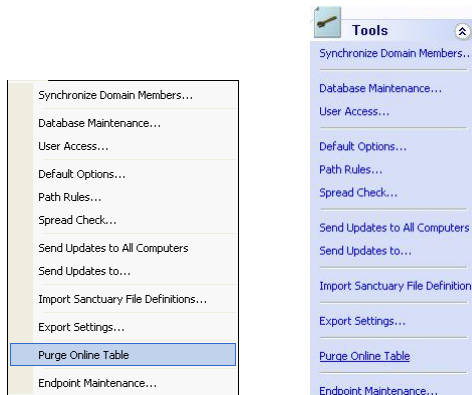


Figure 74. Purging the Online Computers Table



Chapter 12: Generating reports of Sanctuary records and settings

From within any module of the Sanctuary solution (*EXE Explorer*, *Scan Explorer*, etc.), you can easily generate HTML reports to view, save, or print. Simply select the *Reports* menu or module and choose one of the following:

File Groups by User

Generates a report of File Groups for the user or User Group you specify.

Users by File Group

Creates a report of users for all File Groups defined in the system.

User Options

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.

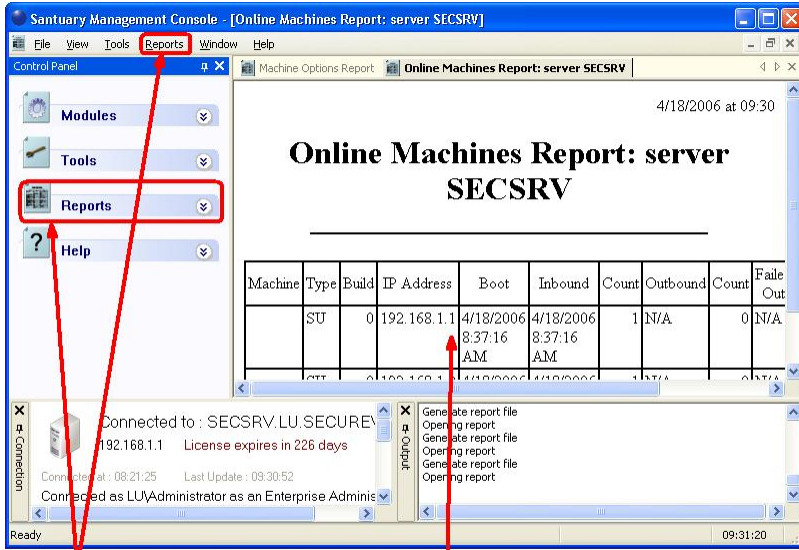
Machine Options

Generates a report of current machine option settings, such as when log files are uploaded to the SecureWave Application Server.

Online Machines

Creates a report that shows which machines are currently online and able to receive updated authorization information for the connected SecureWave Application Server.

The generated reports are HTML files that are viewed in an internal window. Once saved, you can view them using Internet Explorer or any other Web browser defined on your system. The reports can be printed, copied, converted, saved, and modified as required. Reports are provisionally created and saved in the Report folder located in your temporary directory – %TEMP%.



Select the desired report from the menu or Control Panel

You get the selected report in the main window panel

Figure 75. Obtaining a report

✍ Once the output is shown in the window, you can use the 'File → Save as' or 'Print' commands to keep a backup record of your reports. You also have access to the same right click menu as shown for a Web page in Microsoft Internet Explorer.

✍ You can change the way the date is formatted using the 'Regional and Language' options of the 'Control Panel' of your Windows system. Consult Windows' Help for details.

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



File Groups by User

Use this report to view all file groups assigned to a specific user(s). To generate this report, proceed as follows:

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

The report generated has a format similar to this one:

25/11/06 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 76. File Groups by User report



Users by File Group

Use this report to view users assigned to a file group. To generate this report, select *Users by File Group* from the *Reports* menu (or from the *Control Panel*).

The report generated will have a format similar to this one:

25/11/06 at 19:09

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 <<<

4. Windows 2003 Server

Administrators	(Well-known Group)
Everyone	(Well-known Group)
secure\Domain Users	(Domain Group)

Figure 77. Users by File Group report



User Options

Use this report to view the different user's settings. To generate this report, select *User Options* from the *Reports* menu (or from the *Control Panel*).

The report generated will have a format similar to this one:

2006-08-10 at 16:37

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 78. User Options report

Those options that have an asterisk (*) are the default ones.



Machine Options

Use this report to view the different machine's settings. To generate this report, select *Machine Options* from the *Reports* menu (or from the *Control Panel*).

The report generated will have a format similar to this one:

2006-08-10 at 16:44

Machine Options Report

Option	Machine	Setting
Client Hardening	Default	(*) Disabled
Sanctuary Status	Default	Show All
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 79. Machine Options report

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



Online Machines

Use this report to view all machines that are online when the report is generated. It also serves as a help with troubleshooting: you can find why a machine is not receiving updates when you send them. If the machine is not in the list, it will not receive updates. If the machine is in the list but its *Failed Out* counter is not zero, it can indicate a communication problem, configuration error, networking problems, network timeouts not configured, etc. To generate this report, select *Online Machines* from the *Reports* menu (or from the *Control Panel*).

This report lets administrators see which machines are currently online and able to receive updates to authorization information through the *Send updates to all* command.



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

The generated report will have a format similar to this one:

2006-08-10 at 16:46

Online Machines Report: server APPSERV1

M a c h i n e	Type	Build	IP Address	B o o t	Inbound	Count	Outbound	Count	Failed Out	Count	Consecutive
SecureWave	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 80. Online Machines report



Below is an explanation of the columns:

<i>Column</i>	<i>Description</i>
Machine	This column holds the computer's name of the machine found in the online table. A machine not listed in this table will not receive updates when using the Send updates to all or Send Updates to command on the Tools menu. The table updates when the client machine reboots or logs.
Type	This column holds the kind of client driver installed on the client computer: SN for Sanctuary Device Control client drivers version 3.1 or older; SX for Sanctuary client drivers version 2.1; SU for Sanctuary client drivers version 3.2 or later.
Build	Always zero.
IP Address	This column holds the IP address of the machine as registered in the online table.
Boot	The date and time the SecureWave Application Server last received a boot notification from the client machine. A value of 'N/A' indicates that the 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.
Inbound	This field contains the date and time the SecureWave Application Server last accepted a connection from the client computer.
Count	(Referring to the Inbound connection) Contains the number of connections accepted from the client computer by the SecureWave Application Server.
Outbound	This field contains the date and time of the last connection initiated from the SecureWave Application Server towards the client computer.
Count	(Referring to the Outbound connection) Contains the number of connections that the SecureWave Application Server initiated with the client computer.
Failed out	This field contains the date and time of the last unsuccessful connection between the SecureWave Application Server and the client computer.
Count	(Referring to the failed out connection) Contains the total number of connections that failed between the SecureWave Application Server and the client computer. This number will increase in the case of poor connections between the client and the server or in the case of high load on the server side.
Consecutive	Contains the number of consecutive connections 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



Chapter 13: Setting system options; using the Exe Explorer


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:

- > The default options for the *Exe Explorer* module
- > 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* (page 156).

 *Older versions of Sanctuary Application Control Suite will 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.*



Changes from previous versions

Options have changed from previous versions of Sanctuary Application Control Suite. You can find complete details in the readme file located in your installation CD.

The following table summarizes these changes:

<i>New name</i>	<i>Old name (version 3.x or previous)</i>
Client Hardening	Client Hardening
Execution Blocking	Blocking Mode
Execution Eventlog	Eventlog Mode
Execution Log	Log Mode
Execution Notification	Notification Mode
Local Authorization	Local Authorization
Log Upload Interval	Log Upload Interval
Log Upload Threshold	Max Log Lines Before Log Upload
Log Upload Time	Log Upload Time
Log Upload Delay	Log Upload Delay
Macro and Script Protection	Macro and Script Protection
Relaxed Logon	Relaxed Logon
Relaxed Logon Time	Relaxed Logon Time
Sanctuary Status	**
Server Address	SecureWave Application Server Address
*	Notification Text
*	Server Connect Timeout
*	Server Connect Failure Lockout
* discontinued	
** new	

Table 20: Option name comparison

Setting default options for the Exe Explorer module

The *Exe Explorer* module is used to search in computer directories finding executable files, which are then added to the Sanctuary database of approved files. Default settings define the way the *Exe Explorer* module performs this task, unless otherwise specified.

The *EXE Explorer* is one of the available means to build a list of files that can be assigned to File Groups that the users will be granted the right to use. The list may contain:

- > The executables contained in a single directory



- > The executables contained in a directory and all of its sub-directories (which, if you choose the root directory, means the whole computer)

Briefly, the procedure consists in scanning the files and then traversing the list to assign the executables to the appropriate File Groups. You can then repeat this procedure for all other directories that contain executable files.

We recommend that you use a newly configured reference computer to carry out this task. This ensures that you only authorize 'clean' files for execution.




Your reference computer does not necessarily need to be the machine on which the console is installed. You can browse your network to select files from other computers.




You may also 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.

To build a list of executable files from a computer directory

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 from the *Control Panel*) to display the *Options* dialog. Select the *Exe Explorer* tab.
3. Choose whether you want the system to check every file or just files with specific extensions.

To search for specific executable files extensions

Having clicked on the *EXE Explorer* icon , select *Default Options* from the *Tools* menu (or from the *Control Panel*) to display the *Options* dialog. Make sure *Disable File Filters* is unchecked, and check the *File Filters* boxes to indicate which types of files to include, by standard extensions (.exe, .com, etc.).




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

To search for executable files with non-standard extensions, enter one or more custom extensions in the *Custom Field*. To enter several extensions in this field, separate them by a semi-colon with no space.



To have the system check every file to determine if it is an executable

1. Having clicked on the *EXE Explorer* icon , select *Default Options* from the *Tools* menu (or from the *Control Panel*) to display the *Options* dialog.
2. Check *Disable File Filters and check all files (executables only)*. This option is slower but ensures that you will not miss any executable files just because they have non-standard file extensions.

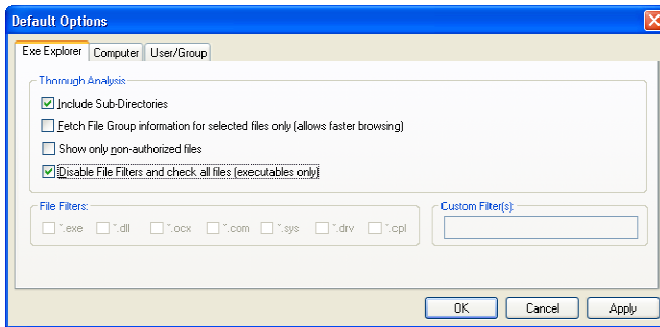


Figure 81. Checking for Executable Files



When using this option you do not include 16 bits applications. If you also want to include this kind of programs, use the 'File filters' option. Please see previous section for details.

3. Set the other checkboxes as appropriate:

Include Sub-Directories

- Select files from the named directory and its sub-directories.
- Select files only from the named directory (faster).

Fetch File Group information for selected files only

- Display File Group information only for files you select (faster).
- Show File Group information for all files.

Show only non-authorized files

- Filter out previously authorized files, show only the rest (faster).
- Show all files, authorized or unauthorized.

4. Click OK to return to the *EXE Explorer* module.
5. Click on the directory that contains the executable files you want to select on the left panel of the browser window. Executable files in that



directory (and its subdirectories, if appropriate) are displayed in the right panel of the same window.

You can also use a standard Windows method to designate the directory to use. Select the *Map Network Drive* item from the *Explorer* menu.

This process 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 will appear like this sample image:

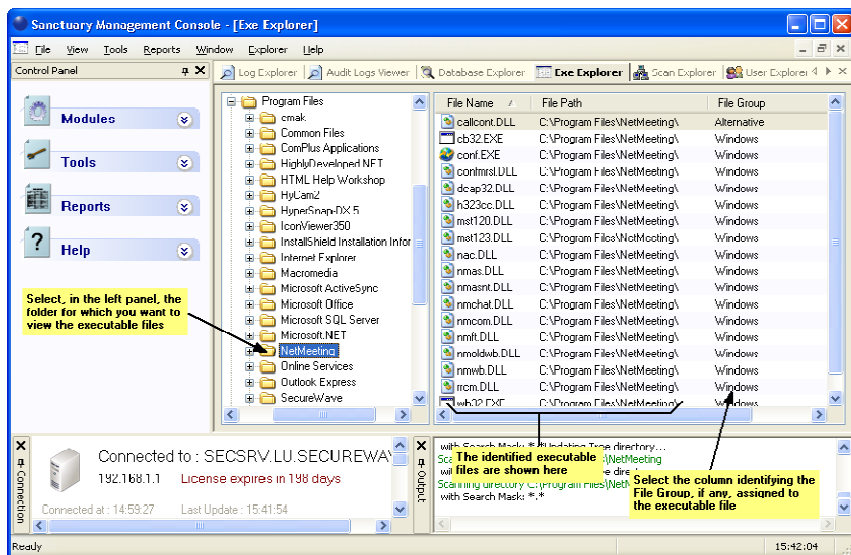


Figure 82. The Exe Explorer Module Window



The program does not uncompress archive files (Zip, Cab, RAR, LZH, ARI, etc.). To do so, use the 'Authorization Wizard' or the 'FileTool.exe' tool. Please see Using the Authorization Wizard on page 66 and Versatile File Processor tool on page 174 for more details.



Use the 'Choose columns' item from the right click menu to select and organize those columns you want to display.


Now that you have created a list of executable files, you are ready to organize them into File Groups and assign these to users and User Groups. See *Chapter 8: Assigning access permissions to users and groups* on page 89 for more details.



Setting default options

Using the *Default Options* dialog item of the *Tools* menu (or from the *Control Panel*), you can change some aspects of the program's behavior and the way protected clients & computers interact with your Sanctuary solution. The next sections describe these options.

To set an option

For each option, if the *Not configured* checkbox has a tick, then a predefined setting for that option is being used. The dialog shows for each option the current setting in the *Current Value* column. If there is a star symbol  shown, this indicates that the Sanctuary default is still in use. The predefined default setting is also indicated for each individual option in this chapter.

If you change an option, the client computers need to be updated. You can do this by selecting *Send Updates to All Computers* or *Send Updates to* on the *Tools* menu (or from the *Control Panel*).

To change an option setting:

1. Select *Default Options* from the *Tools* menu (or from the *Control Panel*).
2. Select the item in the *Option* list box.
3. Deselect the *Not configured* checkbox.
4. Set the new value for the option.
5. Type-in a message (if available)
6. Click OK to save the setting and exit the *Default Options* dialog or click **APPLY** to save the setting and keep the dialog open.

Once you finish changing the settings, send the updated information to protected clients.

Setting default options for protected clients

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



To set default options for protected clients

1. Select *Default Options* from the *Tools* menu (or from the *Control Panel*) and choose the *Computer* tab from the dialog.
2. In the *Default Options* dialog box, click the *Computer* tab. The left panel shows all the available options. The right panel shows the current value for the selected option.

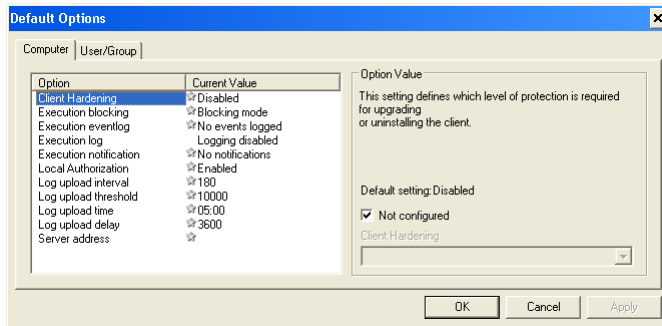


Figure 83. Default Computer Options

The tab label 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 Sanctuary database.

If you are currently using the Exe Explorer module you will see a third tab in the dialog related with the File Filter and Analysis settings.

Individual options

You will find a description of all computer options, default settings, and available values for each selection in the next sections.

Client Hardening

The Client Hardening option controls if a user with administrative privileges on a machine can uninstall or not Sanctuary's client. When the client driver starts, it generates a 15-byte random value used for protection purposes. This key – we call it Salt – is used to guarantee that the machines are uniquely identified.



You can choose from these settings:

- > *Disabled* – (default value) Sanctuary's client 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 36 for more information).

Execution blocking

Use the Execution Blocking option to determine whether to block execution approval of a file that is not centrally authorized.

You can choose between:

- > *Blocking mode* – (default value) Files that are not centrally authorized will not run. There is no local authorization
- > *Non-blocking mode* – Files that are not authorized can be run. This is useful for installing applications

Execution eventlog

The Execution EventLog option is used to configure 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

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



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
- > *Logging disabled* – Do not keep a log

Execution notification

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 148) 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

Use this option to determine whether to permit local authorization of unknown files after prompting the user.



*This option has to be set together with the 'Execution Blocking' option for the specific user in order to work. It is not enough to allow a general 'Local Authorization', you need to complement it by activating the corresponding 'Execution Blocking' (as either 'Ask user for *.exe only' or 'Ask user always') for the user.*

Select between:

- > *Disabled* – Files that are not centrally authorized will 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



This 'Local Authorization' does not applies to those files that already form part of a 'File Group' that is not assigned to the user who is trying to authorize the file.

Log upload threshold

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 delay

This field 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.

Log upload interval

Defines the time, in seconds that log entries are collected before being uploaded to the SecureWave Application Server. The Sanctuary client 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 time

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.

Server address

Define here 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).

Sanctuary status

This option allows you to select whether the Sanctuary Client icon is displayed in the system tray of the client computer. The possible settings are:

Do not Show – The Sanctuary Client icon is not displayed

Show All – (default value) The Sanctuary Client icon is displayed. The client user receives information of all changes done

Setting default options for users and groups

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

To set default options for protected users and groups

1. Select *Default Options* from the *Tools* menu (or from the *Control Panel*).
2. In the *Default Options* dialog box, click the *Users/Group* tab. The left panel shows all available options. The right panel shows the current value for the selected option.

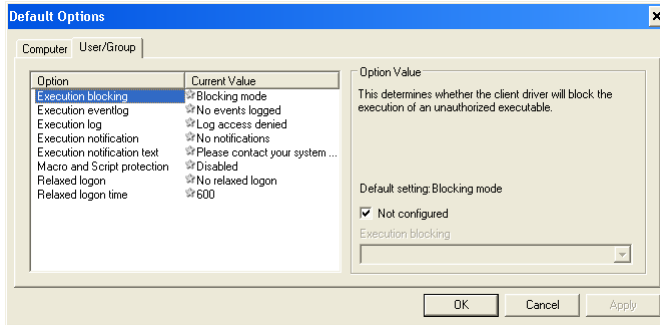


Figure 84. Default User/Group Options

Typically, these changes are automatically downloaded whenever a client connects to the network.

Individual options

The next sections describe all user/group options, default settings, and available values for each selection.

Execution blocking

This option determines whether to block execution of unauthorized files or not.

The available settings are:

- > *Blocking mode* – (default value) Files that are not centrally authorized will not run. There is no local authorization except for the Administrators and Local System 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 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 Sanctuary database. The user must locally authorize the main executable and control the loading of each additional module or ActiveX



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.

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

Execution EventLog

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 152)



This option is only included for backward compatibility.

Execution Log

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

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 (see *Execution blocking* on page 152) 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

This option determines whether scripts and macros can run or not.

You can select the following values from the pull-down list:

- > *Disabled* – (default value) No scripts protection is applied
- > *Ask User* – Every time a script (VBscript, Jscript, office VBA) is loaded, the user has the possibility to allow or deny its execution
- > *Deny All* – No script can be executed



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.

If you select *Ask user*, you can also type the desired message to display.

Relaxed logon

Use this option to allow the user to run logon scripts without having to authorize them. This setting permits to run those 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

This 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.



Setting options that apply to specific machines or users

The default settings you defined in the *Computer* tab of the *Default Options* dialog boxes apply to all computers being protected by Sanctuary. You can override these default settings for specific computers.

To override default settings on a specific computer, user, or user group

1. Open the *User Explorer* module (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. Select the File Groups by User tab.
3. Right click on any computer, user, or user group in the list and select Options. The system displays an Options dialog box that looks just like the global Default Options dialog box except that it specifies User/Group Options for [COMPUTER NAME].
4. In this dialog box, set *User/Group* options that apply to this user/group/machine. These option settings take precedence over the global *Default Settings*.

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.

Computer options

For the options that apply to computers, the order of precedence is as follows:

- > If a value has been set for the specific computer, that value is in force and supersedes all other option settings.
- > If no value has been explicitly set for the computer, global *Default Option* setting in the *Computer* tab applies.



- > If no global *Default Option* setting has been defined for this option, SecureWave system default settings apply.

The following flowchart shows the precedence order process:

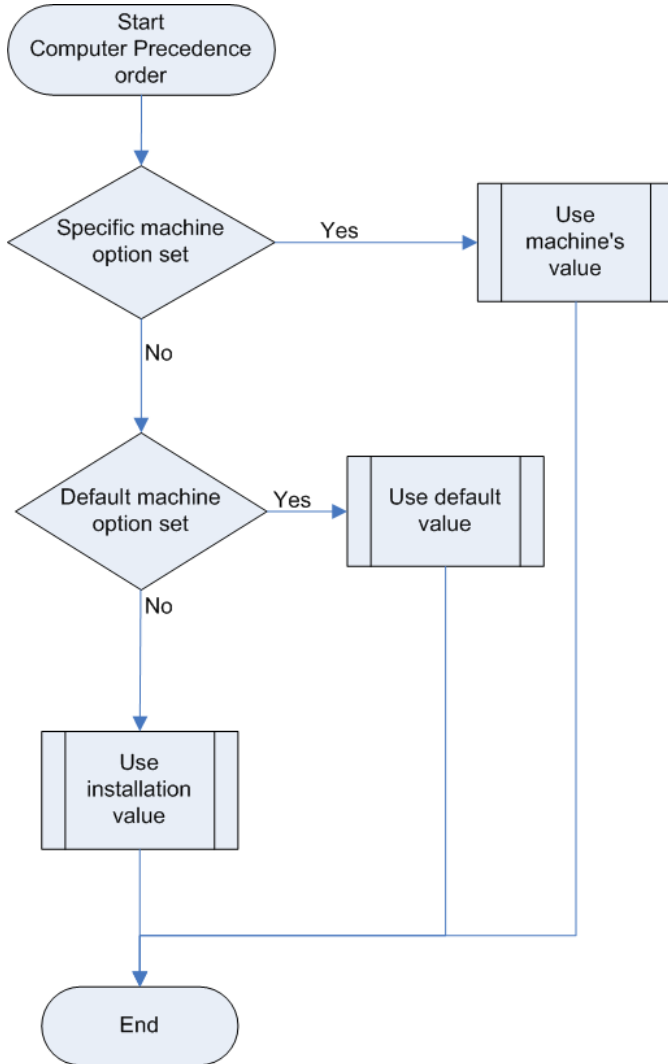


Figure 85. Computer Precedence Order Process



The following table summarizes the default options installed for computers:

<i>Option</i>	<i>Default installation value</i>
Certificate Generation	Automatic
Client Hardening	Disabled
Execution Blocking	Blocking mode
Execution EventLog	No events logged
Execution Log	Log access denied
Execution Notification	No notifications
Local Authorization	Enable
Log Upload Interval	180 sec.
Log Upload Threshold	10,000 lines
Log Upload Time	05:00 AM
Log upload Delay	3,600 sec.
Sanctuary Status	Show all
Server address	Read from registry

Table 21: Computer options: default installation values

User and group options

For most options that apply to users and groups, the order of precedence is as follows:

- > If a value has been set for the specific user, that value is in force and supersedes all other option settings
- > If no value has been explicitly set for the user, but a value has been set for a group to which that user belongs, the group option setting applies
- > If the user belongs to several groups that have varying option settings, the highest option setting applies (typically the value with the greatest scope)
- > If no value has been set for the user or group to which the user belongs, the global *Default Option* settings in the *User/Group* tab apply
- > If no global *Default Option* has been set in the *User/Group* tab, SecureWave system default settings apply



The following flowchart shows the users/groups precedence process:

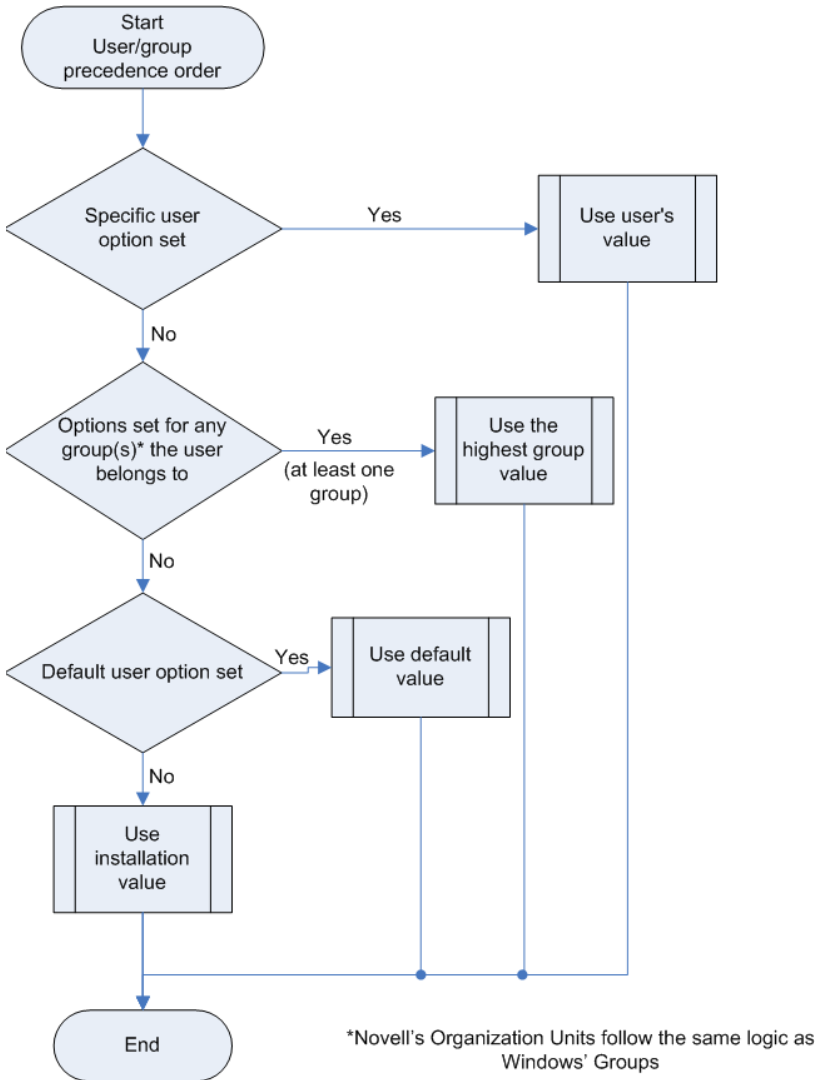


Figure 86. Users/Groups Precedence Order Process



The following table compares computer vs. user/group default installation options:

<i>Option</i>	<i>Computer's default value</i>	<i>User/group's default value</i>
Execution Blocking	Blocking mode	Blocking mode
Execution Eventlog	No events logged	No events logged
Execution Log	Log access denied	Log access denied
Execution Notification	No notifications	No notifications
Execution Notification Text	n/a	'Please contact your system administrator'
Local Authorization	Enable	n/a
Log Upload Interval	180 sec.	n/a
Log Upload Threshold	10,000 lines	n/a
Log Upload Time	05:00 AM	n/a
Log Upload Delay	3,600 sec.	n/a
Macro and Script Protection	n/a	Disabled
Server Address	Read from registry	n/a
Relaxed Logon	n/a	Disabled
Relaxed Logon Time	n/a	600 sec.

Table 22: Computers vs. user/group default values

As an example, user 'Bill' who belongs to group 'Marketing' has *Relaxed logon* disable (default value). The group was given 'Enable' for the same option (*Relaxed logon active*). 'Bill' has a relaxed logon rule applied since he belongs to a group that has the same option but with higher precedence (*Relaxed logon=Enable*).

In the following examples, 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"* option is applied as it has the highest priority.
- > 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 an *"Ask user for *.exe only"* or an *"Ask user always"* option has been defined either for Bill, one of the groups he is a member of, or in the *Default Options* dialog. This option takes precedence over the 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!



The User Options and Machine Options reports present a summary of all options defined in the system. See the description of the User Option – page 137– and Machine Options – page 138 – reports.



*If the Local Authorization option is disabled, the “Ask user for *.exe only” or “Ask user always” is ignored.*

Computer, user, and group options

For options that govern computer, user, and group options, the priority is as follows:

- > Options explicitly set for a specific user (these settings take precedence over all others).
- > Options explicitly set for a group to which the user belongs. If the user belongs to several groups that have varying option settings, the highest option setting applies (typically the value with the greatest scope).
- > Global settings from the *User/Group* tab of the *Default Options* dialog.
- > Options explicitly set for the machine the user is using.
- > Global default settings from the *Computer* tab of the *Default Options* dialog.
- > SecureWave default settings.



The following flowchart shows the process:

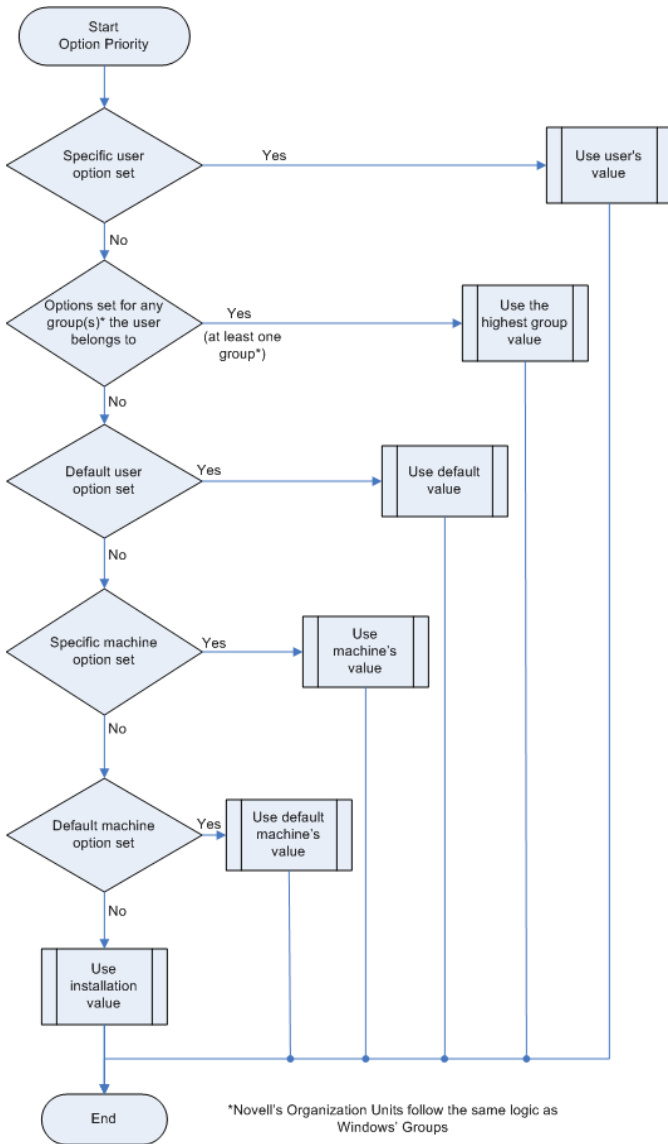


Figure 87. Option Priority



Execution Blocking option

Note that 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 has been set, it is used.
5. If no value has been set for the machine, then the default is applied as set in the *Default Machines Options* dialog.
6. If no default machine option has been set, then the installation default (*Execution Blocking*) is applied.

The following flowchart describes the process graphically.

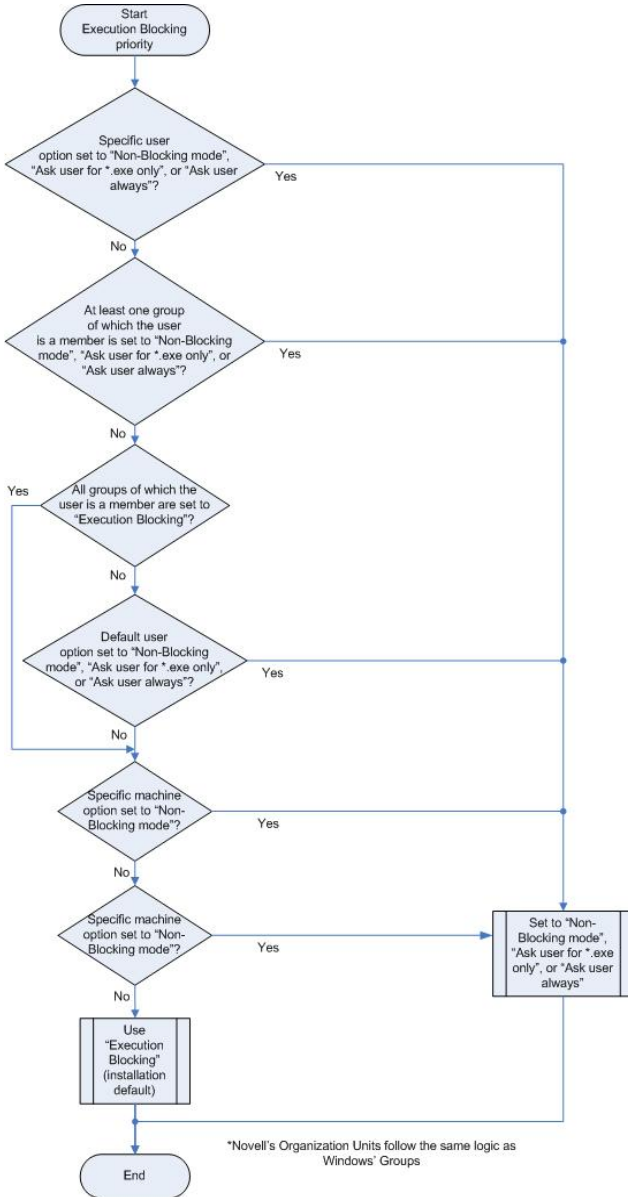


Figure 88. Blocking Mode Priority



You can follow this flowchart using as an example *Execution Blocking* set for a specific computer. Of course, if *Local Authorization* option is disabled altogether – either via global system settings or because the *Spread Check* mechanism has been enacted to stop self-propagating code – that condition overrides all *Local Authorization* (blocking or non-blocking) option settings at all levels.

The following table shows the option precedence:

<i>Option</i>	<i>Value precedence</i>
Execution Log	<ol style="list-style-type: none">1. Log everything2. Log access denied3. Logging disabled
Execution Blocking	<ol style="list-style-type: none">1. Ask user always2. Ask user for *.exe only3. Non-blocking mode4. Blocking mode
Execution Notification	<ol style="list-style-type: none">1. No notifications2. Access-denied3. Non-blocked access-denied
Execution Eventlog	<ol style="list-style-type: none">1. No events logged2. Access-denied logged3. Non-blocked access-denied
Macro & Script protection	<ol style="list-style-type: none">1. Disabled2. Ask User3. Deny all

Table 23: Option precedence

Informing client computers of changes

Whenever you make a change to the File Groups or to the assignment of File Groups to users, you can notify the client computers that something has changed instead of waiting for the next logon.

Under normal circumstances, the driver applies the changes at the next logon but sometimes it may be desirable to push the updates to either one computer or all of them.

When you have completed the changes, go to the *Tools* menu (or from the *Control Panel*) and select *Send Updates to All Computers* if you wish that these changes are conveyed immediately to all logged users. You can also send updates to a specific computer by right clicking on it from the *User Explorer* and selecting *Send Updates to: <name>* from the popup menu.

Any computer that is switched off or disconnected from the network receives the updates next time it is booted – you can also export/import them, if necessary (see *Export file permissions* on page 54 for more information).



Chapter 14: Windows Updates

Sanctuary Authorization Service Tool

This section provides you with useful information about the Sanctuary Authorization Service Tool.

What is the Microsoft Software Update Services (SUS)?

Software Update Services (SUS) assists Microsoft Windows administrators with the distribution of security fixes and critical update releases provided by Microsoft. SUS is like running a Windows Update service 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.

What is the Windows Server Update Services (WSUS)?

Windows Server Update Services (WSUS, previously SUS v2.0) is a new version of Software Update Services (SUS). WSUS supports updating Windows operating systems as well as all Microsoft corporate software.

What is the Sanctuary Authorization Service tool?

You can use *Sanctuary Authorization Service* (AuthSrv.exe) to monitor changes on the approved and synchronized files done by SUS or WSUS, and process them, when needed, using our *Versatile File Processor Tool* 'FileTool.exe' (explained in the *Versatile File Processor tool* section, on page 174 of this same chapter). The goal of this process is a 'zero' administration effort. All Microsoft Authorized updates and fixes are automatically authorized, their Hash created, and the database updated. Once installed, you should not worry anymore about it. However, sometimes there is a need to fine-tune its features manually.



To use AuthSrv.exe you need:

- > SUS or WSUS (Windows Server Update Services) installed on your machine.
- > You may need, depending on the chosen options, a mail server and an e-mail account.

Be aware that WSUS requires, depending on the configuration of your machine:

- > Microsoft Internet Information Services (IIS) 5.0
- > Microsoft .NET Framework pack
- > The Background Intelligent Transfer Services (BITS) 2.0 that lets you download updates in the background using available network bandwidth.
- > SQL Server 2000/2005, MSDE 2000, or SQL Server 2005 Express Edition

AuthSrv.exe can trigger a full SUS directories scan when it is unable to determine the new approved files. AuthSrv.exe monitors SUS ('history-sync.xml' and 'history-approve.xml') and WSUS logs to trigger the *Versatile File Processor* (VFP, see page 173 for more info) tool on the new files.



If the registry configuration is not valid (invalid paths, etc.), AuthSrv.exe will not execute.



Do not use network drive mapping with Authorization Service, only UNC (Universal Naming Convention) names. Drive maps are assigned per logon session and AuthSrv runs in a different one from where the mapping was originally created.

The following diagram summarizes AuthSrv.exe behavior:

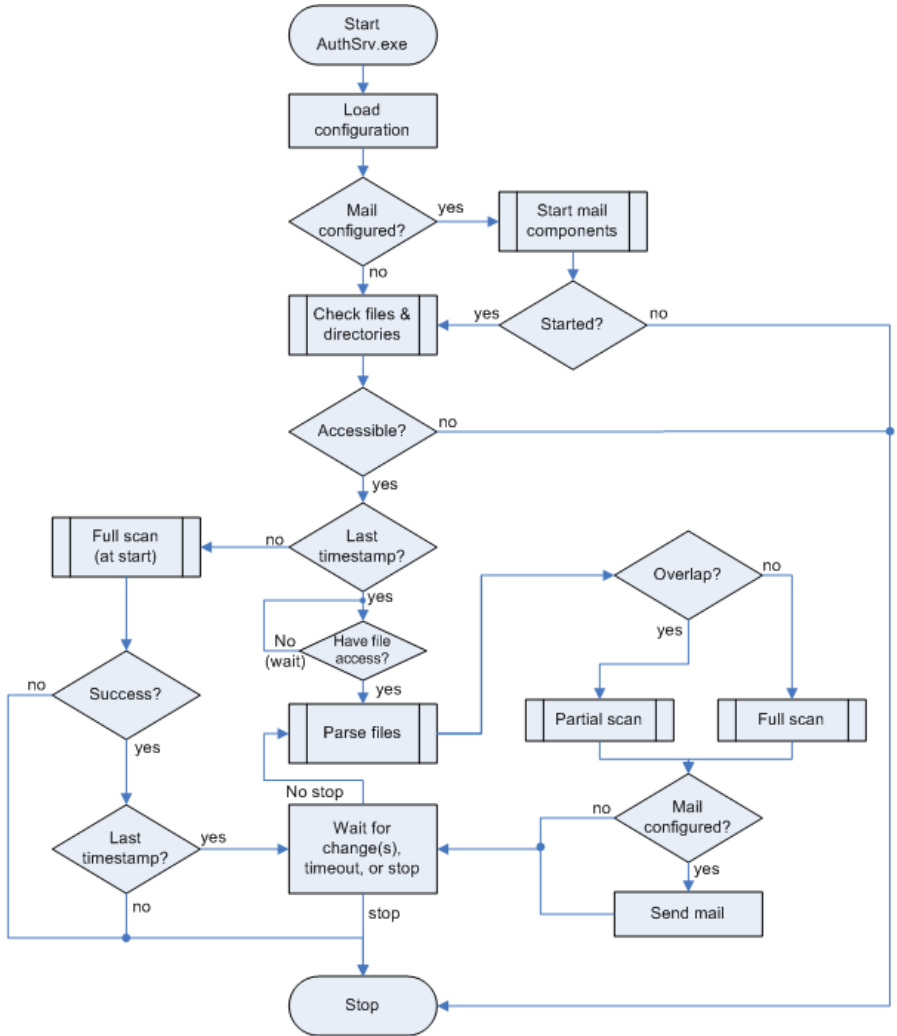


Figure 89. Authsrv.exe internal flowchart

Notice the block marked as *Wait for change(s), Timeout, or stop*. This forms the main loop of this tool exiting 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.

Every time there is an update and Authsrv.exe locates and scans the corresponding files, a XML log file is created on the installation folder, normally



%PROGRAMFILES%\SecureWave\Sanctuary\Sanctuary Authorization Service.

Installing the Authorization Service tool

The installation of the Authorization Service Tool (AuthSrv.exe) is done through a setup Wizard. To install the tool follow the steps outlined on the Setup Guide.

If you did not activate the *Do not automatically start Sanctuary Authorization Service when Setup is finished* option, the program starts once the installation ends.

The tool waits until:

- > A change is done by WSUS in the default update folder
- > The administrator approves the updates in the SUS console
- > Each hour

Once installed and loaded, you get a screen similar to this one when choosing *Microsoft Update Files* in the *Database Explorer* module (supposing you have some update files ready to authorize):

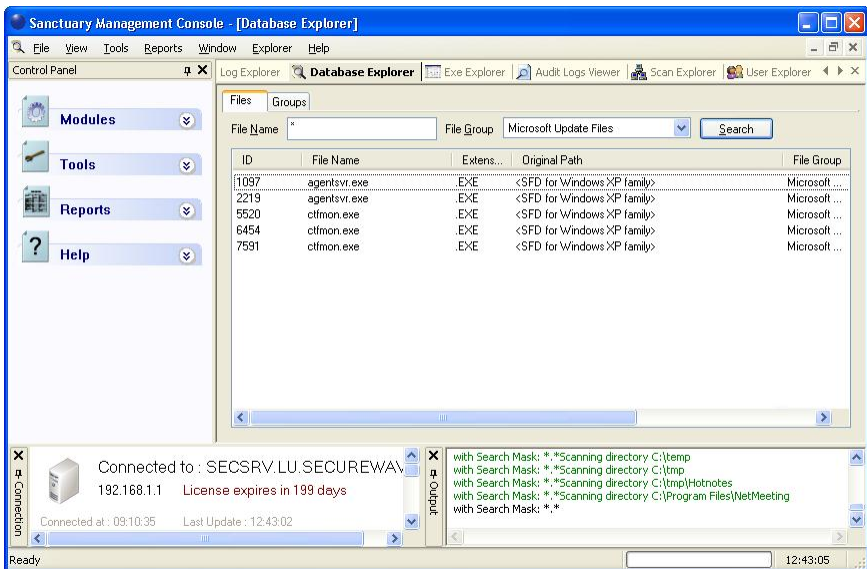


Figure 90: Sanctuary's initial scan



Sanctuary Authorization Service tool configuration

The configuration of Sanctuary Authorization Service Tool is done during the setup. Subsequent modification can be done using again the setup or, if you wish, modifying directly the corresponding Windows registry key.



Notice that we do 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 AuthSrv configuration. Furthermore, the 'LoadConfiguration' registry key parameter is always set to '3'.

To modify the parameters using the setup wizard

If you prefer to modify the parameters in a graphic user interface, proceed to the setup wizard located on your Sanctuary CD and follow these steps:

1. Run the setup wizard. The first screen informs you that the product is already installed. Click on the NEXT button.
2. The next screens allows you to modify the installation. Activate the *Modify* option and click on NEXT.
3. The third screen is used to change the server's address and port and finish the modification process.

To manually modify the parameters

If you wish to fine tune the tool's parameters, you can manually modify it directly using the following Windows registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AuthSrvHlpr\Parameters
```



Modify or add the parameters using the following table as a guide:

<i>Parameter</i>	<i>Type</i>	<i>Description</i>	<i>Default value</i>
<i>Standard Parameters</i>			
HistoryDirectory	REG_SZ	Absolute directory path where 'history-sync.xml' and 'history-approve.xml' are located.	
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 will use WSUSContentDirectory.	
OutputDirectory	REG_SZ	Directory path where output XML reports will be located.	
VerboseReport	REG_SZ	Yes Verbose report mode. No Normal report mode.	"No"
SXSServer	REG_SZ	Name or IP address of the SXS server.	
<i>Mail Parameters</i>			
SendMail	REG_SZ	If enabled ('yes'), the service will send 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 will try to load the user's Outlook or IIS Mail configuration. 1 CDO mail objects will try to load the user's IIS Mail configuration. 2 CDO mail objects will 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"



<i>Parameter</i>	<i>Type</i>	<i>Description</i>	<i>Default value</i>
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"			
<i>Advanced Parameters</i>			
CmdLineExecutable	REG_SZ	Allow an absolute path configuration of the Versatile File Processor. It is normally located in the same directory where Sanctuary Authorization Service Tool is installed.	'FileTool.exe'
CmdLineGlobalParams	REG_SZ	Using -v and C:\temp as values: '-v'c:\temp\FileTool <date and time>.xml'	is dependent of the VerboseReport and OutputDirectory entries
CmdLineBlockParams	REG_SZ	Allow user to setup assignment mode, group name(s), filters, etc. in FileTool.exe command line parameters.	'-a1 FileTool'
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"

Table 24. Sanctuary Authorization Service Tool Configuration Parameters

Here is an example of a key setting and its meaning:

'log to file' = 1; 'log file name'='c:\temp'

Create a log file and place it on the c:\temp directory



Versatile File Processor tool

The Versatile File Processor tool is a new application that supersedes AddFiles.exe and is used to scan files in specific locations. It consists of two parts:

- > A DLL (filetool.dll) that provides the underlying functionality and is employed by other SecureWave tools, for example, Sanctuary Authorization Service tool.
- > A command line executable, filetool.exe, which uses the DLL.

The tool is used to scan file locations. It can work in two modes:

- > **Online:** In the online mode, it scans file locations (that must be specified) and connects to an SXS server to assign those files. It can assign files automatically, using SXS suggestions, if configured. It connects, by default, to the local SXS, 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 SXS 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. The offline mode requires an output file name only if using the `-o <scan>` option. File assignment cannot be performed in the offline mode. The resulting file can be copied to the SXS drive to compare with other scanned files.



The FileTool.exe tool can scan files contained in archives files (cab, zip, rar, ace, jar, cx from PatchLink).



Some CAB archives do not have a standard cabinet structure despite having a .cab extension and, therefore, it may not be possible to correctly scan their contents.



FileTool.exe command line parameters

If you execute the Versatile File Processor Tool without parameters, it displays a help output:

<i>Parameter</i>	<i>Description</i>
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# <group>] [-x#]	
-s	SXS server (default is this machine).
-u	User/password to connect to SXS (default: current user).
-o	Offline mode, generate a scan.
-do	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: '*').
-co	File group creation, use only existing groups.
-c1	File group creation, create if necessary**.
-ao	Keep existing assignment, auto-assign new files, assign rest to group**. Accepts a list of groups <group1>;<group2>;...;<groupN>. 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.
-xo	Process all files. There is a risk here since this option scans files even if they are not executables (*.txt, *.doc, etc.).
-x1	Only process executables (16 and 32 bits)**.
-p	Push updates to all online clients.
**These are the default options.	

Table 25: The FileTool.exe command line parameters

The command line parameters have three sections: mode parameters, global options, and file blocks.



Versatile File Processor tool 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 will load the list of previously scanned files, `-d2` will clear the list (thus resetting the delta mode); both options will store the list of scanned files upon exit. The `-do` option (default value) will disable 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 will 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 -xo 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 <group1>;<group2>;...;<groupN>

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 group <groupN>.

If the file is unknown, and only one group is suggested, the file is assigned to that group.

If the file is unknown, and two or more groups are suggested, the file is assigned to the first one, <group(i)>, matching the suggested group, or, if no match is found, to the last one (<groupN>).

> -a1 <group> assigns unknown files to <group>. If the file is known, the assignment is not changed.

> -a2 <group> always assigns files to <group>, even those already assigned to other groups. If <group> is empty, using '' (single quotation marks) for the group name, known files will be removed from their groups.

By default, any non-existent group specified in the -a# options will be created, which may be prevented using the -co option. This is useful as a precaution against typing errors.



Be sure to specify the correct options or you risk creating hashes for unusable files (.doc, *.txt, etc.). You can avoid this by either specifying the correct extensions or by using the -xo 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:



<i>Attribute</i>	<i>Description</i>
Mask	empty by default, set with <code>-e</code> .
Files	"executables" by default, set to "all" with <code>-xo</code> .
Name	"..." matches the group(s) specified with <code>-ao</code> , <code>-a1</code> or <code>-a2</code> .
Assignmentpolicy	"auto" for <code>-ao</code> , "standard" for <code>-a1</code> , "overwrite" for <code>-a2</code> .
creation	"yes" by default, "no" when <code>-co</code> is used.

Table 26. FileTool.exe File Block Report Options

FileTool.exe usage 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 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 -dl  
c:\to_scan_directory -p
```



Chapter 15: Best practices for Sanctuary security

Sanctuary in an organization-wide strategy

As your organization grows, you will need to implement appropriate security policies when implementing your network. Addressing these issues early in your preparation ensures that security cannot be breached. Using the right tools for the job guarantees that your security controls are pro-active, consistent, and automatic. The evaluation of your network security risks, the training of your staff, and the early identification of potential breaches and security risks play an important part in your global security strategy.

As part of this global protection strategy, Sanctuary products provides the most basic, and important, services of them all: Protecting your software and hardware investment by impeding illegal use of programs, external and internal attacks, and data theft of your valuable and sensitive information.

Gone are those days where it was enough to have a proper firewall and anti-virus program to protect your organization from external and internal attacks. Users get more sophisticated, equipment evolves, and there are new ways to do old things. Sanctuary products will protect you of present and future attacks in a very simple way: denying or limiting all access to programs and devices unless told to do so explicitly.

Setting up your new Sanctuary solution

Follow these simple steps to setup your Sanctuary protection:

1. Create a software inventory
2. Define organizational security policies (permissions, file groups, administrators, roles, etc.).
3. Plan the system architecture and sizing requirements.
4. Install system components (database, application server, and management console, key pair, and schedule domain sync).
5. Populate the database application's hashes.
6. Assign file groups to users/user groups.



7. Install a client machine.
8. Validate permissions.
9. Prepare to make a smooth transition from an uncontrolled environment to a protected one.

By defining a small number of user groups in your domain, granting those groups permissions, and then assigning users to groups, you can manage a small number of groups instead of a large number of users.

Setting the driver to non-blocking and the notification mode to 'Notify of non-blocked denial' is a very effective way of managing the transition of an organization from an uncontrolled environment. The logs can be used to indicate files in regular use which are candidates for adding to File Groups. The logs can indicate two possible cases:

- > Files you forgot to authorize
- > Viruses that tried to execute

Use the logs carefully and authorize only those files from reliable sources.

The Sanctuary Client is used on the client computer to provide notifications to the user about blocked files. It is essential that you authorize all its components for all users. When first installing the program, these files are classified under the 'SecureWave Support Files' file group. You can directly assign this file group to the user or to the group the user belongs to.

Routine system administration

In your everyday administration, you should:


- > Monitor logs of application execution watching for illegal activity (executable trying to run without authorization).
- > Run new scans, create scan templates, and gather new executables and authorize them if necessary.
- > Modify authorizations for new software or service packs.
- > Do daily maintenance, backups, and machine updates.



Verifying new software

After installing new software on a computer and authorizing it – see *Chapter 5: Building a list of executable files to be managed* on page 53 for more information on how to do this –, you may want to verify that new applications authorizations are working correctly and that new drivers are not obstructing other software on the machine.

To verify the performance of new software on a client

1. Launch the software on the target client, use it for a while, and then close it down.
2. Open the *Log Explorer* module (click on the corresponding icon  located in the Modules section of the *Control Panel* of the main window or use the *View→Modules* command).
3. Select *Fetch Log* from the *Explorer* menu.
4. Select the appropriate machine and fetch the up-to-date logs in the dialog.
5. Click on the *Access* column header to sort the files by this field. You may have to use the lower navigation bar to find it.
6. Make sure that no files have *Denied*, *ok-nonBlocking*, or *ok-nonBlockUser* shown in the *Access* column. If there are no such files, the new software has been properly authorized, included in the appropriate File Groups, and has not upgraded any files used by other applications.

Assigning File Groups to user groups instead of users

When you begin to use *Sanctuary Application Control Suite*, you will probably be tempted to directly assign the File Groups (default or created) to individual users as you go. Although this is practical when the number of assigned authorizations is kept small and while you get accustomed to the inner works of the program, this becomes quickly unmanageable as the deployment grows and you control more and more users and applications in your organization. You will have the double task of maintaining Windows' users and their possible *Sanctuary Application Control Suite* assignments.



A more pragmatic approach is to invest more time in the designing phase deciding which applications should be restricted and to which File Group they must belong beforehand. The object of this exercise is to define Windows' Groups to control application execution. Once this determined, you should proceed to define a naming convention, the actual groups, and all necessary group nesting so that it meets your business requirements. You should aim to create the fewest possible groups. This first phase design pays off as you can define Windows' user groups precisely and then proceed to grant authorization to these groups instead of assigning them directly to specific users. The user, of course, should then be member of one or more of these previously defined groups.

As soon as your groups are determined, you can then proceed to define File Groups (and their possible relationships) for your applications in the Sanctuary Management Console. You get the distinguished advantage of controlling application execution by assigning File Groups directly to one or more specific Windows' groups. You can also use these same groups to do all kind of house keeping (Windows' public folder and mailboxes permissions for example).

By defining a small number of user groups in your domain, defining File Groups, and then assigning File Groups to user groups, you can manage a small number of groups instead of a large number of users.

Another benefit of this approach is that you are keeping User Management where it belongs: in your Directory structure (Windows' Active Directory or Novell's eDirectory).

Tips for maximum security

If your organization has extremely stringent requirements for client protection, confidentiality, and reliability, you will want to use Sanctuary to its maximum power. Here are some option settings and practices to consider using the solution at maximum strength.

Preventing Local Authorization

If you leave a user the chance to locally authorize applications, you are exposing your network to a security risk. The user may authorize a malicious application on the computer. To prevent the spreading of such malicious applications throughout the company, you should disable the local authorization option. This global machine option, if disabled, will prevent local authorization altogether. See *Local authorization* on page 45 for more details. The *Blocking mode* enabled is the default option (no local authorization allowed).



Preventing 'Relaxed logon'

Blocking can also be activated at the workstation at the end of the logon script by running the `EndLogon.exe` command at the end of the script. `Endlogon.exe` is a utility that activates blocking immediately, even if the relaxed logon time has not yet expired. `Endlogon.exe` is included in the installation of the Sanctuary. The *Relaxed logon* disabled is the default setting.

If you want to prevent logon scripts from running asynchronously, then you need to make the following change in the registry of each client computer.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon
```

The value `RunLogonScriptsSync` should be set as a `REG_DWORD` with a value of one.

Doing this will mean that users are unable to run unauthorized files by double clicking them 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 Task Manager. You can disable this behavior by setting the blocking mode for Local System and Administrators. Beware that this is dangerous if the file groups have not been assigned to the local system because you can block the whole system.

You can also do this using Group Policies. This entry corresponds to the "Run logon scripts synchronously" group policy that you can find in the User Configuration → Administrative Templates → System → Logon.



Chapter 16: Troubleshooting your Sanctuary solution

Your normal use of Sanctuary should be trouble-free. However, if you do encounter any problems, then refer to this chapter. It explains some of the more common problems, provides solutions for them and ways of preventing them recurring.

You can find more troubleshooting information and tips on our Web site at: www.securewave.com

Please consult the Setup Guide for further troubleshooting techniques.

I am an administrator. I can view access privileges but not change them. Why?

The Sanctuary system recognizes two types of administrators: Enterprise Administrators, who have complete administrative privileges, and regular Administrators who have restricted privileges. Your access privileges have probably been set as read-only in the system to limit access to this function. An Administrator or Enterprise Administrator with appropriate privileges must change this setting.

To change access privileges for an Administrator

1. Select *User Access* from the *Tools* menu (or from the *Control Panel*). The system displays the *User Access Manager* dialog.
2. Enter a user name in the *User Name* field.
3. Click **SEARCH** 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. The *Settings (App.Control)* field will probably be set to *None*, which means that application control is in force. Remember that you should set the *Access* field to *Administrator*.
5. Change this attribute to *Yes*, so that the application control measures are not in force. The selected Administrator can now change permissions and system options for the objects for which he/she has write permission in the Active Directory.

Another cause for this could be that you do not have the appropriate rights for the object you are trying to manage in the Active Directory. Please see our Control Access Tool (CtrlAcx.vbs) file located on the installation CD and consult the



Appendix D of the Sanctuary Device Control Administrator's Guide for further instructions on how to use this tool (also included in the help file).

The information in the User Explorer display is not up-to-date. I know we have added users, User Groups, or computers that are not showing up on the list.


When you make changes to a domain, such as adding users, User Groups, or computers, you should explicitly synchronize this information in the Sanctuary database. You can do this from any module of the Sanctuary management console.


Select *Synchronize Domain Members* from the *Tools* menu (or from the *Control Panel*). Type the name of the domain to synchronize and click the OK button. The system updates the database records for all users and computers in the specified domain.

Some perfectly harmless applications that were authorized are being denied.

If an administrator informs you that one of their applications will not run while it should, follow this procedure to identify and correct the problem:

1. In the *Log Explorer* module, select *Fetch Log* from the *Explorer* menu. Choose the appropriate computer and retrieve the up-to-date logs.
2. Click on the *Access* column header. All files that have been denied will be shown at the top of the list.

 *If the client is running in Non-Blocking mode, files that are not members of an appropriate File Group are permitted to run. When this happens, the entry in the Access column is either '<ok nonBlockUser>' or '<ok nonBlocking>', depending on whether Non Blocking mode has been set for the user or for the computer.*

 *If the client is running in 'Ask user for *.exe only' or 'Ask user always' mode, files that are not authorized can be permitted to run if the user decides to do so. When this happens, the entry in the Access column is 'ok-localAuth'. You should pay attention to these records as they are related to applications that were not approved by you and that the user decided to run anyway.*

3. Check whether any of these are required for the application that will not run. If they are required, you should:
 - > See the *File Group* column to check whether the files are assigned to the appropriate File Group. If they are not, assign them. Only assign those files



that come from reliable sources. See *Assigning File Groups to users*, page 90.

- > See the *User Explorer* to check whether the user is permitted to use the File Group. If not, grant the user (or a group the user is a member of) permission to use it.

If the *blocking mode* option is active, any application that is not centrally authorized will be barred from running. This remark is particularly important if the *Spread check* option is activated since it will change automatically the global computer Local Authorization option from 'Enabled' to 'Disabled' once the spreading threshold is reached. When the *Local Authorization* option is set to *Disabled*, the *Ask user for *.exe only* and *Ask user always* user options are ignored and the blocking mode option is applied by the client. This is why is extremely important to centralize application authorization.

Administrators are supposed to have local authorization rights (for unknown files, scripts, or macros), but the alert/authorize/deny dialog does not pop up. They just get a denial message.

Make sure the correct options have been set. In particular, activate the *Ask user for *.exe only* (Blocking mode) and *Local authorization* global options.

There are no files showing when I switch to the Exe Explorer and traverse the disk tree.

You have not defined the options specifying which type of files to scan for (exe, com, dll, etc.). Select the desired options (see *Setting default options for the Exe Explorer module* on page 142) and try again.



Glossary

ACL

Acronym for *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

Acronym for *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 Sanctuary Terminal Services Edition controls.

CSV

The CSV, *Comma Separated Value*, file format 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.).



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 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 Management Console, e.g. by double-clicking on a file in the *Database Explorer*, *EXE Explorer*, *Log Explorer* or *Scan Explorer*.

GUID

A *Global Unique Identifier* number 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 (2^{128} or 3.4028×10^{38}) is so large that the possibility of using the same number twice is nearly zero.



Hash

A complex digital signature calculated by Sanctuary Terminal Services Edition to uniquely identify each executable 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.

LDAP

Lightweight Directory Access Protocol. An LDAP directory entry consists of a collection of attributes and is referenced unambiguously with a name, called a distinguished name (DN). For example, "cn=Bill Dove: ou=marketing: o=securewave" – "cn" for common name, "ou" for organizational units, "o" for organization. LDAP directory entries feature a hierarchical structure that reflects political, geographic, and/or organizational boundaries.

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 *SecureWave 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

Acronym for *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.

SXS

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

Acronym for *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 flow.

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

Acronym for *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: Sanctuary components	18
Figure 2: How the Sanctuary solution works	23
Figure 3. Connecting to the SXS Server.....	27
Figure 4. Connection & Output window.....	29
Figure 5. The main screen	29
Figure 6. License status warning.....	30
Figure 7. Docked Control Panel	31
Figure 8. Docked window	31
Figure 9. Floating Control Panel	31
Figure 10. Floating windows	32
Figure 11. Minimized windows.....	33
Figure 12. Endpoint Maintenance.....	37
Figure 13: Local authorization screen	45
Figure 14. Spread Check Dialog	46
Figure 15. User Access Manager Dialog.....	50
Figure 16: Importing a permission file.....	54
Figure 17. Import SecureWave File Definitions (SFD)	58
Figure 18. Scan Explorer module main window	61
Figure 19. Create New Template Dialog	61
Figure 20. Insert New Path Rule Dialog.....	62
Figure 21. Perform New Scan Dialog	63
Figure 22. Perform New Scan: Comment.....	63
Figure 23. Scan Explorer window after a scan	64
Figure 24. Select Two Scans to Compare.....	65
Figure 25. Authorization Wizard.....	67
Figure 26. Authorization Wizard: Selecting the Source Directory	68
Figure 27. Authorization Wizard: Media Statistics	69
Figure 28. Authorization Wizard: Processing the Files	69
Figure 29. Authorization Wizard: Assigning Files to File Groups	70
Figure 30. File Group Management.....	72
Figure 31. File Group parent relationship	74



Figure 32. File group child relationship.....	75
Figure 33. File group parent-child relationship	75
Figure 34. File group indirect assignment	75
Figure 35: Assigning files to file groups	77
Figure 36. Assigning a File Group from the EXE Explorer module	77
Figure 37. The Database Explorer Module	79
Figure 38. The Path Rules Dialog	82
Figure 39. Editing the Path Rules	82
Figure 40. Adding a Path Rule.....	83
Figure 41. Setting Trusted Owners.....	86
Figure 42. Setting Path Rules with Ownership Checking	87
Figure 43. The User Explorer Module Window: File Groups by User	91
Figure 44. The User Explorer Module Window: Users by File Groups	93
Figure 45. A user having several File Groups indirectly authorized	94
Figure 46. User's tree	96
Figure 47. The Log Explorer main window	99
Figure 48. Saving your new template.....	100
Figure 49. Managing your templates.....	101
Figure 50. Components of the Log Explorer window	102
Figure 51. Navigation/Control bar	102
Figure 52. Column Headers	103
Figure 53. Show/hide columns.....	103
Figure 54. How to open the Settings dialog	104
Figure 55. Settings dialog.....	104
Figure 56. Stacking the query.....	105
Figure 57. Example of filter settings.....	108
Figure 58. Filter/Properties window.....	108
Figure 59. Control button bar.....	109
Figure 60. Fetching New Logs.....	113
Figure 61. The Audit Logs Viewer Module.....	115
Figure 62. Using the calendar pull-down to select a search date	116
Figure 63. Using the Author field to do a search	117
Figure 64. Using the Action Field to do a search	118
Figure 65. Using the sorting facilities of the Audit Logs Viewer Module	119



Figure 66. Filtering actions in the Audit Logs Viewer Module	120
Figure 67. A filtering pop-up dialog example	120
Figure 68. The Database Explorer Module	124
Figure 69. Selecting columns to show in the Database Explorer Module	125
Figure 70. The Choose Columns dialog.....	125
Figure 71. Synchronizing Domains	126
Figure 72. Connecting as a Different User	127
Figure 73. Database Maintenance.....	129
Figure 74. Purging the Online Computers Table.....	131
Figure 75. Obtaining a report	134
Figure 76. File Groups by User report	135
Figure 77. Users by File Group report.....	136
Figure 78. User Options report.....	137
Figure 79. Machine Options report	138
Figure 80. Online Machines report	139
Figure 81. Checking for Executable Files.....	144
Figure 82. The Exe Explorer Module Window.....	145
Figure 83. Default Computer Options	147
Figure 84. Default User/Group Options	152
Figure 85. Computer Precedence Order Process.....	157
Figure 86. Users/Groups Precedence Order Process	159
Figure 87. Option Priority	162
Figure 88. Blocking Mode Priority	164
Figure 89. Authsrv.exe internal flowchart.....	169
Figure 90: Sanctuary's initial scan	170



Index of Tables

Table 1. New Features & Differences from Previous Versions	26
Table 2. The File Menu.....	33
Table 3. The View Menu	34
Table 4: The Window menu items	34
Table 5. The Tools Menu	35
Table 6. The Reports Menu	38
Table 7. The Explorer Menu.....	39
Table 8. The Help Menu	39
Table 9. The System Modules	39
Table 10. SecureWave File Definitions (SFD).....	55
Table 11. File status when comparing to scans.....	65
Table 12. File Group relationship status icons.....	74
Table 13. Resulting permissions when applying Path Rules.....	88
Table 14: Limitations while using the Log Explorer module under other user/domain account	98
Table 15: How to use the available criteria dialogs	107
Table 16: Log Explorer module column meaning	110
Table 17. Possible Access Field Values	111
Table 18. Audit Logs Viewer Result Information	122
Table 19. Columns of the 'Online Machines' Report	140
Table 20: Option name comparison	142
Table 21: Computer options: default installation values.....	158
Table 22: Computers vs. user/group default values	160
Table 23: Option precedence	165
Table 24. Sanctuary Authorization Service Tool Configuration Parameters	173
Table 25: The FileTool.exe command line parameters	175
Table 26. FileTool.exe File Block Report Options.....	178



Index

A

- ACL, 189
- Active directory, 109, 117
- Active Directory Service Interface, 189
- Administration tools, 18, 21
- Administrator, 49, 117
- ADSI, 189
- Advanced Encryption Standard, 189
- AES, 189
- AFD, 18, 19, 26
- Anti-virus, 14
- Applications
 - Allow, 14
- Access permissions, 89
- Audit File Directory, 18, 19, 26
- Audit Logs Viewer, 115
 - Actions, 119
 - Search options, 116
- Authorization strategies, 41
- Authorization Wizard, 66
 - Add executables to the database, 67
- AuthSrv.exe, 167

B

- BITS, 168
- Black list, 14
- Building a list of executables, 53

C

- CAB, 189
- Central authorization, 42
 - By file location, 43
- Change file assignments, 78
- Choose columns, 145
- CIM, 194
- Client computer, 146, 151, 189
- Client Hardening, 36
- Client ticket, 36

- Create, 37
- Rules, 36
- Common Information Model, 194
- Common problems, 185
- Compare two templates' scans, 64
- Conventions, 9
- Create template, 61
- CSV, 113, 189
- CtrlAcx.vbs, 185

D

- Database, 18, 19, 21, 96, 127
 - Backup, 128
 - Delete file, 79
 - Routine maintenance, 126
- Database Explorer, 123
- DataFileDirectory, 18
- Default options
 - Groups, 151
 - Protected servers, 146
 - Users, 151
- Delegation, 190
- Delete
 - Old audit logs, 129
 - Old logs, 128
- Dependencies, 190
- DFD, 18
- Disable scripts and macros, 43
- Disconnected, 23
- DN, 190
- Domain, 95
 - Administrators, 95
- DVD-ROM, 21

E

- EndLogon.exe, 183
- Endpoint Maintenance, 36, 148
- Enterprise administrator, 49, 117
- EXE Explorer, 59, 142
- Executable
 - Files, 14, 95, 143, 190



- Program, 190
- Viruses, 14
- Exploit, 190
- Explorer menu, 38
- Export file permissions, 54

F

- FAQ, 185
- File Groups, 15, 40, 94, 95, 142, 143, 190
 - Assign executables, 76
 - Assign to users, 90
 - Change file assignment, 78
 - Create, 71
 - Delete, 72
 - Remove file, 78
 - Rename, 73
- File menu, 33
- FileTool.exe, 174
 - Archive files, 176
 - Command line parameters, 175
 - Delta mode, 176
 - File block, 176
 - Report options, 176
 - Retry logic, 176
 - Usage examples, 178
 - Usage notes, 176
 - Versatile File Processor tool, 174

G

- Global Users, 95
- GUID, 190

H

- Hash, 23, 42, 191
- Help menu, 39
- How Sanctuary works, 21

I

- Identify executable files, 59
- iFolder, 191
- Indirectly authorized through Domain Groups, 94
- Informing client computers, 165

- Internal structure, 13

K

- Key Pair Generation, 21

L

- LDAP, 191
- Local authorization, 45
 - Prevent, 182
- Local users, 96
- LocalSystem, 95
- Log Explorer
 - Authorize unknown files, 112
 - Force latest log, 112
 - Interpreting, 111
 - Save to CSV, 113

M

- Maintenance ticket, 36
- MAPI, 191
- MDAC, 191
- Microsoft Data Access Components, 191
- Microsoft Software Update Services, 167
- Monitor logs, 98
- Monitor system activity, 97
- MSDE, 191

N

- NDAP, 191
- NDS, 191
- New features, 25
- NICI, 192

O

- Options
 - Changes, 142
 - Client hardening, 147
 - Default options
 - For specific machines, 156
 - Execution blocking, 148, 152



- Execution eventlog, 148, 153
- Execution log, 149, 153
- Execution notification, 149, 154
- Local authorization, 149
- Log upload delay, 150
- Log upload interval, 150
- Log upload threshold, 150
- Log upload time, 151
- Macro and script protection, 154
- Relaxed logon, 154
- Relaxed logon time, 155
- Sanctuary status, 151
- Server address, 151
- Settings
 - Precedence, 156
- Organizing files, 71
- OU, 192
- Overview, 18
- Ownership Check, 81
- P**
- Path rule
 - Create, 81
 - Delete, 84
 - Delete all, 84
 - For a specific user or use group, 83
 - Modify, 84
 - Pathname conventions, 85
 - Precedence, 88
- Private key, 192
- Public key, 192
- R**
- Recursive, 81
- Relaxed logon
 - Prevent, 183
- Remove
 - Old scans, 128
- Reports, 133
 - File groups by user, 135
 - Machine options, 138
 - Menu, 38
 - Online machines, 139
 - User options, 137
 - Users by file group, 136
- Root specifier, 85
- RPC, 192
- RSA
 - Definition, 192
- RTNotify.exe, 180
- S**
- Salt, 20, 36
- SAM, 28
- Sanctuary Authorization Service tool, 21, 167
 - Configuration, 171
- Sanctuary Client, 18
 - Driver, 19
- Sanctuary Database, 123
- Sanctuary Management Console, 20, 27, 28
 - Connection window, 30
 - Control panel, 30
 - Main page panel, 30
 - Menu, 30
 - Menus, 29
 - Modules, 29, 39
 - Output window, 30
 - Status bar, 30
 - Tools, 29
- Scan
 - A computer, 59
 - Automatic, 59
 - Selected directories, 64
- Scan Explorer, 60
- Search
 - by Action, 116
 - by Author, 116
 - by Computer, 116
 - by Date, 116
 - by Target, 116
 - by User Name, 116
 - Executable files, 143
 - 16 bits, 143, 144
- SecureWave Application Server, 18, 19, 27, 33
- SecureWave File Definitions, 192
- Sending updates, 47



- Send updates to a specific computer, 146
- Send updates to all computers, 146
- Server administrators, 49
- Setting a system administrator, 49
- SFD, 192
 - Automatically imported, 56
 - Manually imported, 56
- SHA-1, 191, 193
- SID, 193
- SMC, 20, 143
- Software Unlicensed, 13
- Spread Check, 161
- SQL, 193
 - Server, 191
- SUS, 167, 193
- SX Domain command-line tool, 127
- SXDomain, 21
- SXS, 18, 27, 193
- Synchronize
 - Domain, 35
 - Domain members, 126
- System
 - Administrator
 - Full management privileges, 50
 - Restricted access privileges, 51
 - Components, 18
 - Options, 141
- T**
- TCP/IP, 193
- Technical support, 11
- Tools
 - Menu, 34, 96
- Trojans, 14
- Troubleshooting, 185
- Trusted owners, 86
- Typefaces, 9
- U**
- Unlicensed software, 13
- User Explorer, 90, 95
- User groups, 93
 - define, 94
- Users, 13, 23, 93, 94, 95, 127, 142
- V**
- VBScript, 193
- Verify new software, 181
- Versatile File Processor tool, 21
- View
 - File assignments, 79
 - Menu, 34
- Viruses, 14
- Vulnerability, 194
- W**
- Well-known
 - Groups, 95
 - Security Identifiers, 194
- White list, 14
- Window menu, 34
- Windows
 - Macros, 43
 - Management Instrumentation, 194
 - Scripts, 43
 - Server Update Services, 167, 168
- WMI, 194
- Workstation, 95
- Worms, 14
- WSUS, 167, 168, 194