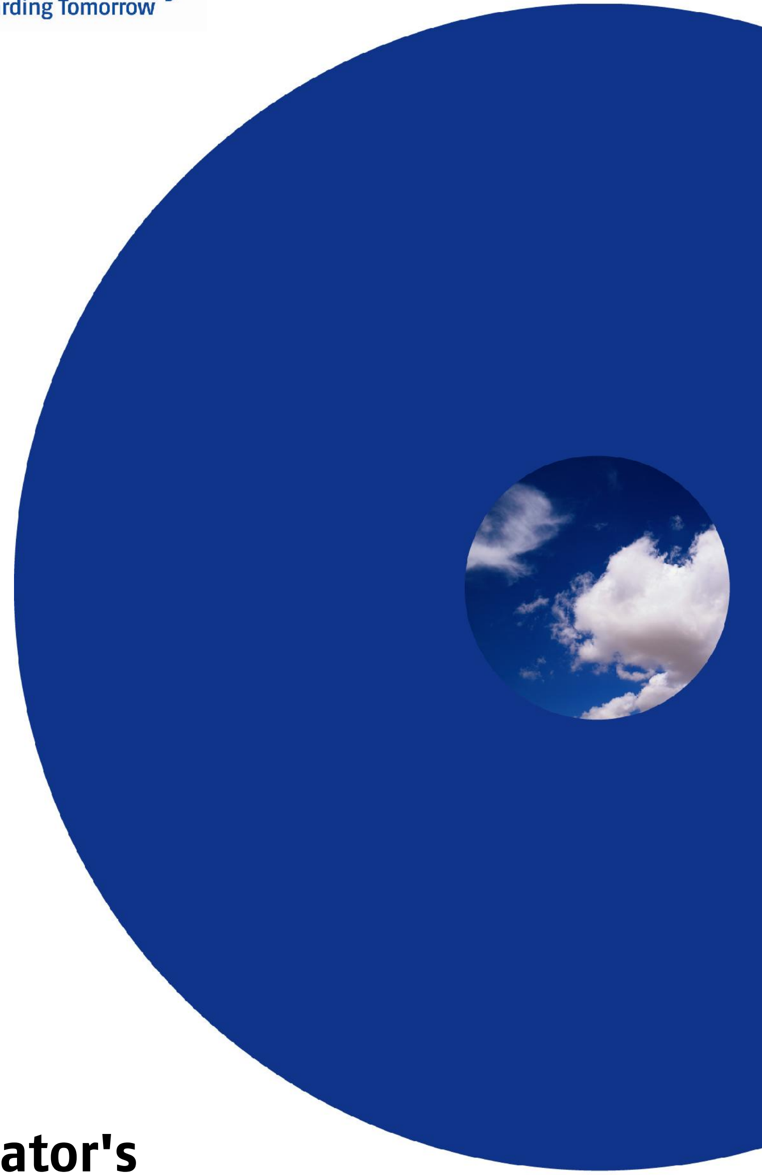
SecureWave
Sanctuary®
Safeguarding Tomorrow



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SecureWave claims copyright in this program and documentation as an unpublished work, revisions of which were first licensed on the date indicated in the foregoing notice.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.

Trademarks

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

Phone:	+352 265 364-11 (from USA & Canada, dial 011 352 265 364 11)
Fax:	+352 265 364-12 (from USA & Canada, dial 011 352 265 364 12)
Web:	www.securewave.com

Technical Support hours are Monday to Friday, 8:30 to 18:00 CET/CEST (2:30 AM to 12:00 PM ET/EDT).

You can contact our technical support team at:

+352 265 364 300 (international),
+1 800 571 9971 (US Toll Free),

or by sending an email to support@securewave.com

Published on: March 2006

Sanctuary Suite Administrator's Guide v3.2.0

Contents

Introduction

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 suite formed by:

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 extends 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 suite (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 how it 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:

Italic text	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:

Phone:	+352.265364-300 (from USA & Canada, dial 011 352 265 364 300) +1 800 571 9971 (US Toll Free)
Fax:	+352.265364-12 (from USA & Canada, dial 011 352 265 364 12)
Web:	www.securewave.com
eMail:	support@SecureWave.com

Technical Support hours are Monday to Friday, 8:30 to 18:00 CET/CEST (2:30 AM to 12:00 PM ET/EDT).

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 *157*) 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 all the rest.

In short, with Sanctuary, you have a robust shield of protection covering your organization's server & 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.

2. 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, or all database management applications used by your database administrators.

3. 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 all authorized administrators and servers.

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 users, even though they are not end-users in the typical sense of the word. Sanctuary recognizes both local and domain users and groups.

Now you 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 touched on 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 smallest 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 assignment details for the respective files can be accessed from the log and maintained if required.

> 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*

> One or more *SecureWave Application Server* (also known as *SXS*)

> The *Sanctuary Client Driver* (SK)

> Administrative tools – especially the *Sanctuary Console* or (SMC)

The following diagram shows these relations:

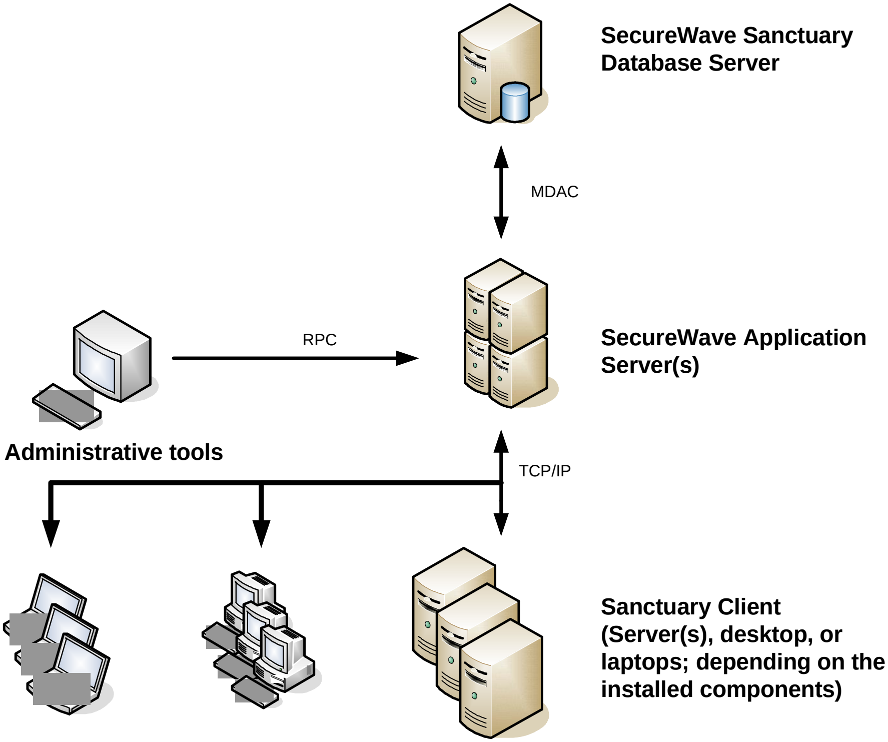

SecureWave Sanctuary Database Server
MDAC
RPC
SecureWave Application Server(s)
Administrative tools
TCP/IP
Sanctuary Client (Server(s), desktop, or laptops; depending on the installed components)

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 7/2000 or Microsoft Database Engine (MSDE). For organizations with fewer than 200 users, the MSDE is sufficient. Larger organizations need to use Microsoft SQL Server. Please note that there are inherent limits while using MSDE:

- 2 GB Database size limit
- No index optimization
- No enterprise management
- Only 2 CPUs supported
- No query analyzer
- etc.

The SecureWave Application Server

The SecureWave Application Server (SXS) communicates between SecureWave Sanctuary Database and the protected servers or computers. This component runs as a Windows Service under any domain user account and performs the following functions:

- Gets the latest information about access privileges from the database
- Passes this 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
- Sends log data that can be viewed via the management console.

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 database of authorizations
- Monitoring system activity logs and option settings
- Getting all kind of useful reports.

These components are linked through the RPC protocol. 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 updates are sent to them.

Administration Tools

We provide other tools to manage the system:

- The *Client Deployment Tool* (see description in the Setup Guide): 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
- The *Authorization Wizard:* to identify the files that are copied to computers by installation routines, and to incorporate these files into the Database. The source can be either the original CD/DVD-ROM or the files held on the target system hard drive.
- The *Sanctuary Authorization Service Tool* to monitor changes and create updates (using Microsoft's SUS or WSUS)
- The *Versatile File Processor Tool* used with the Sanctuary Authorization Service to scan files
- The *Key Pair Generation:* to create a unique set of private and public keys
- 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

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, and specified which users and User Groups may run these executable files.

This information is maintained in 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
- Automatically downloads this authorization information to the requesting user/machine

This authorization information is then stored locally in a secure location on the server'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 in 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.

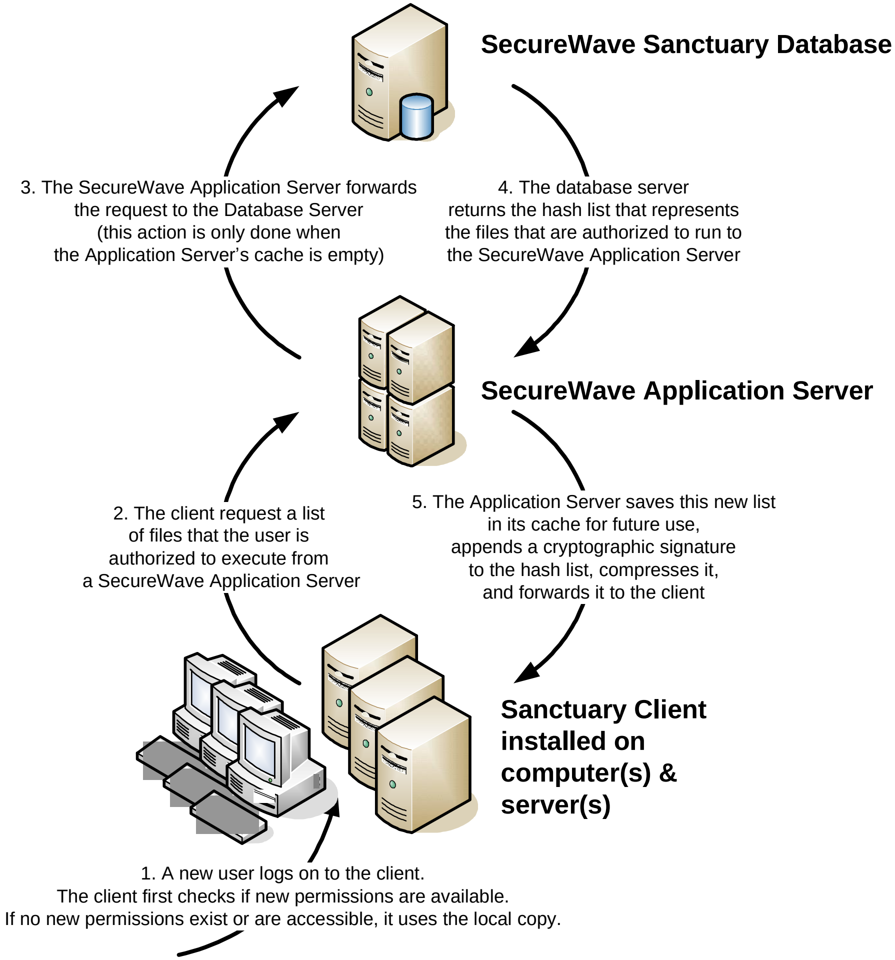

SecureWave Sanctuary Database
3. The SecureWave Application Server forwards the request to the Database Server (this action is only done when the Application Server's cache is empty)
4. The database server returns the hash list that represents the files that are authorized to run to the SecureWave Application Server
SecureWave Application Server
2. The client request a list of files that the user is authorized to execute from a SecureWave Application Server
5. The Application Server saves this new list in its cache for future use, appends a cryptographic signature to the hash list, compresses it, and forwards it to the client
Sanctuary Client installed on computer(s) & server(s)
1. A new user logs on to the client. The client first checks if new permissions are available. If no new permissions exist or are accessible, it uses the local copy.

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:

New features & differences from previous version	
Previous version	Modified in this version
Tree objects in the User Explorer are sometimes difficult and slow to traverse. Some information was buried in, difficult to reach, low-level trees of the Active Directory structure.	A more flexible list control is now available in the User Explorer module. This permits finding useful information quicker and with fewer encumbrances.
New to this version	
Each one of the programs that form our Sanctuary suite previously required an independent client component. We have design a unified client component — Sanctuary Client — that now works with our entire software suite, depending on those modules that you have purchased and installed in your server.	
The client now resolves UNC (Universal Naming Convention) Novell names allowing correct Path Rules and file authorization interpretation when using our Sanctuary series.	
New Sanctuary Client Deployment options to control whether the installation is going to be done with or without a reachable server and, if this is the case, to include or not the policies file in this kind of deployment. The program shows these options in new columns of the main window.	
New search criteria added to the Audit Logs Viewer that allows you to search by action, target, user, computer, etc.	
The Event Viewer now logs all client driver Stop/Start actions and allows you to detect the presence of the Sanctuary client.	
Windows updates are handled automatically. SUS and WSUS are supported. 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. WSUS (previously SUS v2.0) supports updating operating systems as well as all Microsoft corporate software (please refer to *Chapter 14: Windows Updates* on page *143* for more details).
A new command-line application, Versatile File Processor (FileTool.exe), is included to scan a given directory or work in conjunction with the AuthSrv.exe Service. You can use it with the scheduler program included on your operating system (AT.exe or WinAt.exe) and scan directories and subdirectories on a regular basis to 'discover', and eventually authorize, new applications and packages placed on the machine (please refer to *Versatile File Processor tool* on page *150* for more details).
The file hash calculated by the program now appears in the DB Explorer, Exe Explorer, Scan Explorer, and Log Explorer module granting more flexibility and at-a-glance info to see if two files having the same name are really identical in content.
The sort capabilities have been enhanced in all modules.
The Scan Explorer now has two levels of file sorting: by file path and by file group.
You now have more columns to choose from in the DB Explorer, Exe Explorer, Log Explorer, and Scan Explorer module. You can show/hide and place these columns on any desired order.
We enhanced the DB Explorer module, an already useful tool, by adding practical criteria fields to fine-tune your searches.
The Authorization Wizard, that uses filetool.exe in the background, allows traversing archives in its search of executable files to authorize. It supports RAR and other popular file compression formats.
The Assign File to file group dialog shows the file name AND path providing easy recognition of otherwise hard to find software.

Table 1. New Features & Differences from Previous Versions

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

> 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

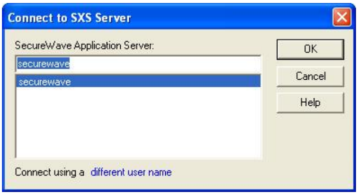
If you have already installed solution components by using the simple installation wizards or following the steps in the Setup Guide, then you are ready to get going!

Starting up the Sanctuary management application

To start up the management console of your Sanctuary application

The steps are the same as for any typical Windows application:

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



Connect to SXS Server

SecureWave Application Server: securewave

securewave

Connect using a different user name

Figure 3. Connecting to the SXS Server

To connect to the SecureWave Application Server

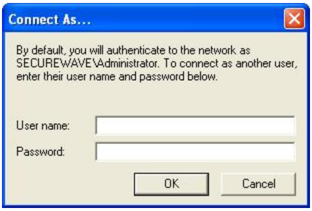
1. Type the name of the SecureWave Application Server (SXS) to connect to, or select it from the list.

   You can identify the server by IP address, NetBios name, or fully qualified server name. If the server is configured to use a fixed port, enter the port number after the server name, as in this example: `secrsrv.secure.com[1234]`

2. Click OK. The system displays the management console main display (*Figure 5*). This display looks much like a Microsoft Outlook screen — with similar menus, toolbars, icons, and Explorer workspaces — so it is familiar and easy to use, if you have worked with Microsoft Windows interfaces.

To change the name you use for logging onto the system

In the *Connect to SXS Server* dialog box that appeared when you started up the application, click CONNECT USING A DIFFERENT USER NAME. The system displays a *Connect As* dialog box.



Connect As...

By default, you will authenticate to the network as SECUREWAVE\Administrator. To connect as another user, enter their user name and password below.

User name:

Password:

Figure 4. Connecting to the SXS Server using a different user name

If your account is a local account, type the workstation name, a backslash, then your user name, such as:

```
marketing\john
```

If your account is a domain account, type the domain name, a backslash, then your user name, such as:

```
domain1\admin1
```

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

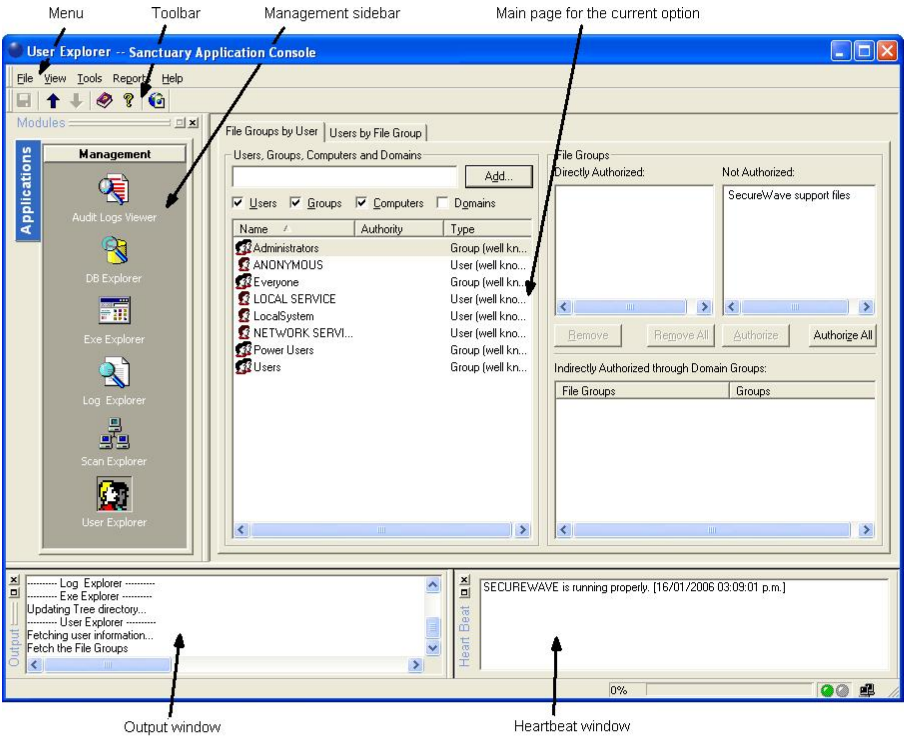
✍ *A local account is created on a single computer and is stored in its Security Account Manager (SAM) database on its hard disk. Domain accounts are created on the domain controller and stored in the Active Directory. To log onto the local machine (selecting its name in the logon dialog box), you need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

If you are not able to log onto the Sanctuary system

The system's internal checking procedures identified problems. You might not have the required permissions to connect to that server, use administrative functions, or you do not have the license to run the program. See *Chapter 4: Setting up a Sanctuary system administrator* on page *45* for more information.

Summary of Sanctuary management modules, menus, and tools

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.



Name	Authority	Type
Administrators		Group (well kn...
ANONYMOUS		User (well kno...
Everyone		Group (well kn...
LOCAL SERVICE		User (well kno...
LocalSystem		User (well kno...
NETWORK SERVI...		User (well kno...
Power Users		Group (well kn...
Users		Group (well kn...

SecureWave support files

```
--------- Log Explorer ---------
--------- Exe Explorer ---------
Updating Tree directory...
--------- User Explorer ---------
Fetching user information...
Fetch the File Groups
```

SECUREWAVE is running properly. [16/01/2006 03:09:01 p.m.]

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 *Toolbar* gives you quick access to different modules and the help file.

The *Main Page panel* changes its contents depending on the module selected on the left panel. You can refine even more the resulting information in some modules.

In the left panel is the *Management Sidebar* where you can select the available modules directly without using the menu.

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.

The *Heartbeat* window shows all the system messages generated by the real-time operation of the program. Use the sidebars to navigate through the text.

The File menu

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

Use this option	*To*
Connect	Connect to a SecureWave Application Server to perform administrative tasks.
Disconnect	Disconnect from a SecureWave Application Server after completing administrative tasks.
Save As	Save the content of the List View in CSV comma-separated values (CSV) format. You can use it to export it to any compliant program, for example Excel.
Exit	Exit from the Sanctuary management application. (Note that this command does not quit the Sanctuary program, 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:

Use this option	*To*
Previous	View the previous module on the list.
Next	View the next module on the list.
Modules List	Show a submenu that enables you to select any module.
Modules	Show or hide the module icons on the left of the screen.
Toolbar	Show or hide the toolbar below the menus.
Output	Show or hide the Output window — the window located on the lower left corner of the screen on *Figure 5*— that displays a log of system activity.
Heartbeat	Show or hide the Heartbeat window — the window located on the lower right corner of the screen on *Figure 5* — that displays real-time operating information.
Choose Columns	Select visible columns for some modules.
Refresh	Refresh the contents of the screen. You can also use the shortcut function key F5.

Table 3. The View Menu

The Tools menu

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

Use this option	*To*	*See page*
Synchronize Domain Members	Update the database with the current list of users and groups of a domain.	*107*
Database Maintenance	Delete log files and items generated from a database scan created before a specified date.	*105*
User Access	Define access privileges for administrators.	*45*
Default Options	Change the option settings.	*121*
Path Rules	Use path locations and file 'owners' to define which applications can run.	*75*
Spread Check	Prevent the spread of self-propagating code by disabling suspicious executables that have been locally authorized on too many computers.	*41*
Send Updates to All	Send the latest changes to all computers in the SecureWave Application Server(s) online table(s).	*43*

Use this option	*To*	*See page*
Computers		
Send Updates to	Send updates to one or more selected computers.	*43*
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.	*51*
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.	*50*
Purge Online Table	Remove all computers entries in the SecureWave Application Server(s) online table(s).	*111*

Table 4. The Tools Menu

The Reports menu

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

Use this option	*To*	*See page*
File Groups by User	Select one or more Users and/or Groups and generate a report of the File Groups they may use.	*114*
Users by File Group	Select one or more File Groups and generate a report of the Users and Groups given access to them.	*115*
User Options	Display all the user options defined in the system.	*116*
Machine Options	Display all the computer options defined in the system.	*117*
Online Machines	Show all machines currently recognized by the SecureWave Application Server that you are connected to.	*118*

Table 5. The Reports Menu

The Explorer menu

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

Use this option	*To*
In the Audit Logs Viewer module	
Clear all filters	Clean the searching info fields.
In the DB 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 *67* 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 *Map Network Drive* command.
Assign	Change the File Group to which a file is assigned.
Manage File Groups	Add, rename, and delete a File Group. See page *67* for more details.
In the Log Explorer module	
Fetch new log	Obtains the latest log from a client computer. See page *98* 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 *67* 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.
Assign	Change the File Group to which a file is assigned.
Manage File Groups	Add, rename, and delete a File Group. See page *67* for more details.
In the User Explorer module	
No options are available in the Explorer menu for this module.	

Table 6. The Explorer Menu

The Help menu

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

Use this option	*To*
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 7. The Help Menu

The six system modules

The functions you need for configuring and managing Sanctuary are logically grouped into six modules, represented by the icons on the left side of the screen:

Use this module		*To do this*	*See page*
Audit Logs Viewer		View logs of the administrators actions.	*101*
DB Explorer		View the list of executable files that have been entered into the Sanctuary database and manage file assignment details.	*105*
EXE Explorer		Build a list of executable files that are allowed to run, assigning these files to File Groups.	*55*
Log Explorer		View logs of applications that have been run, those to which access was denied, or those locally authorized after denial.	*91*
Scan Explorer		Scan a computer or domain to identify executable files that need to be authorized, and assign those files to a File Group.	*55*
User Explorer		Align users or User Groups with File Groups, to grant them permission to use the files in those File Groups.	*83*

Table 8. 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 *67*.

You will find detail information about how to use these functions 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 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 to be able to use at any time.

3. Organize approved executables into File Groups. An authorized Sanctuary system administrator can assign these files to File Groups, such as ‘Windows Operating System’, to simplify administration of related and/or interdependent files.

4. Associate files and File Groups with users. An authorized Sanctuary system administrator designates which files and File Groups can be used by which users and user 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 DB 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. Please see *Chapter 7: Authorizing software by location (path* rules) on page *75* 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.

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.*

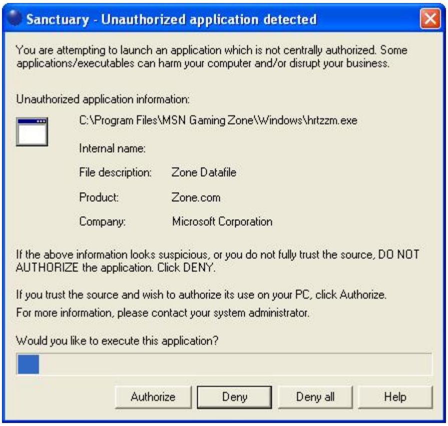
Local authorization

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.

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.



Sanctuary - Unauthorized application detected

You are attempting to launch an application which is not centrally authorized. Some applications/executables can harm your computer and/or disrupt your business.

Unauthorized application information:

C:\Program Files\MSN Gaming Zone\Windows\hrtzzm.exe

Internal name:

File description: Zone Datafile

Product: Zone.com

Company: Microsoft Corporation

If the above information looks suspicious, or you do not fully trust the source, DO NOT AUTHORIZE the application. Click DENY.

If you trust the source and wish to authorize its use on your PC, click Authorize.

For more information, please contact your system administrator.

Would you like to execute this application?

Figure 6: 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 *121* 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

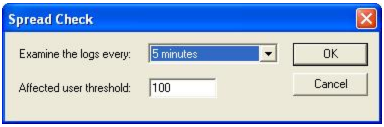
> Set the *Local Authorization* option to *Enable* (the default setting).

> Configure the *Blocking Mode* option to either *Ask user for *.exe only* or *Ask user always*.

See *Chapter 13: Setting system options* on page *121* for more details.

To prevent the malicious spread of locally authorized files

1. Select *Spread Check* from the *Tools* menu. The system displays the following dialog.



Spread Check

Examine the logs every: 5 minutes

Affected user threshold: 100

Figure 7. 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 Blocking mode 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. 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.

To push updates to a designated computer

1. Activate the *User Explorer* module (click on the corresponding icon in the Management sidebar).
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.
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.

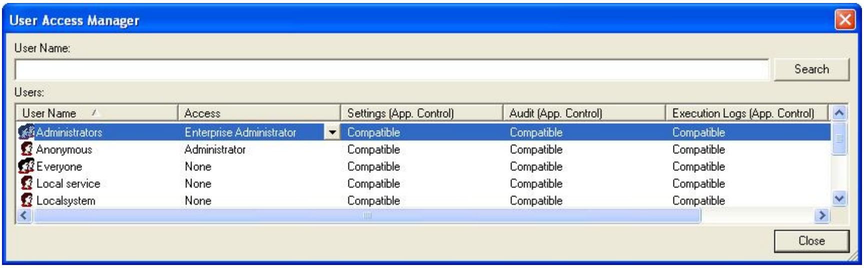
Once an Enterprise Administrator has been defined, he is the only one allowed to assign other users as regular Administrators. This chapter describes the process of setting up administrators to manage the Sanctuary system: an authorized Sanctuary *Enterprise Administrator* and a Sanctuary system *Administrator(s)*.

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 toolbar at the top of the management console display. The system displays the *User Access* dialog shown below.



User Name	Access	Settings (App. Control)	Audit (App. Control)	Execution Logs (App. Control)
Administrators	Enterprise Administrator	Compatible	Compatible	Compatible
Anonymous	Administrator	Compatible	Compatible	Compatible
Everyone	None	Compatible	Compatible	Compatible
Local service	None	Compatible	Compatible	Compatible
Localsystem	None	Compatible	Compatible	Compatible

Figure 8. 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 in the Sanctuary suite Console 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**

*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 permissions for a range of programs to a file and then import it 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 permissions. 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'. Please consult the *Setup Guide* for more information.

To export your settings:

1. Select the *Export Settings* item from the *Tools* menu.
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.

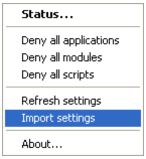


Figure 9: Importing a permission file

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 NT, 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.

You can import SecureWave File Definitions during the installation. This is the recommended process. 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 assignations are made. You can use them to save you time when you logically regroup executables files into file groups:

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

Table 9. 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 DB 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.

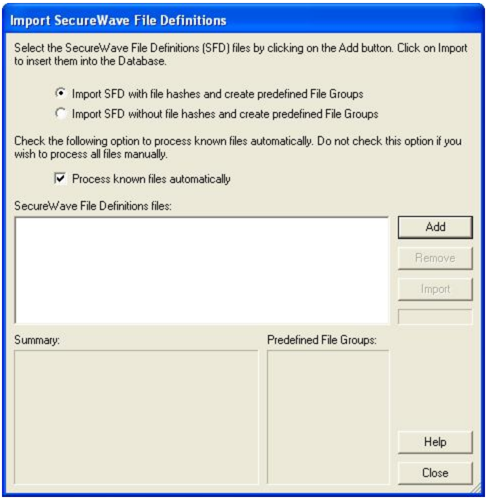
✍ *You should not import SFD files for OS or languages you do not use (or plan to use) in your environment.*

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. You 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 9. SecureWave File Definitions (SFD).*)



Import SecureWave File Definitions

Select the SecureWave File Definitions (SFD) files by clicking on the Add button. Click on Import to insert them into the Database.

● Import SFD with file hashes and create predefined File Groups

○ Import SFD without file hashes and create predefined File Groups

Check the following option to process known files automatically. Do not check this option if you wish to process all files manually.

☑ Process known files automatically

Figure 10. 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 specially important when doing system updates.*

✍ *When installing other products of our suite, check that the computer and user/group 'Blocking Mode' option is set to 'Non-blocking mode'. If this is not done, the setup cannot proceed. See Chapter 13: Setting system options on page* 121 *for more information.*

Selecting executable files from network directories

Using the EXE Explorer module (no 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* 45 *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* 63 *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 in 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
- a range of files in sub-directories of the \Program Files directory

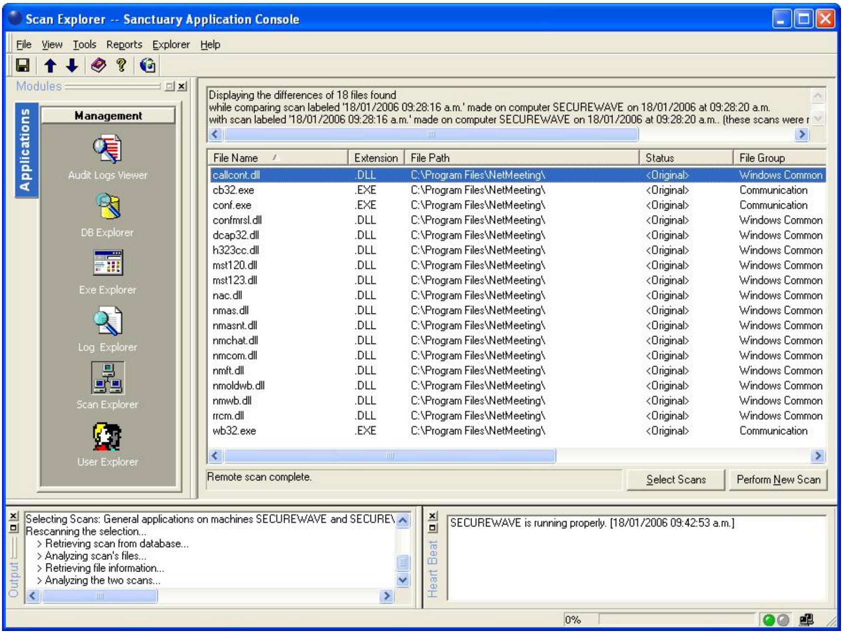
In this case, you could scan for these files by creating a template with the following two rules:

```
Scan all executables matching the pattern
*.exe or *.dll (without regard to case)
in directory
C:\WINDOWS
and its subdirectories

Scan all files matching the pattern
* (without regard to case)
in directory
C:\Program File\
and its subdirectories
```

See *To create a new template for scanning computers for executable files on page 57* for details on how to create a template.

The following illustration shows the Scan Explorer module main window:



Displaying the differences of 18 files found
while comparing scan labeled '18/01/2006 09:28:16 a.m.' made on computer SECUREWAVE on 18/01/2006 at 09:28:20 a.m.
with scan labeled '18/01/2006 09:28:16 a.m.' made on computer SECUREWAVE on 18/01/2006 at 09:28:20 a.m.. (these scans were r

File Name	Extension	File Path	Status	File Group
callcont.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
cb32.exe	.EXE	C:\Program Files\NetMeeting\	<Original>	Communication
conf.exe	.EXE	C:\Program Files\NetMeeting\	<Original>	Communication
confmrsl.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
dcap32.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
h323cc.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
mst120.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
mst123.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
nac.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
nmas.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
nmasnt.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
nmchat.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
nmcom.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
nmft.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
nmoldwb.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
nmwb.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
rrcm.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
wb32.exe	.EXE	C:\Program Files\NetMeeting\	<Original>	Communication

Remote scan complete.

```
Selecting Scans: General applications on machines SECUREWAVE and SECURE\
Rescanning the selection...
  > Retrieving scan from database...
  > Analyzing scan's files...
  > Retrieving file information...
  > Analyzing the two scans...
```

SECUREWAVE is running properly. [18/01/2006 09:42:53 a.m.]

Figure 11. Scan Explorer module main window

To create a new template for scanning computers for executable files

1. Click the *Scan Explorer* icon from the Management sidebar.
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:

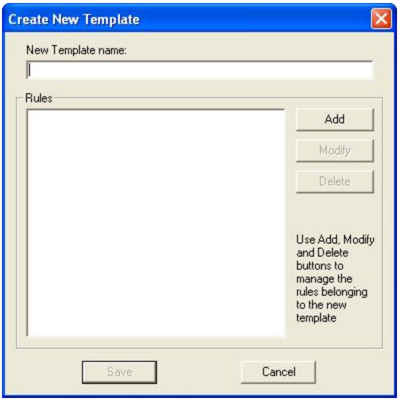

Create New Template
New Template name:
Rules
Add
Modify
Delete
Use Add, Modify and Delete buttons to manage the rules belonging to the new template
Save
Cancel

Figure 12. 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 at all).*

In directory

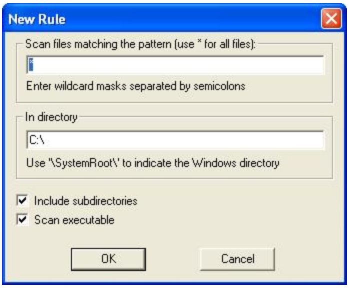
Enter the path of the directory you want to scan.
Use '`\SystemRoot\`' with this capitalization to indicate the Windows directory.

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.



New Rule

Scan files matching the pattern (use * for all files):

Enter wildcard masks separated by semicolons

In directory

C:\

Use '\SystemRoot\' to indicate the Windows directory

☑ Include subdirectories

☑ Scan executable

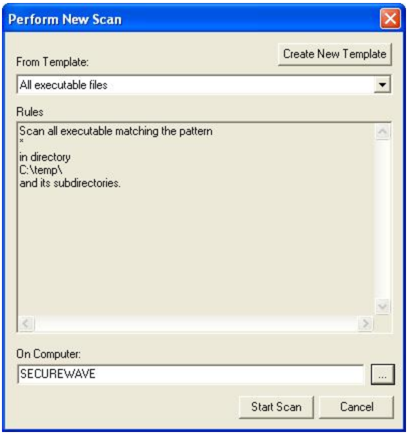
Figure 13. Insert New Path Rule Dialog

1. 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 from the Management sidebar.
2. Click on the PERFORM NEW SCAN button. The following dialog opens:



Perform New Scan

From Template: All executable files

Rules

Scan all executable matching the pattern
*
in directory
C:\temp\
and its subdirectories.

On Computer: SECUREWAVE

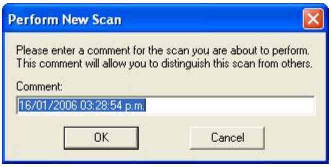
Figure 14. Perform New Scan Dialog

3. In the *From Template* field, choose all files (we are supposing that you already created a template with that name. See *To create a new template for scanning computers for executable files* on page *57*).

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.



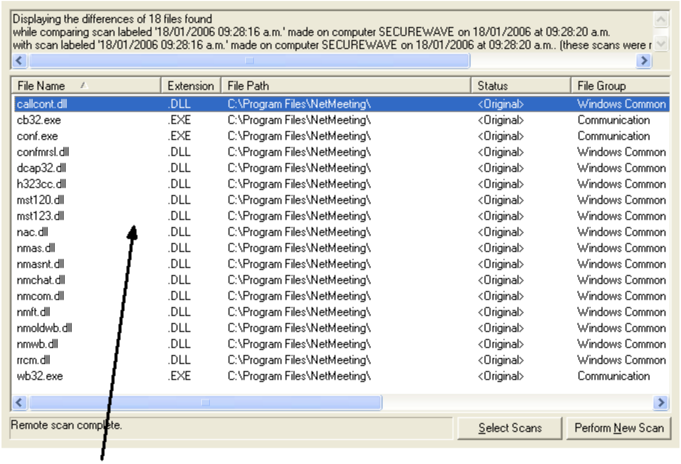
Perform New Scan

Please enter a comment for the scan you are about to perform.
This comment will allow you to distinguish this scan from others.

Comment: 16/01/2006 03:28:54 p.m.

Figure 15. 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 something like this:



Displaying the differences of 18 files found
while comparing scan labeled '18/01/2006 09:28:16 a.m.' made on computer SECUREWAVE on 18/01/2006 at 09:28:20 a.m.
with scan labeled '18/01/2006 09:28:16 a.m.' made on computer SECUREWAVE on 18/01/2006 at 09:28:20 a.m.. (these scans were r

File Name	Extension	File Path	Status	File Group
callcont.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
cb32.exe	.EXE	C:\Program Files\NetMeeting\	<Original>	Communication
conf.exe	.EXE	C:\Program Files\NetMeeting\	<Original>	Communication
confmrsl.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
dcap32.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
h323cc.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
mst120.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
mst123.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
nac.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
nmas.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
nmasnt.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
nmchat.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
nmcom.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
nmft.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
nmoldwb.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
nmwb.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
rrcm.dll	.DLL	C:\Program Files\NetMeeting\	<Original>	Windows Common
wb32.exe	.EXE	C:\Program Files\NetMeeting\	<Original>	Communication

Remote scan complete.

Files are displayed with a *Status* that determines the difference between two scans (if already done)

Figure 16. 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.

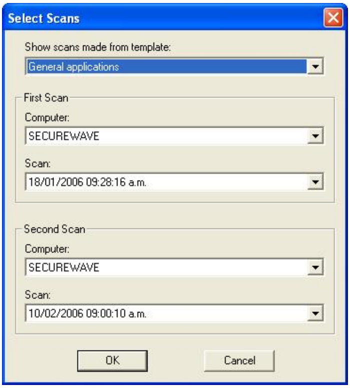
5. Click on the START SCAN button to display the *Comment* dialog. If you wish, enter a comment that defines this scan. Use a descriptive name, especially if you plan to compare two scans afterwards.

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 *Explorer* and *Select Scans* from the toolbar at the top of the screen. The following dialog is displayed.



Show scans made from template: General applications

First Scan
Computer: SECUREWAVE
Scan: 18/01/2006 09:28:16 a.m.

Second Scan
Computer: SECUREWAVE
Scan: 10/02/2006 09:00:10 a.m.

Figure 17. 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 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:

   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.

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. For more information, refer to *Chapter 8: Assigning access permissions to users and groups* on page *83*.

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

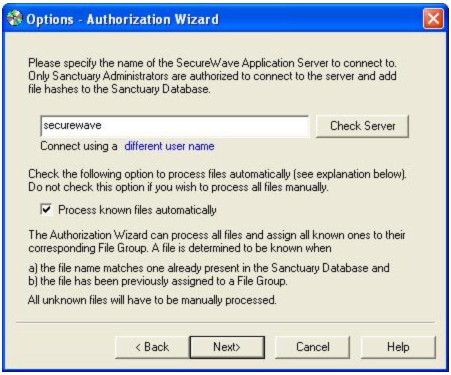
The Authorization Wizard can perform these tasks for Windows operating systems, applications, and service packs, even those packaged in ZIP files, self-extracting ZIP archives, RAR, MSI, and Microsoft CAB files.

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 APPLICATION CONTROL → 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*.*



Please specify the name of the SecureWave Application Server to connect to. Only Sanctuary Administrators are authorized to connect to the server and add file hashes to the Sanctuary Database.

securewave

Connect using a different user name

Check the following option to process files automatically (see explanation below). Do not check this option if you wish to process all files manually.

☑ Process known files automatically

The Authorization Wizard can process all files and assign all known ones to their corresponding File Group. A file is determined to be known when

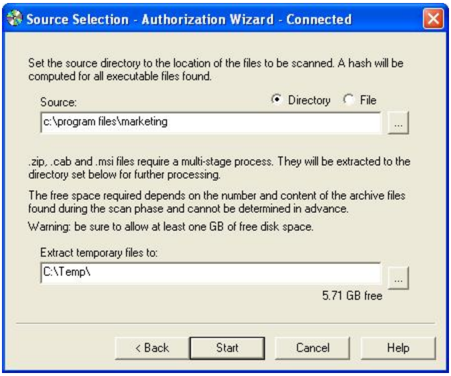
a) the file name matches one already present in the Sanctuary Database and
b) the file has been previously assigned to a File Group.

All unknown files will have to be manually processed.

Figure 18. 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.

5. 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.



Set the source directory to the location of the files to be scanned. A hash will be computed for all executable files found.

Source: ● Directory ○ File

c:\program files\marketing

.zip, .cab and .msi files require a multi-stage process. They will be extracted to the directory set below for further processing.

The free space required depends on the number and content of the archive files found during the scan phase and cannot be determined in advance.

Warning: be sure to allow at least one GB of free disk space.

Extract temporary files to:

C:\Temp\

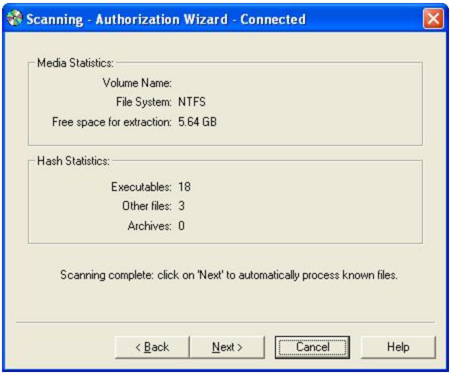
5.71 GB free

Figure 19. 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 this directory has sufficient free disk space.*

6. 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.



Media Statistics:

Volume Name:

File System: NTFS

Free space for extraction: 5.64 GB

Hash Statistics:

Executables: 18

Other files: 3

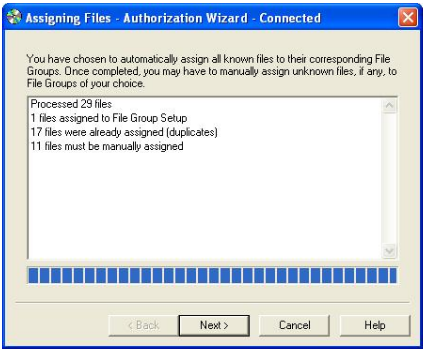
Archives: 0

Scanning complete: click on 'Next' to automatically process known files.

Figure 20. 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.



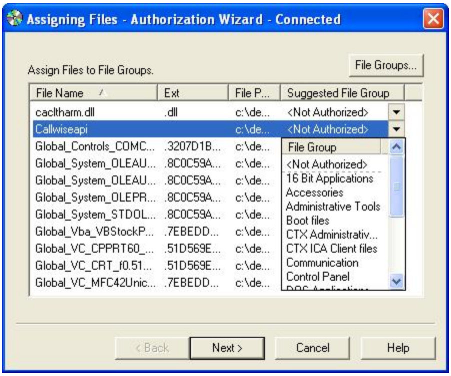
You have chosen to automatically assign all known files to their corresponding File Groups. Once completed, you may have to manually assign unknown files, if any, to File Groups of your choice.

```
Processed 29 files
1 files assigned to File Group Setup
17 files were already assigned (duplicates)
11 files must be manually assigned
```

Figure 21. 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 assign files to File Groups.



Assign Files to File Groups.

File Name	Ext	File P...	Suggested File Group
cacltharm.dll	.dll	c:\de...	<Not Authorized>
Callwiseapi		c:\de...	<Not Authorized>
Global_Controls_COMC...	.3207D1B...	c:\de...	
Global_System_OLEAU...	.8C0C59A...	c:\de...	
Global_System_OLEAU...	.8C0C59A...	c:\de...	
Global_System_OLEPR...	.8C0C59A...	c:\de...	
Global_System_STDOL...	.8C0C59A...	c:\de...	
Global_Vba_VBStockP...	.7EBEDD...	c:\de...	
Global_VC_CPPRT60_...	.51D569E...	c:\de...	
Global_VC_CRT_f0.51...	.51D569E...	c:\de...	
Global_VC_MFC42Unic...	.7EBEDD...	c:\de...	

Figure 22. Authorization Wizard: Assigning Files to File Groups

11. Once you finish assigning, click on NEXT to insert the new definitions into the database. Note that you have to update access permissions to enable users/administrators — using the *User Explorer* module — to run these new applications. The updated applications are placed on the existing File Groups already assigned to users.

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 can logically group them to be managed together.

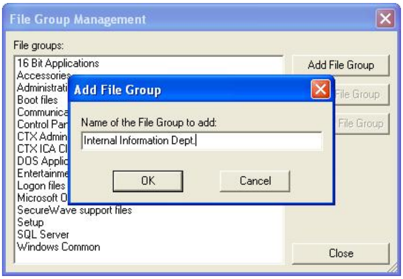
You may set up File Groups to reflect the way you want to administer the solution. For example, you might create an IIS (Internet Information Server) group to associate together all network services needed by your Web master when protecting servers in your organization or a Marketing group to cluster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

Creating and managing File Groups

To create a new File Group

1. Open either the DB Explorer, Scan Explorer, Log Explorer, or Exe Explorer module (click the appropriate icon in the Management sidebar of the management console).
2. Select *Manage File Groups* from the *Explorer* menu. The system displays the corresponding dialog.

   If you are working in the DB Explorer, Exe Explorer, or Log Explorer module, you could also select *Assign* from the *Explorer* menu and then click on the FILE GROUPS button in the *Assign Files to File Groups* dialog.
3. Click the ADD FILE GROUP button at the top right of the dialog. The system displays the corresponding dialog.



Name of the File Group to add: Internal Information Dept.

Figure 23. 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. Working in the DB Explorer, Exe Explorer, Log Explorer, or Scan Explorer module, select *Manage File Groups* from the *Explorer* menu. The system displays the *File Group Management* dialog.

   If you are working in the DB Explorer, Exe Explorer, or Log Explorer module, you could also select *Assign* from the *Explorer* menu and then click FILE GROUPS in the dialog.

2. 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.

3. 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.*

To rename a File Group

1. Working in the DB Explorer, Exe Explorer, Log Explorer, or Scan Explorer module, select *Manage File Groups* from the *Explorer* menu. The system displays the *File Group Management* dialog.

   If you are working in the DB Explorer, Exe Explorer, or Log Explorer module, you could also select *Assign* from the *Explorer* menu and then click FILE GROUPS in the dialog.

2. Click the RENAME FILE GROUP button. The system displays the *Rename File Group* dialog.

3. Type the new name of the File Group and click OK. The new File Group name will appear in the *File Group Management* dialog.

Assigning executable files to File Groups

Now that you have created the File Groups 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 DB Explorer, Scan Explorer, Log Explorer, or Exe Explorer module (click the appropriate icon in the Management sidebar). 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.
3. Right-click the mouse button and select ASSIGN TO FILE GROUP

   — or —

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

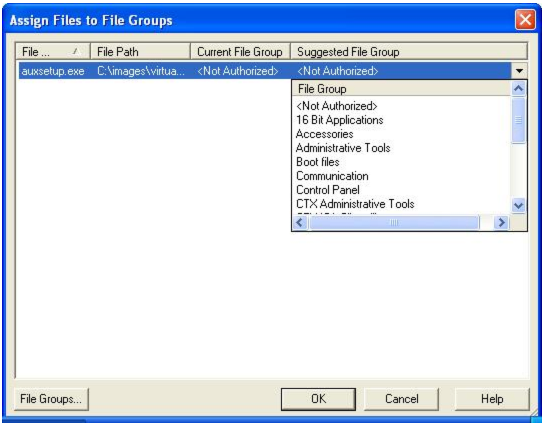
   — or —

   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>.

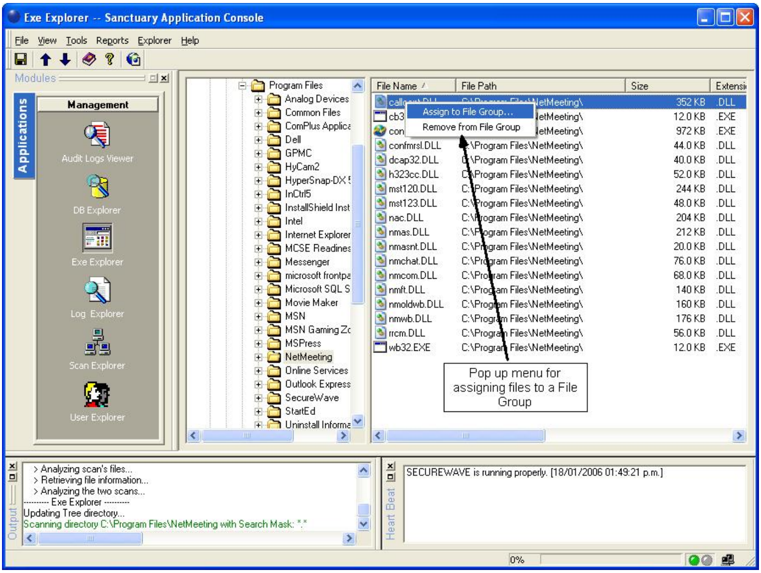
   The *Suggested File Group* column proposes a File Group based on the filename. If a file with the same name already appears in the database (perhaps a different version of the same application), the system suggests the same File Group to which the earlier file belongs — typically a very appropriate choice.



File ...	File Path	Current File Group	Suggested File Group
auxsetup.exe	C:\images\virtua...	<Not Authorized>	<Not Authorized>

Figure 24: Assigning files to file groups

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



File Name	File Path	Size	Extensi
call	…etMeeting\	352 KB	.DLL
cb3	…etMeeting\	12.0 KB	.EXE
con	…etMeeting\	972 KB	.EXE
confmrsl.DLL	C:\Program Files\NetMeeting\	44.0 KB	.DLL
dcap32.DLL	C:\Program Files\NetMeeting\	40.0 KB	.DLL
h323cc.DLL	C:\Program Files\NetMeeting\	52.0 KB	.DLL
mst120.DLL	C:\Program Files\NetMeeting\	244 KB	.DLL
mst123.DLL	C:\Program Files\NetMeeting\	48.0 KB	.DLL
nac.DLL	C:\Program Files\NetMeeting\	204 KB	.DLL
nmas.DLL	C:\Program Files\NetMeeting\	212 KB	.DLL
nmasnt.DLL	C:\Program Files\NetMeeting\	20.0 KB	.DLL
nmchat.DLL	C:\Program Files\NetMeeting\	76.0 KB	.DLL
nmcom.DLL	C:\Program Files\NetMeeting\	68.0 KB	.DLL
nmft.DLL	C:\Program Files\NetMeeting\	140 KB	.DLL
nmoldwb.DLL	C:\Program Files\NetMeeting\	160 KB	.DLL
nmwb.DLL	C:\Program Files\NetMeeting\	176 KB	.DLL
rrcm.DLL	C:\Program Files\NetMeeting\	56.0 KB	.DLL
wb32.EXE	C:\Program Files\NetMeeting\	12.0 KB	.EXE

```
  > Analyzing scan's files...
  > Retrieving file information...
  > Analyzing the two scans...
--------- Exe Explorer ---------
Updating Tree directory...
Scanning directory C:\Program Files\NetMeeting with Search Mask: *.*
```

```
SECUREWAVE is running properly. [18/01/2006 01:49:21 p.m.]
```

Figure 25. Assigning a File Group from the EXE Explorer module

✍ *You can perform the same action on files displayed in the Exe Explorer, DB 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 any more.

> 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 you are confident that the files can be trusted, you can add them to the Sanctuary database directly from the Log Explorer screen. 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 DB Explorer, Scan Explorer, Log Explorer, or Exe Explorer module, select the file or a range of files to reassign.
2. Right-click the mouse button and select *Assign Files to File Groups* to display the corresponding dialog.
3. To accept the suggested file group, select the file(s) and click OK. To choose a different one, click the FILE GROUPS button 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 DB 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 as <Not Authorized>.

To delete a file from the Sanctuary database altogether

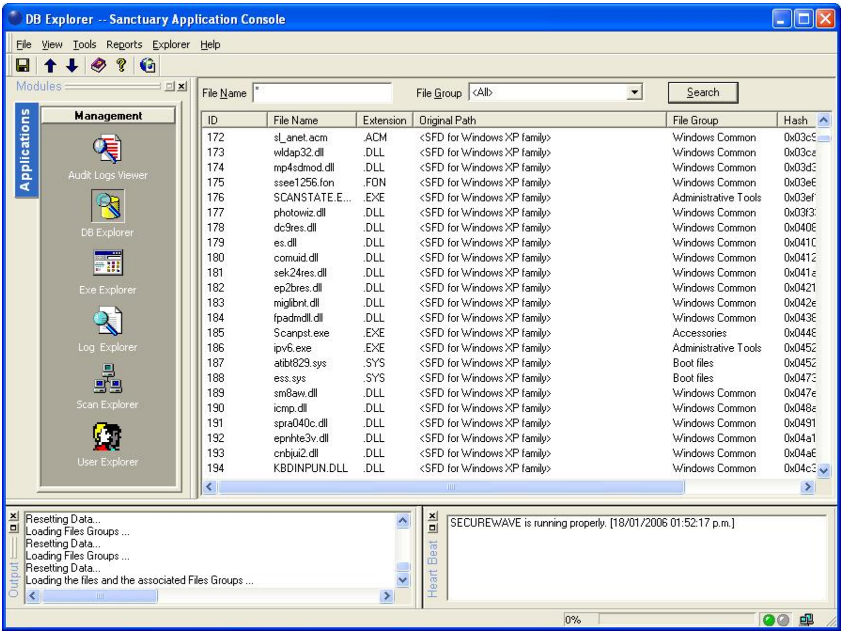
1. In the DB Explorer screen, select the file or range of files you want to delete.
2. Right click and select *Delete* from the pop-up dialog box. Click OK.

You cannot undo this delete operation. If you accidentally delete a file you wished to keep, use the DB 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 DB 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.

Here is a typical DB Explorer listing:



File Name *

File Group <All>

ID	File Name	Extension	Original Path	File Group	Hash
172	sl_anet.acm	.ACM	<SFD for Windows XP family>	Windows Common	0x03c5
173	wldap32.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x03ca
174	mp4sdmod.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x03d3
175	ssee1256.fon	.FON	<SFD for Windows XP family>	Windows Common	0x03e6
176	SCANSTATE.E...	.EXE	<SFD for Windows XP family>	Administrative Tools	0x03ef
177	photowiz.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x03f3
178	dc9res.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x0408
179	es.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x0410
180	comuid.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x0412
181	sek24res.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x041a
182	ep2bres.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x0421
183	miglibnt.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x042e
184	fpadmdll.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x0438
185	Scanpst.exe	.EXE	<SFD for Windows XP family>	Accessories	0x0448
186	ipv6.exe	.EXE	<SFD for Windows XP family>	Administrative Tools	0x0452
187	atibt829.sys	.SYS	<SFD for Windows XP family>	Boot files	0x0452
188	ess.sys	.SYS	<SFD for Windows XP family>	Boot files	0x0473
189	sm8aw.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x047e
190	icmp.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x048a
191	spra040c.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x0491
192	epnhte3v.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x04a1
193	cnbjui2.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x04a6
194	KBDINPUN.DLL	.DLL	<SFD for Windows XP family>	Windows Common	0x04c3

```
Resetting Data...
Loading Files Groups ...
Resetting Data...
Loading Files Groups ...
Resetting Data...
Loading the files and the associated Files Groups ...
```

```
SECUREWAVE is running properly. [18/01/2006 01:52:17 p.m.]
```

Figure 26. The DB Explorer Module

This display works just like a typical 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 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 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.

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 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 administrators, 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 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 belongs or is member of the group of Trusted Owners and is the owner of the executable file.

To create a new path rule that applies to everybody

1. Select *Path Rules* from the *Tools* menu. The following dialog appears:

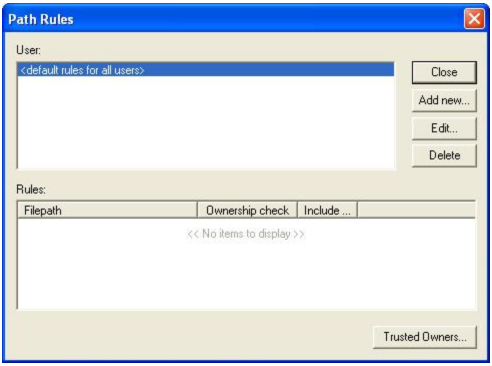


Figure 27. The Path Rules Dialog

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

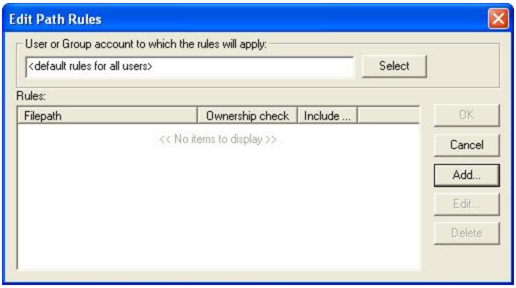

Edit Path Rules
User or Group account to which the rules will apply:
<default rules for all users>
Select
Rules:
Filepath
Ownership check
Include ...
<< No items to display >>
OK
Cancel
Add...
Edit...
Delete

Figure 28. 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 to display the corresponding dialog.
2. Click on the ADD NEW button. The following dialog appears:

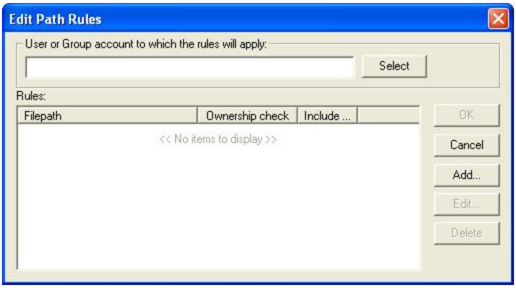


Figure 29. Adding a Path Rule

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 or empty file specification, the file will not be found, but no error or warning message is issue.*

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* check box when setting a Path Rule, the Sanctuary system will only permit execution of files owned by a user who is a Trusted Owner or a member of a Group listed as a Trusted Owner.

To define or delete a Trusted Owner

1. Select PATH RULES from the *Tools* menu.
2. Click the TRUSTED OWNERS button in the *Path Rules* dialog. The following dialog appears:

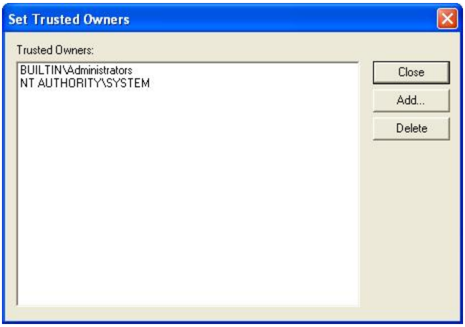


Figure 30. Setting Trusted Owners

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

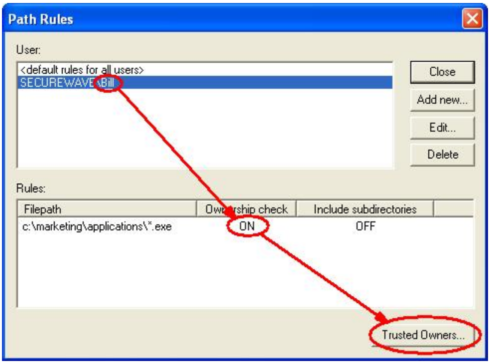
You can use this same dialog to delete a Trusted Owner by selecting it and clicking on the DELETE button.

Trusted Owner and Path Rule example

As an Administrator, you can create different Path Rules (see *Creating, changing, and deleting path rules* on page *75*) 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.



<default rules for all users>
SECUREWAVE\Bill

Filepath	Ownership check	Include subdirectories
c:\marketing\applications*.exe	ON	OFF

Figure 31. Setting Path Rules with Ownership Checking

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

If you are using Sanctuary in a Novell environment, be aware that Trusted Owners will not work with Novell’s users.

Path rules precedence

When defining Path Rules (*Tools→Path Rules*), 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:

Type of Path Rule defined:	The user does not forms part of the group	The user forms part of the group
	Will the application run?	
Default rule for all users	Yes	Yes
For the group	No	Yes
For the specific User	Yes	Yes

Table 10. 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 and User Groups, to define who can do what.

✍ *An explanation note about 'administrators' and 'users.'*

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 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 and bind them to File Groups

— or —

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

Both functions are easily accessible in the User Explorer module, and both approaches yield the same result — linking users and 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

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 this File Groups to a user. In this section, we also explain you how to perform this last step.

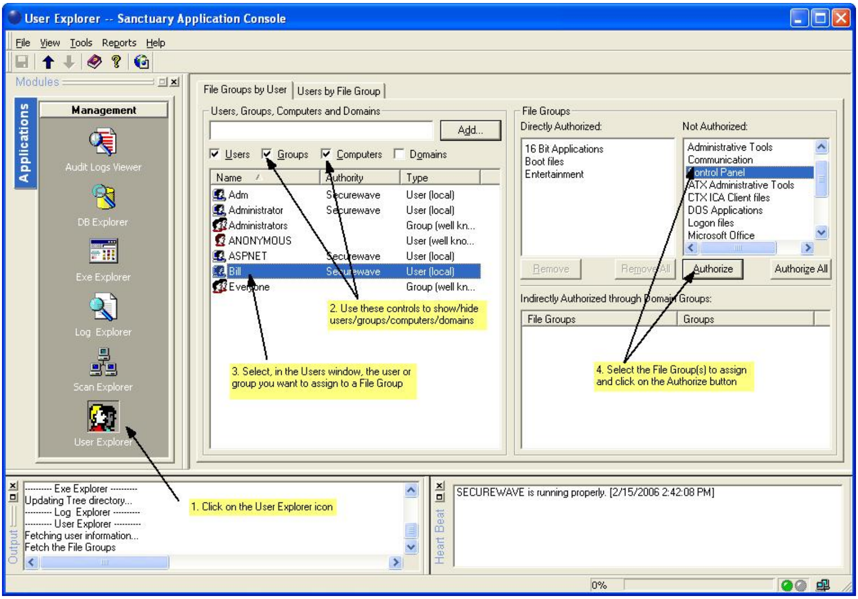
To assign/remove File Groups to/from a user

1. Open the *User Explorer* module (click the User Explorer icon in the Management sidebar).
2. Click on the *File Groups by User* tab.
3. In the *Users* panel, select a user or group of users. The *File Groups* panel shows you the File Groups for which this user/group already has authorization, which ones are not authorized, and which are indirectly authorized because the user belongs to a domain group that has authorization.

   To add a 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 he belongs to changes.



Name	Authority	Type
Adm	Securewave	User (local)
Administrator	Securewave	User (local)
Administrators		Group (well kn...
ANONYMOUS		User (well kno...
ASPNET	Securewave	User (local)
Bill	Securewave	User (local)
Everyone		Group (well kn...

Directly Authorized:

16 Bit Applications
Boot files
Entertainment

Not Authorized:

Administrative Tools
Communication
Control Panel
ATX Administrative Tools
CTX ICA Client files
DOS Applications
Logon files
Microsoft Office

```
---------- Exe Explorer ----------
Updating Tree directory...
---------- Log Explorer ----------
---------- User Explorer ----------
Fetching user information...
Fetch the File Groups
```

```
SECUREWAVE is running properly. [2/15/2006 2:42:08 PM]
```

1. Click on the User Explorer icon

2. Use these controls to show/hide users/groups/computers/domains

3. Select, in the Users window, the user or group you want to assign to a File Group

4. Select the File Group(s) to assign and click on the Authorize button

Figure 32. The User Explorer Module Window: File Groups by User

4. If you want to activate the change immediately, send the updated authorization to affected machines.

   To send the new authorization information to all machines, select *Send Updates to All Computers* from the *Tools* menu.

   To push updates to a specific computer, select *Send Updates to <name>* from the *Tools* menu 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* 121*.*

Assigning users to File Groups

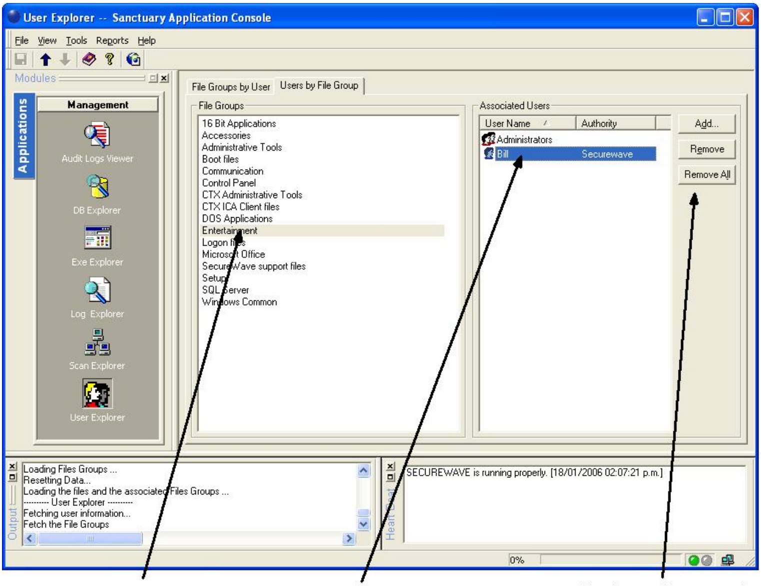
You may want to assign users to new File Groups, rather than the other way around. For instance, you may have created a File Group for all the executables in an updated version of an already authorized application. The next step is to grant users the access to the newly created File Group.

To assign/remove users to/from a File Group

1. Open the *User Explorer* module (click the User Explorer icon in the Management sidebar).
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. Click on the ADD, REMOVE, or REMOVE ALL button to insert or delete users from the File Group.



File Groups:

16 Bit Applications
Accessories
Administrative Tools
Boot files
Communication
Control Panel
CTX Administrative Tools
CTX ICA Client files
DOS Applications
Entertainment
Logon files
Microsoft Office
SecureWave support files
Setup
SQL Server
Windows Common

User Name	Authority
Administrators	
Bill	Securewave

```
Loading Files Groups ...
Resetting Data...
Loading the files and the associated Files Groups ...
--------- User Explorer ---------
Fetching user information...
Fetch the File Groups
```

```
SECUREWAVE is running properly. [18/01/2006 02:07:21 p.m.]
```

Select, in the File Groups window, the one you want to analyze.

Select, in the Associated Users window, the association you want to delete/add.

Use the control buttons to select the desired action.

Figure 33. 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's 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 a user in the system and checking his access privileges. When a request comes from a user to activate an application:

> The SecureWave Application Server checks the digital signature of the requested application against those of approved applications in the database.

> If the application is on the approved list, then the program runs. Only authorized applications 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.

You can also find other useful information in these sections:

> *Chapter 5: Building a list of executable files to be managed* on page *49*, describes several key ways to populate the database of approved applications.

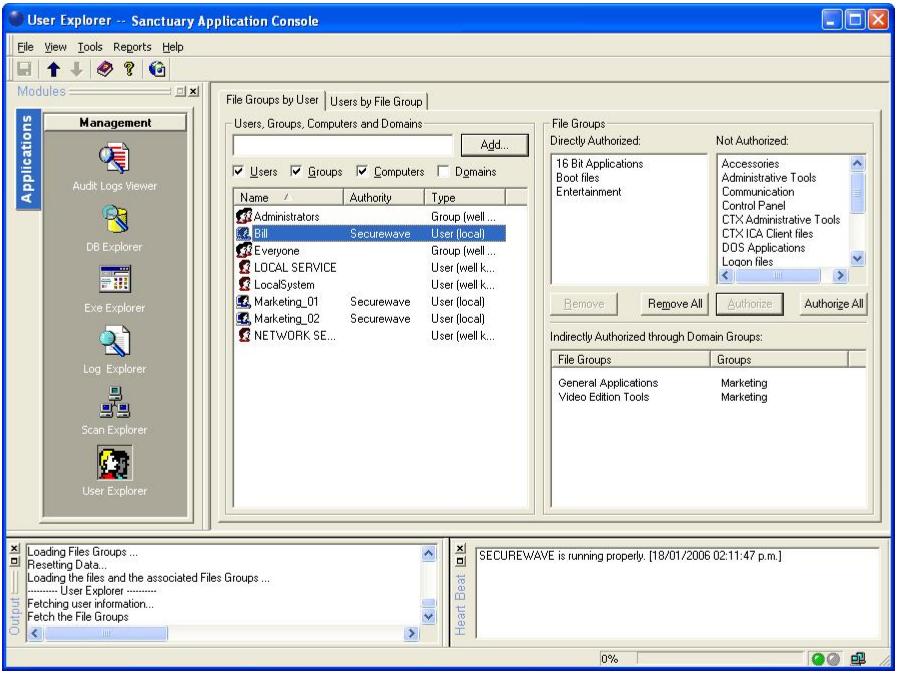
> *Assigning File Groups to users*, in this chapter, describes the process of linking approved files and approved users to establish a robust security strategy.

Defining user groups

Most of the time, File Groups will be associated with Domain 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 then use all programs that are authorized for the groups of which he is a member.

The following image shows an example of the domain user ‘Bill’ having three File Groups indirectly authorized because of assignments made to Domain Users domain group, several not authorized, and two groups directly authorized.



Name	Authority	Type
Administrators		Group (well ...
Bill	Securewave	User (local)
Everyone		Group (well ...
LOCAL SERVICE		User (well k...
LocalSystem		User (well k...
Marketing_01	Securewave	User (local)
Marketing_02	Securewave	User (local)
NETWORK SE...		User (well k...

Directly Authorized:

16 Bit Applications
Boot files
Entertainment

Not Authorized:

Accessories
Administrative Tools
Communication
Control Panel
CTX Administrative Tools
CTX ICA Client files
DOS Applications
Logon files

Indirectly Authorized through Domain Groups:

File Groups	Groups
General Applications	Marketing
Video Edition Tools	Marketing

```
Loading Files Groups ...
Resetting Data...
Loading the files and the associated Files Groups ...
--------- User Explorer ---------
Fetching user information...
Fetch the File Groups
```

```
SECUREWAVE is running properly. [18/01/2006 02:11:47 p.m.]
```

Figure 34: 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

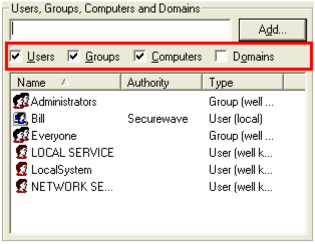
This is a built-in account that is used to run services on Windows 2000, XP, and 2003 operating systems. Services run under dedicated accounts like LocalSystem. You must grant these accounts the right to use the corresponding File Groups. For example, if you create a 'Windows' File Group where you put all operating system executable files (including Windows services that run with the *LocalSystem* account), you should grant *LocalSystem* the right to use the '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. This is not true if you are using a SecureWave Application Server from a Sanctuary Device Control installation.

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:



Users, Groups, Computers and Domains

☑ Users ☑ Groups ☑ Computers ☐ Domains

Name	Authority	Type
Administrators		Group (well ...
Bill	Securewave	User (local)
Everyone		Group (well ...
LOCAL SERVICE		User (well k...
LocalSystem		User (well k...
NETWORK SE...		User (well k...

Figure 35. User's tree

Use the 'Synchronize Domain Members' item on the 'Tools' menu to include the local users of a computer in the Database or if you do not see all your users/groups.

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)

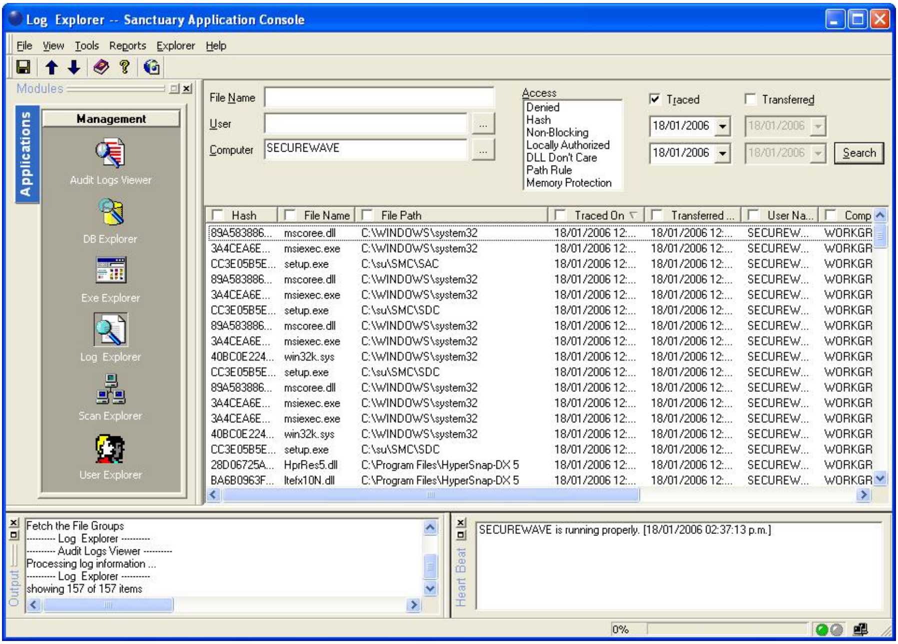
The Log Explorer module does more than display this information. From within the log displays you can also:

- Authorize the use of files that have been denied
- Save the logs to a CSV file (comma-separated values)

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.

Here is a typical *Log Explorer* screen:



File Name
User
Computer SECUREWAVE

Access: Denied, Hash, Non-Blocking, Locally Authorized, DLL Don't Care, Path Rule, Memory Protection

☑ Traced 18/01/2006 – 18/01/2006

□ Transferred 18/01/2006 – 18/01/2006

Search

□ Hash	□ File Name	□ File Path	□ Traced On	□ Transferred ...	□ User Na...	□ Comp
89A583886...	mscoree.dll	C:\WINDOWS\system32	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR
3A4CEA6E...	msiexec.exe	C:\WINDOWS\system32	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR
CC3E05B5E...	setup.exe	C:\su\SMC\SAC	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR
89A583886...	mscoree.dll	C:\WINDOWS\system32	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR
3A4CEA6E...	msiexec.exe	C:\WINDOWS\system32	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR
CC3E05B5E...	setup.exe	C:\su\SMC\SDC	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR
89A583886...	mscoree.dll	C:\WINDOWS\system32	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR
3A4CEA6E...	msiexec.exe	C:\WINDOWS\system32	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR
40BC0E224...	win32k.sys	C:\WINDOWS\system32	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR
CC3E05B5E...	setup.exe	C:\su\SMC\SDC	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR
89A583886...	mscoree.dll	C:\WINDOWS\system32	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR
3A4CEA6E...	msiexec.exe	C:\WINDOWS\system32	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR
3A4CEA6E...	msiexec.exe	C:\WINDOWS\system32	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR
40BC0E224...	win32k.sys	C:\WINDOWS\system32	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR
CC3E05B5E...	setup.exe	C:\su\SMC\SDC	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR
28D06725A...	HprRes5.dll	C:\Program Files\HyperSnap-DX 5	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR
BA6B0963F...	ltefx10N.dll	C:\Program Files\HyperSnap-DX 5	18/01/2006 12:...	18/01/2006 12:...	SECUREW...	WORKGR

```
Fetch the File Groups
--------- Log  Explorer ---------
--------- Audit Logs Viewer ---------
Processing log information ...
--------- Log  Explorer ---------
showing 157 of 157 items
```

```
SECUREWAVE is running properly. [18/01/2006 02:37:13 p.m.]
```

Figure 36. The Log Explorer Module

To view existing logs of system activity

1. Click the *Log Explorer* icon 🔍 in the Management sidebar.
2. Choose the criteria to refine your log search from these fields:

Criteria field	*Description*	
File Name	Restrict the query to files that match a given pattern. You can use standard Windows wildcards, such as ? and *. For instance, 'Notep*' will return all log entries that have filenames beginning with 'Notep'. You can also use a semicolon to separate file names. Other special characters are considered part of the file's name.	
Traced	Restrict the query to a period, based on when the execution attempt took place on the protected client.	
Transferred	Restrict the query to a period, based on when execution logs were uploaded to the SecureWave Application Server.	
User	Display log files for a designated user.	
Computer	Display log files for a designated computer.	
Access	Limit the query to certain access types:	
	Denied	Only files that were not allow to execute.
	Hash	Only those files that were allowed to execute.
	Non-blocking	Files that could be run because a non-blocking option was on (for computer/user/group).
	Path Rule	Only those files that were run because they correspond to a Path Rule.
	Locally authorized	Files that users locally authorized (overriding a denial from the central system) — including the application modules for which the user had to make a decision.
	DLL don't care	Files that users locally authorized implicitly as being attached to a locally authorized executable.

✍ *When searching by 'User name' or 'Computer name', you can enter part of the field and display the 'Search' dialog by pressing* E*NTER* *or clicking the ellipsis [...] button.*

Table 11. Criteria to Refine Log Searches

3. Click on the SEARCH button to display log entries that match your criteria.

Navigating in the Log Explorer display

When you enter search criteria and click on the SEARCH button, the system returns a list of records that match your criteria. This can be a vast amount of information, so it is helpful to know:

- What type of information you can see in the Log Explorer display.
- How to sort that information to find just what you want.
- A shortcut for authorizing files that seem to be required and safe.

The information shown in the Log Explorer display

The *Log Explorer* result panel returns the following information for each entry:

Column	*Description*
Hash	The digital signature of the file, created by SHA-1 (Secure Hash Algorithm -1). Knowing the hash enables you to differentiate between dissimilar files with the same name.
File Name	The file whose execution was authorized or denied.
File Path	The path of the file whose execution was authorized or denied.
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.
User name	The name of the user who attempted to execute the file.
Computer	The name of the machine that attempted to execute the file.
Access	Show the status of the file as defined on *Table 13. Possible Access Field Values.*
File Group	The file group to which the file has been assigned. Can also be <Not Authorized>.
Count	How many times the file has been acceded, it does not matter if the file was authorized or not to run.
Extension	The extension of the file.

Table 12. The Log Explorer Module Result Panel Information

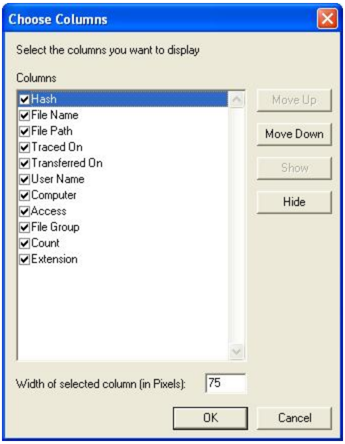
The ACCESS field will show any of the following values, which are affected by system-wide option settings for blocking mode and logging mode:

Value in the Access Field	*Description*	*The file ran?*
Denied	The file was not allowed to run because it was neither centrally nor locally authorized (and the blocking option or mode was set to prompt users for local authorization).	No
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-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-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-pathRule	This file would have been denied based on central authorization based on hashes, but it was executed because it matched a Path Rule.	Yes
ok-localAuth	This file would have been denied because it is not centrally authorized, but the user was prompted to locally authorize, and he/she allowed execution.	Yes
ok-dllDontCare	An executable file dependency (for example, an EXE file that needs a DLL to run) was not centrally authorized, but the user was prompted to authorize the file locally, and chose to do so.	Yes
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
Logon	An unauthorized program (script, application) tried to run during the logon. This depends on the *Relaxed logon* setting. See *Table 17* for more details.	Yes

Table 13. Possible Access Field Values

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.

You can choose which columns to display using the *Choose Columns* dialog. To open it, select the *Choose Columns* item of the *View* menu (valid only while you are on the *Log Explorer* module). Check/uncheck/move the columns to suit your needs:



Select the columns you want to display

Columns

☑ Hash
☑ File Name
☑ File Path
☑ Traced On
☑ Transferred On
☑ User Name
☑ Computer
☑ Access
☑ File Group
☑ Count
☑ Extension

Width of selected column (in Pixels): 75

Figure 37: Choose columns dialog for the Log Explorer module

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 a file from running:

> The file is unknown and, hence, it is not authorized. It has never been scan, does not exit on the 'white list' definition 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.

You should never authorize applications by direct inference from the log file 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.

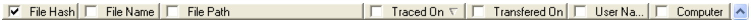
The ok-dllDontCare access relates to using programs that need an external DLL(s). This is a special ‘Local Authorization’ mode where the user should not only locally allow the unauthorized application to run but also all its related DLLs. In this way a user can, for example, locally authorize the execution of a software, be warned of all necessary external elements, and control the loading of each additional component or ActiveX.

Sorting entries in the Log Explorer display

Each column in the *Log Explorer* display has a check box in the column header. Click a check box to sort/group the elements by that attribute.

For instance, if you click the check box in the *File Name* column, the system will group all files with the same name, and display a new Count column that shows how many times a file with the same name is in the log.

You can group by multiple columns, but grouping is not cumulative and there is no hierarchy of order. For instance, if you group by ‘File name’ and date ‘Traced On’, you will get a list of unique file names for every date.



☑ File Hash | □ File Name | □ File Path | □ Traced On | □ Transfered On | □ User Na... | □ Computer

Figure 38. Sorting entries in the Log Explorer

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.

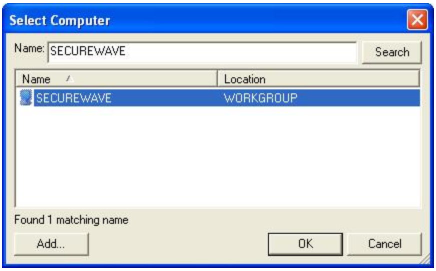
Be careful when authorizing files directly from the 'Log Explorer'. There is no guarantee that they are not infected with a virus or that the end user has attempted to run a rogue application under another name. For maximum security, it is best to authorize applications only from trusted sources. A user may also try to fool you renaming the file to an apparently inoffensive one.

Forcing an upload of the latest log files

Once a day, 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 in the Management sidebar.
2. Select *Fetch New Log* from the *Explorer* menu. The system prompts you to specify the machine from which you want to fetch an up-to-date log. Only computers configured for Sanctuary protection will appear on this list.



Name: SECUREWAVE

Name	Location
SECUREWAVE	WORKGROUP

Found 1 matching name

Figure 39. Fetching New Logs

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

The log display reflects real-time information for the selected computer.

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

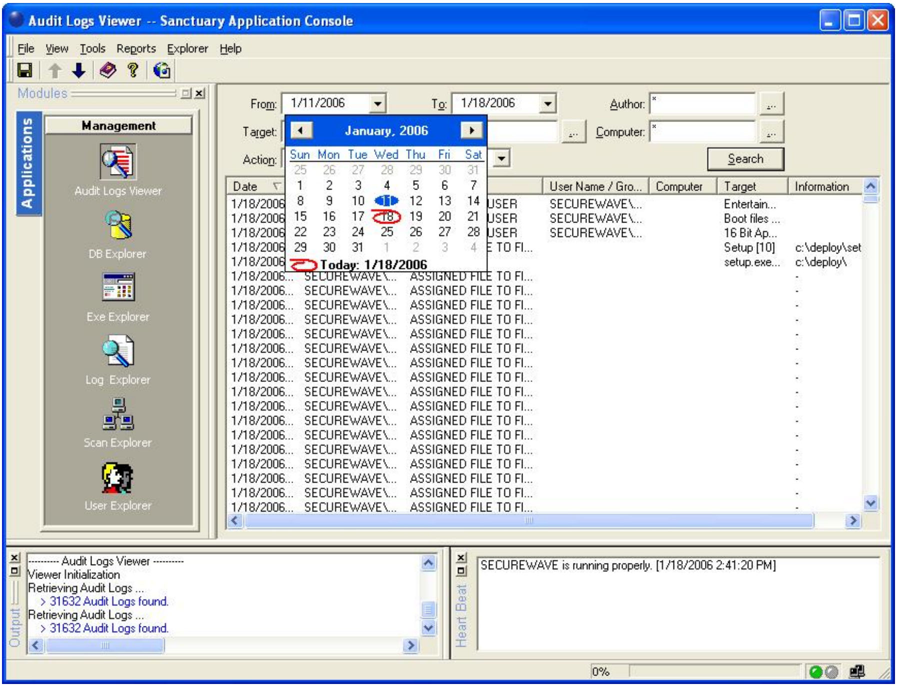
Sanctuary keeps a full audit trail of all activities carried out by its administrators. You can view records of changes made to files, File Groups, and assignment of those resources to users and User Groups.

If you have appropriate administrative privileges, you can use the *Audit Logs Viewer* module of the Sanctuary management console to monitor this activity.

To view system administrator activity

1. Click the *Audit Logs Viewer* icon in the Management sidebar. 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.*



From: 1/11/2006

To: 1/18/2006

Author: *

Computer: *

Date			User Name / Gro...	Computer	Target	Information
1/18/2006		USER	SECUREWAVE\...		Entertain...	
1/18/2006		USER	SECUREWAVE\...		Boot files ...	
1/18/2006		USER	SECUREWAVE\...		16 Bit Ap...	
1/18/2006		E TO FI...			Setup [10]	c:\deploy\set
1/18/2006					setup.exe...	c:\deploy\
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-
1/18/2006...	SECUREWAVE\...	ASSIGNED FILE TO FI...				-

```
--------- Audit Logs Viewer ---------
Viewer Initialization
Retrieving Audit Logs ...
   > 31632 Audit Logs found.
Retrieving Audit Logs ...
   > 31632 Audit Logs found.
```

```
SECUREWAVE is running properly. [1/18/2006 2:41:20 PM]
```

Figure 40. The Audit Logs Viewer Module

Once you have the list, you can:

- Sort it by clicking on any column heading. Click again to sort in reverse order.
- Right-click on any field of any register and choose to filter on that item. This action restricts the displayed list to only those registers that match the filter. Right-click again to remove the filter.

The *Audit Logs Viewer* displays the following columns:

Column	*Description*	
Date	Date when the administrator action was made. This field is always present.	
Author	Who did the action. This field is always present.	
User name/group	Name of the user or group to which the action was applied.	
Computer	The target computer to which the action was applied.	
Target	File, group, path rule, file group, etc.	
Information	Additional information related to the corresponding register (if applicable).	
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 File Group	This File Group was erased.
	Deleted Option	This option was removed for the specified user or machine.
	Set Option	This option was created 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 User/Machine Option	A change was made to this option for this machine or user.
	Unassigned File from File Group	This file was removed from this File Group.
	Unauthorized User	This user's permission to use the named File Group was revoked.

Table 14. 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 *113*.

Chapter 11: Sanctuary's database; the DB 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

This database is created on the Microsoft SQL Server 7/2000 or on the Microsoft Database Engine (MSDE). For organizations with fewer than 200 users, the MSDE is sufficient. Larger organizations will want to use the Microsoft SQL Server. Please note that there are inherent limitations when using MSDE (for example, 2 GB database limit) specified in the Setup Guide.

The DB 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:

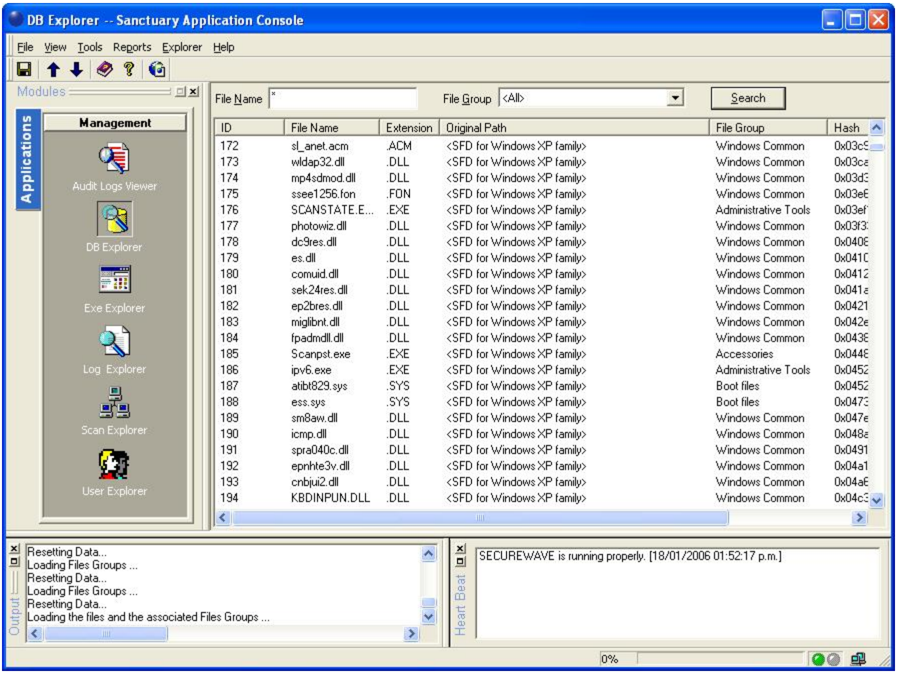
- Viewing database records
- Performing routine database maintenance
- Backing up the Sanctuary database
- Removing old execution logs and machine scans

Viewing database records

The DB 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 DB Explorer module

Click the DB Explorer icon in the Management sidebar. The system displays the DB 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.



File Name *

File Group <All>

ID	File Name	Extension	Original Path	File Group	Hash
172	sl_anet.acm	.ACM	<SFD for Windows XP family>	Windows Common	0x03c9
173	wldap32.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x03ca
174	mp4sdmod.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x03d3
175	ssee1256.fon	.FON	<SFD for Windows XP family>	Windows Common	0x03e6
176	SCANSTATE.E...	.EXE	<SFD for Windows XP family>	Administrative Tools	0x03ef
177	photowiz.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x03f3
178	dc9res.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x0408
179	es.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x0410
180	comuid.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x0412
181	sek24res.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x041a
182	ep2bres.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x0421
183	miglibnt.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x042e
184	fpadmdll.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x0438
185	Scanpst.exe	.EXE	<SFD for Windows XP family>	Accessories	0x0448
186	ipv6.exe	.EXE	<SFD for Windows XP family>	Administrative Tools	0x0452
187	atibt829.sys	.SYS	<SFD for Windows XP family>	Boot files	0x0452
188	ess.sys	.SYS	<SFD for Windows XP family>	Boot files	0x0473
189	sm8aw.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x047e
190	icmp.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x048a
191	spra040c.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x0491
192	epnhte3v.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x04a1
193	cnbjui2.dll	.DLL	<SFD for Windows XP family>	Windows Common	0x04a6
194	KBDINPUN.DLL	.DLL	<SFD for Windows XP family>	Windows Common	0x04c3

```
Resetting Data...
Loading Files Groups ...
Resetting Data...
Loading Files Groups ...
Resetting Data...
Loading the files and the associated Files Groups ...
```

```
SECUREWAVE is running properly. [18/01/2006 01:52:17 p.m.]
```

Figure 41. The DB 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 File Version information

Select the *Choose Columns* item from the *View* menu and add the desired column.

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.

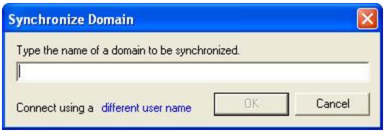
Performing routine database maintenance

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.

To synchronize domain members

1. Select *Synchronize Domain Members* from the *Tools* menu. The system displays the following dialog:



Synchronize Domain

Type the name of a domain to be synchronized.

Figure 42. 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.*

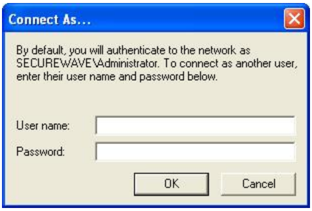
SXDomain command-line tool

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.

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. 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:



By default, you will authenticate to the network as SECUREWAVE\Administrator. To connect as another user, enter their user name and password below.

User name:

Password:

Figure 43. 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

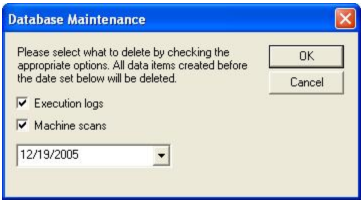
1. Select *Database Maintenance* from the *Tools* menu.
2. In the *Database Maintenance* dialog, check the type of database content you want to delete — execution logs, machine scans.

   ☑ 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.

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.*



Database Maintenance

Please select what to delete by checking the appropriate options. All data items created before the date set below will be deleted.

☑ Execution logs

☑ Machine scans

12/19/2005

Figure 44. 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 *110* 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 localized on the ‘DataFileDirectory’ defined in the following registry key:

```
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.

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 four 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.

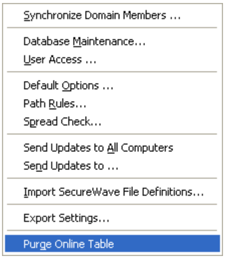


Figure 45. Purging the Online Computers Table

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 reports to view, save, or print. Simply select the *Reports* menu 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 can be viewed 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 provisional files created in the Report folder located in your temporary directory.

✍ *Once the output is shown in your favorite Web browser, you can use the ‘Save as...’ or ‘Print’ options to keep a backup record of your report. Consult your browser help for details.*

✍ *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.*

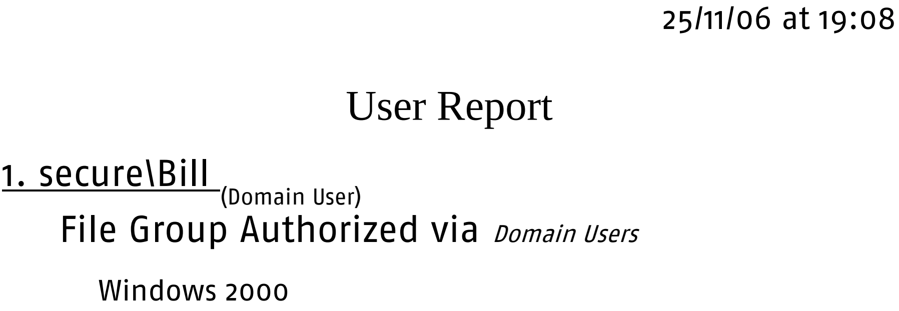
To return to the Sanctuary management console, just close the browser or click the Sanctuary application button on the Windows taskbar.

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.
2. In the *Select Domain User or Group* dialog, select one or more users.

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



25/11/06 at 19:08

User Report

1. secure\Bill (Domain User)

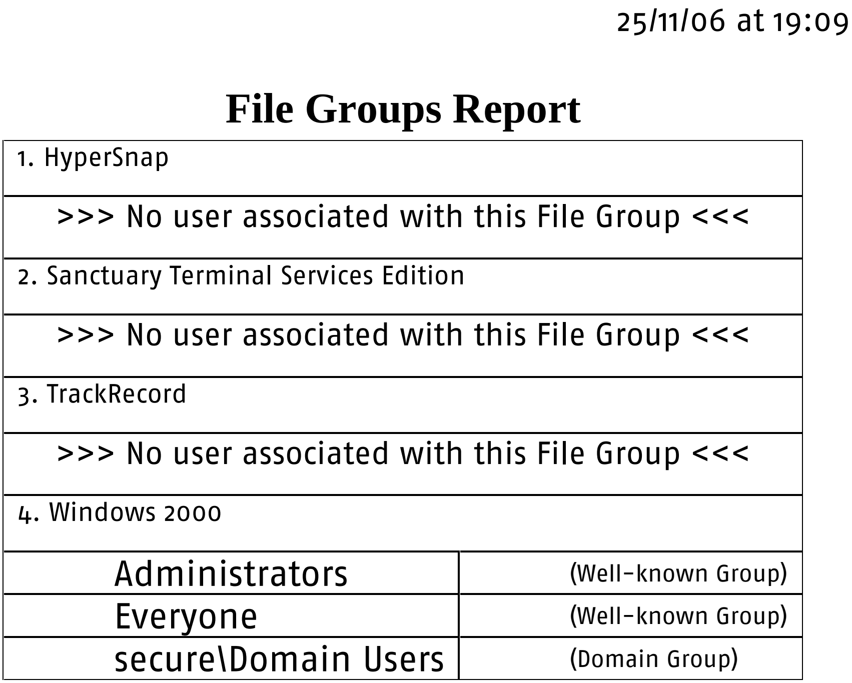
File Group Authorized via *Domain Users*

Windows 2000

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.

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



25/11/06 at 19:09

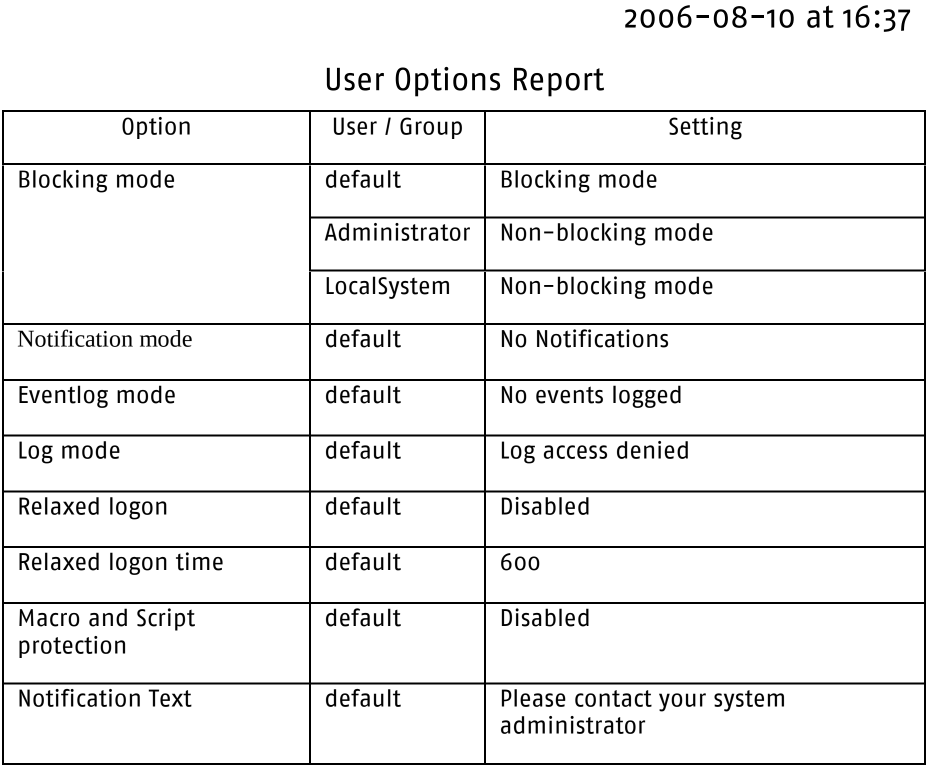
File Groups Report

1. HyperSnap	
>>> No user associated with this File Group <<<	
2. Sanctuary Terminal Services Edition	
>>> No user associated with this File Group <<<	
3. TrackRecord	
>>> No user associated with this File Group <<<	
4. Windows 2000	
Administrators	(Well-known Group)
Everyone	(Well-known Group)
secure\Domain Users	(Domain Group)

User Options

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

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



2006-08-10 at 16:37

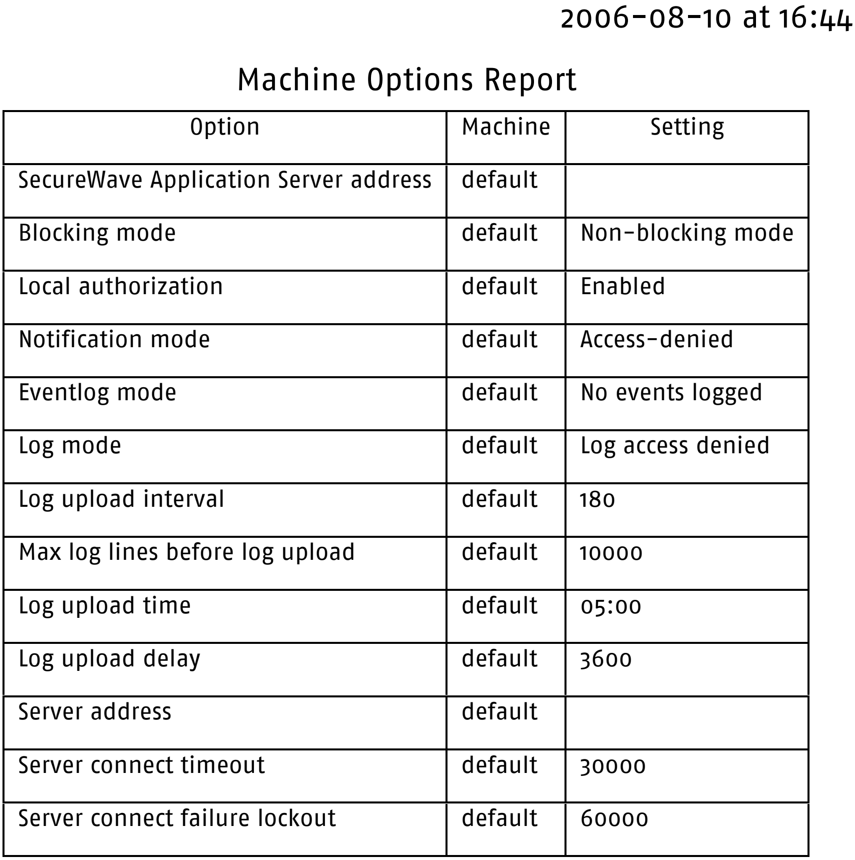
User Options Report

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

Machine Options

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

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



2006-08-10 at 16:44

Machine Options Report

Option	Machine	Setting
SecureWave Application Server address	default	
Blocking mode	default	Non-blocking mode
Local authorization	default	Enabled
Notification mode	default	Access-denied
Eventlog mode	default	No events logged
Log mode	default	Log access denied
Log upload interval	default	180
Max log lines before log upload	default	10000
Log upload time	default	05:00
Log upload delay	default	3600
Server address	default	
Server connect timeout	default	30000
Server connect failure lockout	default	60000

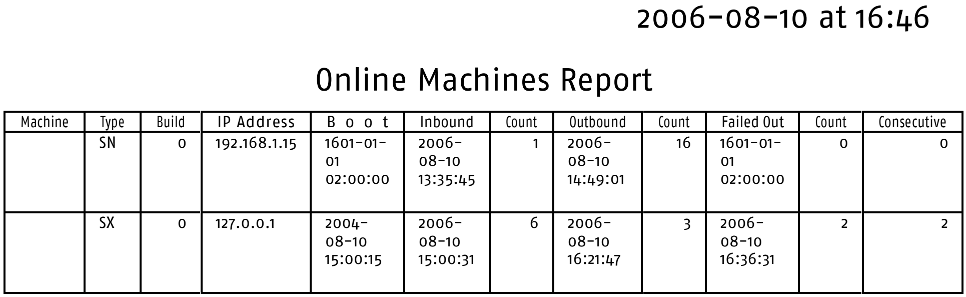
Online Machines

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.

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 here 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

Machine	Type	Build	IP Address	Boot	Inbound	Count	Outbound	Count	Failed Out	Count	Consecutive
	SN	0	192.168.1.15	1601-01-01 02:00:00	2006-08-10 13:35:45	1	2006-08-10 14:49:01	16	1601-01-01 02:00:00	0	0
	SX	0	127.0.0.1	2004-08-10 15:00:15	2006-08-10 15:00:31	6	2006-08-10 16:21:47	3	2006-08-10 16:36:31	2	2

Below is an explanation of the columns:

Column	*Description*
Machine	Always empty.
Type	This column holds the kind of client driver installed on the client computer: *SN* for Sanctuary Device Control drivers and *SX* for Sanctuary drivers.
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 '1601-01-01 02:00:00' 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 between the client computer and the SecureWave Application Server.
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 15. 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 solution
- Default options for all users protected by the Sanctuary solution
- 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 *134*).

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 SMC 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 invokes the standard Windows dialog.*

To build a list of executable files from a computer directory

1. Click the *EXE Explorer* icon from the Management sidebar.
2. Select *Default Options* from the *Tools* menu 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 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.).

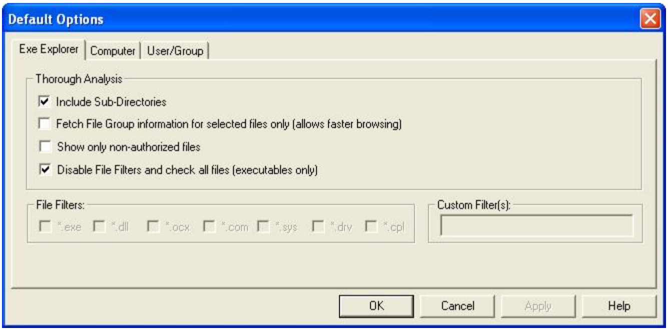
✍ *The program also search 16 bits programs if you select the file filters options (*.exe and *.com).*

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 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.



Thorough Analysis

☑ Include Sub-Directories
□ Fetch File Group information for selected files only (allows faster browsing)
□ Show only non-authorized files
☑ Disable File Filters and check all files (executables only)

File Filters:

□ *.exe □ *.dll □ *.ocx □ *.com □ *.sys □ *.drv □ *.cpl

Custom Filter(s):

Figure 46. 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 on the search, 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.

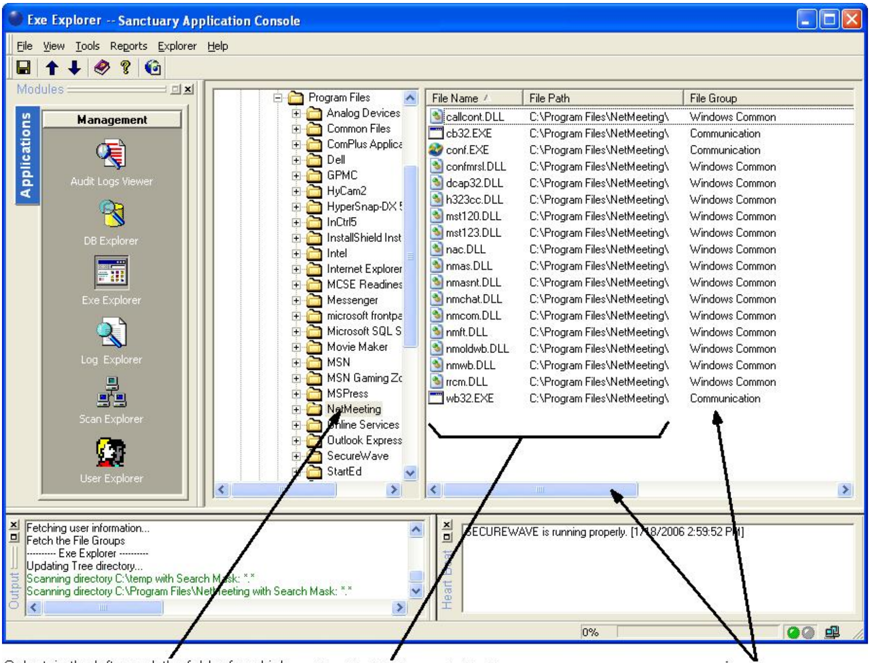
   Show only non-authorized files
   ☑ Filter out previously authorized files, show only the rest (faster).
   □ Show all files, authorized or unauthorized.

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 screen:



File Name	File Path	File Group
callcont.DLL	C:\Program Files\NetMeeting\	Windows Common
cb32.EXE	C:\Program Files\NetMeeting\	Communication
conf.EXE	C:\Program Files\NetMeeting\	Communication
confmrsl.DLL	C:\Program Files\NetMeeting\	Windows Common
dcap32.DLL	C:\Program Files\NetMeeting\	Windows Common
h323cc.DLL	C:\Program Files\NetMeeting\	Windows Common
mst120.DLL	C:\Program Files\NetMeeting\	Windows Common
mst123.DLL	C:\Program Files\NetMeeting\	Windows Common
nac.DLL	C:\Program Files\NetMeeting\	Windows Common
nmas.DLL	C:\Program Files\NetMeeting\	Windows Common
nmasnt.DLL	C:\Program Files\NetMeeting\	Windows Common
nmchat.DLL	C:\Program Files\NetMeeting\	Windows Common
nmcom.DLL	C:\Program Files\NetMeeting\	Windows Common
nmft.DLL	C:\Program Files\NetMeeting\	Windows Common
nmoldwb.DLL	C:\Program Files\NetMeeting\	Windows Common
nmwb.DLL	C:\Program Files\NetMeeting\	Windows Common
rrcm.DLL	C:\Program Files\NetMeeting\	Windows Common
wb32.EXE	C:\Program Files\NetMeeting\	Communication

```
Fetching user information...
Fetch the File Groups
--------- Exe Explorer ---------
Updating Tree directory...
Scanning directory C:\temp with Search Mask: *.*
Scanning directory C:\Program Files\NetMeeting with Search Mask: *.*
```

```
SECUREWAVE is running properly. [17/8/2006 2:59:52 PM]
```

Select, in the left panel, the folder for which you want to view the executable files.

The identified executable files are shown here.

Select the column identifying the File Group, if any, assigned to the executable file.

Figure 47. The Exe Explorer Module Window

The program does not uncompress archive files (Zip, Cab, RAR, LZH, ARJ, etc.). To do so, use the 'Authorization Wizard' or the 'FileTool.exe' tool. Please see Using the Authorization Wizard *on page* 63 *and* Versatile File Processor tool *on page* 150 *for more details.*

> ✍ *Use the 'Choose columns' item from the 'View' menu to select and organize those columns you want displayed.*

Now that you have created a list of executable files, you are ready to organize those files into File Groups and assign File Groups to users and User Groups. See *Chapter 8: Assigning access permissions to users and groups* on page *83* for more details.

Setting default options

Using the *Default Options* dialog item of the *Tools* menu, 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.

To change an option setting:

1. Select *Default Options* from the *Tools* menu
2. Select the item in the *Option* list box.
3. Deselect the *Not configured* checkbox.
4. Set the new value for the option.
5. Click OK to save the setting and exit the *Default Options* dialog or click APPLY to save the setting and keep the dialog open.

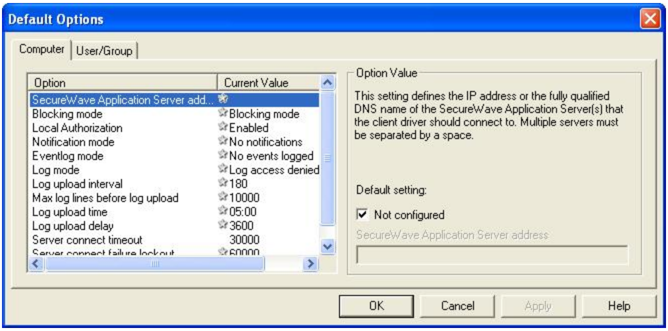
Once you finish changing the settings, send the updated information to protected clients.

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 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.



Option	Current Value
SecureWave Application Server add...	
Blocking mode	Blocking mode
Local Authorization	Enabled
Notification mode	No notifications
Eventlog mode	No events logged
Log mode	Log access denied
Log upload interval	180
Max log lines before log upload	10000
Log upload time	05:00
Log upload delay	3600
Server connect timeout	30000
Server connect failure lockout	60000

Option Value

This setting defines the IP address or the fully qualified DNS name of the SecureWave Application Server(s) that the client driver should connect to. Multiple servers must be separated by a space.

Default setting:

☑ Not configured

SecureWave Application Server address

Figure 48. 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, then these are applied to all machines in Sanctuary Application Server.

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.

Here is a summary of computer options, default settings, and available values for each option.

Computer option	*Default settings and available values*
SecureWave Application Server address	Define here the SecureWave Application Server´s IP address or fully qualified names separated by commas. ☑ Not configured. SecureWave default applies (the IP address specified during the installation). ☐ (Unchecked.) Enter the IP address for one or more SecureWave Application Servers, separated by commas. To specify a port on that server, add it to the end of the IP address after a colon (n.n.n.n:nnnn)
Blocking mode	Determines whether to block authorization of a file that is not centrally authorized ☑ Not configured. SecureWave default applies (Blocking mode). ☐ (Unchecked.) You can choose from the following options: *Blocking mode*. Files that are not centrally authorized will not run. There is no local authorization. *Non-blocking mode*. [default] Files that are not authorized can be run. This is useful for installing applications.
Local authorization	Determines whether to permit local authorization of unknown files after prompting the user ✍ *This has to be set with the 'Blocking mode' 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 'Blocking mode' (as either 'Ask user for *.exe only' or 'Ask user always') for the user.* ☑ Not configured. SecureWave default applies (enabled). ☐ (Unchecked.) You can choose from the following options: *Disabled.* Files that are not centrally authorized will not run. There is no local authorization. *Enabled*. [default] Files that are not authorized can be run if the user *blocking mode* is set either to *Ask user for *.exe only* or to *Ask user always* and the user responds 'Authorize' to the prompt.

Computer option	*Default settings and available values*
Notification mode	Determines whether the user is notified of Sanctuary allow/deny decisions ☑ Not configured. SecureWave default applies (no notification). ☐ (Unchecked.) You can choose from the following options: *No notifications.* [default] 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 and he runs a file that is not centrally unauthorized.
Eventlog mode	Determines what is reported to the Windows Event Log ☑ Not configured. SecureWave default applies (no events logged). ☐ (Unchecked.) You can choose from the following options: *No events logged.* [default] Do not create a log entry when a file access is denied. *Access-denied logged*. Log when 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.
Log mode	Determines what events are reported to SecureWave Application Server logs ☑ Not configured. SecureWave default applies (log access denied). ☐ (Unchecked.) You can choose from the following options: *Log everything*. Log every access to an executable file. ✍ *Using this option generates a large amount of data. Some Windows DLLs can be loaded several times a second. This option should only be used for testing purposes and for short periods.* *Log access denied*. [default] Log every denied access to an executable file. *Logging disabled*. Do not keep a log.

Computer option	*Default settings and available values*
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.) ☑ Not configured. SecureWave default applies (180 seconds). ☐ (Unchecked.) Enter any value in seconds.
Max log lines before log upload	Defines how many log entries are gathered before being automatically uploaded to the SecureWave Application Server ☑ Not configured. SecureWave default applies (10,000 lines). ☐ (Unchecked.) Enter any value.
Log upload time	Determines when each day log entries are uploaded to the SecureWave Application Server, if the other log upload thresholds have not already been reached ☑ Not configured. SecureWave default applies (05:00, 5 AM). ☐ (Unchecked.) Enter any value, using the 24-hour clock format (HH:mm).
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. ☑ Not configured. SecureWave default applies (random value between zero and 3600 seconds or 1 hour). ☐ (Unchecked.) Enter any value in seconds.
Server connect timeout	How long a computer waits before declaring failure in an attempt to connect to the SecureWave Application Server—and then using locally cached authorization information. If the client is configured to connect to multiple servers (see previous option), it attempt to reach the next one on the list. If none of them responds, the client assumes that it has been disconnected from the network, and uses the locally cached authorization list obtained from the last successful logon. This value depends on the network traffic, the type of switch, communication channel speed, if you are using a WAN or a LAN, etc. If you are using a big WAN with very dense traffic you can go up to 60,000 milliseconds. ☑ Not configured. SecureWave default applies (5,000 milliseconds). ☐ (Unchecked.) Enter another value in milliseconds.

Computer option	*Default settings and available values*
Server connect failure lockout	Defines the interval after which the client will not longer try to connect to a SecureWave Application Server ☑ Not configured. SecureWave default applies (60,000 milliseconds). □ (Unchecked.) Enter a value in milliseconds. The default time is reasonable, but you might set a longer period (perhaps an hour, 360,000 milliseconds, or more) for a server that might periodically be offline.

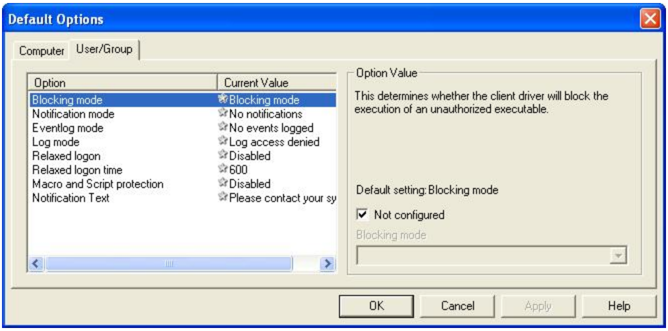
Table 16. Computer's Default Options Values

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.
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.



Option	Current Value
Blocking mode	Blocking mode
Notification mode	No notifications
Eventlog mode	No events logged
Log mode	Log access denied
Relaxed logon	Disabled
Relaxed logon time	600
Macro and Script protection	Disabled
Notification Text	Please contact your sy

This determines whether the client driver will block the execution of an unauthorized executable.

Default setting: Blocking mode

☑ Not configured

Blocking mode

Figure 49. Default User/Group Options

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

Here is a summary of user/group options, default settings, and available values for each option.

User/Group option	Default settings and available values
Blocking mode	Determines whether to block execution of unauthorized files. ☑ Not configured. SecureWave default applies (blocking). ☐ (Unchecked.) You can choose from the following options: *Blocking m*ode. [default] 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. *Ask user always*. Prompt the user to explicitly authorize any file for which a hash is not found in the Sanctuary database. ✍ *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.*
Notification mode	Determines whether the user is notified of Sanctuary decisions. ☑ Not configured. SecureWave default applies (no notification). ☐ (Unchecked.) You can choose from the following options: *No notifications.* [default] 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 and runs an unauthorized file.
Eventlog mode	Determines what events are reported to the Windows Event Log. ☑ Not configured. SecureWave default applies (no events logged). ☐ (Unchecked.) You can choose from the following options: *No events logged.* [default] Do not log system events. *Access-denied logged*. Log when file execution is denied. *Non-blocked access-denied*. Log unauthorized file

User/Group option	Default settings and available values
	executions, such as files that would have been denied if *Blocking Mode* was on.
Log mode	Determines what events are reported to SecureWave Application Server logs. ☑ Not configured. SecureWave default applies (log every denial). ☐ (Unchecked.) You can choose from the following options: *Log everything*. Log every access to an executable file. ✍ *Be careful with this option since it can consume a lot of space in your hard disk as some Windows DLLs are loaded several times a second.* *Log access denied*. [default] Log every denied access to an executable file. *Logging disabled*. Do not keep a log.
Relaxed logon	Allows 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. ☑ Not configured. SecureWave default applies (disabled). ☐ (Unchecked.) You can choose from the following options: *Enabled.* A delay occurs before blocking is activated. Unauthorized files can execute during logon. *Disabled*. [default] No delay occurs before blocking is activated. Unauthorized files cannot even run during logon. ✍ *If you want to prevent logon scripts from running asynchronously, then change this registry key on each client computer:* `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	Defines the length of time, in seconds, of the 'Relaxed logon'

User/Group option	Default settings and available values
logon time	grace period. ☑ Not configured. SecureWave default applies (600 ms). □ (Unchecked.) You can specify your own value. 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 is included in the installation of Sanctuary.
Macro and Script Protection	Determines whether scripts and macros can run. ☑ Not configured. SecureWave default applies (disabled). □ (Unchecked.) You can choose the following values from the pull-down list: *Disabled*. [default] 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. 💣 *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.*
Notification text	Defines a custom message that users will see when they attempt to execute an authorized application. This is only displayed if the *Local Authorization* option is enabled for the computer. ☑ Not configured. SecureWave default applies: 'Please contact your system administrator'. □ (Unchecked.) Enter a new message.

Table 17. User/Groups Default Options Values

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. Click the *User Explorer* icon in the Management sidebar.

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:

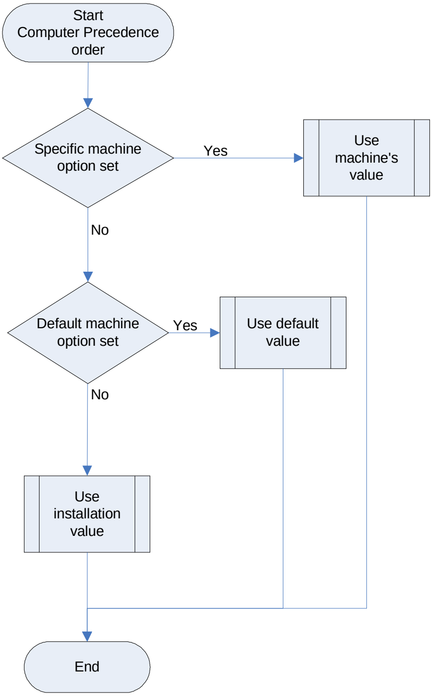

Start
Computer Precedence order
Specific machine option set
Yes
Use machine's value
No
Default machine option set
Yes
Use default value
No
Use installation value
End

Figure 50. Computer Precedence Order Process

The following table summarizes the default options installed for computers:

Option	*Default installation value*
Blocking mode	Blocking mode enable
Local authorization	Enable
Notification mode	No notifications
Eventlog mode	No events logged
Log mode	Log access denied
Log Upload interval	180 sec.
Max log lines before log upload	10,000 lines
Log upload time	05:00 AM
Log upload time delay	3,600 sec.
Server address	Read from registry
Server connect timeout	5,000 milliseconds
Server connect failure lockout	60,000 milliseconds

Table 18: 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:

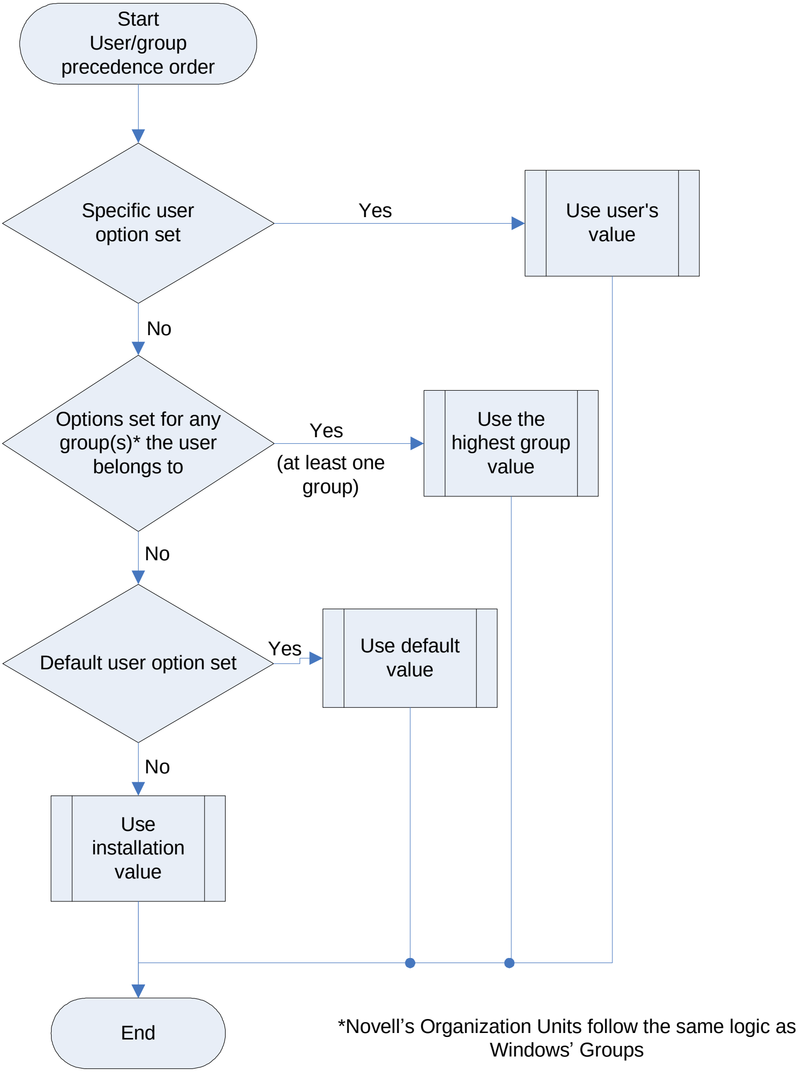


Figure 51. Users/Groups Precedence Order Process

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

Option	*Computer's default value*	*User/group's default value*
Blocking mode	Blocking mode enable	Blocking mode enable
Local authorization	Enable	n/a
Notification mode	No notifications	No notifications
Eventlog mode	No events logged	No events logged
Log mode	Log access denied	Log access denied
Log Upload interval	180 sec.	n/a
Max log lines before log upload	10,000 lines	n/a
Log upload time	05:00 AM	n/a
Log upload time delay	3,600 sec.	n/a
Server address	Read from registry	n/a
Server connect timeout	5,000 milliseconds	n/a
Server connect failure lockout	60,000 milliseconds	n/a
Relaxed logon	n/a	Disabled
Relaxed logon time	n/a	600 sec.
Macro and script protection	n/a	Disabled
Notification text	n/a	'Please contact your system administrator'

Table 19: 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 blocking mode 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 blocking mode 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 blocking mode 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 116— and Machine Options — page 117 — reports.*

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

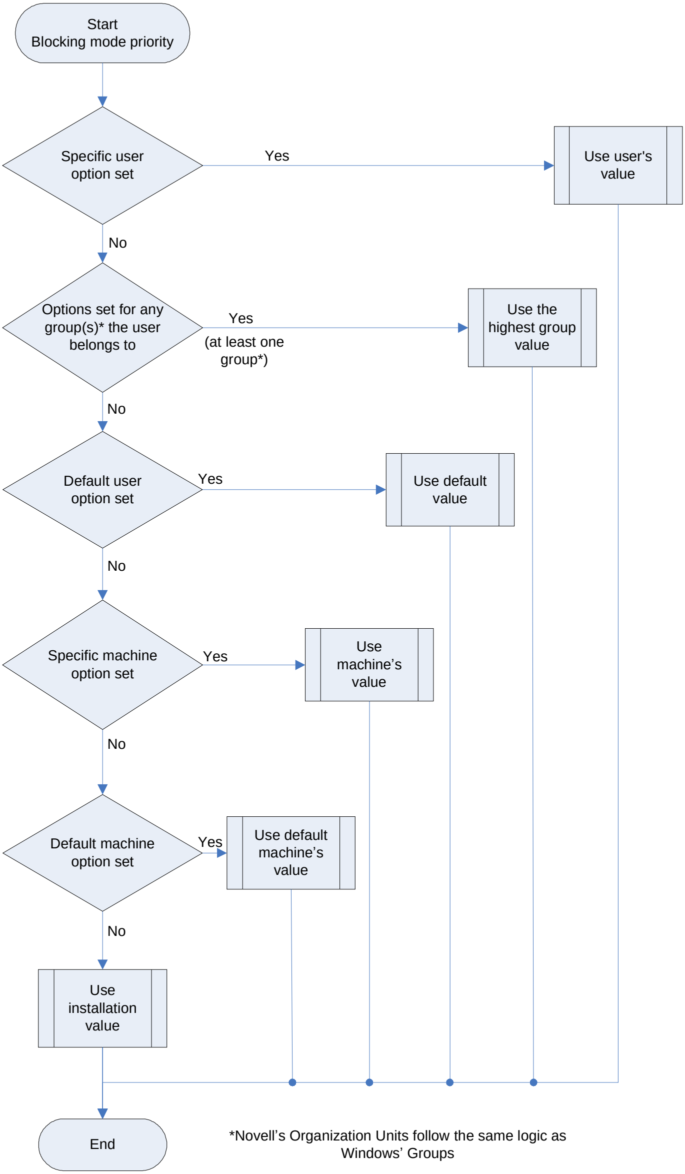

Start
Blocking mode priority
Specific user option set
Yes
Use user's value
No
Options set for any group(s)* the user belongs to
Yes
(at least one group*)
Use the highest group value
No
Default user option set
Yes
Use default value
No
Specific machine option set
Yes
Use machine's value
No
Default machine option set
Yes
Use default machine's value
No
Use installation value
End
*Novell's Organization Units follow the same logic as Windows' Groups

Figure 52. Blocking Mode Priority

You can follow this flowchart using as an example *Blocking Mode* 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:

Option	*Value precedence*
Log mode	1. Log everything 2. Log access denied 3. Logging disabled
Notification mode	1. No notifications 2. Access-denied 3. Non-blocked access-denied
Eventlog mode	1. No events logged 2. Access-denied logged 3. Non-blocked access-denied
Blocking mode	1. Ask user always 2. Ask user for *.exe only 3. Non-blocking mode 4. Blocking mode

Table 20: 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 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.

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 *150* 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.
- MSDE2000a, SQL Server 2000 with SP3.or SQL Server 2005

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* (see page *150* for more info) tool on the new files.

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

The following diagram summarizes AuthSrv.exe behavior:

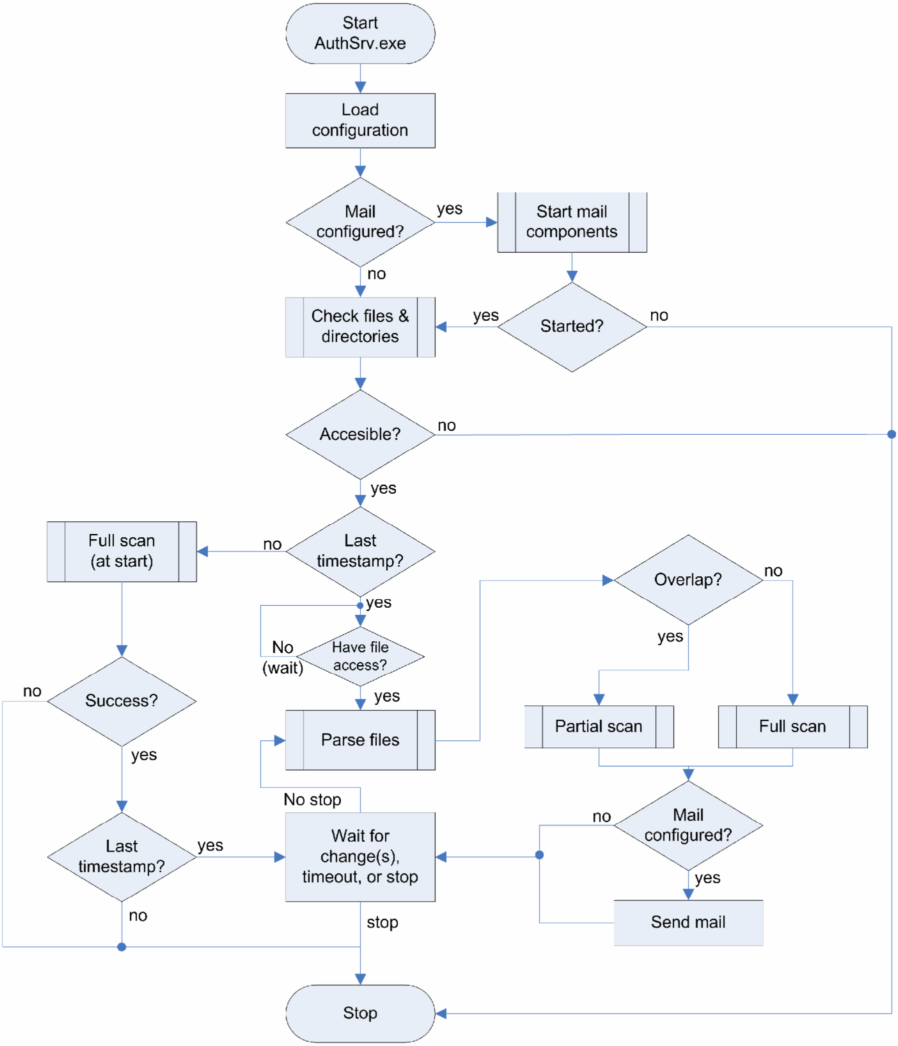


Figure 53. Authsrv.exe Internal Flowchart

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

```
c:\program files\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 start once the installation ends.

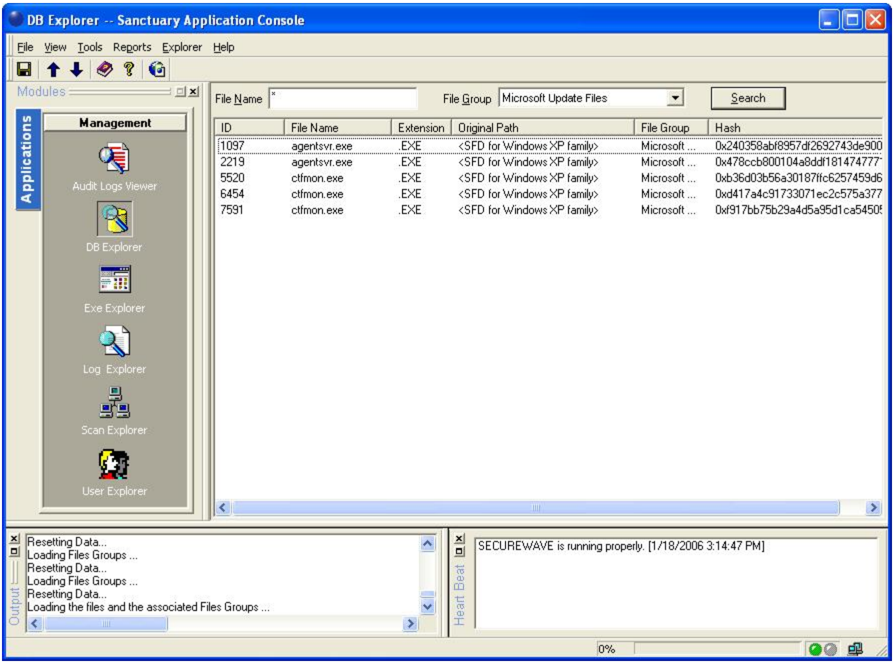
The tool waits until:

> 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 DB Explorer module (supposing you have some update files ready to authorize):



File Name *

File Group Microsoft Update Files

ID	File Name	Extension	Original Path	File Group	Hash
1097	agentsvr.exe	.EXE	<SFD for Windows XP family>	Microsoft ...	0x240358abf8957df2692743de900
2219	agentsvr.exe	.EXE	<SFD for Windows XP family>	Microsoft ...	0x478ccb800104a8ddf181474777
5520	ctfmon.exe	.EXE	<SFD for Windows XP family>	Microsoft ...	0xb36d03b56a30187ffc6257459d6
6454	ctfmon.exe	.EXE	<SFD for Windows XP family>	Microsoft ...	0xd417a4c91733071ec2c575a377
7591	ctfmon.exe	.EXE	<SFD for Windows XP family>	Microsoft ...	0xf917bb75b29a4d5a95d1ca5450

```
Resetting Data...
Loading Files Groups ...
Resetting Data...
Loading Files Groups ...
Resetting Data...
Loading the files and the associated Files Groups ...
```

```
SECUREWAVE is running properly. [1/18/2006 3:14:47 PM]
```

Figure 54: 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 neither Outlook Express nor 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\AuthSrvHl
pr\Parameters
```

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

Parameter	*Type*	*Description*	*Default value*
Standard Parameters			
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.	

Parameter	*Type*	*Description*	*Default value*
Mail Parameters			
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 request login.	
Password	REG_SZ	Password if SMTP request login. We suggest using IIS or Outlook mail configuration to avoid having the plain text password in Windows registry.	
AuthenticateLevel	REG_SZ	0 none 1 basic 2 NTLM	1
UseSSL	REG_SZ	Use Secure Socket Layer (SSL) communication between the mail client and the SMTP server.	"No"
Since mail configuration may not be straightforward and needs some tuning, you can set these parameters using a script: e.g., create a text file with .reg extension containing: REGEDIT [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AuthSrvHlpr\]"UserName"="TheAdministrator"			
Advanced Parameters			
CmdLineExecutable	REG_SZ	Allow an absolute path configuration of the Versatile File Processor. It is normally located in the same directory where Sanctuary	'FileTool.exe'

Parameter	*Type*	*Description*	*Default value*
		Authorization Service Tool was installed.	
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 21. 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, etc.).*

FileTool.exe command line parameters

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

Parameter	*Description*
usage: filetool [-s <server>] [-u user password] [-o <scan>] [-d#] [-f <n> <m>] [-v <report>] [-r <report>] [-i] <block> [<block> ...] [-p] <block>: target [target ...] [-e <mask>] [-c#] [-a# <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.
-d0	Delta mode off**.
-d1	Delta mode on, avoid rescanning files already scanned.
-d2	Delta mode on, clear the list then memorize files already scanned.
-f	Access failure; retry <n> times with a least <m> sec. in between.
-v	Verbose report; generate an xml report.
-r	Report; generate an xml report, errors only.
-i	Ignore archive contents.
target	File or directory to scan. To avoid recursive scan on directory, terminate with \\ (e.g., C:\temp\\). The target may also be one of these keywords in brackets: [drives] all hard drives.

Parameter	*Description*
	[media] all removable media. [all] all hard drives and removable media.
-e	An optional wildcard mask, e.g., '*.ex?' (default: '*').
-c0	File group creation, use only existing groups.
-c1	File group creation, create if necessary**.
-a0	Keep existing assignment, auto-assign new files, assign rest to group**. Accepts a list of groups <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.
-x0	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 22: The FileTool.exe command line parameters

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

Useful notes about using the Versatile File Processor tool

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 –x0 option to scan all files (subject to the target and wildcard restrictions).

All other file block options apply only to the online mode.

The file assignments obey the –a# option:

> –a0 <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 –c0 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 –x0 option carefully.*

The information on the file blocks is included in the report, one option tag per each file block. The following attributes are included in the report:

Attribute	Description
Mask	empty by default, set with **–e**.
Files	"executables" by default, set to "all" with **-x0**.
Name	"…" matches the group(s) specified with **-a0**, **-a1** or **-a2**.
Assignmentpolicy	"auto" for **–a0**, "standard" for **–a1**, "overwrite" for **–a2**.
creation	"yes" by default, "no" when**–c0** is used.

Table 23. 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 not 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
```

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 antivirus 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.
- Virus 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.

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 *49* 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 the Log Explorer icon 🔍 on the Management sidebar).
3. Select *Fetch New 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.

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.

Prevent Local Authorization

If you leave a user the chance to locally authorize applications, he is exposing his computer to a security risk. He may authorize a malicious application on his 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* 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 *RunLogonScriptSync* 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 all the 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. 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) help file located on the installation CD.

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. 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 New 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 *84*.

> 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 particularly, 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 *121*) 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.

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.).

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.

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

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.

MAPI

Messaging Application Programming Interface enables Windows applications to access a variety of messaging systems.

MDAC

Microsoft Data Access Components. Required by Windows NT4/2000/XP computers to connect to SQL Server or MSDE databases.

MSDE

Microsoft Data Engine (also known as Microsoft SQL Server 2000 Desktop Engine), is a SQL Server compatible database server, suitable for small and medium size organizations. MSDE is supplied with some versions of Sanctuary Terminal Services Edition. MSDE databases can subsequently be migrated to SQL Server 2000/2005.

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.

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.

Vulnerability

A weakness or other kind of opening in a system, usually caused by a bug or other design flow.

WSUS

Windows Server Update Services (previously SUS v2.0) is a new version of Software Update Services (SUS).

Index of Figures

Index of Tables

Index