

**SecureWave**  
Safeguarding Tomorrow

# **Sanctuary Device Control Administrator's Guide**

[www.securewave.com](http://www.securewave.com)





## Liability Notice

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

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

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

SecureWave claims copyright in this program and documentation as an unpublished work, revisions of which were first licensed on the date indicated in the foregoing notice.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

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

## Trademarks

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

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

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

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

You can contact our technical support team by calling:

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

or by sending an email to [support@securewave.com](mailto:support@securewave.com)

Published on: August 2007



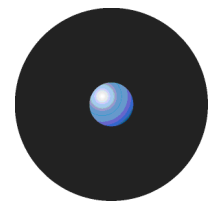
---

# Contents

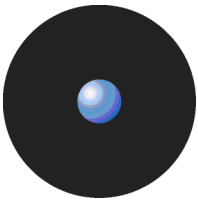
About this guide.....	5
Introduction.....	5
Complete security.....	6
What's in this guide.....	6
For more information.....	7
Conventions.....	8
Notational conventions.....	8
Typographic conventions.....	8
Keyboard conventions.....	8
To contact us.....	8
Chapter 1: Introducing Sanctuary Device Control.....	11
Welcome to Sanctuary Device Control.....	11
What is Sanctuary Device Control.....	11
What can you do with Sanctuary Device Control.....	11
Benefits of using Sanctuary Device Control.....	12
Major features of Sanctuary.....	12
What is new on this version.....	15
Device types supported.....	16
Conclusions.....	18
Chapter 2: Using the Sanctuary Console.....	19
Starting the Sanctuary Management Console.....	19
Connecting to the Server.....	19
Log in as a different user.....	20
The Sanctuary Management Console screen.....	21
Customizing your workspace.....	22
The Sanctuary Device Control modules.....	24
The Sanctuary Management Console menus and tools.....	25
File menu.....	25
View menu.....	26
Tools menu.....	26
Endpoint Maintenance.....	27
Reports menu.....	28
Explorer menu.....	29
Window menu.....	30
Help menu.....	30
Other administrative functions.....	30
Setting and changing default options.....	30
Synchronizing domain members.....	30
Synchronizing with Novell eDirectory.....	31
Adding workgroup computers.....	31
Performing database maintenance.....	32
Defining Sanctuary administrators.....	32
Sending updated permissions to client computers.....	34
Everyday work.....	35
Identifying and organizing users and user groups.....	35
Identifying the devices to be managed.....	35
Working with the Sanctuary system's pre-defined device classes.....	36
Adding your own, user-defined devices to the system.....	36
Identifying specific, unique, removable devices.....	37
Organizing devices into logical groups.....	38
Identifying specific computers to be managed.....	39
Defining different types or permissions.....	39
Encrypting removable media & authorizing specific DVDs/CDs.....	40
Forcing users to encrypt removable media.....	40
Practical setup examples.....	41
DVD/CD burner permissions assignments.....	41
Removable permissions assignments.....	42



Assigning permissions to groups instead of users.....	42
Shadowing notes .....	42
<b>Chapter 3: Using the Device Explorer.....</b>	<b>47</b>
How does the Device Explorer work .....	48
Restricted and unrestricted devices .....	49
Optimizing the way you use the Device Explorer .....	50
Context menu and drag & drop .....	50
Keyboard shortcuts.....	51
Adding comments to an entry .....	51
Computer groups .....	51
Renaming Computer Groups/Device Groups/Devices .....	52
Event notification .....	52
Device Groups .....	55
Supported devices types .....	56
Managing permissions.....	56
<b>Chapter 4: Managing permissions/rules.....</b>	<b>57</b>
Using the Permissions dialog .....	57
Special case: Working with Removable Storage Devices .....	59
Using file filters .....	60
To remove File Filtering settings from a permission .....	63
File Filtering examples .....	64
Adding a user or group when defining a permission.....	66
To assign default permissions .....	67
Root-level permissions.....	67
To assign default permissions to users and groups.....	68
Priority of default permissions .....	69
Read/Write permissions .....	70
To assign computer-specific permissions to users and groups.....	71
To modify permissions.....	72
To remove permissions .....	73
To assign scheduled permissions to users and groups .....	73
To modify scheduled permissions.....	74
To remove scheduled permissions.....	75
To assign temporary permissions to users .....	75
To remove temporary permissions.....	76
To assign temporary permissions to offline users .....	76
To assign online and offline permissions .....	80
To remove offline or online permissions .....	81
To export and import permission settings .....	81
Shadowing devices.....	82
To shadow a device .....	83
To remove the shadow rule .....	84
To view a 'shadowed' file .....	84
Copy limit.....	84
To add a copy limit.....	85
To remove a copy limit .....	86
Applying multiple permissions to the same user.....	86
Forcing users to encrypt removable storage devices.....	87
Setting permissions to force users to encrypt removable storage devices .....	87
Managing devices .....	92
To add a new device .....	93
To remove a device.....	94
Specific, unique, removable devices .....	94
Changing permissions mode .....	95
Priority options when defining permissions .....	95
Informing client computers of permission changes .....	96
<b>Chapter 5: Using the Log Explorer .....</b>	<b>99</b>
Introduction .....	99
Monitoring user input/output device actions .....	99
Monitoring administrator actions.....	100
Accessing the Log Explorer.....	101
Log Explorer templates .....	102
To use an existing template.....	103
To create and use a new template .....	103
Log Explorer window.....	104
Navigation/Control bar .....	105
Column headers.....	105
Results panel / custom report contents.....	109
Criteria/Properties panel .....	111
Control button panel .....	111
Select and edit templates window .....	111



Template settings window .....	113
Simple Query tab .....	114
Criteria .....	115
Query & Output tab .....	116
Schedule tab .....	118
Format tab .....	118
Delivery tab .....	119
Viewing access attempts to devices .....	120
Viewing client error reports .....	122
Viewing shadow files .....	122
When the Data File Directory is not available .....	123
Shadowing file names only .....	124
DVD/CD Shadowing .....	124
Forcing the latest log files to upload .....	124
To manage devices using the Log Explorer module .....	125
Viewing administrator activity .....	126
Audit events .....	126
<b>Chapter 6: Using the Media Authorizer .....</b>	<b>129</b>
Introduction .....	129
Creating a DVD/CD hash .....	130
What happens when a user wants access to the DVD/CD .....	130
Accessing the Media Authorizer .....	131
Authorizing users to use specific DVDs/CDs .....	131
Pre-requisites .....	132
To authorize the use of a specific DVD/CD .....	132
Encrypting removable storage devices .....	132
Pre-requisites .....	133
Decentralized encryption .....	134
Limitations .....	134
To encrypt a specific removable storage device .....	135
Removable device encryption methods comparison .....	136
Problems encrypting a device .....	136
Authorizing access .....	138
Selecting users for a device .....	138
Selecting devices for a user .....	140
Removing media from the database .....	141
To remove a DVD/CD .....	141
To remove an encrypted removable storage device .....	141
To remove lost or damaged media from the database .....	142
Other Media Authorizer utilities .....	142
To rename a DVD, CD, or removable storage device .....	142
Exporting encryption keys .....	143
Ejecting a CD or DVD .....	143
Recovering a password for decentralized encryption when connected .....	143
Permissions Priority .....	146
Encrypting devices without a Certificate Authority .....	148
To encrypt a removable media without installing a Certificate Authority .....	148
<b>Chapter 7: Accessing encrypted media outside of your organization .....</b>	<b>149</b>
Exporting encryption keys .....	149
Exporting encryption keys centrally .....	149
Exporting encryption keys locally .....	150
To export the encryption key to a file .....	151
To export the encryption key to the device itself .....	152
Accessing encrypted media outside your organization .....	153
Accessing media on a machine with Sanctuary Client Driver installed .....	153
Accessing media without using Sanctuary Client Driver .....	158
Using encryption inside and outside your organization .....	162
Decentralized encryption .....	163
How to configure Sanctuary so that users can encrypt their own devices .....	163
Recovering a decentralized encryption password without Sanctuary Client .....	163
<b>Chapter 8: Setting and changing options .....</b>	<b>169</b>
Options set in old Sanctuary versions .....	169
Default options .....	170
Computer-specific options .....	170
To change an option setting .....	171
Sending updates to client computers .....	171
Individual option settings .....	171
Certificate generation .....	171
Client hardening .....	172



- Device log ..... 172
- Device log throttling ..... 173
- eDirectory translation ..... 173
- Encrypted media password..... 173
- Endpoint status ..... 174
- Log upload interval ..... 174
- Log upload threshold ..... 174
- Log upload time ..... 174
- Log upload delay ..... 174
- Online state detection ..... 174
- Server address ..... 175
- Shadow directory ..... 176
- Update notification ..... 176
- USB Keylogger ..... 176
- Checking settings on a client machine..... 177
- Chapter 9: Generating Sanctuary Reports..... 179**
  - User Permissions report .....180
  - Device Permissions report ..... 181
  - Computer Permissions report ..... 182
  - Media by User report..... 183
  - Users by Medium report..... 184
  - Shadowing by Device report ..... 185
  - Shadowing by User report ..... 186
  - Online Machines report ..... 187
  - Machine Options report ..... 188
  - Server Settings Report ..... 189
- Appendix A: DVD/CD Shadowing ..... 193**
  - Introduction ..... 193
    - Operation of the Sanctuary Client Driver ..... 193
    - Disk space requirements ..... 193
  - Supported formats when shadowing ..... 194
  - Handling of unsupported shadowing formats ..... 194
  - CD image analysis..... 195
    - Files..... 195
    - Logs ..... 195
    - Saved image ..... 195
  - Sample analysis log ..... 195
  - Supported and unsupported CD formats ..... 197
    - Summary ..... 197
    - Supported data block formats and recording modes..... 197
    - Supported and unsupported file system features..... 197
    - Supported DVD/CD burning software ..... 200
- Appendix B: Important notes ..... 201**
- Glossary..... 205**
- Index of Figures ..... 209**
- Index of Tables ..... 215**
- Index ..... 217**



---

## About this guide

### Introduction

Enterprises today are constantly challenged with security and support issues arising from one major area – endpoint users and their PCs. Malware, spyware, data leakage caused by removable media and the resulting regulatory compliance (information privacy) issues dominate enterprise IT companies' 'top 10 concerns' lists<sup>1</sup> from a variety of analyst firms.

Today's existing security solutions have been unable to stem the tide of ever-increasing security threat. This is primarily because enterprise endpoints are porous and becoming more so as new hardware technologies and P2P applications appear on the market. Who would have ever considered an iPod to pose a security risk a few years ago, or expected the wave of boutique spyware crafted to target individual organizations?

Traditional security solutions are not designed to address today's risks. They rely on signatures or some other means to *react to symptoms after a threat has already appeared and been identified*. Sanctuary Application Control Suite addresses the challenges associated with effectively securing endpoint executables and devices. It works in a simple, unique way that puts control back in the hands of IT administrators while giving end users the flexibility that they demand.

Sanctuary provides policy-based control for all devices and applications that can be used on enterprise endpoints. Using a whitelist approach, Sanctuary enables the development, enforcement, and auditing for application and device use in order to maintain IT security, reduce the effort and cost associated with supporting endpoint technologies, and ensure compliance with regulations. By using a whitelist approach, enterprises can literally turn their backs on the volumes of unwanted applications, malware, and unauthorized devices and instead focus on what is authorized and approved.

Sanctuary links application and device policies to eDirectory- and Active Directory-based identities, dramatically simplifying the management of endpoint application and device resources.

Sanctuary Device Control controls access to devices by applying permission rules to each device type. Based on the Least Privilege Principle, access to any device is prohibited by default for all users. To grant access, the administrator associate those users or user groups to the devices or complete device classes to which they should have read and/or write privileges. In essence, Sanctuary Device Control extends the standard Windows security model to control I/O devices.

The Sanctuary Device Control approach is in stark contrast to traditional security solutions that use 'black lists' to specify devices that cannot be used. With Sanctuary Device Control, your IT infrastructure is protected from devices not yet developed until you say the word.

---

<sup>1</sup> Yankee Group 2005, ESG 2005, Forrester 2005



## Complete security

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

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

## What's in this guide

This guide explains how to use Sanctuary Device Control to control end user access to I/O devices, including floppy disk drives, DVDs/CDs drives, serial and parallel ports, USB devices, hot swappable and internal hard drives as well as other devices.

We have divided this manual in three sections.

**Part I** contains a general introduction to the Sanctuary Device Control program. *This is the must read part.*

- > *Chapter 1: Introducing Sanctuary Device Control* provides a high-level overview of Sanctuary Device Control, how it works and how it benefits your organization.
- > *Chapter 2: Using the Sanctuary Console* describes the basic principles of how to use Sanctuary Device Control.

**Part II** is the reference part. It provides information about how you use each of the Sanctuary Device Control modules. The functionality of each module is explained in detail.

- > *Chapter 3: Using the Device Explorer* explains how to set the Access Control List permissions on I/O devices.
- > *Chapter 4: Managing permissions/rules* shows you how to create, delete, modify, organize, and group permissions and rules, and how to force a user to encrypt removable storage devices.
- > *Chapter 5: Using the Log Explorer* provides information both on how to view a copy of traced files, errors, and access attempts on client computers, and how to view administrative logs and copies of files ('shadow files') users have been written/read, to/from certain devices.
- > *Chapter 6: Using the Media Authorizer* illustrates how to create a database of known DVD/CDs and encrypted media and how to assign their rights to individual users and groups.
- > *Chapter 7: Accessing encrypted media outside of your organization* explains how to use encrypted media outside the company.
- > *Chapter 8: Setting and changing options* describes how to tailor the default options and computer-specific options to suit you and your organization.
- > *Chapter 9: Generating Sanctuary Reports* explains how to obtain the various HTML reports generated by Sanctuary Device Control.



**Part III** contains additional information to help you in your everyday work.

- > *Appendix A: DVD/CD Shadowing* describes how to copy the contents of files written/read to/from DVD/CD (shadowing), the DVD/CD disk and file formats supported by the shadowing operations, and how to interpret the files written to the Log Explorer module.
- > *Appendix B: Important notes* shows some key comments you should take into account when using Sanctuary Device Control.
- > The *Glossary* provides definitions of standard acronyms and terms used throughout the guide.
- > The several indexes (*Index of Figures*, *Index of Tables*, *Index*) provide quick access to specific figures, tables, information, items or topics.

## For more information

In addition to the documents and the online help provided with Sanctuary Device Control, further information is available from our support web site at:

[www.securewave.com](http://www.securewave.com)

This regularly updated Web site provides:

- > 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.



## Conventions

### Notational conventions

The following symbols are used throughout this guide to emphasize important points about the information you are reading:



*Special notes. This symbol indicates further information relevant to the topic being considered. These notes may relate to other parts of the system or points that need particular attention.*



*Time. This symbol indicates a paragraph describing a 'short-cut' or tip that may save you time.*



*Caution. This symbol means that proceeding with a particular course of action may result in a risk, for example loss of data or potential problems with your system.*

### Typographic conventions

The following typefaces are used throughout this guide:

- > *Italic* — Represents fields, menu commands, and cross-references.
- > `Fixed width` — Shows messages or commands typed at a command prompt.
- > SMALL CAPS — Represents buttons you click.

### 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 signifies that you must press each of them consecutively. For example 'Alt, R, U' means that you press each key in sequence.

## To contact us

If you have a question that is not answered in the online help, documentation, or the SecureWave knowledge base, you can contact your SecureWave customer support team by telephone, fax, email, or regular mail.

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

You can contact our technical support team by calling:

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

or by sending an email to: [support@securewave.com](mailto:support@securewave.com)

Alternatively, you can write to customer support at:

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

## **Part I: Step-by-step administration**



---

## Chapter 1: Introducing Sanctuary Device Control

This chapter introduces Sanctuary Device Control, and explains how it benefits your organization, protects your data, and improves your productivity. It also contains an overview of the entire Sanctuary system and an explanation of how the program works.

### Welcome to Sanctuary Device Control

Sanctuary Device Control eliminates the majority of dangers associated with people within your organization abusing their access to network resources and mission critical information. This security is achieved by controlling end user access to I/O devices, including floppy disk drives, DVDs/CDs drives, serial and parallel ports, USB devices, hot swappable and internal hard drives as well as other devices. This is a very effective way of preventing data leakage & theft of electronic intellectual property and proprietary information.

Sanctuary Device Control also prevents malicious code, unlicensed software, and other counterproductive applications being uploaded on your system. These could otherwise make inappropriate use of corporate resources and cause unnecessary expenses.

Sanctuary Device Control allows you to increase employee productivity and lower corporate legal liabilities while protecting your organization's reputation, image, and assets.

### What is Sanctuary Device Control

Sanctuary Device Control controls access to I/O devices by applying an Access Control List (ACL) to each device type. By default, access to any device is prohibited for all users. Designed administrators can then assign access and permissions to specific users or groups of users for the devices that they require in their everyday work. These permissions can be temporary, online/offline, scheduled, copy limit, shadow (a copy of transferred data), read, read/write, etc. This means that you are in control, always.

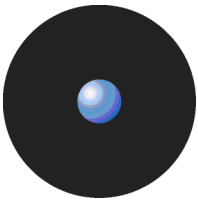
The Sanctuary Device Control approach is in stark contrast to traditional security solutions that utilize a list of specific devices that *cannot* be used, and have administrators scrambling to update systems whenever some new class of device is introduced. With Sanctuary Device Control, your IT infrastructure is protected from devices not yet developed until *you* sanction their use.

### What can you do with Sanctuary Device Control

Sanctuary Device Control is a powerful desktop security enhancer that allows system administrators to implement strict security device use policies by controlling end-user access and I/O devices use. Using Sanctuary Device Control, you can manage devices such as USB memory sticks, CD and DVD R/W, PDAs, etc. In essence, Sanctuary Device Control extends the standard Windows security model to control I/O devices. However, Sanctuary Device Control goes even further by auditing I/O device use as well as attempts to access unauthorized devices. It can even create and log a complete copy of all data (we call it 'shadowing') written/read to/from authorized devices.

With Sanctuary Device Control, you can add or change access rights in a flash — without needing to reboot the computer — and, at the same time control, monitor all activities from a central location.

The solution is network friendly and uses a three-tiered architecture that is designed to minimize policy-checking traffic; the actual control is done within the client computer itself, transparent to the user. Because the implementation of the control feature is also local, the power of Sanctuary Device Control extends even to unplugged laptop workers delivering the same security regardless of their location.



Sanctuary Device Control lets you:

- > Define user/group based permissions on all/specific machines.
- > Prevent unknown devices being installed on your networks.
- > Authorize particular device types within a class.
- > Uniquely identify individual devices.
- > Schedule I/O access for a predefined time or day of the week.
- > Create a temporary device access (same day or planned for future timeframe).
- > Restrict the amount of data copied to a device.
- > Assign administrator's roles.
- > Create shadow files (i.e. copies of transferred data) of all data written or read, to or from external devices or specific ports.
- > Encrypt media with the powerful AES algorithm.
- > Block some media (DVDs/CDs) while permitting other specific ones to be used.
- > Enforce specific users/user groups to encrypt their removable devices.

You can find a full list of characteristics in the *Major features* section on page 12.

## Benefits of using Sanctuary Device Control

When first using Sanctuary Device Control you immediately benefit from:

- > A strict user policy enforcement: With no more data leakage, you are in control of the four w's, who, where, what, and when.
- > The possibility to define specific device permission rules: Permissions boil down to even a specific organization-approved model.
- > A log of all administrators' actions: A complete report of what your administrators are doing.
- > A complete report facility: Useful information to keep everything under the strictest control. For example you can create a daily or weekly scheduled report of all user attempts to access an unauthorized device.
- > The option to scrutiny all data written to a media: you can optionally enable a copy (shadow) of all data written/read to/from certain devices.
- > Limit or hinder copied data: You have the choice of establishing a daily limit on, or simply stopping, data being written to external devices.
- > Authorize specific media that can be used in your organization: Define in advance which DVDs/CDs can be used in your company.
- > Encrypt all information leaving your company: Encrypt data as it is being written to a device.

## Major features of Sanctuary

Sanctuary Device Control is designed for large organizations with complex needs. It offers many powerful features such as:

### Centralized device access management

Sanctuary Device Control's core functionality is its ability to centrally define and manage user, user groups, computers and computer groups access to devices on the computer.





## Intuitive user interface

Access to devices is controlled using a native Access Control List, set up in exactly the same way as navigating through files and folders in Windows Explorer. Permissions can apply at different levels: users, user groups, all machines, machine groups, specific machines, groups of devices, or even specific devices.

## Novell support

Sanctuary Device Control fully supports Novell's eDirectory/NDS structure. The Novell's eDirectory trees are synchronized using an external script. These objects appear on the Device Explorer structure and permissions and rules can be assigned to them explicitly. The administrator can schedule the synchronization script using Windows's scheduler task manager (see Sanctuary's Setup Guide).

## Support for a wide variety of device types and buses

You can grant or deny access permissions for a wide variety of devices using USB, FireWire, ATA/IDE, SCSI, PCMCIA (or Cardbus), Bluetooth and IrDA buses. See *Device types supported* on page 16 for a list of the supported device types.

## Read-only access

Sanctuary Device Control lets you define a particular device as read-only. You can set read-only permissions for all file-system based devices, for example, a floppy drive, DVD/CD writer, PCMCIA hard drive, and so on. Other device permissions you can set restrict writing, encrypting, decrypting, exporting data to file/media and importing data.

## Copy limit

Afraid of letting your users abuse their writing permissions? Limit the quantity of data they can write to floppy disks and removable storage devices on a daily basis.

## Temporary access

Sanctuary Device Control lets you grant users temporary access to their devices. This means that you can switch access on without having to remember to switch it off again later. You can also use it to grant access 'in the future' for a limited period.

## Scheduled device access

Sanctuary Device Control lets you grant or deny permissions to use a device during a specific period. This lets you develop sophisticated security policies where certain devices can only be used from, for example, 9 am to 5 pm, Monday to Friday.

## Context-sensitive permissions

Different permissions can be applied depending on their contexts. Many permissions can be created that are valid regardless of the connection status. However, you can create others that are only relevant when the machine either is or is not connected to the network. This allows, for example, disabling the WiFi cards when laptops are connected to the company network and enabling them when the machine is not wired to the system.

## File shadowing

Sanctuary Device Control's shadow technology enables full auditing of all data written/read to/from file-system based devices such as Recordable DVD/CD, removable storage devices, floppy disks, Zip and PCMCIA drives, as well as to serial and parallel ports (only written data). This feature is available on a per user basis. Some of these devices only support a partial shadowing — only the file's name and not the complete content.

## User-defined devices

Sanctuary Device Control gives administrators the ability to manage other kind of devices in addition to those supported by default. Any device that is not managed in the default installation can be added to the database as a user-defined device and permissions can be applied in the usual way.



## Offline updates

You can update the permissions of remote machines that cannot establish a network connection to the company. New permissions can be exported to a file that is later imported onto the client computer.

## Per-device permissions

Sometimes a device type is too general for you to satisfactorily control access to sensitive data. Therefore, it may be desirable to implement a finer grained control at a lower level — down to the device model or even to a specific device within a model. For instance, rather than grant permissions to use any type of removable media, you may want to restrict access to a specific device of a company-approved model.

## Unique, serial identified, removable devices

Administrators can control devices by defining permissions at a class level (for example, all DVD/CD devices), classify devices in logical entities called device groups, or include a device model. When working with removable devices, administrators can go up to a fourth level by defining permissions for a unique, serial identified removable device.

## Per-device encryption

Restricting access for a specific device to a particular user also incorporates an encryption process to ensure that sensitive data is not inadvertently exposed to those without authorized access.

## Centralized and/or decentralized encryption

Sanctuary Device Control means that administrators can not only grant user(s)/group(s) access to a removable storage device (defined at the class, group, model, or uniquely identified device level) but they can also force users to encrypt their devices locally. This decentralized encryption schema is a work-around for those organizations that do not want (or need) to manage device encryption centrally while ensuring that the company's data is not inadvertently exposed.

## DVD/CD recorder shadowing

Shadowing, a copy of the file's data, can be used in the following writable media formats: CD-R, CD-RW, DVD-R, DVD+R, DVD-RW, DVD+RW and DVD-RAM. Shadowing means that data written/read to/from these media is intercepted and made available to the administrators. The recent spread of writable media and the Plug and Play capabilities of Windows XP make it extremely easy, for example, for any user to plug in a CDR unit and copy large amounts of potentially sensitive data. By default, Sanctuary Device Control disables writing to such media and, when writing must be enabled, you can optionally select to shadow the data.



*DVD/CD Recorder shadowing is supported on Windows 2000 (Service Pack 4 or later) and later only. Windows NT4 is no longer supported by Sanctuary Device Control.*

## Administrators' roles

Sanctuary's User Access module allows you to set precise controls on who has access to the different components of the Sanctuary Management Console. For example, you can restrict the access to the shadowing information to only the company's auditors. You should also consult Sanctuary's Setup Guide to learn how to set rights to control Organizational Units/ Users/ Computers/ Groups.

## Tamper-proof client component

Sanctuary Device Control depends on the Sanctuary Client Driver installed on each protected computer or server to do its work. Since this is a critical part of the installation, this driver is protected against uninstalling — even for authorized administrators. Sanctuary Administrators may emit an 'endpoint maintenance ticket' (see *Client hardening* on page 172 and *Endpoint Maintenance* on page 27) or explicitly deactivate this protection.

## File filtering

Control which file types can be copied to/from removable devices (see *Using file filters* on page 60).



## What is new on this version

A full list features and changes can be found in the *Readme.txt* file located on your CD installation disk.

### Custom reporting

In addition to the standard reports (showing, for example, device permissions, shadowing by user or computer, online machines and so on), you can now generate your own custom reports. For example, you could schedule a report showing attempts to access unauthorized devices emailed to you on a daily or weekly basis, or produce daily reports of Sanctuary administrators' actions.

### Client hardening of Shadowed files and logs

Sanctuary Client, which is installed on computers, is protected from tampering by malicious users by client hardening. This prevents users from uninstalling or deleting the kernel driver that monitors their use of devices. This client hardening has now been extended so that copies of files transferred to devices (shadow files) and log files cannot be removed before they are uploaded to the SecureWave Sanctuary Database, even by Sanctuary administrators.

### Wireless online/offline permissions

Vulnerabilities from Wireless users bypassing your organization's firewall, connecting to the Internet while also connected to your company networks, are now prevented using Sanctuary. Sanctuary Client now supports separate online and offline permission rules.

### Temporary permission offline

If you are not connected to a SecureWave Application Server you can extend your permissions on a temporary basis by contacting a Sanctuary administrator by phone. Once you have agreed the terms of the extension, you can give the administrator a key code and they can respond with a passphrase that, when entered on the protected computer, extends your offline permissions temporarily.

### Password recovery for decentralized encryption

If you are using decentralized encryption for removable storage devices and a user forgets their password they can recover a password that decrypts and re-encrypts the media and gives access to their data. The user contacts a Sanctuary administrator, for example, by phone. Once the administrator has authenticated the user, they can provide a code that can be used to reset the encryption password.

### Expanded file types for filtering

You can limit access to certain types of files on removable storage devices, floppy disk drives and CDs/DVDs. This list of applications that are supported by Sanctuary Device Control has been expanded. File filtering now includes more common file types.

### 64-bit operating systems and Windows Vista support

Sanctuary supports both 32- and 64-bit versions of Windows Vista in a number of different language versions.

### Proxy support

A Sanctuary Client can now establish a connection to a SecureWave Application Server through a proxy server and via the Internet. Communications use the TLS protocol (rather than the 'old' TCP/IP protocol). This enables strong encryption of messages and leads to the possibility of having managed servers owned and run by one organization protecting computers located at a second organization .

### Persistent username in Sanctuary logs

The user names reported in log files are retained even if the user account has been removed from your organization's servers.



## Device types supported

Sanctuary Device Control supports a wide range of device types that represent key sources of security breaches. For some of these devices, you can allow access and activate the shadowing option for that class. If this is done, Sanctuary Device Control enables the administrators to view the content of the files written/read to/from that authorized device.

You can set up permissions for devices that connect using USB, FireWire, PCMCIA, ATA/IDE, SCSI, Bluetooth, and IrDA bus types (see . Devices attached to these buses recognized based on their device type, not on the way they are connected. For example, an external DVD/CD-ROM drive attached to a PC using the USB port is recognized as device type DVD/CD-ROM and is, therefore, controlled using the same mechanism and settings as an internal DVD/CD-ROM drive. It is possible to define a permission at device class level and restrict it to a specific device type, such as USB, FireWire etc.

Device types currently managed by Sanctuary Device Control include:

### Biometric devices

You can find Password Managers and FingerPrint readers in this class of devices. They are connected to the computer using the USB port.

### COM/serial ports

These include serial ports and devices that make use of COM device drivers, such as some types of modems (including null modems) and terminal adaptors. Some PDA cradles also make use of the serial port, even when they are connected through the USB port.



*Some devices, like the Bluetooth print server, only work if the COM port is also enabled. If you use a printer that is configured to use a particular COM port (even if this port is provided by a Bluetooth adapter), then you may need to give access to the COM port as well.*

### DVD/CD drives

CD-ROM and DVD access can be managed in several ways. Sanctuary Device Control allows for full device lock/unlock, access to music CDs only, or access only for uniquely identified DVDs/CDs previously authorized. You can also restrict write privileges to CD-R/W and DVD -/+R/W devices.

### Floppy disk drives

Access to the floppy drive can be managed as either completely locked/unlocked or on a read-only basis. Floppy disk drive devices include conventional diskette drives, as well as high-capacity drives such as the LS-120. This applies no matter how the devices are connected to the system, whether IDE, parallel, USB, or by other methods.

### Imaging devices/Scanners

Access to these devices can be managed with Sanctuary Device Control whether they are USB or SCSI. A scanner or a Webcam are examples of this kind of devices.



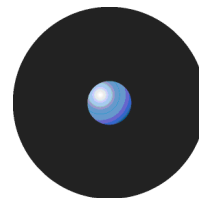
*Some all-in-one models of devices like the HP PSC1350 include a Printer, a Scanner and a memory card reader. There are cases where the scanner functionality cannot be used if the USB Printer functionality is disabled by the Device Control client.*


### LPT/parallel ports


You can control conventional parallel printer ports, as well as variants such as ECB. Dongles are also included.

### Modems/Secondary network access devices

Access to these internal or external devices can be managed with Sanctuary Device Control. 'Secondary' network devices are those that do not connect directly through 'normal' channels.



 *Different modems operate in different ways. Depending on your brand, you may need to allow access to the COM port, to the Modem port, or, possibly, to both, so that you can use your modem. You should experiment with the settings in order to see what works best in your case.*


 *If your users connect via dialup you may need to set a permission rule to the Local System for the Modem.*

### Palm handheld devices

Create permissions rules at your convenience for this type of devices using Sanctuary Device Control.


### Plug and Play devices

Sanctuary Device Control is able to detect Plug and Play devices, even when they are added on the fly. These devices are subject to the same access controls set for fixed devices of the same type.

 *During the plug and play process, Windows registers the device into a class. Sanctuary Device Control uses this information to apply permissions to the device. For example, if Windows registers a camera in the Removable Storage Devices class, the access to this camera is controlled by the permissions set in that class in the Device Explorer module.*

### Printers (USB/Bluetooth )

Sanctuary Device Control allows you to control the access to USB/Bluetooth printers connected to client computers.


 *Some all-in-one models of devices include a Printer, a Scanner and a memory card reader. There are cases where the scanner functionality cannot be used if the Device Control client disables the USB Printer functionality.*

### PS/2 ports

PS/2, the port traditionally used to connect a keyboard, is being rapidly superseded by the USB port for keyboard connections. If you are only using USB keyboards and USB mice in your network, you can opt to block definitely all PS/2 ports. This will render the use of PS/2 Keyloggers (which capture data typed at the keyboard, including passwords and other sensitive data) impossible. Please consult *Chapter 8: Setting and changing options* on page 169 for more information.

### Removable storage devices

This device type includes disk-based devices that are not floppy or CD-ROM drives. Devices such as Jaz and PCMCIA hard drives fall in this category, but also USB memory devices such as memory stick, Disk on Key, ZIP, as well as USB-connected MP3 players and digital cameras.

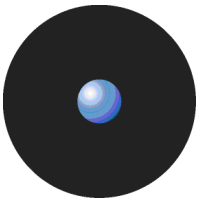
 *Secondary hard disks drives (including SCSI drives) are treated as Removable Storage Devices. By specifying if the permission that applies to 'Hard Drive' or 'Non Hard Drive' you can distinguish between memory keys and secondary hard drives. You can also restrict the permissions to devices that connect through a given bus, such as, USB, SCSI, or PCMCIA.*

### RIM BlackBerry handhelds

Handheld computers/mobile phones from the RIM (Research in Motion) BlackBerry range connected to the computer through a USB port. Access to these PDA/GSM devices can be managed with Sanctuary Device Control.

### Smart Card readers

Access to readers for smart cards, such as eToken or fingerprint readers, can be managed with Sanctuary Device Control.



## Tape drives

Access to internal and external tape drives of any capacity can be managed with Sanctuary Device Control.



*Some backup units that do not use the Microsoft supplied drivers cannot be controlled by Sanctuary Device Control.*

## User Defined devices

Devices that do not fit into the standard categories can also be managed with Sanctuary Device Control. Devices such as some PDAs (non Compaq IPAQ USB, non Palm Handheld USB), iPaq, Qtec, HTC, and Web Cams can be specified as a User-Defined device and permissions added to them in the usual way.

## Windows CE handheld devices

Access to these devices can be managed with Sanctuary Device Control. The HP iPAQ or XDA are Windows Mobile 5 CE Devices (running Windows PocketPC 2002/2003 OS).

## Windows CE handheld devices

Handheld Windows CE computers (using PocketPC OS) connected to the PC through a USB port.

## Wireless network interface cards

When installing the Sanctuary Client Driver, you have the option to configure the client's permissions to use a Wireless LAN adaptor.



*This permission applies only to Wireless cards for which Windows does not require a manufacturer-specific driver or administrative privilege to install.*

# Conclusions

Sanctuary Device Control eliminates the majority of the dangers associated with insiders abusing their access to network resources and mission critical information. It significantly increases the security level on your operating system controlling and auditing end-user access to input/output (I/O) devices.

Using the control console, the security administrator(s) can allow access to an I/O device by assigning permission rules to users/groups.

With the optional 'shadowing' feature, it is possible to track down data written/read to/from certain I/O devices. You can also access a log of what files were copied to various I/O devices on any given day.

Sanctuary Device Control non-obtrusive and flexible nature protects and prevents with practical no overhead for your users or system. Using our products, you can rest confident that your company is safe.

---

## Chapter 2: Using the Sanctuary Console

This chapter explains how Sanctuary Device Control approaches I/O security. It describes the components of the Sanctuary Device Control and explains how they contribute to the enforcement of your company's security policies.

When you first install Sanctuary Device Control, default permission rules are created and configured. These rules include Shadow restrictions and Read/Write permissions for some of the devices. Although these settings meet the needs of some users, most people require additional access rights to carry out their day-to-day jobs. One of the first tasks of an administrator is to define new permissions rules for users, groups, computers, or devices in their network.

Using the Sanctuary Management Console you can:

- > Set default options.
- > Grant general access to all available devices.
- > Define specific rights for certain users.
- > Authorize media types and specific media on a general or user-by-user basis.
- > Send updates to all users or to certain computers.
- > Maintain the database where all info is kept.
- > Synchronize domain users.
- > Configure centralized and decentralized encryption, etc.
- > Generate standard reports, for example showing User permissions, Device permissions, Computer permissions, Media by user, Users by medium, Shadowing by device, Shadowing by user, Online machines, User options, Server Settings, and Machine options.
- > Generate custom reports of device use/attempted use.
- > See the content of a copied/read file (only if Shadow is active).
- > View the log of all changes administrators make to users' policies.
- > Review any attempt to access the configured devices in a computer.

### Starting the Sanctuary Management Console

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

### Connecting to the Server

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

To connect to the server, follow these steps:



Figure 1: Connecting to the server

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

secsrv.secure.com[1234]



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



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

2. Choose to either log in as the current user, or specify a different user's details, using the *Log in as* option.
3. Click on the OK button. The Sanctuary Management Console screen is displayed.

If the Sanctuary Management Console screen does not appear, an error message is displayed. This indicates a problem occurred during an internal test. Check that you have the required permissions to connect to your selected server, on domain rights and Sanctuary Management Console rights. See *Defining Sanctuary administrators* on page 32.

## Log in as a different user

If you selected the *Log in as* option, instead of using your credentials you must enter the user name and password. Prefix the user name by a workstation name and backslash for local accounts, and by a domain name and backslash for domain accounts (e.g. DOMAIN1\ADMIN1).

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



Figure 2: Connection / Output window





## The Sanctuary Management Console screen

When you start a Sanctuary Management Console session, the *Sanctuary Management Console* screen is displayed.

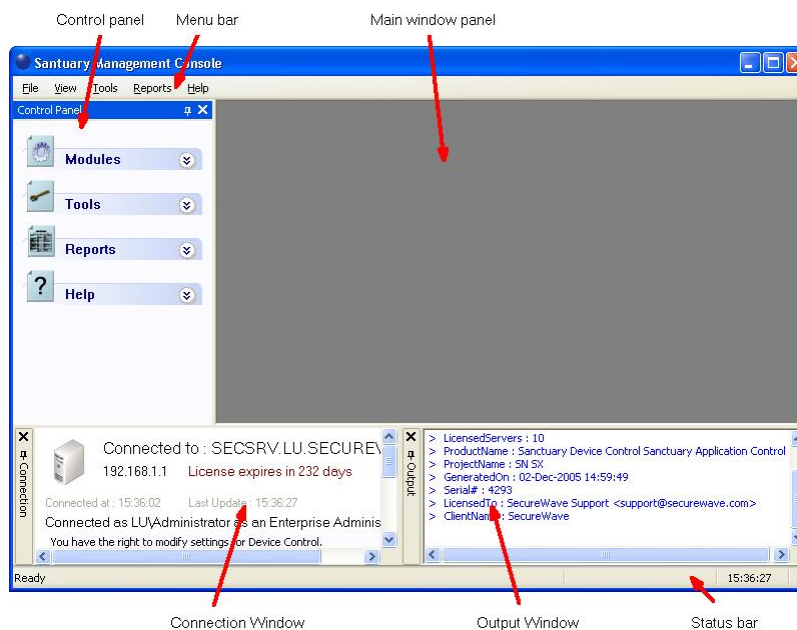


Figure 3: The Sanctuary Management Console screen

The *Menu* in the upper part of the window provides access to different Sanctuary Device Control functions and commands. Some of these depend on the module you are currently using, for example, the contents of the Explorer menu depend whether you are in the Exe Explorer of the Log Explorer. You can use shortcut key combinations to access different commands, for example, ALT+R+O displays an HTML Online Machine report.

The *Control Panel* displays in the left-hand side of the window. This lets you directly select the available modules and options without using the menu. If the *Control Panel* is not visible, use the *View* → *Control panel* command to display it.

The contents displayed in the *Main window* panel depend on the module currently selected on the left panel. You can refine the information displayed in some modules. Every time you open a module, it stays open — arranges in stacked tabs — until explicitly closed. You can use the *Window* command of the menu bar to organize your workspace.

The *Connection* window shows information about the current user. You can use the scrollbar to navigate through the text. If the *Connection* window is not visible, use the *View* → *Connection* to display it.

The *Output* window displays important information messages, for example, messages generated by updates sent to the clients, file fetching, I/O failures, as well as error messages. Use the scrollbar to navigate through the text. If the *Output* window is not visible, use the *View* → *Output* command to display it.

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

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






Figure 4: License status warning

This information is also reported in the *Connection* window of the main screen and generates a log that you can see using Windows' event viewer.



## Customizing your workspace

You can resize and reposition the panels in the main Sanctuary Management Console window to suit your needs. To do this, use the Pin icon  to 'pin down' or 'float' () the *Control Panel*, *Connection*, or *Output* windows. When a window is 'parked' the icon changes to .

Alternatively, you can 'dock' each window or minimize the panel. In *Dock* mode, the window hides itself as a tab at the edge of the Sanctuary Management Console screen, leaving more space for the main window panel. Click again on the pin to 'float' the window panel again.



Figure 5: Docked Control Panel



Figure 6: Docked window

In *Floating* mode, the windows can be moved to any position in the screen, sharing the working area with whatever module is opened.

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

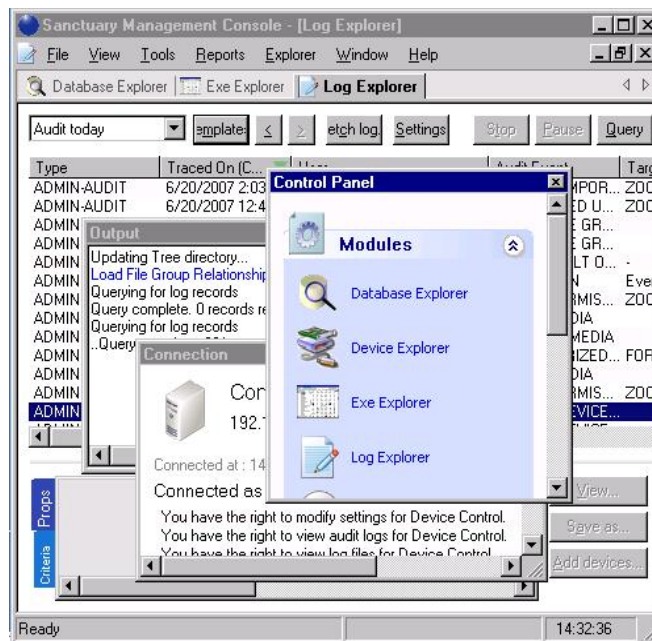


Figure 7: Floating Control Panel

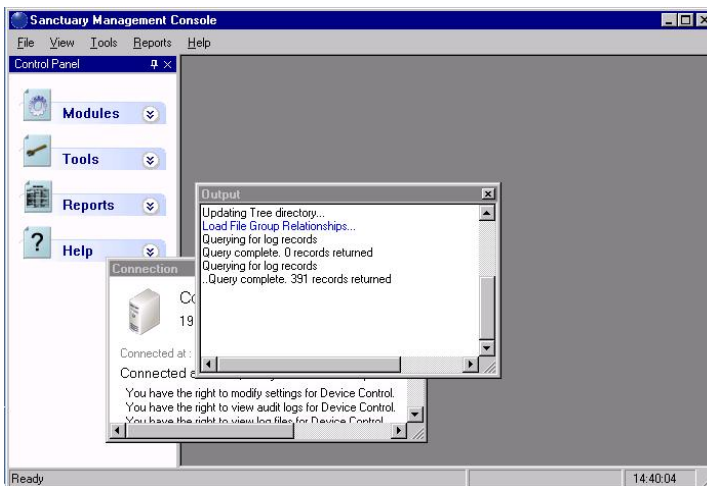


Figure 8: Floating windows

Double click on a window's title bar to dock it to its previous position. You can also drag the window to any edge of the Sanctuary Management Console screen in which case it docks itself — guide yourself with the rectangle shape preview before letting go the mouse button.

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

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

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

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

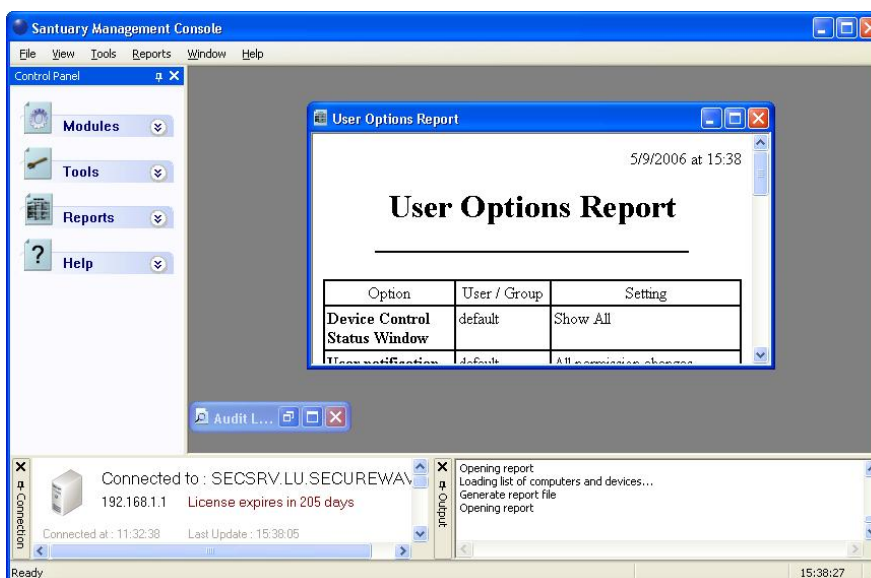


Figure 9: Minimized windows



## The Sanctuary Device Control modules

When you are using Sanctuary Device Control the Sanctuary Management Console screen gives access to the three Sanctuary Device Control modules. These are summarized in the following table:

<b>Module</b>	<b>Icon</b>	<b>Used to ...</b>	<b>See...</b>
<i>Device Explorer</i>		Grant access to I/O devices for specific users or groups. Establish copy limits and activate shadowing. Allows users to encrypt removable devices 'on the fly' (decentralized encryption)	<i>Chapter 3: Using the Device Explorer</i>
<i>Log Explorer</i>		<ul style="list-style-type: none"> <li>&gt; View records of files copied from any PC to authorized I/O devices, and view the contents of the files themselves (two way 'Shadowing').</li> <li>&gt; View attempts to access or connect unauthorized devices.</li> <li>&gt; Create custom reports, for example you can create a daily or weekly scheduled report of all user attempts to access an unauthorized device.</li> </ul>	<i>Chapter 5: Using the Log Explorer</i>
<i>Media Authorizer</i>		<ul style="list-style-type: none"> <li>&gt; Recognize specific DVD/CDs which users can be permitted to use, even where they have not been granted access rights to access the DVD/CD drive, as well as establish specific (encrypted) removable media which users can be permitted to use.</li> <li>&gt; Give permission to use specific DVD/CDs for users who have been barred from using the DVD/CD drive.</li> <li>&gt; Establish permission to use specific (encrypted) media.</li> <li>&gt; Centrally encrypt removable devices.</li> </ul>	<i>Chapter 6: Using the Media Authorizer</i>

Table 1: The Sanctuary Device Control modules

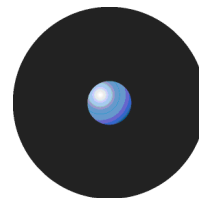
### Device Explorer module

The Device Explorer module is the main nucleus of the Sanctuary Management Console program when used under Sanctuary Device Control. Sanctuary's administrators can use it to:

- > Modify assigned permissions and rules.
- > Create new permissions and rules.
- > Delete already defined permissions and rules.
- > Check permissions and rules.
- > Define user who must encrypt removable storage devices before using them (decentralized encryption).
- > Add uniquely, serial identified, removable storage devices to further control the working environment.
- > Define the bus type where the permission will apply (depending on the device class).

The rules can be any combination (depending on the device) of the following ones:

- > Read data.
- > Read/Write data.
- > No access to data.
- > Only allow access to encrypted removable storage devices.
- > Online permission.
- > Offline permission.
- > Scheduled permission.
- > Temporary permission.
- > Shadow permission (a copy of all data written/read to/from certain I/O devices).
- > Data Copy limit permission.
- > Encrypt/decrypt, export encryption key to file/media, import encryption key (when using removable devices).



You can find more information in *Chapter 3: Using the Device Explorer*.

## Log Explorer module

The Log Explorer module forms the core housekeeping control routine that are carried out by Sanctuary administrators. It displays the information stored in the log files in the format you specify in a template. You can create custom reports showing:

- > User actions – for example, users accessing floppy drives or other device types.
- > Administrator actions – for example the granting of permissions for particular devices.



*In previous versions of Sanctuary administrator actions were reported in the Audit Log Viewer.*

Although the driver enforces defined permissions, the administrators can use this module to check the usage of granted permissions and who is trying to access non-authorized devices.

For more information about the Log Explorer module see *Chapter 5: Using the Log Explorer* on page 99.

## Media Authorizer

Administrators can use the Sanctuary Management Console's Media Authorizer module to scan a DVD/CD and enter its details into the Database of Authorized DVDs/CDs. When this action is finished, the DVD/CD is ready to be assigned to a user or group, define its permissions, and be used in the organization. When a DVD/CD is scanned, the DVD/CD Authorizer calculates a checksum to uniquely identify it.

There is no limit to the number of Authorized CDs that can be added to the database. Authorization of multi-session CDs is only supported when the client and the console are installed on the same machine.

When a DVD/CD is inserted into a client computer, the driver verifies the checksum. If it coincides with the Authorized DVDs/CDs that the user is allowed to access, then the DVD/CD is made available. If the checksum does not correspond to one in the white list access is denied.

You can find more information in *Chapter 6: Using the Media Authorizer* on page 129.

The second use for this module is to encrypt removable storage devices connected to the computer. The administrator uses one of the three proposed methods to cipher the device. As an alternative, you can use the *Device Explorer* module to define permissions that force the user to encrypt any removable storage device plugged to his computer.

The third use for the Media Authorizer module is to add an externally encrypted device (Import) to the database of already encrypted devices and then define permissions for a user to use it. The administrator can also 'force' the user/user group to use only encrypted devices minimizing the risk of losing information if the device is lost.

For more information see *Chapter 7: Accessing encrypted media outside of your organization* on page 149.

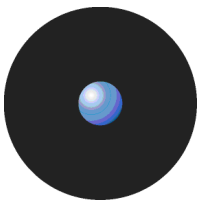
# The Sanctuary Management Console menus and tools

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

## File menu

Use the *File* menu to connect or disconnect from a SecureWave Application Server, save the contents of the main page, or close the program. The *File* menu options are explained in the following table:

<b>Option</b>	<b>Used to</b>
<i>Connect</i>	Communicate with a SecureWave Application Server running on another machine or using a different user name in order to carry out administrative tasks.
<i>Disconnect</i>	Detach the Sanctuary Management Console from the current SecureWave Application Server before using the <i>Connect</i> option.



<b>Option</b>	<b>Used to</b>
<i>Save As</i>	Save the contents of the main window in CSV format (only available for specific modules). You can use this option to export data to any CSV compliant program, for example Excel.
<i>Print</i>	Print the active report window. The standard Internet Explorer print dialog is displayed.
<i>Exit</i>	Exit the Sanctuary Management Console application. This command does not stop the SecureWave Application Server, just your administrative session.

Table 2: File menu options

## View menu

The *View* menu controls how the main elements of the Sanctuary Device Control window are displayed. The *View* menu options are explained in the following table:

<b>Option</b>	<b>Used to</b>
<i>Modules</i>	Display a sub menu from which you can select any available module.
<i>Control Panel</i>	Show/hide the Control Panel, which lets you select modules, tools, reports, and help from a convenient list.
<i>Output</i>	Show/hide the Output window, which displays a log of system activity.
<i>Connection</i>	Show/hide the Connection window, which displays real-time operating information.
<i>Status bar</i>	Show/hide the status bar, which displays program's conditions, clock, and messages.

Table 3: View menu options

## Tools menu

The *Tools* menu is used to update the database, send permissions to Sanctuary clients and so on. The *Tools* menu options are explained in the following table:

<b>Option</b>	<b>Used to</b>
<i>Synchronize Domain members</i>	Update the SecureWave Sanctuary Database with the current list of users and groups of a domain or machine.
<i>Database Maintenance</i>	Delete the device logging entries, audit logs, machine scans, shadow files, and key recovery information created before a given date from the database and data file directory.
<i>User Access</i>	Define Sanctuary Enterprise Administrators and Sanctuary Administrators. This option lets you restrict the right to set permissions, view audit information about administrators' actions or shadowing information. See Sanctuary's Setup Guide to learn how to set rights to control Organizational Units/ Users/ Computers/ Groups.
<i>Key Recovery</i>	Access the administrator's tool to recover a password to unlock an encrypted storage device. See <i>Recovering a password for decentralized encryption when connected</i> on page 143.
<i>Default Options</i>	Change the default options settings for computers. See <i>Chapter 8: Setting and changing options</i> on page 169.
<i>Send Updates to All Computers</i>	Dispatch the latest setting and permission changes to all computers on the network. Changes can be sent in synchronous or asynchronous mode.
<i>Send Updates to</i>	Transmit the latest setting and permission changes to a specific computer on the network.
<i>Export Settings</i>	Place all settings and permissions in an external file that can be sent to all those who are working offline with no connection, and need an update of their permissions. If placed in a special file — policies.dat — it is possible to do a 'Serverless' client installation (see <i>Sanctuary's Setup Guide</i> for more details). See <i>To export and import permission settings</i> on page 81.
<i>Purge Online Table</i>	SecureWave Application Server keeps a record of connected clients. Sometimes, clients are disconnected without notifying their server that they are not available anymore. In this case orphan entries are left in the online table affecting the performance of the 'Send Updates' functionality. When you purge the online table, the application server erases all information it has regarding connected clients. Every time a user logs on/off or unlocks his station the online table is modified.
<i>Endpoint</i>	Create and save maintenance 'tickets' for computers/computer groups



<b>Option</b>	<b>Used to</b>
<i>Maintenance</i>	allowing protected files and/or registries to be modified.
<i>Temporary Permission Offline</i>	Access the administrator's tool for generating a code that can be communicated to a user by phone to enable them to increase their permissions on a temporary basis while offline. See <i>To assign temporary permissions to offline users</i> on page 76.

Table 4: Tools menu options



*All the commands in the Tools menu can also be accessed via the Tools module of the Control Panel.*

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

## Endpoint Maintenance

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

This key value works in conjunction with the *Client Hardening* value established in the *Default Options* dialog (see *Chapter 8: Setting and changing options* on page 169). If the client hardening option is set to 'Basic' you do not need salt. If the client hardening option is set to 'Extended' you need to enter or query the salt and relax the protection using the endpoint maintenance. The generated 'ticket' can be saved and transported to the client computer(s) by any available mean (shared directory, email, or removable device).



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



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

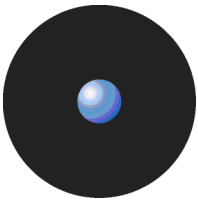


*Do not use the 'Send to' right-click menu option to transfer the Maintenance ticket file, use Copy & Paste instead.*

## Client ticket rules

The client ticket follows these rules:

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



5. Your comments appear on the audit log. You can review them by using the Log Explorer module (see *Chapter 5: Using the Log Explorer* on page 99).



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

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

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

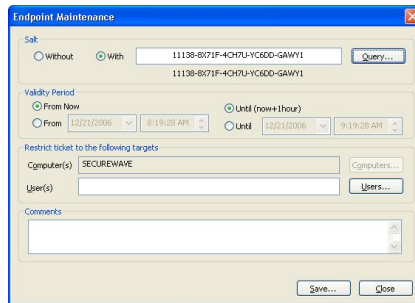


Figure 10: Endpoint maintenance

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

### Reports menu

The *Reports* menu can be used to save or print many types of information. The *Reports* menu options are explained in the following table:

<b>Option</b>	<b>Used to</b>
<i>User Permissions</i>	Generate a report of the device permissions associated with one or more users.
<i>Device Permissions</i>	Generate a report of users' permissions for each device.
<i>Computer Permissions</i>	Generate a report of the permissions assigned to each user for the use of the different devices associated with a particular computer.
<i>Media by User</i>	<p>Generate a report of the types of DVDs/CDs a selected user is allowed to access.</p> <p><i>DVDs/CDs authorized as a result of a User being a member of a Group are not listed.</i></p> <p>Specific (encrypted) media that users have permission to use are also listed in this report.</p>
<i>Users by Medium</i>	Generate a report of the users or groups allowed to use each authorized DVD/CD. Users who have been granted the right to





<b>Option</b>	<b>Used to</b>
	access a specific encrypted media are also listed in this report.
<i>Shadowing by Device</i>	Create a report showing the users copying/reading data to/from particular devices.
<i>Shadowing by User</i>	Generate a report showing the total amount of data copied/read to/from different devices for all users.
<i>User Options</i>	Generate a report with all related permissions and settings for a specified user.
<i>Machine Options</i>	Generate a report showing all computers' options as currently defined in the system. These can be changed using the command <i>Tools → Define Options</i> .
<i>Online Machines</i>	The SecureWave Application Server(s) keep record of the connected clients. The online table is updated every time a user logs on or unlocks his/her station. This report shows a list of connected machines.
<i>Server Settings</i>	Generate a report showing how your SecureWave Application Server (s) is configured. This is provides you with very useful troubleshooting information.

Table 5: Report menu options

See *Chapter 9: Generating Sanctuary Reports* on page 179 for more detailed information.



*In addition to the standard reports that are available through the Reports menu, you can define your own criteria for selecting log entries and producing reports using the Log Explorer module. For more information see Chapter 5: Using the Log Explorer on page 99.*

## Explorer menu

The *Explorer* menu contains different menu options depending on which module you are currently using. The *Explorer* menu options are explained in the following table:

<b>Option</b>	<b>Used to</b>
<b>In the Device Explorer module</b>	
<i>Manage Devices</i>	Add/remove devices that can be administrated using permissions.
<i>Insert Computer</i>	Add a machine to the machine-specific settings section or a computer group.
<i>Add/Modify Permissions</i>	Define/change general permissions.
<i>Add/Modify Online Permissions</i>	Define/change device permissions to apply when a computer is connected to the network.
<i>Add/Modify Offline Permissions</i>	Define/change device permissions to apply when a computer is not connected to the network.
<i>Add/Modify Scheduled Permissions</i>	Define/change programmed permissions.
<i>Add/Modify Shadow Settings</i>	Create/modify the rules used to obtain a copy of those files users have copied/read into/from certain devices.
<i>Add/Modify Copy Limits</i>	Define/change copying quota limits.
<i>Temporary Permissions</i>	Define provisional permissions.
<i>Remove</i>	Delete the current selected permission, device group, computer, or computer group.
<i>Insert Device Group</i>	Add a device-classifying group.
<i>Rename Device Group</i>	Change the name of device-classifying group.
<i>Insert Computer Group</i>	Add a computer-classifying group.
<i>Rename Computer Group</i>	Change the name of a computer-classifying group.
<b>In the Log Explorer module</b>	
<i>Fetch log</i>	Obtain the latest log entries from a client computer.

Table 6: Explorer Menu options



## Window menu

The *Window* menu controls how the panels and windows in the Sanctuary Management Console screen are displayed. The *Window* menu options are explained in the following table:

Option	Used to
Cascade	Place all open windows in an overlapping arrangement.
Tile	Lay all open windows side by side in a non-overlapping fashion.

Table 7: Window menu options

## Help menu

The *Help* menu is used to access information about the Sanctuary Management Console and Sanctuary Device Control. The *Help* menu options are explained in the following table:

Option	Used to
Contents	Go directly to the contents tab of the help file.
Search...	Look up information in the help file.
Index...	Show the help index.
About...	Display information about the current version of Sanctuary Device Control, when contacting SecureWave technical support staff.
SecureWave on the Web	Go to the SecureWave home page, where you can find updated information about all Sanctuary products.
SecureWave Knowledgebase	Go directly to SecureWave's knowledge database. This includes tips, questions and answers, and how-to articles.

Table 8: Help menu options

## Other administrative functions

This section explains the use of other administrative functions.

### Setting and changing default options

Sanctuary Device Control allows you to set default options for various aspects of the Sanctuary Client Driver behavior. You do this using the *Default Options* dialog.

You can access the *Default Options* dialog by selecting *Default Options* from the *Tools* menu (or from the *Control Panel*):

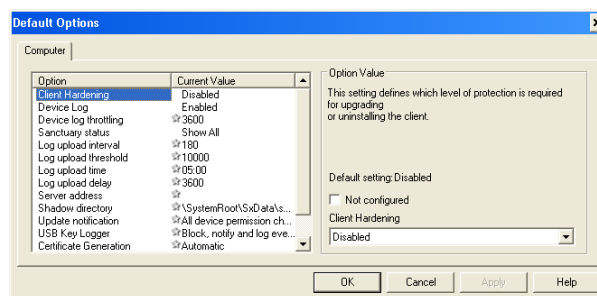


Figure 11: The Default Options dialog

Please refer to Chapter 8: Setting and changing options on page 169 for detailed information.

### Synchronizing domain members

If Sanctuary Device Control is protecting the computers in a domain, and you wish to synchronize to that domain, then select *Synchronize Domain members* from the *Tools* menu (or from the *Control Panel*). The following dialog appears.

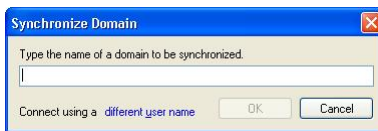
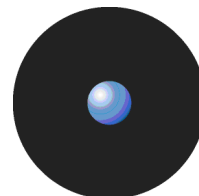


Figure 12: The Synchronizing Domains dialog

Type the name of the domain you want to synchronize and click the OK button. The list of users and groups held by Sanctuary Device Control is updated.



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

## Synchronizing with Novell eDirectory

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

## Adding workgroup computers

If Sanctuary Device Control is protecting the computers in a workgroup instead of a domain, then there is no domain controller from which you can obtain a list of users. In this case, you need to add the computers in the workgroup individually. To do this, select *Synchronize Domain members* from the *Tools* menu (or from the *Control Panel*). The following dialog appears:



Figure 13: Adding workgroup computers

Type in the name of the computer you want to add, and then click on DIFFERENT USER NAME. The following dialog is displayed:

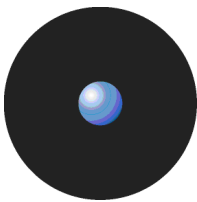


Figure 14: The Connect As dialog

Type in the user name and password for the local administrator for the computer you want to add. Make sure you include the computer's name in the user name. When you have done so, click the OK button twice (to close the corresponding dialogs). This adds the computer to the database and you can then proceed to assign permissions to its users through the Device Explorer module.



*Windows XP has a feature called 'Simple File Sharing' which can sometimes interfere with the process of synchronizing a computer with Sanctuary Device Control. If the process described above does not make the computer visible to Sanctuary Device Control, you should turn off this option and try again to synchronize the computer. To access the 'Simple File Sharing' option, open 'Windows Explorer' on the target machine, select 'Folder Options' on the 'Tools' menu (or from the Control Panel) and then go to the 'View' tab. It should be the last option in the list.*



You can also synchronize the local users/groups of one or more workstations when a domain is used in case you want to enforce policies on a local user despite being in a domain.

## Performing database maintenance

After you have been using Sanctuary for a while, your database will have accumulated a large number of activity logs, scan results, shadow files and key recovery information. Older records take up unnecessary database space and may no longer be needed for your daily operations. If this is the case, you can periodically clean up the database by removing obsolete records.

To delete database records prior to a given date from the database, go to the Database Maintenance dialog, accessible from the *Tools* → *Database Maintenance* menu (or from the *Control Panel*):



Figure 15: Performing database maintenance

You can click on the arrow to the right of the date field to select the date from a calendar. The maintenance you can do when using Sanctuary Device Control is to delete device log information, audit logs, shadow files (if they exist) and any key recovery information. Clicking on the OK button deletes the database records written before the chosen date.



*Database maintenance operations cannot be undone. If you wish to keep this information for future reference, you should first do a backup using the SQL Server utilities. You also need to make a backup of the data file directory.*



*You should make sure that there is enough free space on the database server hard disk BEFORE starting database maintenance. If the operation fails because the database engine cannot create the transaction logs, you should perform the maintenance on a shorter period basis.*

## Defining Sanctuary administrators

Before proceeding to use the program, we recommend that you define the administrators. You can assign different roles for each one of them, but you should have at least one called 'Enterprise Administrator'. You should be careful not to lockout yourself when modifying these roles.



*Local machine users cannot manage Sanctuary Management Console even if they are assigned as Enterprise Administrators. They cannot connect the Sanctuary Management Console to the SecureWave Application Server using such an account.*



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

All members of the local Administrators group on servers running SecureWave Application Server are Sanctuary Administrators and have access to all objects by default. To restrict access to defined users, go to the *User Access* dialog, accessible from the *Tools* → *User Access* menu (or from the *Control Panel*) as shown below.

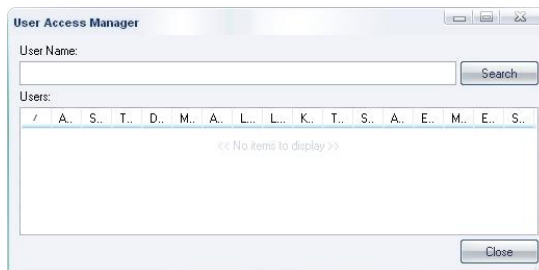
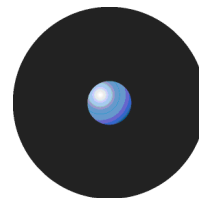


Figure 16: Searching for users

Enter a user name in the *User Name* field and click on SEARCH to locate the user, or group, to whom you want to grant administrative rights. You can use wildcards (\* or ?) in the name. The

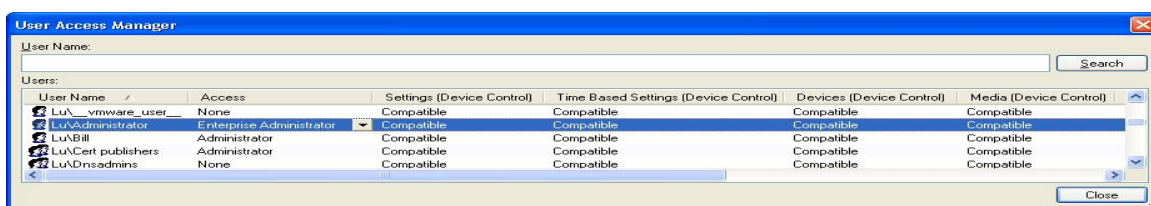


Figure 17: Defining the administrators' roles

Select the user in the *Users* list and click on the *Access* column. If you now click on the down arrow icon located at the right side of the field, you get a menu with all available options. Set a user to Enterprise Administrator to grant him/her the right to connect to the SecureWave Application Server and manage any object (Users/Groups/Computers/Default Options).

*Only the 'Enterprise Administrators' can assign other users as 'Administrators'.*

Set the user as 'Administrator' when you want him/her to use the Sanctuary Management Console without being able to assign other users as administrators.

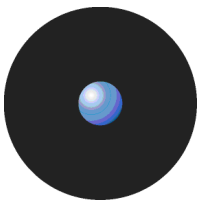
If you are delegating administrative rights using Active Directory Organizational Units, the Sanctuary Management Console Administrators have the following permissions:

Action	Type of Administrator	Comments
View all permissions.	All Administrators	
Modify global-level permissions.	Enterprise Administrators	
	Members of the 'Manage Device ControlSettings' role.	ONLY for the users that the administrator is allowed to manage.
Modify machine-level permissions.	Enterprise Administrators (for ALL accounts, including the WELL-KNOWN accounts).	
	Members of the 'Manage Device Control Settings' role (for ALL accounts, including the WELL-KNOWN accounts).	ONLY for the machines that the administrator is allowed to manage.
Modify machine-group permissions.	Enterprise Administrators (for ALL accounts, including the WELL-KNOWN accounts).	
	Members of the 'Manage Device Control Settings' role (for ALL accounts, including the WELL-KNOWN accounts).	IF AND ONLY IF the administrator is allowed to manage ALL the machines in the machine group for ALL accounts in BOTH CASES, including the WELL-KNOWN accounts.

Table 9: Administrator's prerogatives




*When you define at least one user as Enterprise Administrator, the members of local Administrators group (default setting) no longer have access to SecureWave Application Server /Sanctuary Management Console. Be careful when adding/removing 'Administrators' from the list and ensure that there is always at least one Enterprise Administrator.*

Sanctuary Management Console administrators' access can be restricted to pre-defined roles when activating the 'Yes' option. These are summarized in the following table (please see also the notes after the table):





<b>Option</b>	<b>Administrator actions available when option set to 'Yes'</b>	<b>Comments</b>
Settings (Device Control)	Change permissions and options for the objects he has write permissions in the Active Directory.	Can also see the 'Media Authorizer' module.
Time based settings (Device Control).	Set time-related permissions: Temporary and scheduled permissions. Administrator cannot set standard permissions.	This option is a sub group of 'Settings (Device Control)'.
Devices (Device Control)	Add new devices in the system using the manage devices functionality and group them.	
Media (Device Control)	Encrypt and authorize media but cannot change the permissions in the Device Explorer module.	Can also see the 'Media Authorizer' module and get more reports ('Media by User' and 'Users by Medium'). This option is a sub group of 'Settings (Device Control)'.
Audit (Device Control)	View and search Audit Logs.	Can also see the Administrator actions, if you have the appropriate privileges, using the Log Explorer module.
Logs (Device Control)	Review central logging and access shadow files.	Can also see the Log Explorer module and get more reports ('Shadowing by Device' and 'Shadowing by User').
Logs without File Access (Device Control)	Same actions done by the Logs (Device Control) option but cannot see the content of a shadow file.	This option is a sub group of 'Logs (Device Control)'.
Key Recovery (Device Control)	Generate a passphrase used to access an encrypted device when the user has forgotten a decentralized encryption password.	This is done with a lower security risk when the user is connected to your network as Sanctuary Client Driver can provide a Security Code containing the public key (whereas Sanctuary Volume Browser cannot).
Temporary Permissions Offline (Device Control)	Set temporary permissions for users who are not connected to the SecureWave Application Server yet require extended access permissions for a short time. Administrator cannot set standard permissions.	
Endpoint maintenance	Create tickets to update, delete, and install the client driver.	See <i>Endpoint Maintenance</i> on page 27.
Scheduled Reports	Generate custom reports at pre-scheduled intervals between start and end dates.	See <i>Schedule</i> tab on page 118.

Table 10: Administrator's roles

-  *There are no restrictions on an administrator when choosing the 'Compatible' mode.*
-  *The opposite of the 'Yes' rule applies when selecting the 'No' option for an Administrator.*
-  *There are default rights that apply to all Administrators: see the Device Explorer module and get some 'Reports' ('Users Permissions', 'Device permissions', 'Computer permissions', 'Online Machines', and 'Options'). When selecting the 'Yes' option, you add to this default rights.*

The *Compatible* mode is to be used when Sanctuary Device Control and Sanctuary Application Control Suite use a common SecureWave Sanctuary Database and SecureWave Application Server. This is the default mode for first-time installations and after an upgrade from SecureNT 2.7.x to Sanctuary Device Control. In compatible mode, there are no restrictions on the roles of the administrators. It is called compatible mode because it is compliant with older versions and useful when upgrading.

-  *You can only change these options for 'Administrators'. For all other type of user, they are set to 'Compatible'.*
-  *You should also consult Sanctuary's Setup Guide to learn how to set rights to control Organizational Units/ Users/ Computers/ Groups.*

## Sending updated permissions to client computers

Administrators use the Device Explorer module in the Sanctuary Management Console to modify permissions and rules. When a policy changes, the Sanctuary Client downloads it at the next event, for example, when the user logs in.



If, however, the administrator wishes the changes to take effect immediately, they can be transmitted to the affected client(s), in this case the administrator updates the database via the Application Server. At the same time, the Application Server sends a small message to the connected client computers to indicate that the client should contact the Application Server and download the latest permissions rules.

If the permissions are the same, no changes are applied and the existing rules remain in use. If the permissions differ, the client contacts the Application Server and downloads the latest ones.

When the client receives the new set of permissions, the kernel mode driver effects the changes immediately. There is no requirement for the user to reboot or log-off and log-back onto their system — except for certain devices, see *Table 16*.

Use the *Send Updates to All Computers* or *Send Updates to* items from the *Tools* menu (or from the *Control Panel*) to communicate immediately the changed rules and permissions to the client computers.

You can send permissions updates to computers not connected to the network using a file transfer. See *To export and import permission settings* on page 81 for more information. Alternatively users can temporarily increase their offline permissions by contacting an administrator and obtaining a passphrase. See *To assign temporary permissions to offline users* on page 76.

## Everyday work

In this section, we present you with the most common cases encountered in your daily work with Sanctuary Device Control. You can find practical tips and advices in the following subsections.

### Identifying and organizing users and user groups

Only members of the Domain Administrators or Enterprise Administrators group can create, modify, or delete users and user groups in Windows using the *Active Directory Users and Computers* Microsoft Management Console snap-in. To activate it, select *Start* → *Programs* → *Administrative Tools* → *Active Directory Users and Computers* from Windows' desktop. The users and user groups are automatically published.


Publishing is the act of making an object publicly browseable and accessible. Most objects are automatically published, but you must explicitly publish Windows NT shared printers and computers outside the domain.

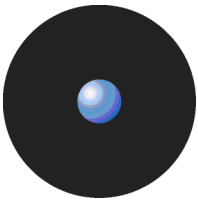
Published resources allow users to find and use objects (users, groups, printers, servers, etc.) without knowing in which server they reside. Published resources are seen across subnets. The *Computer Management* or *Active Directory Users and Computers* administrative tool is used to publish resources in the Active Directory structure.

When you make changes to a domain, such as adding groups, users, or computers, you must publish them, if necessary. You should use the *Synchronize Domain Members* item on the *Tools* menu (or from the *Control Panel*) in Sanctuary Device Control to refresh the content of the devices, users, and group information before proceeding to do any modification to the permissions and rules. This is especially true if you are not the only member of the Administration group. On a Novell network, you should use our synchronization script described in the Sanctuary's Setup Guide.

### Identifying the devices to be managed

When first installing Sanctuary Device Control, all those devices belonging to the standard Windows classes are identified and fill-in with the default values. However, if you add new devices to a computer or an independent computer that forms part of a subnet and is not included in the active directory structure, some of the devices will not be accessible since the most restrictive policy applies. Please see *Table 15* on page 49 and *Table 16* on page 50 for details.

If this policy suits your needs, you would not have to take any action. On the other hand, if you want to change the rules and permissions for a specific computer or a specific model of device, you first need to publish it (see previous section) or add the devices. To add new devices from a specific computer, use the *Manage Devices* dialog. It is accessible if you are using the Device Explorer module () by using the *Explorer* → *Manage Devices* item or by making a right-click on the Default Settings section located on the right panel of the Device Explorer window. Alternatively it is accessible through the Log Explorer by right-clicking on a *Device Attached* entry. See *Managing devices* on page 92 for more details.



You should only add the models of devices for which you want to assign specific permissions. If you only want to set permissions at the class-level, you do not need to add specific models of devices. Do not add devices for which you don't want to define access permissions.

## Working with the Sanctuary system's pre-defined device classes

Once the program installed, the standard Windows' device classes are created:

<i>Standard Windows' device classes</i>			
Biometric Devices	LPT/Parallel Ports	PS/2 Ports	Tape Drives
COM/Serial ports	Modem/Secondary Network Access Devices	Removable Storage Devices	User Defined Devices
DVD/CD Drives	Palm Handheld Devices	RIM BlackBerry Handhelds	Windows CE Handheld Devices
Floppy Disk Drives	Printers (USB/Bluetooth)	Smart Card Readers	Wireless NICs
Imaging Devices			

Table 11: Standard Windows' device classes as seen on the Device Explorer module in the Default Settings section

These classes are given access rights according to *Table 15* on page 49. You DO NOT have to do anything else if you are satisfied with this or if a new device is connected to a computer: the most restrictive access rules already apply for it – no access whatsoever (except for PS/2, WiFi, and IrDA). This is the real magic of our solution: Impeding data leakage for new or unknown devices.

If you need to adapt permissions rules for certain users/groups, you just do a right-click and select the type of permission you want to add. Depending on the device type, you can add:

- > Read or Read/Write permissions. See *Read/Write permissions* on page 70 for more information.
- > Define permissions so that users are forced to encrypt all removable storage devices plugged to their computers. See *Forcing users to encrypt removable storage devices* on page 87.
- > Online/Offline permissions. See *To assign online and offline permissions* on page 80 for more information.
- > Scheduled permissions. See *To assign scheduled permissions to users and groups* on page 73 for more information.
- > Temporary permissions. See *To assign temporary permissions to users* on page 75 for more information.
- > Temporary permissions for offline users. See *To assign temporary permissions to offline users* on page 76 for more information.
- > Shadow. See *Shadowing devices* on page 82 for more information.
- > Copy limit. See *Copy limit* on page 84 for more information.



*When upgrading from older versions of Sanctuary it is possible that some wireless cards appear in the 'Modem/Secondary Network Access Devices' device class rather than the 'Wireless NICs' class. To correct this, simply delete the wireless card from the 'Modem/Secondary Network Access Devices' device class and add it again using the Device Explorer's Explorer → Manage Devices menu option.*

## Adding your own, user-defined devices to the system

Permissions rules for all other devices that do not fall into the 'normal' categories, such as iPaq, Qtec, HTC, or webcams, are defined in the User Defined Device class. Imagine that a user connects a webcam to a computer, a webcam that needs no special drivers to be identified and make it work. In an unprotected environment, the user can immediately begin recording and sending potentially illegal images over email or other medium. Since this webcam is not included on the other device classes, the policies defined here, if they exist, control the access behavior of this device. This user is forced to ask for special permissions in order to use the device since no rule has been defined and the most restrictive applies – no access at all.





On the other hand, if you need to administrate a special kind of device connected to a computer, you can do so by adding it to the list of the managed devices that appear in the Default Settings section of the Device Explorer module. Please refer to *Managing devices* on page 92 for more details.

You can add specific models to all the base device classes located on the Default Setting section of the Device Explorer module with exception of Wireless NICs and PS/2 Ports, since they already form part of the standard device classes you find there.

You can also define permissions at the device class level (the nodes of the Default Settings tree shown in the Device Explorer module), computer level (the nodes of the Machine-Specific Settings tree shown in the Device Explorer module) and even at deeper levels (Computer Groups or Device Groups). The final permission that applies depends on the user and priority settings.

## Identifying specific, unique, removable devices

Administrators have the option to manage device permissions at different levels depending on the company's needs:

<b>Level</b>	<b>Permissions applies to</b>	<b>Example</b>
Base class	All devices classified in that class including groups, models, and specific devices	A temporary permission defined for the 'Removable Storage devices' class
Device Group: a group defined in the base class (only available for some classes) and used as an aid to rearrange your devices into logical clusters	All devices included in that precise group (see <i>Organizing devices into logical groups</i> on page 38 for an explanation)	A read permission created for a device group named 'Marketing USB keys' defined in the base class 'Removable Storage Devices'
Specific device model included in the class itself or in a group.	For all devices belonging to the same, exclusive, model	Offline permissions for a device model Sony Storage Media USB Device'
Precise, unique individual device identified by its serial number	Only to that specific device	Online permissions for a user device with a serial # 4ed552fd755cefd3f1db4be291e16aeaacb9d177
<p><i>✍ The Vendor ID (VID), Product ID (PID), and serial number are obtained from the standard Device Descriptor that every USB device must support.</i></p> <p><i>✍ Some cheap devices do not comply with the USB standards and do not have unique numbers. Others do not comply with the rules as all devices produced in a single batch have the same identical 'unique' serial number.</i></p>		

Table 12: Managing unique individual removable devices

The following image shows this four level structure:



Figure 18: The four level removable device class structure





As an example of the permission structure depicted in *Table 12* (page 37), consider the following example:

Removable Storage Devices	Everyone	23 MB		Copy Limit
	Everyone	Read/Write	Low	
	LU\Accounting Dept	5 MB		Copy Limit
Disk drive	Everyone	HDD: Read/Write	Low	
Marketing USB devices	LU\Marketing LU	Encrypted/Non-HDD: Read/Write	Low	
M-Sys Xkey USB Device	LU\Presales	USB: Read/Write	Low	
	830943fc66952377d70384c64...			
	LU\mary	FileName		Shadow Option
	LU\mary	Read	High	
Sony Storage Media USB Device	LU\Accounting Dept	W:Enabled		Shadow Option
Maxtor 6Y160M0				
Sales dept.	LU\Presales	Read/Write	Low	
	LU\Presales	W:Enabled, R:FileName		Shadow Option


Figure 19: The four level removable device class structure with permission examples

As you can see, at the last level of the 'Marketing USB Devices' hierarchy there is a unique serialized device. Defining permissions for a unique, serialized, USB key has the clear advantage of unmistakably denying/allowing a user or group the right to use this device.

To insert a device model follow these steps:

1. Attach the user device to a computer that has Sanctuary's client.
2. Activate the *Device Explorer* module by clicking on the  icon located on the *Modules* section of the *Control Panel* in the main window.
3. Use the *Explorer* → *Manage Devices* item from the menu.
4. Click on the ADD NEW button.
5. Type the name of the computer where the device is attached or search for it using the ellipsis  button.
6. Click the GET DEVICES button, select the device model from the list, and click on the ADD DEVICES button.

To insert a specific, unique, device or a device model follow these steps:

1. Activate the *Log Explorer* module by clicking on the  icon located on the *Modules* section of the *Control Panel* in the main window.
2. Search for the attached device in the list using the filters, templates, or by manually traversing the list. Once the register is located, right-click on it and select *Manage Devices* from the popup menu. You can also use the ADD DEVICES button located at the lower right corner of the *Log Explorer* window. See a detailed description in *Chapter 5: Using the Log Explorer* on page 99.
3. Follow steps 4 to 6 of the 1st method.

### Organizing devices into logical groups

Sometimes you want to organize your devices in logical units within a device class and assign them special permissions (rules, notifications, etc.). You can, for example:

1. Create a new Device Group in the DVD/CD Drives class on the Default Settings section of the Device Explorer module
2. Label this freshly created device group with the name of your preference
3. Add comments
4. Place here all your double-sided high-capacity DVD burners



5. Create an Offline permission rule and, finally,
6. Create an Online permission rule

This is not strictly necessary, but it helps visualize and organize your permission rule space more effectively.

Not all device classes accept this organization. Please refer to *Device Groups* on page 55 for more information.

## Identifying specific computers to be managed

Sometimes you require special rules for specific computers. In this case, you can add them directly on the Machine-Specific Settings section of the Device Explorer module. All computers that are added go directly to their Workgroup or Domain tree structure. From there, you can proceed to define all needed rules or organize them in computer groups like those shown in the following image:



Figure 20: Computers and computer groups


Here we add a new group in the 'Workgroup' section, rename it 'Marketing', add a comment (Special rules), and then proceed to add computers to this group and change the permissions rules (expanding the Group Settings tree and modifying the rules for each device class). Be aware that if they are conflicting rules in the Default Settings and in the Machine-Specific Settings sections, they apply depending on the priority selected. Please refer to *Priority options when defining permissions* on page 95 for further details.

## Defining different types or permissions

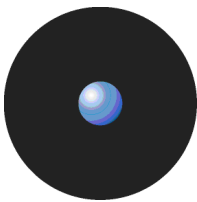
You are normally confronted with what kind of permissions you can define for a device class. Take for example the Floppy Disk Drives, Sanctuary Device Control offers the best of both worlds: total control and flexibility when the time comes to assign multiple permissions to access devices. For this specific example, you can add independent Read, Read/Write, Online, Offline, Schedule, Temporary, Copy Limit, and Shadow rules and permissions: define only one or a combination of them at the same time (depends on the device class as specified on *Table 13* found on page 40).

To furthermore extend our example, let's consider a user called Emily who works in the Sales Department and who has a Floppy Disk Drive on her company's laptop:

- > She has Read/Write permission for this device.
- > She can use the floppy only when connected to the network (online permissions).
- > She can only use the device from 8 AM to 5 PM, Monday to Friday (temporary permissions).
- > We want to know what she writes to the floppy. Not only do we need the name of the file, but also the content.
- > To limit her a bit, we only allow her to copy a maximum of 5 MB per day.

All this is done using the Device Explorer  module and defining the corresponding permission rules:

- > Permissions: read/write access.
- > Online Permissions: read/write access.
- > Offline Permissions: no access.



- > Schedule permissions: define the days (Monday to Friday) and timeframe (from 8 AM to 5 PM).
- > Shadow rule: Enable it in the Write Permissions panel.
- > Copy Limit rule: define 5 MB.

We can complicate or simplify as needed adding event notifications, encryption, file filtering, etc.

The following table summarizes the type of simultaneous permissions by Windows' standard device classes you can define in the Device Explorer module:


Name of the class	Section in the Device Explorer module*													
	Default Settings							Machine-Specific Settings						
	P	ON	OF	SC	TP	SH	CL	P	ON	OF	SC	TP	SH	CL
Biometric devices	✓	✓	✓	x	x	x	x	✓	✓	✓	x	x	x	x
COM/Serial ports	✓	✓	✓	✓	x	✓	x	✓	✓	✓	✓	✓	✓	x
DVD/CD drives	✓	✓	✓	✓	x	✓	x	✓	✓	✓	✓	✓	✓	x
Floppy disk drives	✓	✓	✓	✓	x	✓	x	✓	✓	✓	✓	✓	✓	✓
Imaging devices	✓	✓	✓	✓	x	x	x	✓	✓	✓	✓	✓	x	x
LPT/Parallel ports	✓	✓	✓	✓	x	✓	x	✓	✓	✓	✓	✓	✓	x
Modem/Secondary Network Access Devices	✓	✓	✓	✓	x	✓	x	✓	✓	✓	✓	✓	✓	x
Palm handheld devices	✓	✓	✓	✓	x	x	x	✓	✓	✓	✓	✓	x	x
Printers (USB/Bluetooth)	✓	✓	✓	✓	x	x	x	✓	✓	✓	✓	✓	x	x
PS/2 Ports	✓	✓	✓	x	x	x	x	✓	✓	✓	x	x	x	x
Removable storage devices	✓	✓	✓	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
RIM BlackBerry handhelds	✓	✓	✓	✓	x	x	x	✓	✓	✓	✓	✓	x	x
Smart Card Readers	✓	✓	✓	x	x	x	x	✓	✓	✓	x	x	x	x
Tape drives	✓	✓	✓	✓	x	x	x	✓	✓	✓	✓	✓	x	x
User defined devices	✓	✓	✓	✓	x	x	x	✓	✓	✓	✓	✓	x	x
Windows CE handheld devices	✓	✓	✓	✓	x	x	x	✓	✓	✓	✓	✓	x	x
Wireless NICs	✓	✓	✓	x	x	x	x	✓	✓	✓	x	x	x	x

\* Code used: P=Permissions; ON=Online permissions; OF=Offline Permissions; SC=Schedule; TP=Temporary Permissions; SH=Shadow; CL=Copy limit.  
Permissions can include one or several of the following: file filters, encryption, decryption, drive & bus type, export & import key file.

Table 13: Simultaneous permissions definitions for all Windows' standard device classes in the Device Explorer module

## Encrypting removable media & authorizing specific DVDs/CDs

If you deal with media containing sensible data that is moved around between computers or leaves the company premises, you should consider encrypting it. If the medium is lost or stolen, the intruder must defeat several layers of protection before having access to the actual data. The encryption process alters the data in such a way that it is not useful. Encryption makes data unreadable to those not having the correct password and deciphering information.

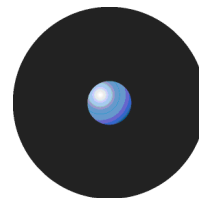
The first step in this process consists in activating the *Media Authorizer* module  and use the ADD REMOVABLE button to centrally encrypt a removable media.


Once the procedure is finished and the associated users defined - no groups allowed here - the access to the device is completely transparent for the user(s). Among the encryption options, you can find our 'Easy Exchange' method that formats and ciphers the media so that the user can use it in another computer without the need to install software and without being an administrator.

You can also authorize the use of specific media in your company. You can precisely determine which DVDs/CDs are allowed in your organization. For example, you can allow the use of a data warehouse DVD or authorize the use of music CDs to certain users or groups. Once the media is encrypted in the SecureWave Sanctuary Database, 'malicious' users that may want to add other kind of information to the CD or DVD – for example, by duplicating it and then including programs, images, music, or other kind of info – are left in the dark since the media does not correspond to what was initially encrypted and registered. The result is that the user can no longer access the DVD/CD.

## Forcing users to encrypt removable media

As an alternative to controlling centrally all removable media management, the administrator can opt for a distributed schema. In this scenario, users who plug removable media in their computers are forced to



encrypt them before they can be used. This is controlled by defining a simple permission for the 'Removable Storage Devices' class located in the Device Explorer module . An administrator can force the encryption of a hard disk, memory stick, or any other device recognized as removable storage (depending on their respective drivers: cameras, phones, etc.). See *Decentralized encryption* on page 163.



*Data recorded on a removable storage device before it is encrypted can be read following encryption.*

## Practical setup examples

We illustrate different common uses of Sanctuary Device Control in this section. For example we consider how to:

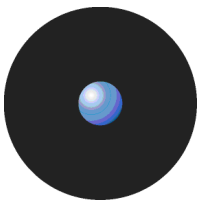
- > Control device use and installation.
- > Regain employer's lost productivity due to intensive use of games, MP3 players, video players, etc.
- > Enforce the compliance with internal security policies and those external regulations that the enterprise must face in its everyday work.

### DVD/CD burner permissions assignments

We illustrate the sheer power Sanctuary Device Control offers you, in simple every-day situations. In our first example, an employee — let us call him Bob — without the permission to use a DVD/CD writer assigned to him or the groups he belongs to, buys a new DVD USB burner and wants to share it with all his colleagues at work. Next day he arrives at the company and connects it directly to his computer. In a 'standard' situation, he can immediately begin burning DVDs with all kind of data, even your precious information. Fortunately enough, Sanctuary Device Control protects you and access is denied. He now has to ask the administrator for this permission. The administrator has several choices:

- > He can grant Bob access to the DVD by making him a member of an Active Directory Group that has received access to the device class (DVD/CD drives, in this case). To do this, he only changes the domain group membership using the Microsoft Management Console (MMC) —no modification to the Sanctuary permission rules is required.
- > If a computer group exists (a one-click operation to create using Sanctuary) and access to DVD/CD drives has been defined, the administrator can move Bob's computer into this group. His machine automatically receives the permissions that apply to the existing computer group.
- > Assign Bob the necessary permissions (temporarily, scheduled, or definitive ones).
- > Grant Bob Read & Write access on his new DVD burner.
- > Give permissions for using the device, except during working hours.
- > Allow access to the device only when the computer is offline (or online).
- > Decide that Bob can only use specific DVD/CD media.
- > Allow Bob to read but not to write data.
- > Give Read/Write permissions but store the contents (shadow) of the copied/read files to control what has been done.
- > The administrator can decide to do NOTHING. Bob has no right to use the DVD/CD burner and it should stay that way...

As you can see from this simple example, the possibilities are endless and flexible enough to adapt to each kind of imaginable situation.



## Removable permissions assignments

For our second example, we consider another real-life case:

Rather than grant permissions to all removable media in exactly the same way, you may want to allow access only to a specific company approved model. For example, if the corporate standard USB memory stick is a SanDisk 2GB, it is possible to define it in the Sanctuary Device Control and assign group or user permissions to that specific model. Access is denied to any other type of removable media connected. In this way, it is possible to build up a 'White List' of corporate-approved devices and deny everything else. Permissions for a newly defined device can be assigned without having to log off/log on.



*You can apply device class permissions and device type permissions at the same time.*

You can go a step further by managing unique user devices identified by their exclusive serial number. This way, your control boils down to a specific device.

## Assigning permissions to groups instead of users

When you begin to use Sanctuary Device Control, you are probably tempted to traverse the *Device Explorer* module assigning permissions to individual users for different classes and devices as you go. Although this is practical when the number of assigned permissions is kept small and while you get accustomed to the inner works of the program, this becomes quickly unmanageable as the deployment grows and you control more and more users and devices in your organization. You will have the double task of maintaining Windows' users and their possible Sanctuary Device Control assignments.

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

As soon as your groups are determined, you can then proceed to define permissions for them in Sanctuary Device Control. You get the distinguished advantage of controlling device access by assigning permissions directly to one or more specific Windows' groups. You can also use these same groups to do all kind of house keeping (Windows' public folder and mailboxes permissions for example).

By defining a small number of user groups in your domain, 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.

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

As a possible naming convention, you can use the following two examples:

- > Group's name based on the device classes, Ex. SDC\_Floppy\_Grp.
- > Group's name based on the 'Access-Profile', Ex. SDC\_Standard or SDC\_Laptop.

## Shadowing notes

The 'Shadowing' — a "carbon" copy of transferred data — of removable devices gives you a clear advantage when trying to decide who has to be controlled more closely. As you have a complete control of the copied (read) data or the file names, you can quickly decide corrective or preventive actions or limit access to certain groups or users.

Although this is a very powerful feature, it should be used with care. The hard disk drive assigned to contain the data file directory should be ample enough to receive all copied data. This can amount to several Mbytes, read Gbytes, very quickly not to mention the possible network saturation in case of using slow lines. A judicious compromise between receiving all data or just the file name should be made. As there is no rule or thumb here, there has to be a case-by-case analysis for each organization's needs.



- ✍ *Since secondary hard disk are consider as removable devices, you should consider shadowing repercussion — as described in the previous paragraph — when applying a general rule to the 'Removable Storage Devices' class.*
- ✍ *Even if you control shadow upload frequency, shadowed files are not sent to the SecureWave Application Server while the device is still connected unless explicitly demanded by a Sanctuary administrator. This is done so that the device is not un-mounted and mounted repeatedly by the client driver leading to sever operation disruption (while copying or reading data, a possible format or encryption process, etc.).*

You have to be careful with permissions priorities conflicts when defining shadowing rules. Write and read permissions follow this priority:

Permission	Priority order
Disable (highest)	↓
Enabled	
Filename (lowest)	

Table 14: Shadow permissions priorities

For example, let us say that you define shadow permission for the same user and the same device class, one at the **Default Setting** node stating a “Disabled Write permission” permission and another one for a specific machine at the **Machine-specific Settings** node defining an “Enabled Write permission” one. The prevailing one will be the higher — disabled — priority. Remember this simple conventions to avoid surprises when defining, otherwise conflicting, Shadowing rules.





## **Part II: Sanctuary Device Control modules and functions**




---

## Chapter 3: Using the Device Explorer

The main purpose of Sanctuary Device Control's Device Explorer module is to allow you to assign permissions to users and groups to use any kind of I/O devices available in your network. However, you can also use the Device Explorer to setup and maintain device types.

Using the Device Explorer module you can define the rules and permissions that determine which devices users and groups can use. Users (or groups of users) can gain access to I/O devices as long as they have the appropriate permissions to do so.

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

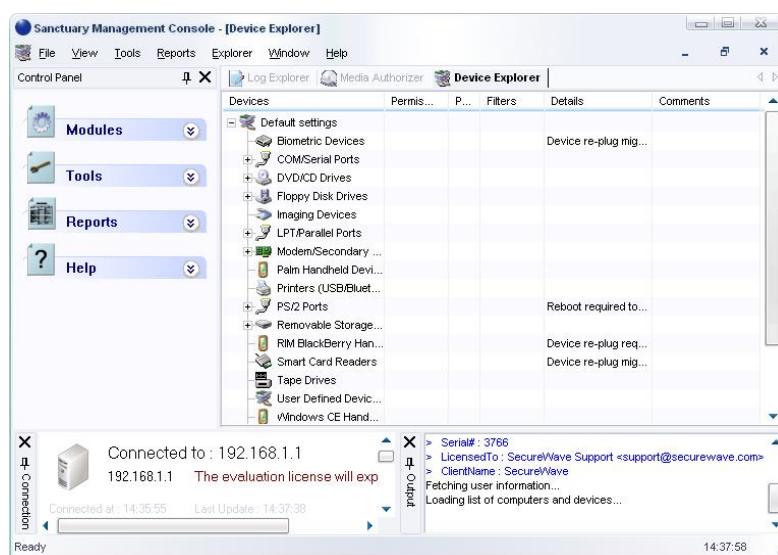


Figure 21: Device Explorer main window



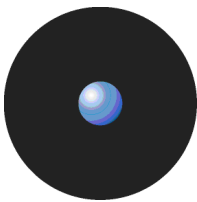
*When you make changes to a domain, such as adding groups, users or computers, you must use the 'Synchronize Domain Members' item on the 'Tools' menu (or from the Control Panel) to refresh the content of the database. If you want to synchronize Novell's objects, you should use our Synchronization Script instead of this command. See Sanctuary's Setup Guide for instructions on how to do this.*



*If the 'Settings (Device Control)' access of the Sanctuary Management Console Administrator User Access is set to 'No', the administrator has limited access. See Table 9 and Table 10 on pages 33 & 34.*



*In some cases you must use the 'Send Updates to All Computers' or 'Send Updates To' option on the 'Tools' menu (or from the Control Panel) or the right-click (context) menu of a specific computer to be sure all modifications are effective immediately.*



The Device Explorer module allows you to decide who can access to I/O devices on the network. For instance, you might want to do the following:

- > Grant read-only access to the DVD/CD-ROM to all members of the group 'Domain Users'.
- > Make a floppy disk drive read-only for everyone.
- > Explicitly deny access to a specific user. You simply need to select a user and leave the Read and Write checkboxes unchecked. This might be appropriate to permit a user access to the floppy drive in normal circumstances, but deny it on a specific machine containing sensitive data.
- > Grant read/write access to the DVD/CD-ROM for all members of group 'Marketing' from 9h00 to 17h00, Monday to Friday – after 17h00 access is denied. This is called 'scheduled permission'.
- > Add a temporary permission for a group/user to use a particular device.
- > Deny access to a device when a user is online but allow it when offline (or vice versa).
- > Copy (shadow) all data written, or read, to, or from, a device for a specific computer or user.
- > Limit the quota of data written to a device for a user or group.
- > Create an Event Notification rule that informs the user when someone is trying to gain access to an otherwise unauthorized device.
- > Force a user or user group to encrypt a decentralized removable storage device.

## How does the Device Explorer work

When you first install the software, all permissions have their default settings (see the following *Table 15*). The main task you carry out using Sanctuary Device Control is to assign the proper permissions to each user/group/computer as needed.

You can do this using the two available parts of the tree shown on the right panel of the Device Explorer module:

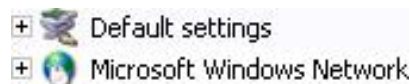
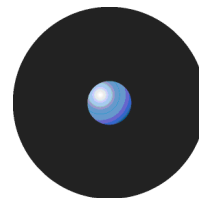


Figure 22: The Device Explorer module two main sections

- > **Default Settings** contains the permissions that apply to every machine. Here you can modify all authorizations used as general settings for the computers in your network. You must take into account that not all combinations of users/groups are valid for every device listed in this section. Please refer to the table located in the *Restricted and unrestricted devices* section on page 49 for a complete description of the different kinds of groups/users that you can add to a device. If one of your computers has a specific device not listed in this section, you can add it using the *Manage Devices* dialog as described in the *Managing devices* section on page 92.
- > **Machine-Specific Settings**, on the other hand, contains specific permissions granted to users/groups that apply to a specific computer or group of computers. These set of rules combine with those located in the *Default Settings* section — as defined in *Table 28*. Here you can also add a 'computer group' to reorganize some computers in a logical way that lets you to define special permissions for them. For instance, you can add a new computer group called 'Special scheduled access' that includes some computers that only have restricted access to their floppy disk drive during working hours (from 8:00 AM to 5:00 PM).



<b>Device</b>	<b>Permissions</b>	<b>Shadow</b>	<b>Copy limit</b>
COM/serial port		Disable	
DVD/CD drives		Disable	
Floppy disk drive		Disable	
LPT/Parallel port		Disable	
Modem/Secondary Network Access Devices		Disable	
PS/2 port (normally the keyboard and mouse)	Read/Write with Low priority		
Removable Storage Devices		Disable	No limit
Wireless Network Interface Cards	Read/Write with High priority		

Table 15: Default settings following installation (these apply to 'Everyone')



*Do not block the PS/2 port unless you only use USB keyboards.*



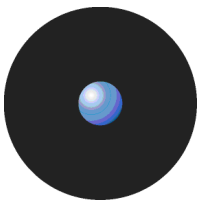
*If you are using a Wireless NIC as a unique network card in some clients and you change its permissions to 'None' (leaving the Read and Write checkboxes empty) for Everyone you will have no way to send updates to the block-out users — unless done by exporting permissions — and you must reinstall the client.*

## Restricted and unrestricted devices

By the nature of the drivers designed by Microsoft, or the manufacturer of each device known to Windows, there can be some restrictions when assigning permissions to those devices.

The following table shows the possible assignments, for each class of device:

<b>Device Class</b>	<b>Allowed Permissions</b>		<b>Applies to</b>	<b>Notes</b>
Biometric devices	Read-Write /None; Select bus type		Only to Local System or Everyone.	Device re-plug might be required to grant access for an already blocked device.
COM/Serial ports	Read-Write/None; Select bus type		Any user or group.	-
DVD/CD drives	Read only/ Read-Write/None; Select bus type		Any user or group.	-
Floppy disk drives	Read only/ Read-Write/None; Select bus type		Any user or group.	-
Imaging devices (such as scanners)	Read-Write /None; Select bus type		Any user or group.	-
LPT/Parallel ports	Read only/Read-Write/None; Select bus type		Any user or group	-
Modem/Secondary Network Access Devices	Regular modems	Read-Write/None; Select bus type	Any user or group.	-
	ISDN modems or network adapters	Read-Write/None; Select bus type	Only the Everyone group.	Device re-plug or reboot required to enforce updated permissions.
Palm handheld devices	Read-Write /None; Select bus type		Any user or group.	-
Printers (USB/Bluetooth)	Read-Write /None		Any user or group.	-
PS/2 Ports	Read-Write /None		Only to Local System or Everyone.	Reboot required to enforce updated permissions.



Device Class	Allowed Permissions	Applies to	Notes
Removable storage devices	Read only/ Read-Write/None	Any user or group.	-
	Encrypt, Decrypt, Export, Import; Select bus and drive type		
RIM BlackBerry handhelds	Read-Write /None	Any user or group.	-
Smart Card Readers	Read-Write/None; Select bus type	Only Local System or Everyone.	A device re-plug or machine restart might be required to grant access for an already blocked device.
Tape drives	Read-Write/None; Select bus type	Any user or group.	Some backup units do not use the Microsoft supplied drivers and cannot be controlled by Sanctuary Device Control.
User Defined Devices	Read-Write/None	Any user or group.	-
Windows CE handheld devices	Read-Write /None	Any user or group.	-
Wireless NICs	Read-Write /None	Only to the Everyone group.	-

Table 16: Possible assignments by device



*It is important to distinguish between the absence of permission and a negative permission ('None' — the most restrictive access).*

*In the latter case, when creating a permission for which neither the Read nor the Write flags are selected, you deny the user access to the device even if they are indirectly authorized to use the device. You specifically deny the access to a device for the user.*



*The File Filtering dialog is only available for the DVD/CD Drives, Floppy Disk Drives, and Removable Storage Devices classes.*

## Optimizing the way you use the Device Explorer

This section explains how to use your mouse and keyboard to full effect within the Device Explorer module.

### Context menu and drag & drop

You can assign permissions using the right-click context menu, saving you considerable time and effort:

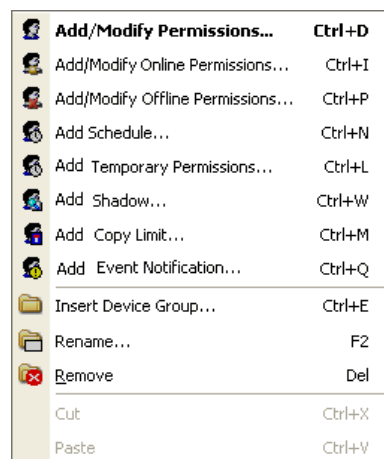


Figure 23: Contextual menu



## Keyboard shortcuts

A number of keyboard shortcuts are available in the Device Explorer module. The convention used in this guide to represent keyboard shortcuts in which you press two or more keys simultaneously, is a plus sign (+) between the key characters. The following table explains the available keyboard shortcuts:

<b>Shortcut</b>	<b>Used to...</b>
CRTL+D	Add/Modify permission for the selected item(s).
CRTL+P	Add/ Modify offline permission for the selected item(s).
CRTL+I	Add/ Modify online permission for the selected item(s).
CRTL+N	Add/ Modify a schedule for the selected item(s).
CRTL+L	Add/ Modify a temporary permission for the selected item(s).
CRTL+W	Add/ Modify shadow settings.
CRTL+M	Define the copy limit for the selected item(s).
CRTL+E	Insert a device group.
F2	Rename a computer group/device.
DELETE	Delete an entry (see note below).
CRTL+A	Insert a computer.
CTRL+C	Copy and cut a computer(s) from a computer group to place in another one (same as CTRL+X).
CTRL+V	Paste a computer(s) previously cut or copied from a computer group to place in the selected one.
CTRL+X	Cut and copy a computer(s) from a computer group to place in another one.
CTRL+Q	Add/ Modify event notifications.
F5	Refresh screen information.

Table 17: Keyboard shortcuts in the Device Explorer module



*Using Delete for a computer entry in a computer group, erases all permissions, shadows, copy limits, etc. for this machine. This computer is not visible but still exists in this computer group; you can use the right-click menu to display it again. See Show All Members on page 52 for more information.*

## Adding comments to an entry

When you have dozens or hundreds of entries on your Device Explorer list, it is handy to add a comment either to remind yourself why you made an entry, or as a useful note for other Sanctuary administrators. You can add comments to every entry. For example, you can add a permission rule and then modify its comment typing 'Special rule for the CEO. Please do not remove'.

To modify or add a comment to an item, click once to select the line and then once more on the *Comments* column to edit it. You can also click on the *Comments* column and press the F2 key. Type a brief explanatory notice and finish by pressing ENTER.

## Computer groups

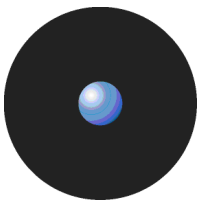
Computer groups are 'virtual' groupings, formed by several computers not having any relation with those in the Active Directory structure. These 'virtual computer groups' help you organize your permissions in a more logical way - reorganizing several machines that should share permissions to specific devices.

A good permission policy is to FIRST define as many 'Default Settings' as possible to apply to all computers and then define 'Computer groups' for the exceptions. You can then proceed to set permissions to specific machines.

Computer groups are defined to make the same exceptions for a series of machines.



*It is a good idea to add comments to the permission modifications you make. It helps you remember why each modification was made as your permission structure grows in complexity.*



## Renaming Computer Groups/Device Groups/Devices

Computer Groups, Device Groups, and devices in a device class (those belonging to the Default Settings tree in the Device Explorer module) can be renamed. While renaming a Computer Group, Device Groups, or Device, you should be aware that internal names are not case sensitive: 'My Device Name' is the same as 'MY device NAME'. This can cause errors when trying to change lower to uppercase letters in descriptions.

### Show All Members

Sometimes you find that there are 'hidden' computers in a computer group inside the *Machine-Specific Settings* section of the *Device Explorer* module. This happens mainly when inserting computers but not assigning them rights. These computers are hidden to avoid crowding the computer group with data that is not meaningful. When you delete a group with 'invisible' computers, they are all moved back to their domain along with those that have permissions rules and are shown. If you need to change permissions to such type of computer(s), move them to other computer groups, or just plainly display them, use the *Show all members* item from the right-click computer group popup menu.

If the *Show all members* item on the popup menu is grayed-out, this means that you do not have this kind of 'invisible' computers in that computer group.

To delete or change permissions for a computer that is 'hidden' in the computer group:

1. Right-click on the computer group where you have this situation.
2. Select the *Show All Members* item from the popup menu. This displays the 'hidden' computer(s).

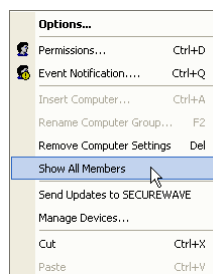


Figure 24: Show all members

3. Click on the computer on which you want to erase its permissions to select it and then press the DELETE key. You can also select the computer and then use the *Remove* item of the *Explorer* menu.

— or —

Right-click on the computer's name or on the device classes and change its permissions.

## Event notification

If you want your users/user groups to be informed when trying to gain access to an otherwise unauthorized device, you should create an *Event notification* rule. This rule can be created at one of the following levels:

- > Root level — when selecting the *Default Setting* node. The notification applies to all devices for the user(s)/user group(s) defined.
- > Device class root level — when selecting any of the sub-nodes of the *Default Settings* root node, for example, the *DVD/CD Drives* class. The event notification applies only for the devices belonging to that particular class.
- > Device level — when selecting a specific device within a device class, for example, a XXXX 48x DVD drive contained in the *DVD/CD Drives* class. The event notification applies only in the case of the specific device use.
- > Device Group level — when selecting a group created within a device class, for example, the Marketing DVD Rewritable previously created in the *DVD/CD Drives* class.






- > Computer level — for a specific computer in the Machine-Specific Settings node and following the guidelines establish in all previous points (at the computer's root level, computer's device class, computer's device within a device class, computer's Device Group within a device class).

*If you set an event notifications for the Everyone group, your users may receive constant messages when some programs try to access their removable devices — for example antivirus applications trying to scan these kind of devices. Setting it for specific users/groups instead resolves this issue.*

*When event notifications using the same priority are defined at the root-level and the computer-specific level, only one of the rules is taken into account. The priority of event notification rules are not handled based on machine vs. global settings, they are ordered purely based on their priority.*

### To create an Event Notification

To add an event notification for a specific user, follow these steps:

1. Activate the Device Explorer module by clicking on the  icon in the Modules option of the Control Panel.
2. Click on the device class where you want to create the rule and then use the CTRL+Q shortcut key or right-click and select the *Event Notification* item from the context menu.
3. Click on the Add button on the following dialog and choose the users/groups for which you want to create the rule by typing the name or clicking on the SEARCH or BROWSE button. Click OK when you finish.

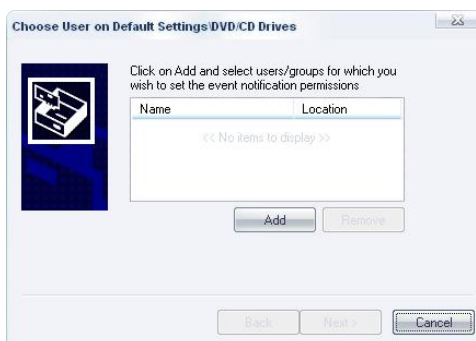


Figure 25: Event notification: selecting the users/groups

4. Choose between not notifying (default behavior) or the *Notify* option. Select the *Priority* and type a message (optional). Click on NEXT.

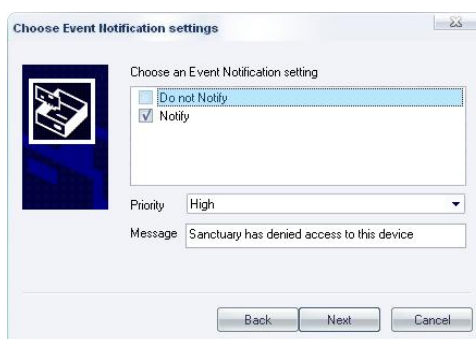


Figure 26: Event notification: options

5. Click on Finish to close the dialog and accept the rule.

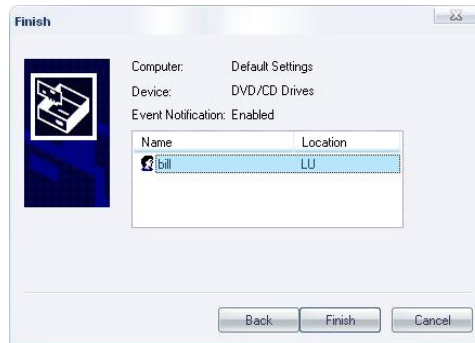


Figure 27: Event notification: finish the rule definition

You now can see a new event notification defined for the device class. The following image shows an example for the DVD/CD Drives class for user Bill:

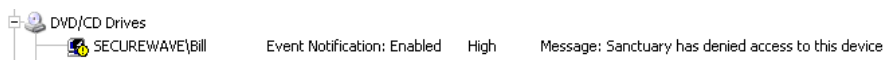


Figure 28: Event notification: new permission rule as shown for the device class



*Event notifications can also be created/modified/deleted at root level — by right-clicking directly on the 'Default Settings' icon. You can assign, this way, a notification for all illegal access to devices.*

### To delete an Event Notification

If you want to remove the Event Notification rule defined for a device class and assigned to a user(s)/group(s), you can either:

- > Click on the permission and then press the DEL key.
- or —
- > Right-click on the permission and then select the *Remove Event Notification* item from the context menu.

### To modify an Event Notification

If you want to change the Event Notification rule defined for a device class and assigned to a user(s)/group(s), you can either:

- > Click on the permission and then press the Ctrl+Q shortcut key.
- or —
- > Right-click on the permission and then select the *Modify Event Notification* item from the context menu.

Change the setting, priority, and message as needed. Click on the NEXT button and then on FINISH.

### Some practical examples

You can use the event notification rule to your advantage by carefully planning some rules. For example, let us say that you establish an event notification rule at the root level informing the members of the group 'Marketing' with a general message 'You do not have permission to use this device. If you need help, please dial extension 300' with a 'Medium' priority. Furthermore, you established a copy limit rule for these same users that you have wisely clustered in two distinctive device groups called 'Removable with copy limit rule. German section' and 'Removable with copy limit rule. English section'. You can now proceed to add two new event notification messages (one in German and the other one in English) with 'High' priority informing those users: 'If you think you need to extend your quota limit, please dial extension 200'. You also assigned a temporary permission for user 'Bill' for a specific device in the *Removable Storage Devices* class of his computer, defined in the *Machine-Specific Settings*, and you decide to improve a little more the communication defining also an event rule specifying 'To obtain new temporary permissions, dial 310'.



The exercise can be as complicated or as simple as you wish or decide — No message at all, a single simple message, or a complicated set of rules defining every possible deny access scenario imaginable.

## Device Groups

Device groups are used to organize your devices into logical units with special permissions. You can, for example, create a new device group for the Imaging Devices class and then place in this new group all your HP scanners. Furthermore, you can then add special permission rules for particular device group.



*Permissions cannot be applied to an empty device group. You must first add a device to it.*

### To add a device group

To add device groups to any device class inside the Default Settings section of the Device Explorer module do one of the following actions:

- > Select any device, at its upper level or class, and use the shortcut key Ctrl+E.
- > Right-click on any device, at its upper level or class, and select Insert Device Group from the popup menu.
- > Select any device, at its upper level or class, and use Insert Device Group from the Explorer menu.

You can only group the following device classes (upper levels of a device):

DVD/CD devices	Floppy disk drives
Imaging devices	Modem/Secondary network access devices
Palm handheld devices	Printers (USB/Bluetooth)
Removable storage devices	RIM BlackBerry handhelds
Smart card readers	Tape drives
User defined devices	Windows CE handheld devices

Table 18: Device classes that can have Device Groups

You can add any device of the same class to this newly created class group. You can move devices among different groups by using the Shift or Ctrl keys and then the Drag & Drop functionality. You can also use the shortcut key commands: Cut (Ctrl+X), Copy (Ctrl+C), and Paste (Ctrl+V) for the same purpose. These commands are also available from the right-click context menu:



Figure 29: Using Drag & Drop to move devices to a newly created group

Remember that you can further extend this classification by adding device models and, in the case of removable storage devices, unique, serialized, devices.



## Supported devices types

The Device Explorer module can be used to control access to a variety of I/O devices. Setting access at the *Default settings* level class, allows the user to access that device class on *any computer* in the network. Information about the device types supported is given in *Device types supported* on page 16.



*If you notice an unexpectedly blocked device, you might want to try to give it LocalSystem access. Some devices are not accessed directly but through a service running under the Local System account, the Sanctuary Device Control might block this access. This is, for example, the case for some printer models connected through the LPT or COM ports.*

## Managing permissions

The main purpose of the Device Explorer module is to manage permissions and rules for every conceivable device and then associate them with user(s)/user group(s). A second use is to define decentralized encryption in organizations that do not need/want a centralized control of this aspect of our solution. Since Sanctuary Device Control offers a great range of options in this respect, we reserved a complete chapter describing in detail the process.

Please refer to the next chapter for a complete description on how to administrate permissions/rules using the Device Explorer module.

Remember, when there is no permission/rule defined, the default applies: no access at all.

---

## Chapter 4: Managing permissions/rules

This chapter explains the different types of permissions/rules that can be administered using the Device Explorer module. Please refer to *Chapter 3: Using the Device Explorer* on page 47 for a detailed description on how to use the Device Explorer module.

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

As explained in the previous chapter, the Device Explorer lets you administer the rules and permissions that determine which devices your users and user groups can use or and which they cannot use.

Users (or groups of users) can only gain access to I/O devices if they have the appropriate permissions to do so. To define permissions, you first select the appropriate section of the Device Explorer tree, either *Default Settings* or *Machine-Specific Settings*, choose the desired device class and proceed to the Explorer menu or right-click on the item. From here you can select all type of permissions and rules to assign to a device and associated user(s)/user group(s). If you double-click on the device class (the higher level of the tree nodes), the Permissions dialog opens from where you can define Read, Read/Write, or None rights — and set decentralized encryption and filters on some classes.



*You should not use permissions other than Read and Read/Write when working on a system that uses older versions of the Sanctuary Client Driver. The client cannot interpret these types of permissions, resulting in 'no permissions applied'.*

### Using the Permissions dialog

When defining all type of permissions the following dialog is displayed as the first screen (except for *Shadow* where a subset is used as depicted in *Figure 31*):

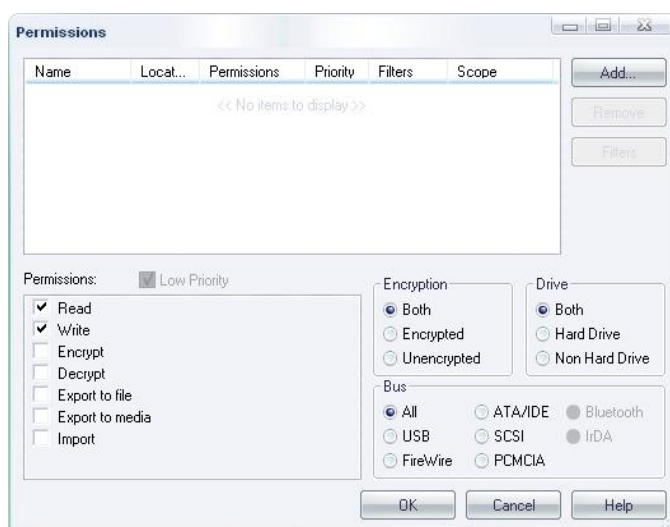


Figure 30: Main permissions dialog



Figure 31: Bus dialog used for Shadow

Choose between Read Only, Read/Write, Encrypt, Decrypt, Export to file, Export to media, Import, and/or None (not selecting any option). The Encrypt, Decrypt, Export to file, Export to media, and Import options as well as the Encryption and Drive panels are only available for the Removable Storage Devices class. (They are fully explained in the corresponding sections of this chapter.)

Once you have selected the user(s)/group(s) — using the Add button (see *Adding a user or group when defining a permission* on page 66) — you can reselect all, or some, of them to define Permissions, Encryption, Drive, and Bus type (if applicable) individually or globally.

You can add as many permissions to user(s)/user group(s) as you want without closing the dialog. To do this, just keep clicking on the ADD button.

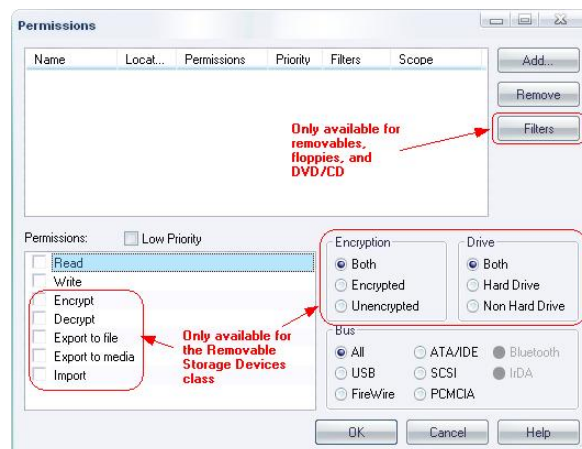


Figure 32: General Permissions dialog exceptions

The options that are available to you in this dialog depend on the device class that you are defining permissions for.

The Bus panel displays the available interface standards for the class you are working with. For example, if working with the Tape Drives class, you can choose among SCSI, USB, FireWire, ATA/IDE, and All (meaning, in this case, SCSI, USB, FireWire, and ATA/IDE bus, and any other from which the tape drive works).

The User/Group panel, at the top of the Permissions dialog, contains the following fields:

- > *Name* — shows the user/group name.
- > *Location* — indicates the user domain or workgroup (if available). This is the same field that is shown in the *Select User* dialog (opened with the Add button).
- > *Permissions* — reflects the options selected on the *Permissions* panel (lower left side of the dialog).
- > *Priority* — shows if the permission is applied with a high or low priority (depending whether the *Low Priority* option is selected). See the description of priorities and how do they apply in *Priority of default permissions* on page 69.



- > *Filters* — shows which types of files the user can access.
- > *Scope* — changes to reflect the extent of this permission definition. It is adjusted when you modify the options located on the *Encryption*, *Bus*, or *Drive* panel.



You can add permissions to multiple users/groups without closing the dialog. To do this, click on *ADD* to select the required user(s)/group(s), click on *OK* to close the user selection dialog, and then select the desired options from the permission dialog and file filters (if available).

### Special case: Working with Removable Storage Devices

If you are defining permissions or a 'Shadow' rule for removable storage devices, you can choose to apply the permission(s) to encrypt and/or decrypt devices. To further limit permissions, you can also choose the required scope options from the *Encryption* and *Drive* panels.



Some USB memory sticks are recognized as external hard disk drives. This may lead to confusion and undesirable behavior if you select 'All' in the *Bus* panel and/or 'Both' in the *Drive* panel sections while defining permissions or a 'Shadow' rule. You may accidentally specify that 'real' secondary hard disk drive(s) may be blocked/allowed/shadowed or forced to be encrypted/decrypted.

You can use the following settings when working with the removable storage devices:

Parameter	Description
None (neither read nor write)	The user/group is specifically denied access to the device
Read	The user/group can do read operations
Read/Write	The user/group can read and/or write to/from the removable media
Encrypt	The user/group is allowed to encrypt the device, This option is related with the Export and Import settings
Decrypt	The user/group can decrypt a device
Export to file	The public key that was used to encrypt the device can be exported to a file — that can then be transmitted by a secure channel. You must first choose the Encrypt setting.
Export to media	The public key that was used to encrypt the device can be exported to the medium itself — if doing this, the device can be decrypted directly without the need of providing an external key. You must first choose the Encrypt setting.
Import	The user/group can import data from an external encrypted key. You must first choose the Encrypt setting.

Table 19: Allowed settings when working with the Removable Storage Devices class

### Examples

1. The user/group has read only rights for encrypted and decrypted USB memory key devices with a high priority.

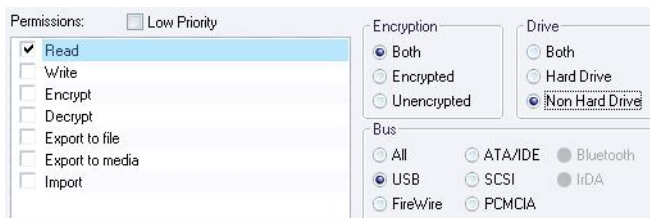


Figure 33: Removable permissions settings example 1



- 2. Read/Write permissions for encrypted SCSI hard disks with a low priority.

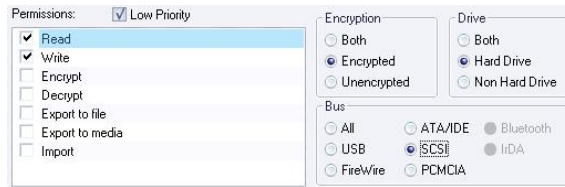


Figure 34: Removable permissions settings example 2

- 3. User has Read/Write permissions for all encrypted removable devices in all kind of buses with high priority. The user can also locally encrypt and export the key to the encrypted device or a file. In this case we force the user to encrypt all his removable devices but he cannot read (nor write) them unless they are already encrypted.

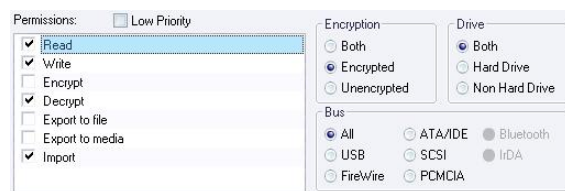


Figure 35: Removable permissions settings example 3 – Encrypted

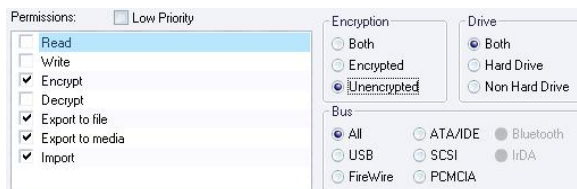


Figure 36: Removable permissions settings example 3 - Unencrypted

- 4. The user can format (Decrypt) his USB memory key, have Read/Write permissions only for encrypted devices connected to the USB port (Bus) and can export and/or import the device's encryption key, all this with high priority.

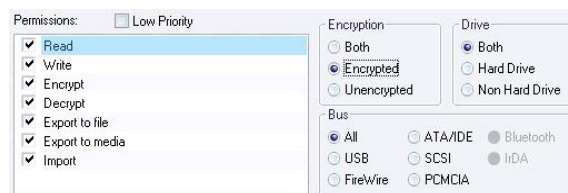


Figure 37: Removable permissions settings example 4

See *Decentralized encryption* on page 163 to define permissions that force the user to encrypt Removable Storage Devices.

## Using file filters

The Permission dialog includes a FILTER button. This is used to limit access to certain file types depending on the nature of the permission defined (see Table 22). Filters are ONLY available for the *Removable Storage Devices*, *Floppy Disk Drives*, and *DVD/CD Drives* classes.

To define a filter, select it from the list in the *File Type Filtering* dialog that opens when you click on the FILTERS button. To delete a filter, deselect the desired row.

Once a filter is set, click on the OK button in the Permissions dialog to accept (or on CANCEL to close the dialog without selecting the filter). The filter details are shown in the corresponding field of the permission dialog. Once filter permissions have been defined, their details are also visible in the *Filters* column of the *Device Explorer* module window.













When using permissions that include File Filters you can use the following file type filtering:

<b>File type filtering</b>	<b>Result</b>				
Not defined when creating the permission	The type of file is not taken into account to enforce permissions settings as defined in the dialog.				
Defined when creating the permission	<input type="checkbox"/> Read <input type="checkbox"/> Write	'None' (neither Read nor Write)	File filter is enforced in a 'deny' state	<input checked="" type="checkbox"/> Import <input type="checkbox"/> Export	Deny file copy from floppy disks, removable storage devices, and CDs/DVDs to the local HDD
				<input type="checkbox"/> Import <input checked="" type="checkbox"/> Export	Deny file copy from the local HDD to floppy disks, removable storage devices, and CDs/DVDs
				<input type="checkbox"/> Import <input type="checkbox"/> Export	Filters are not enforced. The end result is like not defining filters at all.
	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write	Read only	File filter is enforced in a 'grant' state and controlled ONLY by the Import/Export settings — plus the state of the file types selected in the list. The Read/Write part of the permissions only controls directory access (Read = directories & files can be listed, Write = directories can be created, deleted and renamed).	<input checked="" type="checkbox"/> Import <input type="checkbox"/> Export	Allow file copy from floppy disks, removable storage devices, and CDs/DVDs to the local HDD
				<input type="checkbox"/> Import <input checked="" type="checkbox"/> Export	Allow file copy from the local HDD to floppy disks, removable storage devices, and CDs/DVDs
	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	Read /Write		<input type="checkbox"/> Import <input type="checkbox"/> Export	Filters are not enforced. The end result is like not defining filters at all.
The 'All File Types (Import/Export)' and 'Only files selected from this list' parameters control if the permissions are applied solely to all types of files (even those not included in the list) or to those files selected in the list panel.					

Table 20: File type filtering options

See *File Filtering examples* on page 64 for a complete set of examples showing how to use file filtering

-  You cannot copy image files bigger than 4GB, unless they are Portable Network Graphic files (.PNGs) or Tagged Image File Format files (.TIFFs) for which there is no limit on the size of the file you can copy.
-  You can define different file filters for read, write, or read/write permissions.
-  The Filters button is disabled when you select more than one user/group in the permissions dialog. Nevertheless, you can define different file filters for each user/group individually.
-  Users cannot copy files directly from a FTP disk to an external device — or vice versa — if file content filtering is active. Users should first copy the files to the hard disk drive.
-  Permissions without file filtering always have priority over those where file filtering is defined.
-  The 'File Type Filtering' dialog contains the two options: 'All Known Files' and 'All File Types'. These control whether the filters apply solely to the files selected in the list panel or to all types of files (even those not included in the list).
-  File filtering is useless when using burning software to copy files to a CD/DVD.
-  File Type Filtering rules cannot be combined with Encrypt, Decrypt and Bus-specific permissions inside the same rule. ONE permission cannot have both file type filtering defined and Encrypt / Decrypt / Bus-specific options selected, but SEPARATE permissions can, and will be enforced properly.

If no filter is defined or the Import/Export options of the filter dialog are not activated — even if some files are selected — the profiled permission applies to all type of files.

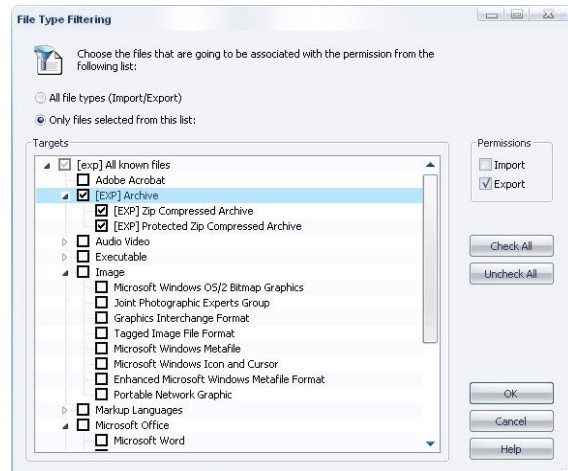


Figure 38: Defining a file filter

File filters can be used to limit access to various types of files listed in the following table:

<b>'Families' of file type</b>	<b>File types</b>		
<b>Microsoft Office</b>	Microsoft Word		
	Microsoft Excel		
	Microsoft Visio		
	Microsoft PowerPoint	Microsoft PowerPoint Slideshow	Microsoft PowerPoint Presentation
		Microsoft PowerPoint Template	Microsoft PowerPoint Add-in
		Microsoft Graph	
		Microsoft Project	
Microsoft Access			
<b>Microsoft Office 2007</b>	Microsoft Office Open XML Word		
	Microsoft Office Open XML Excel		
	Microsoft Office Open XML PowerPoint		
<b>Open Office</b>	OpenOffice.org Writer	OpenOffice Text Document	
		OpenOffice Text Template	
	OpenOffice.org Math	OpenOffice Formula	
		OpenOffice Formula Template	
	OpenOffice.org Base		
	OpenOffice.org Calc	OpenOffice Spreadsheet	
		OpenOffice Spreadsheet Template	
OpenOffice.org Draw	OpenOffice Graphics		
	OpenOffice Graphics Template		
OpenOffice.org Impress	OpenOffice Presentation		
	OpenOffice Presentation Template		
<b>Adobe Acrobat</b>	<b>Archive</b>		
<b>Executable</b>	Application		
	Dynamic Link Library		
<b>Image</b>	Microsoft Windows OS/2 Bitmap Graphics		
	Joint Photographic Experts Group		
	Graphics Interchange Format		
	Tagged Image File Format		
	Microsoft Windows Metafile		
	Microsoft Windows Icon		
	Microsoft Windows Cursor		
	Enhanced Microsoft Windows Metafile Format		
	Portable Network Graphic		
	Corel vector Graphic Drawing		
<b>Audio Video</b>	Moving Picture and Associated Audio Video	Moving Picture Experts Group	
		MPEG Audio Stream Layer II	
		MPEG Audio Stream Layer III	
	Resource Interchange File Format	Windows Animated Cursor	
		Audio Video Interleave	
		Downloadable Sounds	
		Musical Instrument Digital Interface	
		DirectMusic Style	
		WAVEform audio format	



	Advanced Streaming Format
	Standard MIDI File
	RealNetworks Content
	RealMedia Streaming Media
	RealAudio Streaming Media
<b>Markup languages</b>	
<b>Rich Text Format</b>	
<b>Microsoft Windows Setup</b>	Microsoft Windows Installer File
	Microsoft Windows Installer Patch
	Microsoft Windows SDK Setup Transform Script

Table 21: File types for filtering

File filters work in combination with the permission type that you have set up:

<b>Permission type</b>	<b>Example</b>
Device access set to 'None'	If you select Microsoft Word in the File Type Filtering dialog then access is denied for all .doc files.
Device access set to 'Read'	If you select MPEG Audio Stream Layer III in the File Type Filtering dialog then read access is allowed for .mp3 files.
Device access set to 'Read/Write'	If you select Microsoft Word in the File Type Filtering dialog then read/write access is allowed for .doc files.

Table 22: File filter settings and permission relation

Once a filter has been assigned, you can modify it by editing the related permission. To do this, click on the FILTERS button, and change the required file type(s). Alternatively, you can choose one of the following settings from the Permissions panel:

- > *Export* — allows copying from the system hard disk drive to an external device.
- > *Import* — allows copying from an external device to the system hard disk drive.



*Currently Sanctuary does not support file filtering for the new format \*.wim introduced with Windows Vista.*



*When defining File filters, you cannot open files directly from the external device. You must first copy them to your system (or another authorized hard disk drive).*

## To remove File Filtering settings from a permission

Occasionally situations arise where you want to delete all file filtering conditions from a permission rule but keep all its other settings (bus, encryption, and drive type, etc.).

Obviously, you can do this by deleting the permission and recreating it without using File Filtering, however this solution is unacceptable for all but the simplest cases. For more complicated permissions, use the following procedure:

1. Open the Permissions dialog. To do this, double-click the permission rule in the Device Explorer module, right-clicking the *Removable Storage Device*, *Floppy Disk Drives*, or *DVD/CD Drives* class, or use the Ctrl+D shortcut.
2. Select the desired register by clicking on it or by navigating through the registers using your keyboard Up or Down arrow keys.
3. Click on the FILTERS button.
4. If the permission is defined using the *All file types (Import/Export)* option, deselect the *Import* and *Export* checkboxes. If the permission is valid for a specific file type(s) (*Only files selected from this list*), click on the UNCHECK ALL button.
5. Close the *File Type Filtering* dialog by clicking CLOSE.



## File Filtering examples

In this section, we consider several common cases where you can use File Filtering to block or allow user file access by file type.

### > Allow 'Marketing' users to access all kind of files with the exception of MP3.

To grant 'Marketing' users access all kind of files with the exception of MP3, we first need to define the following rules:

- > Domain users have 'Read/Write' access to removable devices. (This is a File Filtering rule with *All File Types* and *Import/Export* activated.)
- > The 'Marketing' user group has a 'None' permission for the Removable Storage Devices class with a File Filter defined for file type MPEG Audio Stream Layer III. Activate the Import/Export settings.

These two rules mean that:

- > 'Marketing' users can copy everything they want to removable devices except MP3 files since there is a 'negative' permission defined from them (despite the 'positive' permission due to the first rule).
- > All other users (not belonging to 'Marketing') can copy whatever they want to removable devices with no limitation whatsoever. There is no 'negative' rule limiting their behavior.

### > Allow 'Sales' users to copy PDF files to removable media.

To let 'Sales' users to copy PDF files to removable media simply define a 'Read/Write' permission and, using the File Type Filter dialog, define *Export* permissions for files with a file type 'Adobe Acrobat' for the user group 'Sales' in the 'Removable Storage Devices' class. Users belonging to this group can now write and export (copy) PDF files. If no other permission is defined, this is the only type of files that 'Sales' can copy.

### > Allow 'Marketing' users to copy PDF files to removable media and read Microsoft Word and Excel documents.

To let 'Marketing' users copy PDF files to removable media and read Microsoft Word and Excel documents define a 'Read/Write' permission and, using the File Filter dialog, define *Export* permissions for files with a file type 'Adobe Acrobat' and *Import* permissions for Microsoft Word and Microsoft Excel files

Users in the user group 'Marketing' can now copy PDF files to their external devices (but not the other way around) and copy Microsoft Word and Microsoft Excel files to their system hard disk drive (from their external devices). The files can be opened once they reside in the hard disk drive.

### > Allow all users to copy in/out of the company any Microsoft Office documents, PDF files, and images but not MP3 files.

To do this, define a 'Read/Write' permission for domain users to the Removable Storage Devices class with a File Filter set for Microsoft Office, Adobe Acrobat, and Image files. Select the Import and Export checkboxes from the Permissions panel in the File Type Filtering dialog. Since MP3 files are not included in the File Filter, they are NOT accessible.

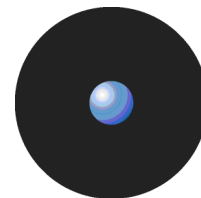
In all cases:



*You cannot define several different permissions relating to the same device class for a single user or user group. For example, 'Marketing' cannot have a 'Read/Write' permission for the Removable Storage Devices (no file filtering) and a 'None' with an import file filter for MP3 files for this same device class. In this case, you MUST use two different groups and include users in one or another.*



*If you define a file filter authorization, all files not in the list are denied. If you deny access to a specific type of file (using the File Filter dialog), all other file types are NOT be denied by this rule. They can be denied by default or by defining another rule.*



The following table contains further examples to clarify file filtering. (In these, users Jack and Jill both belong to the user group 'Marketing' and all permissions are defined for the removable storage devices class.):

Example	Permission type	User/Group	File filter	Import/Export	Resulting permission for the user
1	Read	Jack	<input checked="" type="checkbox"/> Only files selected from this list Microsoft Word selected	<input checked="" type="checkbox"/> Import <input type="checkbox"/> Export	Jack can copy Word documents to his local hard disk drive. All other file types are blocked. All other users cannot read nor write from removable devices.
2	Read	Everyone	<input checked="" type="checkbox"/> All file types	<input checked="" type="checkbox"/> Import <input type="checkbox"/> Export	Jill can copy PDF files to her local hard disk drive. All other members of Marketing can read or write from removable devices. Everyone else can only read from removable devices.
	Read/Write	Marketing	<input checked="" type="checkbox"/> All file types	<input checked="" type="checkbox"/> Import <input checked="" type="checkbox"/> Export	
	None	No_Access*	<input checked="" type="checkbox"/> All file types	<input checked="" type="checkbox"/> Import <input checked="" type="checkbox"/> Export	
	Read	Jill	<input checked="" type="checkbox"/> Only files selected from this list Adobe Acrobat selected	<input checked="" type="checkbox"/> Import <input type="checkbox"/> Export	
3	Read/Write	Marketing	<input checked="" type="checkbox"/> All File types	<input checked="" type="checkbox"/> Import <input checked="" type="checkbox"/> Export	Jack cannot copy Word documents to his local hard disk drive, all other users belonging to the user group Marketing can read or write from removable devices.
	None	Jack	<input checked="" type="checkbox"/> Only files selected from this list Microsoft Word selected	<input checked="" type="checkbox"/> Import <input type="checkbox"/> Export	
4	Read/Write	Marketing	<input checked="" type="checkbox"/> Only files selected from this list Microsoft Word selected	<input checked="" type="checkbox"/> Import <input type="checkbox"/> Export	Jill can copy PDF files from/to her local hard disk to removable devices. All other users of the user group Marketing can only copy DOC files to their local hard disk drive.
	Read/Write	Jill	<input checked="" type="checkbox"/> Only files selected from this list Adobe Acrobat selected	<input checked="" type="checkbox"/> Import <input checked="" type="checkbox"/> Export	
5	Read/Write	Jack	Not defined	n/a	Jack can read or write from removable devices without limitation.
6	Read/Write	Marketing	Not defined	n/a	Jack is blocked from reading or writing to removable devices. On the other hand, all other users belonging to the user group Marketing can read or write to removable devices with no limitation at all.
	None	Jack	Not defined	n/a	
7	Read/Write	Marketing	<input checked="" type="checkbox"/> Only files selected from this list Microsoft Word selected	<input checked="" type="checkbox"/> Import <input type="checkbox"/> Export	Jack and Jill — and all other users in the user group Marketing — can only copy Word documents from removable devices to their local hard disk drive.
8	Read	Marketing	Not defined	n/a	Jack and Jill — and all other users in the user group Marketing — can only read data from removable devices.
9	None	Jack	<input checked="" type="checkbox"/> Only files selected from this list Microsoft Word selected	<input checked="" type="checkbox"/> Import <input checked="" type="checkbox"/> Export	Jack cannot copy Word documents to/from removable devices but can copy all other type of files from removable devices.
	Read/Write	Access*	<input checked="" type="checkbox"/> All file types	<input checked="" type="checkbox"/> Import <input type="checkbox"/> Export	
10	None	Jack	<input checked="" type="checkbox"/> Only files selected from this list MPEG Audio Stream Layer III selected	<input checked="" type="checkbox"/> Import <input checked="" type="checkbox"/> Export	Jack cannot copy to/from removable devices mp3 files but, on the other hand, can copy to/from his removable devices all other kind of files (even those not in the file filter list).
	Read/Write	Access*	<input checked="" type="checkbox"/> All file types	<input checked="" type="checkbox"/> Import <input checked="" type="checkbox"/> Export	
11	Read/Write	Marketing	<input checked="" type="checkbox"/> All file types	<input type="checkbox"/> Import <input checked="" type="checkbox"/> Export	Jack and Jill — and all other users belonging to the user group Marketing — can only copy data to removable devices.
12	Read	Marketing	<input checked="" type="checkbox"/> All file types	<input checked="" type="checkbox"/> Import <input type="checkbox"/> Export	All Marketing user group users can copy all kind of files from their removable devices to their local HDD, but Jill can also copy Word documents from her HDD to removable devices.
	Read/Write	Jill	<input checked="" type="checkbox"/> Only files selected from this list Microsoft Word selected	<input type="checkbox"/> Import <input checked="" type="checkbox"/> Export	

\*Auxiliary file groups created to serve as a 'bridge' to define required permissions.

Table 23: File filter settings examples



## Adding a user or group when defining a permission

When adding a new permission, no matter what kind of permission, you need to associate it with one or several users or group of users. This is done using the *Select Group, User, Local Group, or Local User* dialog.

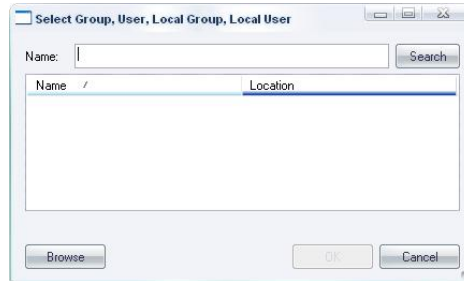


Figure 39: The Select Group, User, Local Group or Local User dialog

The contents of the *Select Group, User, Local Group, or Local User* dialog are explained in the following table:

Object	Description and use
Name field	Used to type in the user/group name. It accepts wildcard symbols.
Search button	To search for the user/group.
Browse button	To browse in the Active Directory for users/groups. Not available for Novell objects
List box	Once the Name field is validated, a list of all possibilities is shown here to select from.
OK button	Accepts the selected user/group and close the dialog.
Cancel button	Interrupts the add user/group operation and close the dialog.

Table 24: Add user/group dialog options

You can select one or more users or user groups by doing one of the following:

- > Leaving the NAME field empty and clicking on the SEARCH button. You can see a complete list of available users/groups/objects in the list box. Double click to select one user or group or use the SHIFT and CTRL keys to do a multiple selection. Once your selection is done, click on OK or ENTER to accept and close the dialog.
- > Typing the complete name of the user or group in the NAME field and pressing ENTER (or clicking on SEARCH). The name of the user/group is verified and, if valid and present, appears in the list box. Double click on it or select it and then click on OK or ENTER to accept and close the dialog.
- > Typing a partial name in the NAME field and pressing ENTER (or clicking on SEARCH). You can use the wildcards \* and ? in the name. Double click to select one user or group or use the SHIFT and CTRL keys to do a multiple selection. Once your selection is done, click on OK or ENTER to accept and close the dialog.
- > Clicking on the Browse button. The standard Windows Select Users or Groups dialog opens. Follow Windows procedures to select the desired user/group. Click on OK or ENTER to accept the selection and close this dialog and then once more on OK or ENTER to close the first dialog and accept the selection.

If the user/group you are looking for is not displayed, make sure you synchronize the domain and check you have the appropriate permissions on the object in the Active Directory (delegation) or Novell's eDirectory. Remember to run the synchronization script if working in a Novell environment as described in *Sanctuary's Setup Guide*.



## To assign default permissions

### Root-level permissions

You can apply 'root-level permissions' using the Device Explorer module. These permissions are not attached to a particular device class or type, but to the root of the Device Explorer tree (or to a specific device class, device group, computer or group settings of a computer group in the Machine-Specific Settings tree). They therefore apply to all devices for a specific user(s)/user group(s). For example, you can have a *non-blocking mode* (Read/Write permissions) for all devices at user/user group level. Of course, applying an *all-blocking mode* (no Read or Read/Write permissions) is equally possible.



*Since access to certain devices (notably those connected to the PS/2 port) is performed in the context of the built-in 'LocalSystem' user, we recommend not using the built-in 'Administrators' group — that includes that user — for root-level permissions. If you do this, you may allow unexpected users to access certain devices (depending on the particular machine's configuration). A safer approach is to define a specific user group for assigning these types of root-level permissions. For example, if you grant 'Administrators' read/write access at the root level, you are also implicitly granting the 'LocalSystem' user — and, therefore, everyone — the same permissions for the PS/2 port.*

### Where default permissions apply

Default permissions can apply to the following:

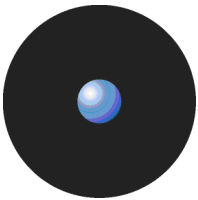
- > The root node of the *Default Settings* tree.
- > The *Device Class* node of the *Default Settings* tree. For example, for the *DVD/CD Devices* class.
- > The *Device Group* within an existing *Device Class* node in the *Default Settings* tree. For example, a previously defined device group called 'DVD recorders Marketing Dept.' of the *DVD/CD Devices* class in the *Default Settings* tree.
- > In the *Group Settings* of a previously defined *Computer Group* within the *Machine-Specific Settings* tree.
- > A computer previously added to an existing domain or workgroup within the *Machine-Specific Settings* tree.

When applying the *non-blocking mode* (Read/Write permissions for a user/user group) you have the advantage of creating a log of device usage (see *Chapter 5: Using the Log Explorer* on page 99 for more details) without denying them access. You can combine this feature with a 'shadow' (see *Shadowing devices* on page 82 for more details) at device class level for a full log control.

### Assigning default permissions

To assign permissions to a node in a tree, follow the steps outlined in the next section. The only difference is that you should select the nodes described on the previous list (root of the Device Explorer tree, a specific device class, device group, computer, or group settings of a computer group in the Machine-Specific Settings tree).

If you assign default permissions at the root-level, they combine with those defined at the class level (the branches of the Default Settings tree) depending on the chosen priority (Low or High) — see *Table 25* on page 87.



## To assign default permissions to users and groups

You can set the access permissions to devices for users and groups so that they apply to any computer that the user uses. Do this using the following procedure:

1. Select a devices class within the 'Default settings' list. Right-click on the selection and choose *Add / Modify Permissions* from the popup menu. Alternatively, select the class and then select *Add / Modify Permissions* from the Explorer menu or use the CTRL+D shortcut key.

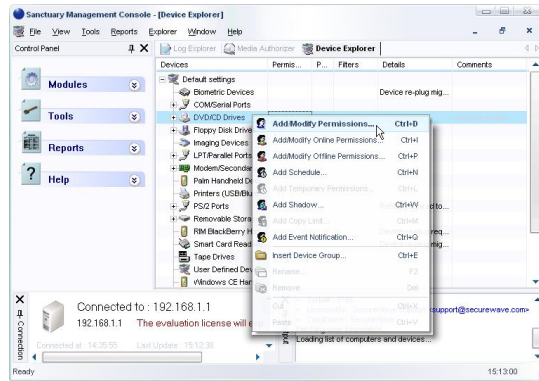


Figure 40: Assigning default permissions to users and groups

The *Permissions* dialog is displayed (some options may or may not be available depending on the class where you are defining the permissions):

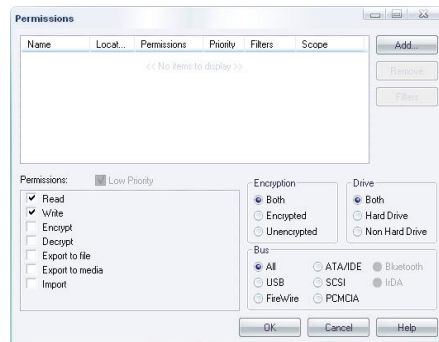


Figure 41: The Permissions dialog

2. The first step consists on adding the user(s)/group(s) for which this permission applies. Click on the ADD button.

The *Select Group, User, Local Group, or Local User* dialog is displayed.

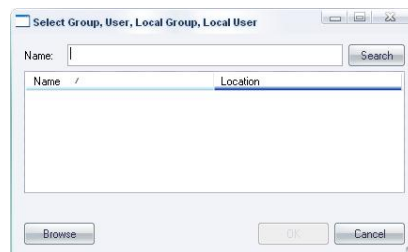


Figure 42: The Select Group, User, Local Group or Local User dialog when adding default permissions

3. Select the user(s)/group(s). See *Adding a user or group when defining a permission* on page 66 for a complete description on how to use this dialog.
4. Back in the *Permissions* dialog, select the user(s)/group(s) you want to assign permissions to (you can use the SHIFT and CTRL keys to do a multiple selection), and then activate the appropriate options. You can define different permissions for each group of selected users/groups. See *Using*








*the Permissions dialog on page 57 for more details (especially if you are working on the Removable Storage Devices class).*

5. If required, select the file filter options by clicking on the FILTERS button. See a description in the *Using file filters* section on page 60.
6. Click OK to finish.

The *Permissions* column in the main window now shows that options activated for the selected users or groups.


 *When setting read-only permissions on the DVD/CD Drives class, some applications, notably CD-R applications, may not notice that access was denied by Sanctuary and erroneously report to the user that a CD has been burned properly when it has not. In this case, we recommend that you use Sanctuary event notification to warn users of this.*

 *If Smart Card readers are used to authenticate the user then they should be granted Read/Write access to the group 'Everyone'.*

 *The list of changes is not sent to the client computer immediately. This list is downloaded the next time a user logs onto that computer. You can, alternatively, send the list immediately by selecting the 'Send Updates to All Computers' or 'Send Updates To' option on the 'Tools' menu (or from the Control Panel). Some devices, such as the TAPE and the Smart Card Reader, require a reboot in order to apply the new permissions. See the notes on page 49 for those devices that require a reboot.*

## Priority of default permissions

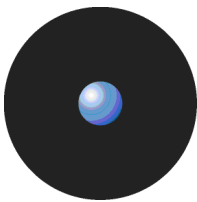
The priority flag can only be set for default permissions. It determines if a negative permission – 'None' — defined at the default permission level can be overwritten by a computer-specific permission.

 *It is important to distinguish between the absence of permission and a negative permission ('None' — the most restrictive access).*

*In the latter case, when creating a permission for which neither the Read nor the Write flags are selected, you deny the user access to the device even if they are indirectly authorized to use the device. You specifically deny the access to a device for the user.*

You should be aware that:

- > When a 'None' permission has a High priority, it cannot be overwritten by a computer-specific one.
- > When a 'None' permission has a Low priority, it can be overwritten by computer-specific one only when its priority is 'High'.
- > When different positive (Read, Read/Write) permissions are defined at the Default and computer-specific levels, the resulting one is an addition of both of them. The permission priority property only applies to negative ones.
- > When a negative permission is defined at the computer-specific level, it takes precedence over the default one depending on the priority.



The following table explains how permissions are applied when they are defined for the same user or group(s) where the user is a member, at the Default level and computer-specific level:

<b>Default Setting</b>	<b>Default Permission Priority</b>	<b>Computer-specific permission</b>	<b>Computer Specific permission priority</b>	<b>Resulting permission</b>	<b>Explanation</b>
Read-only	High	Read/Write	High	Read/Write	See below for the steps to follow to find out which priority applies.
			Low	Read/Write	
		None	High	None	
			Low	Read-only	
		Read-only	High	Read-only	
			Low	Read-only	
	Low	Read/Write	High	Read/Write	
			Low	Read/Write	
		None	High	None	
			Low	None	
		Read-only	High	Read-only	
			Low	Read-only	
Read/Write	High	Read/Write	High	Read/Write	
			Low	Read/Write	
		None	High	None	
			Low	Read/Write	
		Read-only	High	Read/Write	
			Low	Read/Write	
	Low	Read/Write	High	Read/Write	
			Low	Read/Write	
		None	High	None	
			Low	None	
		Read-only	High	Read/Write	
			Low	Read/Write	
None	High	Read/Write	High	None	
			Low	None	
		None	High	None	
			Low	None	
		Read-only	High	None	
			Low	None	
	Low	Read/Write	High	Read/Write	
			Low	None	
		None	High	None	
			Low	None	
		Read-only	High	Read-only	
			Low	None	
<b>Rules:</b> 1. Combine both permissions. 2. Sort them according to their priority. 3. The one with the highest one is applied. 4. If both permissions have the same priority, follow this precedence:				None	Highest Lowest
				Read/Write	
				Read-only	
Note: You can substitute the 'Default Setting' column heading with 'Class Setting' & 'Computer Specific Permission' with 'Device Permission'. This substitution works for any group → subgroup you create, for example, Class → Device; Class → Device Group; Device Group → Model; Model → Specific device, etc.					

Table 25: Applied permissions



Please refer to *Permissions Priority* on page 146 for an explanation of the priority rules interacting between those permissions defined at the Device Explorer level and those defined at the Media Authorizer level.

## Read/Write permissions

Only those devices that support a file system can be set to read-only mode. For all others, the only possible permission is either None or Read/Write. Read-only applies to floppy drives, DVD/CD drives, and Removable media. See *Table 16* on page 50 for device's restrictions.



## To assign computer-specific permissions to users and groups

You can assign permissions on a per-computer basis in a similar way to how you assigned default permissions. Settings that are specific to a particular computer override the *Default Settings* for the given machine.

To assign permissions computer-specific permissions to users and groups.

1. If the computer is not listed in the *Machine-Specific Settings* section, right-click on the section title and select *Insert Computer*. Alternatively, select *Insert Computer* from the *Explorer* menu or use the CTRL+A shortcut key.



*The Device Explorer does not show every computer in the domain. It includes those computers for which permissions or options are set. Administrators are limited to the users or computers they are allowed to manage when using Active Directory. Permissions for most computers are managed using the 'Default settings' section.*

The *Select Computer* dialog is displayed:

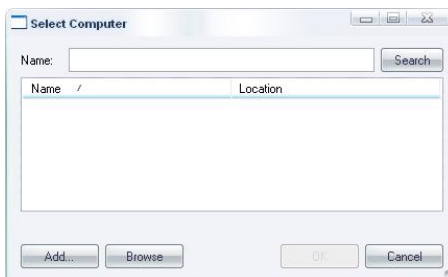


Figure 43: The Select Computer dialog showing multiple selection in action

2. Select the desired computer(s). See *Adding a user or group when defining a permission* on page 66 for a complete description on how to use this dialog (although the description in that section describes how to select users/groups, the procedure is just the same).

You return to the Device Explorer window.

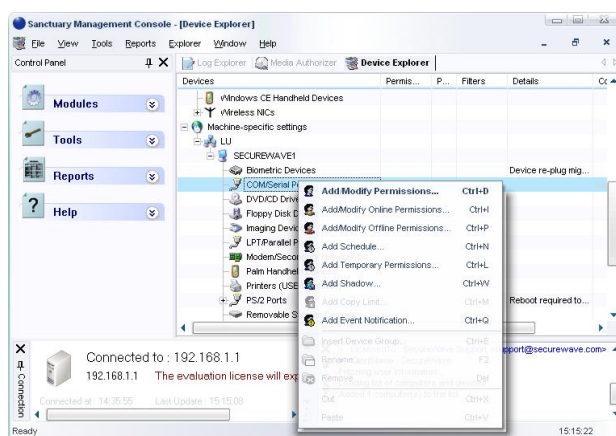


Figure 44: Assigning permissions in the Device Explorer module

3. Select the computer you want to assign permissions to, and click the + box to the left of it to expand the list of devices (or use the -, +, and arrow keys of your keyboard to navigate the tree).
4. Right-click on the device class and then select the *Permissions* option from the popup menu. Alternatively, open the tree structure, select the device, and then select *Permissions* from the *Explorer* menu or use the shortcut key CTRL+D.



The *Permissions* dialog is displayed (some options may or may not be available depending on the class where you are defining the permissions).

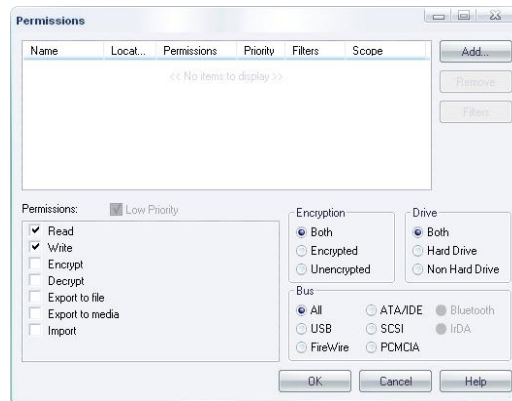


Figure 45: Defining Read, Read/Write, or None permissions when adding permissions

5. Click on Add.

The *Select Group, User, Local Group or Local User* dialog is displayed.

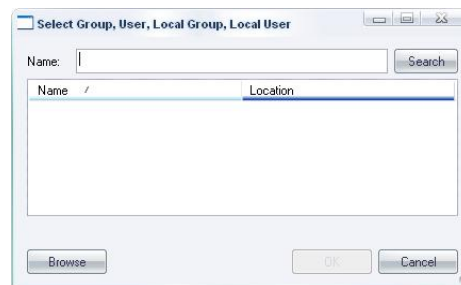


Figure 46: The Select Group, User, Local Group or Local User dialog

6. Select the user(s)/group(s). See *Adding a user or group when defining a permission* on page 66 for a complete description on how to use this dialog.
7. Back in the *Permissions* dialog, select the user(s) you want to assign permissions to, and then activate the appropriate options from the list. Use the SHIFT or CTRL key to make multiple selections. See *Using the Permissions dialog* on page 57 for more details (especially if you are working on the *Removable Storage Devices* class).
8. Click Ok to finish and close the dialog.



*The list of changes is not sent to the client computer immediately. This list is downloaded the next time a user logs onto that computer. You can, alternatively, send the list immediately by selecting the 'Send Updates to All Computers' or 'Send Updates To' item on the 'Tools' menu (or from the Control Panel).*

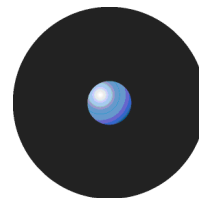
## To modify permissions

To modify the permission assigned to a user or group, proceed as follows:

1. Right-click on the user or group, and select *Modify Permissions* from the pop-up menu. Alternatively, select the *Add/Modify Permissions* from the *Explorer* menu, or use the shortcut key CTRL+D.



Figure 47: Modifying permissions



- In the *Modify Permissions* dialog, change the permissions as appropriate, and then click Ok.

*The list of changes is not sent to the client computer immediately. The list is downloaded the next time a user logs onto that computer. You can, alternatively, send the list immediately by selecting the 'Send Updates to All Computers' or 'Send Updates To' item on the 'Tools' menu (or from the Control Panel).*

### To remove permissions

To delete the permission to use a device from a user or group, right-click on the user or group, and select *Remove Permissions* from the pop-up menu. Alternatively use the *Remove* option from the *Explorer* menu, or press the DELETE key.



Figure 48: Removing permissions

### To assign scheduled permissions to users and groups

You assign this kind of permission when you want to limit the use of certain devices to specific hours and days of the week. The procedure is the same for assigning global or computer-specific scheduled permissions.

*When assigning scheduled permissions (for example, from Monday to Friday, 8 AM to 5 PM), the local client's time applies.*

To assign scheduled permissions:

- Right-click on the device in the *Default Settings* section and select *Add Schedule* from the popup menu. Alternatively, select the device and select *Add/Modify Scheduled Permission* on the *Explorer* menu, or use the shortcut key CTRL+N.

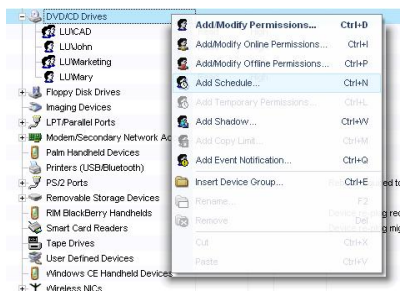
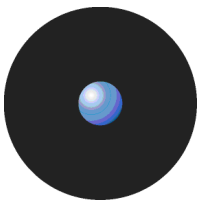


Figure 49: Add a Scheduled permission

The *Choose User* dialog is displayed:



Figure 50: The Choose User dialog when adding a scheduled permission



2. Select the user(s)/group(s). See *Adding a user or group when defining a permission* on page 66 for a complete description on how to use this dialog. Click on NEXT: the *Choose Permissions* dialog is displayed:



Figure 51: Defining Read or Read/Write permissions when adding scheduled permissions

3. Choose the permissions that you want to apply to the schedule (Read or Read/Write) and then click NEXT. The *Choose Timeframe* dialog is displayed:

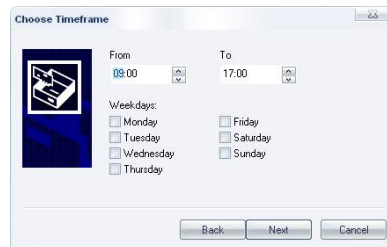


Figure 52: The Choose Timeframe dialog when adding a scheduled permission

4. Define when the permissions will apply: using the *From* and *To* fields enter the period of the day; then, using the checkboxes, specify the days of the week.
5. Click on the NEXT button and then on FINISH.



*If you define scheduled or temporary access for a dial-up modem (using either a COM port or a Modem port), when the access expires, the communication with the modem is immediately terminated. One side effect is that the program that is using the modem does not have the time to send a 'disconnect' command to the modem. Therefore, the modem may remain on-line for a long time, leading to a large call charge.*



*You cannot set a scheduled permission that runs past midnight. If you need a schedule that allows somebody to access a device through midnight, it is necessary to define two scheduled sessions, one up to midnight and one the next day immediately after midnight.*



*The list of changes is not sent to the client computer immediately. The list is downloaded the next time a user logs onto that computer. Alternatively, you can send the list immediately by selecting the 'Send Updates to All Computers' or 'Send Updates To' item on the 'Tools' menu (or from the Control Panel).*

## To modify scheduled permissions

To modify an existing schedule proceed as follows:

1. Right-click on the user or group with the schedule in the Default Setting section, and select *Modify Schedule* from the pop-up menu. Alternatively, you can select *Add/Modify Scheduled permission* from the *Explorer* menu.

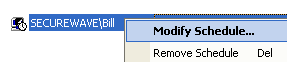


Figure 53: Modifying a scheduled permission

2. In the *Choose Permissions* dialog, change the options if appropriate, and click NEXT.





3. In the *Choose Timeframe* dialog, modify the schedule if appropriate, and then click NEXT.
4. Click FINISH.

## To remove scheduled permissions

To delete an existing schedule, right-click on the user or group with the schedule, and select *Remove Schedule* from the pop-up menu. Alternatively, you can select *Remove* from the *Explorer* menu, or press DELETE. Schedule permissions also disappear once they become due.

## To assign temporary permissions to users

It is possible, on a computer-specific basis only, to assign a one-off time-limited permission to access a device. The main purpose is to allow you to grant access to a device for a limited period without having to go back and delete the permission afterwards.

-  When assigning temporary permissions as a deferred value (for example, from Monday to Friday, 8 AM to 5 PM), the local time on the console is converted to UTC (Coordinated Universal Time) and sent to the client who converts his local time to UTC before comparing these values.
-  You can only define temporary permissions for a computer previously added to the 'Machine-Specific Settings' branch of the 'Device Explorer' tree.

To assign a temporary permission:

1. Right-click on the device in the *Machine-Specific Settings* section and select *Temporary Permissions* from the pop-up menu — you must first insert the computer. Alternatively, select the device and use the *Temporary Permissions* option on the *Explorer* menu, or use the CTRL+L shortcut key.

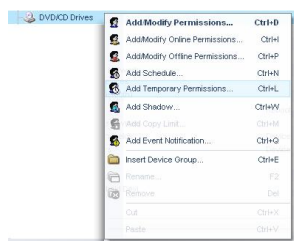


Figure 54: Adding a Temporary permission

The *Choose User* dialog is displayed:



Figure 55: The Choose User dialog when adding a temporary permission

2. Click on the ADD button. Select the user(s)/group(s). See *Adding a user or group when defining a permission* on page 66 for a complete description on how to use this dialog. Click on NEXT: the *Choose Permissions* dialog is displayed:

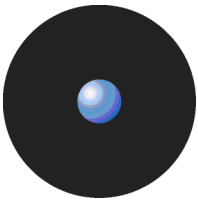


Figure 56: Defining Read or Read/Write permissions when adding a temporary permission

3. Choose the permissions that you want to apply, then click NEXT.

The *Choose Period* dialog is displayed:



Figure 57: The Choose Period dialog when adding a temporary permission

4. Choose the period when you want to apply the permissions, by selecting either *Immediately* or *From*, and then specifying the times and dates involved. The minimum duration is 5 minutes.
5. Click NEXT and then click FINISH.

## To remove temporary permissions

To delete an existing temporary permission, right-click on the user or group with the permission, and select *Remove Temporary Permissions* from the popup menu. Alternatively, you can select *Remove* from the *Explorer* menu, or press DELETE. Temporary permissions also disappear once their time limits are reached.

## To assign temporary permissions to offline users

In some cases users need to increase their permissions while they are not connected to your network, i.e. they are 'out of band'. For example, a user who has no access to the Internet may want to read a file stored on a removable storage device, or he may be meeting a customer at an airport and needs authorization to install the customer's software application on his laptop.

If a user needs increased permissions when offline he can phone a Sanctuary administrator (as he cannot communicate with a Sanctuary server), explain what permissions he requires, and quote a key code provided by Sanctuary Client. The administrator enters these details into the Sanctuary Management Console and, if she approves the request, provides an unlock code which, when entered by the user, grants the required permissions. These permissions are valid until either they expire or the computer reconnects to your network.



*To grant temporary permissions to offline users the administrator requires the appropriate access rights; The Sanctuary Management Console administrator's User Access must have 'Temporary Permission Offline (Device Control)' set to 'Yes'. See Defining Sanctuary administrators on page 32 for more information.*

The procedure to assign a temporary permission for an offline user involves steps carried out by the user requesting permissions, denoted [Offline user] below, and the administrator authorizing the changes, denoted [Administrator]. You can assign offline permissions using the following steps:

1. [Offline user] Right-click on the Sanctuary Client icon, in the Windows system tray (at the bottom right of the Sanctuary Client computer's screen) and select the *Request temporary access offline* option in the context menu. The Request Temporary Access Offline dialog is displayed, showing the Introduction page:





Figure 58: Sanctuary Client's Request Temporary Access Offline dialog – Introduction page

- [Offline user] Telephone your Sanctuary administrator and then click on the NEXT button. The Input page is displayed:

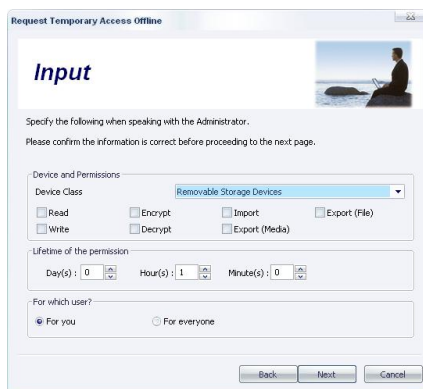


Figure 59: Sanctuary Client's Request Temporary Access Offline dialog – Input page

- [Administrator] Open the Request Temporary Permissions dialog on the Sanctuary Management Console. To do this, select *Temporary Permissions Access Offline* from the *Tools* menu (or from the *Control Panel*). The Authorize Temporary Access Offline dialog is displayed:

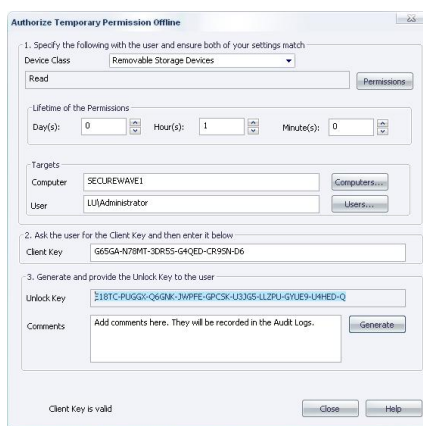
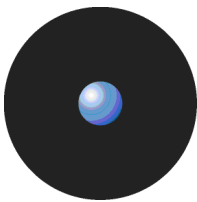


Figure 60: Sanctuary Management Console's Authorize Temporary Access Offline dialog

- [Administrator and offline user] Agree and enter the settings for the device, the required permissions, user, and, in the case of the administrator, the computer.



*The offline user specifies the settings in the Input page of Sanctuary Client's Request Temporary Access Offline dialog. The administrator enters them in Sanctuary Management Console's Authorize Temporary Access Offline dialog.*



The settings specified by the offline user and the administrator must be identical for the Unlock Key generated by the administrator to work when entered by the offline user in step 11.

The contents of the offline user's and administrator's dialogs are explained in the following table:

Field	Used to...
Device Class	Select the type of device that the offline user wants permission to use, for example, 'Removable Storage Device' for a USB memory stick.
(Permissions)	Select the permissions that the user requires, for example 'Read/Write' and/or 'Encrypt'. The available options depend on the device class selected above. Administrators can browse for the appropriate permission by clicking on the PERMISSIONS button.
Lifetime of the Permissions	Select the Day(s), Hour(s), and/or Minute(s) for which the temporary offline permission is required. For example, the lifetime of the permission may be one hour.
For which user?	[Offline User] Select whether the permission change should be made just for the user's login account or for everyone logging into the particular computer within the lifetime of the permission. You should choose the 'For everyone' option when the computer is logged in to a network that is not known to the administrator. Although this makes the device control less secure, it enables administrators to change the offline permissions in some situations where it otherwise would not be possible.
Computer	[Administrator] Either enter the name of the computer directly or click on the COMPUTERS button and browse for it. The computer name is not case sensitive.
User	[Administrator] Either enter the name of the user directly or click on the USERS button and browse for it. When the Offline user has chosen the 'For everyone' option then the Administrator must select the 'Everyone' user.

Table 26: Temporary Access Offline dialog settings

1. [Offline user] On the Input page, click on the NEXT button. The Unlock page is displayed showing a Client key:



Figure 61: Sanctuary Client's Request Temporary Access Offline dialog - Unlock page

2. [Offline user] Read out the 27-character Client Key value (such as Q005F-L7Y72-2PGMJ-09PNN-9WIXU-68) to the administrator.




The client key is valid for up to an hour. If the requested permission is not granted in this time the offline user needs to click on the CANCEL button and repeat steps 1, 2, 4, 5, and 6.


3. [Administrator] Enter the alphanumeric string provided by the offline user in the Client Key field of the middle section of the Authorize Temporary Access Offline dialog.

The Client key value is validated by the Sanctuary Management Console. If correct, the message 'Client key is valid' is displayed at the bottom of the Administrator Authorize Temporary Access Offline dialog. If an error is identified, ask the offline user to repeat the Client key and reenter it.





 *The client key generated by the Sanctuary Client depends on the settings entered in step 4. This enables the Sanctuary Management Console to check whether the same settings were entered by the administrator in the Authorize Temporary Access Offline dialog and the offline user in his Request Temporary Access Offline dialog. If this is not the case, an error is displayed, the offline user must click on the BACK button and you must repeat step 4 onwards.*

4. [Administrator] Enter any comments about the temporary offline permission in the Comments text field at the bottom of the Authorize Temporary Access Offline dialog. For example, you can enter 'Requested for project 1042'. This comment is viewable in the audit log entries.
5. [Administrator] If you approve the offline user's permission request, click on the GENERATE button. An Unlock Key is generated by the Sanctuary Management Console and displayed in the Authorize Temporary Access Offline dialog.

 *The GENERATE button is disabled until all the information in the Authorize Temporary Access Offline dialog is complete and has been validated.*

6. [Administrator] Read out the 46-character Unlock Key value (such as FA9EP-RH74Z-M3FMF-THH69-44LMD-0K55L-NWPKM-R9AZ8-ZA1XQ-4) to the offline user.
7. [Offline user] Enter the alphanumeric string provided by the administrator in the Unlock code field of the Request Temporary Access Offline dialog and click on the NEXT button.

 *The offline user is limited to 15 tries at entering the correct Unlock code before a lockout period comes into effect.*

 *A lockout period also comes into effect if the Sanctuary Client's Request Temporary Access Offline dialog is used to generate a Client key 15 times without a valid unlock code being entered, i.e. it is cancelled more than 15 times.*

Once the unlock key is successfully entered, the Finish page is displayed (and a system tray message informs you that the permission status has been changed up to a certain time):



Figure 62: Sanctuary Client's Request Temporary Access Offline dialog – Finish page

8. [Administrator and offline user] If the temporary permission was successfully granted to the offline user, you can end your phone call and click on the CLOSE/FINISH button.

A message is displayed in the Sanctuary Management Console informing administrators that the temporary offline permissions are deleted when the computer next connects to your Sanctuary server. This reminds you that you may need to create a normal temporary permission (see *To assign temporary permissions to users* on page 75) if you want the permissions to continue once the user is online again.

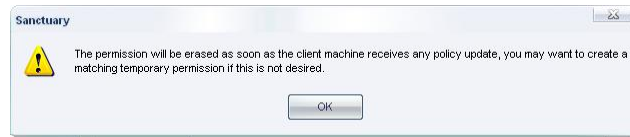


Figure 63: Temporary Access Offline reminder to administrators

## To assign online and offline permissions

You assign this kind of permission to control the use of devices in a different way when the user is offline, as opposed to when they are online. For example, you may let an individual use his DVD/CD writer when at home but not when he is online at the company, or you may ban a user from establishing a WiFi/Modem connection to the Internet when his machine is connected to your company's network (so that he does not circumvent your firewall).

The way the 'online'/'offline' state is detected depends on the 'Online/Offline state definition' option. See *Chapter 8: Setting and changing options* on page 169.

You should be aware that:

- > An 'online' state applies when the client computer is under the control of your server, or is connected to the computer network.
- > An 'offline' state (the opposite to 'online') applies when the client computer is not under the control of your server, or is not connected to the computer network.

The Sanctuary Client Driver 'discovers' when a computer is online or offline when one of the following occurs:

- > The machine boots (and the Sanctuary Client Driver starts). The initial state is 'offline'.
- > The user logs on.
- > The user uses 'Refresh Settings' located on the right-click menu of the system tray Sanctuary Device Control icon.
- > A 'Refresh' message is received from a SecureWave Application Server.
- > The shadow upload time is due.
- > A network interface changes its state. For example, when a network cable, WiFi card or modem is connected or disconnected, a VPN connection is established or terminated, an address (DHCP) is used or released, or a network card is disabled, enabled, deleted, or added.
- > One hour after the different online/offline permissions were set (if none of the above happened in the meantime).



*If you are using different online and offline permissions and the SecureWave Application Server is stopped or disconnected, clients who are already logged in retain their online permissions for up to one hour. This happens because the Sanctuary Client Driver checks updates with the SecureWave Application Server each hour.*

When the online and offline permissions become effective, they are treated the same way as a 'regular' permission. That is, the online/offline permissions COMBINE with the regular ones, in accordance with their mutual priorities.

Use the following procedure to assign online and offline permissions:

1. Right-click on the device (general type or a specific device on the list) in the *Default Settings* section and select *Online Permissions* (or *Offline Permissions*) from the popup menu. Alternatively, select the device and select *Add/Modify Online Permission* on the *Explorer* menu, or use the shortcut key CTRL+I (for online) or CTRL+P (for offline).

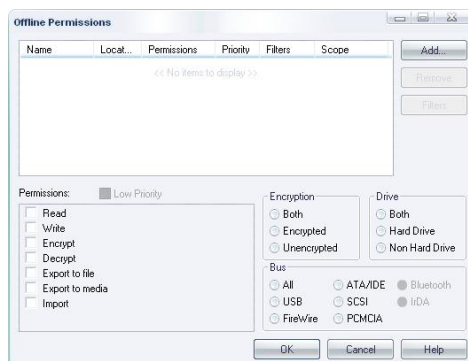
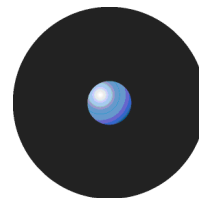


Figure 64: Defining Read, Read/Write, or None permissions when adding online/offline permission

2. Click on the ADD button and select the user(s)/groups(s) from the *Select Group, User, Local Group or Local User* dialog. See *Adding a user or group when defining a permission* on page 66 for a complete description on how to use this dialog.
3. Enable the desired options and accept these by clicking on OK. See *Using the Permissions dialog* on page 57 for more details (especially if you are working on the *Removable Storage Devices* class).



*The list of changes is not sent to the client computer immediately. This is downloaded the next time a user logs onto that computer. You can, alternatively, send it immediately by selecting the 'Send Updates to All Computers' or 'Send Updates To' option on the 'Tools' menu (or from the 'Control Panel'). Some devices require rebooting before new permissions are applied.*

## To remove offline or online permissions

To remove an existing offline or online permission, right-click on the user or group with the permission, and select *Remove Online Permissions* (or offline) from the pop-up menu. Alternatively, you can select *Remove* from the *Explorer* menu, or press DELETE.

## To export and import permission settings

The export and import permission settings are used to export a group of carefully crafted permissions for a range of devices and then import them onto a computer to synchronize them.

You can use this feature to change permissions when a computer is not connected to the network (and cannot be connected for the time being), but it still has access to the Internet. The rules 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 Sanctuary's Setup Guide for more information.



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

To export/import your settings:

1. Select the *Export Settings* item from the *Tools* menu (or from the *Control Panel*).
2. Select the name and destination of the file in the standard *Save As* Windows dialog. Normally the destination is 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 Driver icon to display a pop-up menu. This image may change depending on your license type and installed programs.

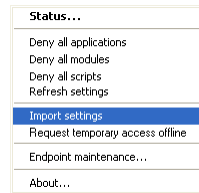
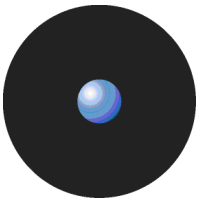


Figure 65: Importing permission settings

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

## Shadowing devices

When you need to control the files and content written/read to/from a device, use the shadowing rule. You can analyze the file(s) using the Log Explorer module (see *Chapter 5: Using the Log Explorer* on page 99). This rule is available for the following:

- > COM/Serial ports.
- > LPT/Parallel ports.
- > DVD/CD drives.
- > Modem/Secondary network access devices.
- > Removable storage devices.
- > Floppy disk drives.

You can define shadowing for a user or group of users on a:

- > Class of devices.
- > Group of devices.
- > Specific model or device for a computer.



*If a user does an operation involving shadowing while the computer is disconnected from the network, the shadow information is transferred to the server as soon as the machine is reconnected.*



*You must choose the 'Encrypted' setting in the first dialog so that the Shadow rule applies to this kind of device. See *Chapter 6: Using the Media Authorizer* on page 129 for more information.*



*If a user traverse a 'shadowed' device folder by using his mouse (or the keyboard), Windows Explorer recovers part of the file to display its thumbnail and extended info. This behavior causes partial shadow files to show in the Log Explorer module.*

The shadow permission details are displayed in the Permissions column of the Device Explorer module. A value of 'R' means that shadowing is on for files read from the device, 'W' means that it is on when files are written to it, and no letter means that it is on for both a reading and writing files.



*When editing a file previously copied to a 'shadowed' device (in the same user's session), no read shadow data is created since Windows saves the file in its cache and, therefore there is no new read operation request. This does not apply if the file initially resides in the device or in a new user session (the cache is empty).*



## To shadow a device

To activate a shadowing rule for a device:

1. Right-click on the device, device class, or device type in the *Default Settings* section and select *Shadow* from the popup menu. Alternatively, select the device and select *Add/Modify Shadow Settings* on the *Explorer* menu, or use the shortcut key CTRL+W.



Figure 66: The Choose User dialog when adding a shadow rule

2. Click on the ADD button and select the user(s)/group(s) from the *Select Group, User, Local Group or Local User* dialog. Click on the NEXT button. The *Choose Bus* dialog opens:



Figure 67: Selecting the bus when adding temporary permissions

The first part of the dialog is only active when you are adding a shadow rule for a removable device. It lets you select if the shadow applies to all type of devices or just encrypted or unencrypted ones. The *Drive* panel lets you select between shadow for hard disk, non hard disks, or all types.

3. Select among the available bus types (they vary from one class to another) or all of them. See *Using the Permissions dialog* on page 57 for more details (especially if you are working on the *Removable Storage Devices* class). Click on NEXT to continue. The *Choose Permissions* dialog is displayed.
4. Select either *Enabled*, *Disabled*, or *Filename* (some devices only support Enable and Disable) to switch shadowing on or off. Select these options either on the Read Permission and/or in the Write Permission panel. When selected on the Read Permission side, the shadow is only activated during the read operations. The same applies to the Write Permission panel.

If you use the *File Name* option, you just get the name of the file being copy to the medium but not the content. In this case, the 'Attachment' field in the Log Explorer module is set to 'False'. This option uses very few network and no hard disk storage resources on the data file directory.

When you use the *Enabled* option, you get the name of the file being copied (read) by the user to the device and an exact copy of what is written. This content is stored on the local client directory and then transmitted to the server. Please note that high capacity devices, such as DVDs, can consume a lot or resources and hard disk space. When full shadowing is enabled, the 'Attachment' field in the Log Explorer module is set to 'True'.

Some classes only have the Write panel active because no data can be read from them — LPT & COM.



Figure 68: Defining the type of shadow for a device

5. Click NEXT to display the *Finish* dialog where you can review the settings.

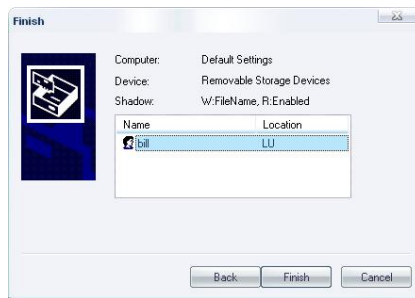


Figure 69: Finishing the shadow rule definition

6. Click FINISH to close the dialog and apply the changes.



*The list of changes is not sent to the client computer immediately. This list is downloaded the next time a user logs onto that computer. You can, alternatively, send the list immediately by selecting the 'Send Updates to All Computers' or 'Send Updates To' item on the 'Tools' menu (or from the Control Panel). Some devices require a reboot in order to apply the new permissions.*

## To remove the shadow rule

To remove an existing shadow permission, right-click on the user or group with the permission, and select *Remove Shadow Permissions* from the pop-up menu. Alternatively, you can select *Remove* from the *Explorer* menu, or press DELETE.

## To view a 'shadowed' file

When the rule to create shadow (read/write) files is selected, these files are kept in the client computer until a transfer is done to the SecureWave Application Server and its associated Data File Directory. You can review these files using the Log Explorer module. Please see *Chapter 5: Using the Log Explorer* on page 99 for more information.

## Copy limit

You can use this rule to limit the quantity of data a user can write to a device on a per-day basis.



*Copy limit can also be applied to administrators. If you do not want this restriction to apply to them, you should modify the default copy limit rule as defined in the 'Device Explorer' module.*



*The copy limit rule is defined per user/per machine. A user that exhausts the establish quota can always login in another machine to renew it.*

You can only limit data for floppy disk drives or removable devices and only for a device class (the upper level of a device).





When a user reaches their copy limit Sanctuary prevents them from copying a file to a device, moving a file to a device or replacing a file on a device. If the user is replacing a file, Sanctuary removes the file that is being replaced.

## To add a copy limit

To change the limit of data copied to such types of devices:

1. Right-click on the device class (the upper level of a device) in the *Default Settings* section (to define this rule for all users) or in the device class of the *Machine-Specific Settings* (to create a rule at a computer level) and select *Copy Limit* from the popup menu. Alternatively, select the device and select *Add/Modify Copy Limits* from the *Explorer* menu, or use the shortcut key CTRL+M.

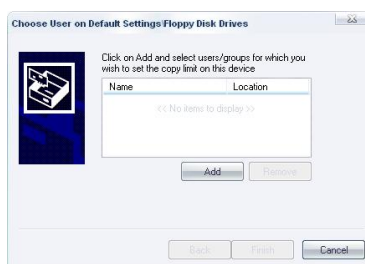


Figure 70: The Choose User dialog when adding a copy limit rule

2. Click on the ADD button and select the user(s)/group(s) from the Select Group, User, Local Group or Local User dialog. Once you have finished adding the users or groups, click on the NEXT button to continue the process.
3. Assign the copy limit (in MB) to the user(s)/group(s):



Figure 71: Defining a copy limit

4. Click on the FINISH button to create and apply the rule.

The copy limit rule is reset daily at midnight, local hour.



*Copy limit permissions cannot be defined at the device-type level, only at the device class level (the topmost category of the device).*

When users select the *Status* item of the icon tray pop-up menu in the client machine, they can see how many bytes have been copied and how many remain for their working day. This only applies to those devices that have the copy limit rule set as shown on *Figure 72*.

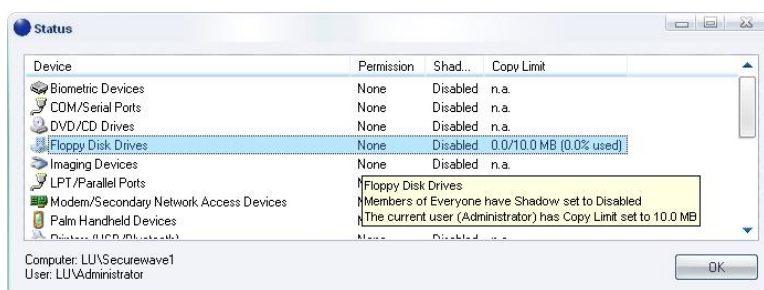


Figure 72: The status screen on the client's side: copied/remaining bytes



## To remove a copy limit

To remove an existing copy limit permission, right-click on the user or group with the permission, and select *Remove Copy Limit* from the pop-up menu. Alternatively, you can select *Remove* from the *Explorer* menu, or press DELETE.

## Applying multiple permissions to the same user

It is possible to apply several sets of permissions to a user for a specific device. This can happen if the user is a member of different groups. Permissions can be set for domain groups, domain users, well-known groups, local groups, or local users.



*You need to synchronize computers so that the local groups and users appear in the system. By default, only well-known groups and users as well as domain groups and users are visible to the system. Please refer to the Synchronizing domain members section on page 30 for more information.*

Overlapping permissions have the following effects:

- > The default setting is 'no access available'. If you do not take any further action, you are accepting this default scenario for a user or group.
- > You can explicitly authorize access to a user or group.
- > You can explicitly deny access to a user or group – negative permission – 'None'.

The overall effect is that you deny access if any of following cases is true:

- > The default setting is still in effect (i.e., no permissions have been set).
- > You explicitly deny access with high priority at the default or computer-specific level to a user or any of the groups he belongs. This is also true if you explicitly allow access to other groups.
- > You explicitly deny access with low priority at the default level to the user or any of the groups he belongs to and none of the groups is explicitly allowed access at the computer-specific level.



*If access to a particular device has been explicitly denied with high priority at the default permission level, then the 'Scheduled' and 'Temporary' permissions are ignored.*

When a user logs onto a machine, the sum of all permissions assigned directly to him and to the groups he belongs to are applied (refer to *Table 25* on page 70).

Example: The domain user Bill, uses the computer 'BillLaptop', he is member of the domain groups 'Marketing' and 'Remote users'. The company policy for device access is the following one:

- > Read-only access to DVD/CD for 'Everyone'.
- > 'None' – Low priority access to DVD/CD for 'Remote Users'. You want everybody to have read-only access to the DVD/CD except the members of the 'Remote Users' group. The low priority means that you accept computer-specific exceptions to this rule.
- > Read/Write access to Floppy for 'Domain Users'.
- > Read/Write access to Modem for 'Remote Users'.
- > Read-only access to Removable storage devices for 'Domain Users' Monday to Friday from 07h00 to 18h00.
- > Read/Write access to Removable storage devices for 'Marketing'.
- > Read/Write access to BlackBerry (USB) for user 'Bill' on 'BillLaptop'.



- > Read/Write – High priority access to DVD/CD for user 'Bill' on the computer 'BillLaptop'. Since Bill is a member of the 'Remote Users', he would otherwise not be able to access the DVD/CD. By setting this permission, you let him have R/W access to his DVD/CD drive but only on his laptop.

The next table summarizes these permissions:

<b>Permission</b>	<b>Filter</b>	<b>Priority</b>	<b>User/User Group</b>
DVD/CD	Read	Low	Everyone
DVD/CD	None	Low	Remote Users
DVD/CD	Read/Write	High	Bill* in computer BillLaptop
Floppy	Read/Write	Low	Domain Users
Modem	Read/Write	Low	Remote Users
Removable Storage Devices	Read	Low	Domain Users from Monday to Friday, 7h00 to 18h00
Removable Storage Devices	Read/Write	Low	Marketing
BlackBerry (USB)	Read/Write	Low	Bill* in computer BillLaptop
*Bill uses computer BillLaptop and is member of user groups Marketing and Remote Users (as well as member of Everyone, as all users, and Domain Users if he belongs to the Domain)			
**There is no File Filter defined			

Table 27: Permissions example

When Bill logs onto his laptop, he has the following permissions (refer to previous table and to *Table 25* on page 70):

- > Read/Write access to DVD/CD only on his laptop, Read everywhere else. The priority of 'None' is low and can be overwritten by computer-specific permissions (only when setting its priority as 'High').
- > Read/Write access to Floppy. He gets this right from the 'Domain Users' group.
- > Read/Write access to Modem. He has access to the modem because he is also a member of the 'Remote Users' group.
- > Read/Write access to Removable storage devices. This is the result of the combination of 'Marketing' and 'Domain Users' rights.
- > Read/Write access to BlackBerry (USB). Here there is an exception made just for Bill, and only on his laptop.

## Forcing users to encrypt removable storage devices

Permissions can also be used to force users to encrypt all/some removable storage devices that they use. This decentralized approach can be used for those companies that do not need or do not want to handle a centralized encryption schema using the *Media Authorizer* module (see *Chapter 6: Using the Media Authorizer* on page 129 and *Chapter 7: Accessing encrypted media outside of your organization* on page 149).

The encryption process itself uses our 'Easy Exchange' method to cipher the medium. Please refer to the *Easy Exchange* section on page 159 for more information.

## Setting permissions to force users to encrypt removable storage devices

Forcing a user to do a decentralized encryption is as simple as defining permissions from the Device Explorer module. Once these permissions have been defined, a user that plugs in a removable storage device must encrypt it before being able to use it. In the following sections, we analyze how this encryption is achieved and the vast available alternatives an administrator has.



*Decentralized encryption can only be used for removable storage device between 16MB and 4GB in size.*



## To force decentralized encryption


The process to force a user to do a decentralized device encryption consists of two main phases:

- > The first phase consists of defining permissions for the specific user that must do the encryption. There are two cases here:
  - In a first case you can assign a unique user/group that must do the encryption but do not have access to the media itself. This 'middle agent' can be someone designated to do this ciphering process for all other users. Since this encryption is done in the *Easy Exchange* mode (see page 159), other users do not need to have the Sanctuary Client Driver installed nor have administration rights to use these, as the device has already been encrypted by somebody else.
  - As a second case, you define permissions for each user/group that must do a device encryption before using the media. You define as many permission rules as you need and always two per user/group: one to define that the user must encrypt the device and the other one defining the mode (read/write, etc.).
- > The second, optional phase is to set the Device Log option to 'Enabled' (see *Device log* on page 172). This means that MEDIUM-INSERTED log events are generated when the user inserts a device on his computer. You can use these log events to generate a message pop-up that invites the user to encrypt their device.

In the most complex case, there should be two permission settings for a user/group plus an Event Notification. These permissions can be defined at any level of the *Removable Storage Devices* class: root level, device group, device model, or a specific — uniquely identified — device.

Notice that you can define these permissions at the *Default Settings* level of the *Device Explorer* module (effective for all computers), at the *Machine-Specific Settings* level (to activate decentralized encryption for a specific computer) or at the computer group level.

The following steps summarize this procedure (please refer to *Using the Permissions dialog* on page 57 for a complete description on how to define permissions):

1. Activate the *Device Explorer* module by clicking on the  icon located on the *Modules* section of the *Control Panel* in the main window.
2. Right-click on the Removable Storage Devices class icon and select Permissions (or select the class and use the Ctrl+D shortcut key).
3. Turn on the Device Log option (see *Chapter 8: Setting and changing options* on page 169).
4. Proceed to define encryption permissions for the required user/group with the Encrypt, Export, and Import options activated and the Unencrypted option of the Encryption panel selected. Choose the type of drive and bus. This must be done so that the user/group is forced to encrypt all those unencrypted devices plugged to the computer.
5. Define Read/Write permissions as required. Activate the Decrypt and Import options so that the user can unblock the medium afterwards. Do not forget to add the Encrypted option in the Encryption panel.
6. Optionally — if you want to inform the user of other possible actions or a help message — define an Event Notification for the user/group or class. Please see page 52 for a full description on how to define Event Notifications.
7. The user now receives a Deny Access message along with an invitation to encrypt the device when trying to access the removable media. Encryption is carried out using the *Encrypt* contextual menu option.

The following images are displayed in this process:

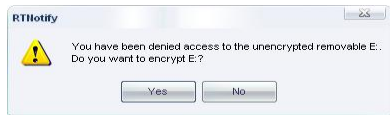
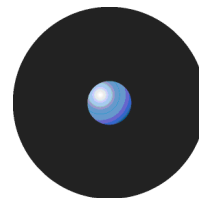


Figure 73: Decentralized encryption: The Access Denied message and inviting the user to encrypt it

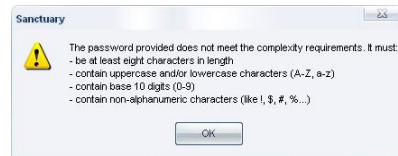


Figure 74: Password complexity is required to encrypt the device

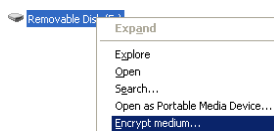


Figure 75: Decentralized encryption: The Encryption option of the contextual menu



Figure 76: Decentralized encryption: Encryption begins

## Examples

### Example 1:

In this first example, we define a decentralized encryption rule for a group at the Removable Storage Devices class root level. All users of the group 'Management' must encrypt their own USB keys and have Read/Write access to encrypted devices. A notification must be defined to inform these users that they must encrypt their devices and should include a help desk number.

The procedure involves the following steps:

1. Define a device group called 'Management removable devices' where all permissions are going to be defined. You can also add some device models here to further classify and outline devices.
2. Define an encryption permission for the group 'Management' at the devices group level.
3. Define a Read/Write permission for the group 'Management' at the devices group level.
4. Define an Event Notification for the group 'Management' informing the need to encrypt removable devices and providing a help phone number.

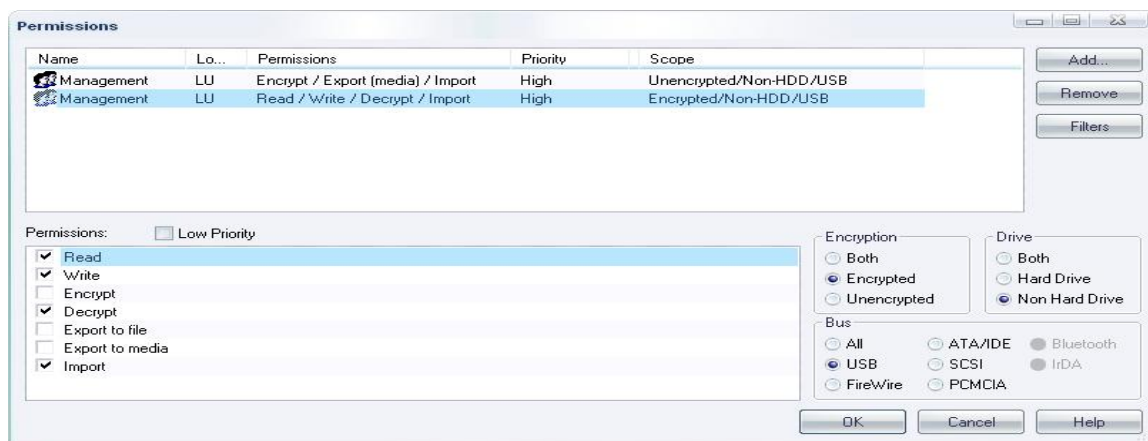


Figure 77: Decentralized encryption for a group defined at a device group level (1/2)



Figure 78: Decentralized encryption for a group defined at a device group level (2/2)



**Example 2:**

The second example deals with a particular user that **MUST** encrypt a unique device: User 'Bill' must encrypt the USB key that he daily uses to show sales info to selected customers. He must, of course, have also read/Write permissions for this, uniquely identified, USB key. He is not informed since he already knows that he must cipher this USB key.

The procedure involves the following steps:

1. Define an encryption permission for 'Bill' for the specific model.
2. Define a Read/Write permission for 'Bill' for the specific model.

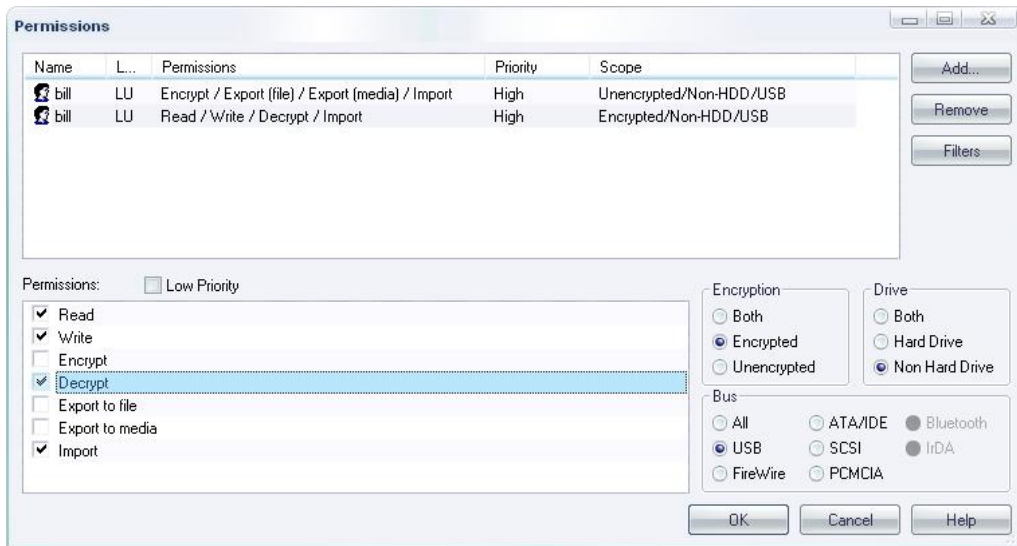


Figure 79: Decentralized encryption at the unique device level (1/2)

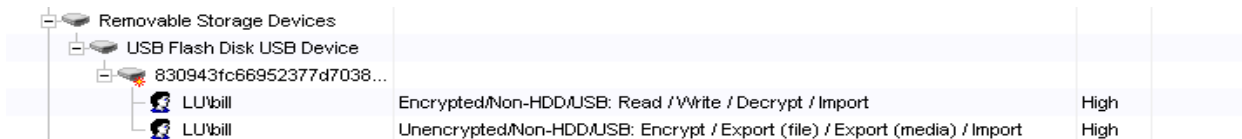


Figure 80: Decentralized encryption at the unique device level (2/2)



### Example 3:

The next example shows how to force everyone to encrypt all devices recognized by the system in the Removable Storage Device class. All users must encrypt their own USB keys and have Read/Write access to encrypted devices.

The procedure involves the following steps:

1. Define an encryption permission for Everyone at the Removable Storage Devices class root level.
2. Define a Read/Write permission for Everyone at the Removable Storage Devices class root level.
3. Optionally define an Event Notification for Everyone informing the need to encrypt removable devices.

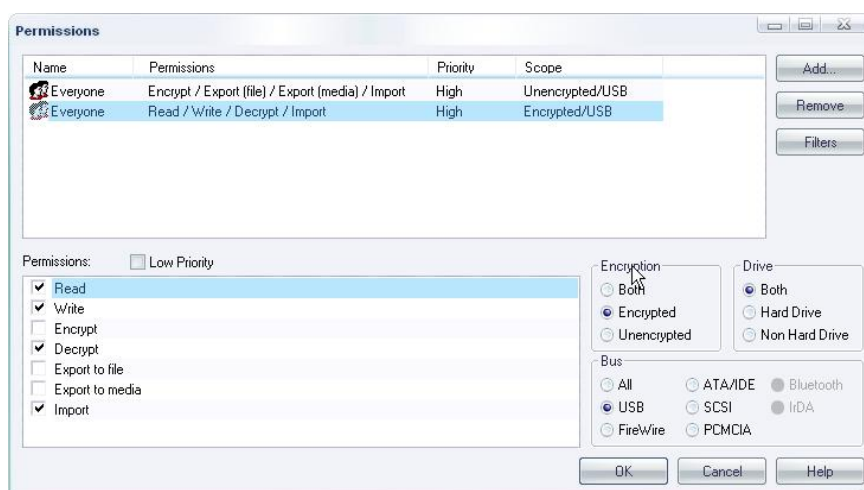


Figure 81: Decentralized encryption at the class level (1/2)

Removable Storage Devices			
Everyone	Encrypted/USB: Read / Write / Decrypt / Import	High	
Everyone	Event Notification: Enabled	High	Message: Call help desk for more info
Everyone	Unencrypted/USB: Encrypt / Export (file) / Export (media) / Import	High	

Figure 82: Decentralized encryption at the class level (2/2)

### Example 4:

The next example shows how to 'delegate' the encryption process to a user and then force all those belonging to a particular group to use only encrypted media. A user is assigned as 'middle agent' to encrypt all Sony USB keys (only approved model for the company). This user has no access to these devices. All user of the 'Marketing' group have Read/Write access for encrypted devices.

The procedure involves the following steps:

1. Define an encryption permission for 'Bill' at the 'Sony USB devices' level.
2. Define a Read/Write permission for 'Marketing' at the 'Sony USB devices' level.
3. Optionally define an Event Notification for 'Marketing' exclusively for the USB Bus informing the need to encrypt removable devices — this should be done at the 'Sony USB devices' level.

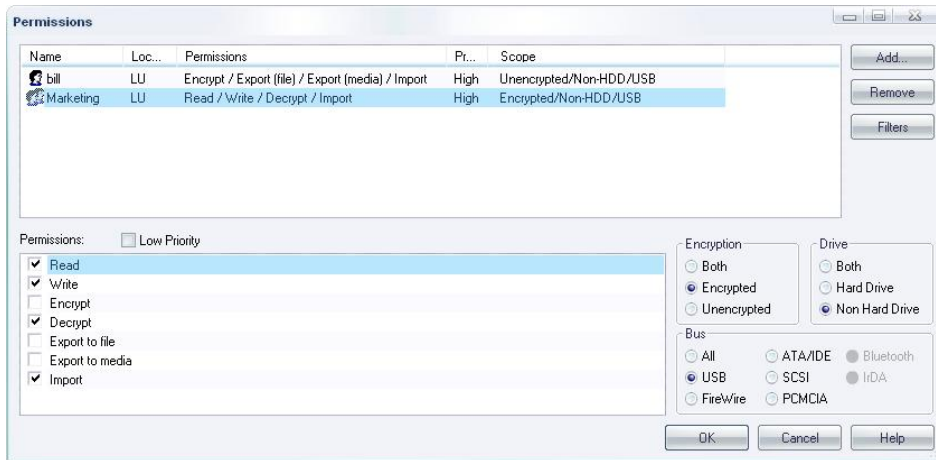


Figure 83: Decentralized encryption using a 'delegated' user (1/2)



Figure 84: Decentralized encryption using a 'delegated' user (2/2)



If the 'Device Log' option is set to 'Enabled', the users that insert a non-encrypted device is automatically prompted to encrypt the device. If the 'Device Log' option is 'Disabled', you must inform the user(s)/group(s) that they receive a 'Drive not accessible message' when trying to access a non-encrypted device. The user must right-click on the device in a Windows Explorer window and choose 'Encrypt medium' to do the device ciphering. You can inform the user via an 'Event Notification' rule. Once the device encrypted, all authorized users have direct access to its data (see Easy Exchange method on page 159).

## Managing devices

All kinds of devices can be attached to the computers in your network. You do not need to know them all in order to protect your company from abuse. When you first install our product, you get a standard list of devices. You can define a general policy for all devices based on the classes of devices that appear by default in the Device Explorer module. If a particular device is not recognized in one of the classes listed in the Device Explorer module — or if it belongs to a class for which the user has no access defined — then the user cannot access the device even though it is attached to the computer.

Nevertheless, if you want to define permissions more precisely, you can set rules for certain models of devices (device types) or specific ones in certain cases (removable devices). In this case, and only in this case, it is your responsibility to set up and manage the different models and specific devices for which you want to define permissions. You do not need to do that for all possible devices plugged on your network.

You can access the *Manage Devices* dialog directly from the *Explorer* → *Manage Devices* item or by making a right-click on the Default Settings section located on the right panel of the *Device Explorer* window.

As an alternative way of managing devices, you can activate the central logging for all machines or a specific one — it is turned off by default —, proceed to the *Log Explorer* module and check the attached device registers. You can then use the right-click menu to open the *Device* dialog (or use the *ADD DEVICES* button). You can enable central logging either for all computers (*Tools*→*Default Options*→*Device Log*) or for a specific one by means of the detailed options of that computer.



You can sometimes find a 'de-synchronization' between the time shown in the 'Manage Device' dialog, the 'Device' dialog, and your local clock. This is due to the dialogs showing respectively the 'connect', 'managed', and 'system' times — not necessary the same in all cases.





## To add a new device

You can add specific models to all the base device classes with exception off the Wireless NICs and PS/2 ports classes.

When you initially connect a new type of device (e.g. a webcam) to a computer controlled by Sanctuary Device Control, the Sanctuary Client Driver may initially block it and log the device type. Once this done, the administrator can then add and set permissions for the new device at the Sanctuary Management Console.

Follow this procedure to recognize a new device:

1. Open the *Manage Devices* dialog by selecting EXPLORER → MANAGE DEVICES or by right-clicking on the DEFAULT SETTINGS item. The following dialog (with all the already managed devices) is displayed:

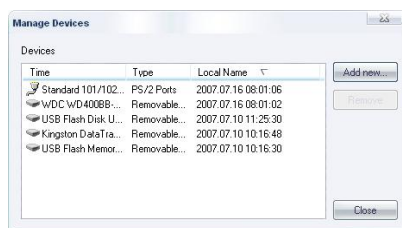


Figure 85: Managing devices

2. Click on the ADD NEW button.
3. Type the computer name and press ENTER. You can use wildcards (\*,?) to do a search or click the ellipsis [...] button to show all available computers logged on to the network:

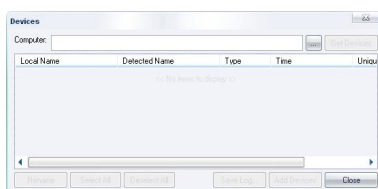


Figure 86: Managing devices - selecting the computer

4. Select a computer from the list by double-clicking or by selecting and pressing ENTER or clicking the OK button.
5. Click the GET DEVICES button. Another dialog is displayed in which you can select the devices you want to add to your Device Explorer control list. Click on the column heading to classify by that field. You can also click the heading of the *Time* column to order the list by the most recent device connected to that computer.

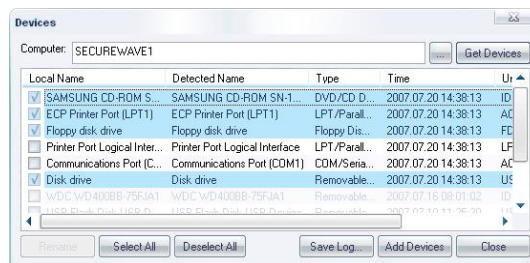


Figure 87: Managing devices - choosing the devices from the selected computer




*The available devices may include different ones within the same or different classes. The list might include, for example, one or more types of digital cameras, and a DiskOnKey memory device, all as separate Removable storage devices. Select the device and use the RENAME button to change to your own description.*



6. Select the devices that you want to add by clicking on the checkbox of the device and then click the ADD DEVICES button. The checkbox disappears and the line grays-out, indicating that the device is now on the list. If you want to keep a log of all devices plugged to the computer, click the SAVE LOG button.
7. Click on the CLOSE button.

Once you close the *Devices* dialog, you return to the *Manage Device* window. This now shows the newly added device(s) as well as the old ones.

Once the new device is listed in the *Device Explorer* window, permissions can be assigned for it just as for any other device.

 *The list of new devices is not sent to the client computer immediately. This list is downloaded the next time a user logs onto that computer. You can, alternatively, send the list immediately by selecting the 'Send Updates to All Computers' or 'Send Updates To' item on the 'Tools' menu (or from the Control Panel).*

## To remove a device

You can delete a device from the list of those available in the Device Explorer list. To do this:

1. Open the *Manage Devices* dialog by selecting EXPLORER → MANAGE DEVICES or by right-clicking on the DEFAULT SETTINGS item.
2. Select the device(s) you want to remove. Use the SHIFT/CTRL key to make multiple selections.

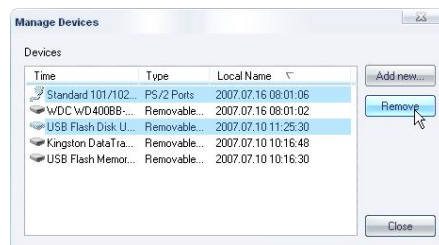


Figure 88: Removing devices

3. Click on the REMOVE button. The following warning message is displayed. Click the YES button to close it.



Figure 89: Confirming the removal of a device

Sanctuary Device Control reverts to the device class permissions for those deleted devices.

## Specific, unique, removable devices

The administrator can also opt for adding a specific, unique, removable USB device identified by its serial number. This has the clear advantage of unmistakably denying/allowing a user or group the right to use this device in a personalized fashion. For example, the administrator can choose to block the access to all removable devices but allow offline access to a personal USB memory key. Follow the steps depicted in *Identifying specific, unique, removable device* on page 37 to add a particular removable device. Alternatively you can do this in the Log Explorer module by right-clicking on *Device-attached* entries (see *To manage devices using the Log Explorer module* on page 125).



## Changing permissions mode

Some devices you add fall into common existing device types. For instance there are various types of removable drives, including devices such as the Iomega Zip drive, notebook PCMCIA card drives and USB DiskOnKey devices, all of which fall into the general category of Removable drives.



*Digital cameras are normally classified as removable drives by Windows. If this is not the case for one of your digital cameras, install the latest drivers of the camera and try again. On rare occasions, some models are classified as Scanners.*

The Device Explorer module lets you apply permissions to a device type as a whole or to control individual devices within the general type. This would allow you, for instance, to permit access to the users members of the domain group 'Marketing' to the Zip drives while prohibiting them access to the DiskOnKey devices and any other removable device for this group. At the same time, your administrators have access to all types of devices whatever their model is. In order to do this, you would have to set permissions on the 'Removable Storage Devices' class for the group 'Administrators' while you add all the different models of zip drives in use to the list of managed devices (see *Managing devices* on page 84 for more information). You would ideally place all different models of Zip drive readers in a device group (see *Device Groups* on page 55 for details) and set permissions for this group of devices for the domain group 'Marketing'.

- > To set permissions to the whole class, select the device on the *Default settings* section and right-click on it selecting the type of *Permissions* you need from the popup menu. You can assign general, online, offline, schedule, shadow, and copy limit permissions to the device as a whole.
- > To set a per-device permissions within the type, open the class (use the + key) on the *Default settings* section, right-click on the device, and select *Permissions*. You can assign general, online, offline, and schedule permissions to specific devices in the general class.

Follow the previously described procedure to assign the desired type of permission needed.

## Priority options when defining permissions

When you change permissions, you can see an option for setting the priority of the rule assigned to a device (at the class or specific level):

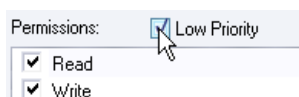


Figure 90: Priority setting

The following practical example clarifies its purpose:

In your 'example' company, every domain has the right to burn CDs. To allow this, you define a Read/Write access for domain users at the Default Settings level. You want to make an exception to this recently created rule: a group of users called 'Key data owners' should not be allowed to burn CDs on every machine. You define a negative permission (None) for this group at the Default Settings level. Now you are set and they cannot burn CDs anymore.

Extending our example further, you want them to be able to burn CDs using a specific computer especially prepared to do this job. This machine should also have a Shadowing rule for all burned data, for all users. You now need to define for this computer or group of computers a special permission with Read/Write rights on the CD for all the 'Key data owners' plus a rule to Shadow the data being burnt (write). This new rule does not work UNLESS you define a 'None' permission (not Read nor Read/Write) at the Default Settings level with a Low priority. This Default Settings permission rule is overridden by a machine-specific permission rule.



The following table explains what is the resulting access when permissions are defined between protecting a general device type (class) and a specific device from that class (see also *Table 25* on page 70).

<i>Device level where the permission is defined</i>	<i>Permission applied</i>	<i>Priority</i>	<i>Result to apply to the specific device</i>
Class	None	High	None
Model	Read/Write	Low	
Class	None	Low	Read/Write
Model	Read/Write	High	
Class	Read/Write	High	None
Model	None	High	
Class	None	Low	None
Model	Read/Write	Low	
Class	Read	High	Read/Write
Model	Read/Write	Low	
Class	Read	Low	Read/Write
Model	Read/Write	High	
Class	Read/Write	High	Read/Write
Model	Read	High	
Class	Read	Low	Read/Write
Model	Read/Write	Low	

Table 28: Resulting access

The permission settings go from high to low level in this order:

<i>Permission setting</i>	<i>Order</i>
None	↓
Read/Write	
Read	

Table 29: Permission settings priority



You can also distinguish between two removable devices of the same make by using the *Media Authorizer* module to centrally encrypt the devices.

## Informing client computers of permission changes

Whenever you make a change to the device permissions in the *Device Explorer* module, the client computers need to be notified that something has changed in the list of authorized devices. You can do this manually, or leave the system to do it automatically at the next client logon or re-boot. Generally, it is advisable to send updates to computers manually.

If you have made a change to a global device class, then select *Send Updates to All Computers* from the *Tools* menu (or from the *Control Panel*).

The following dialog is displayed when you choose the *Send Updates to All Computers* command:

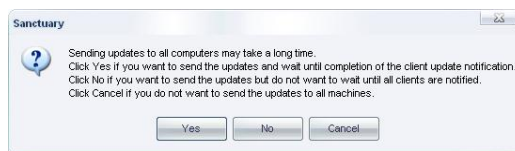


Figure 91: Sending updates to client computers

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

If you have made a change to an individual computer, then right-click on the computer in *Device Explorer* module and select *Send Updates to: <computername>* from the popup menu (or select the same option from the *Tools* menu or from the *Control Panel*).

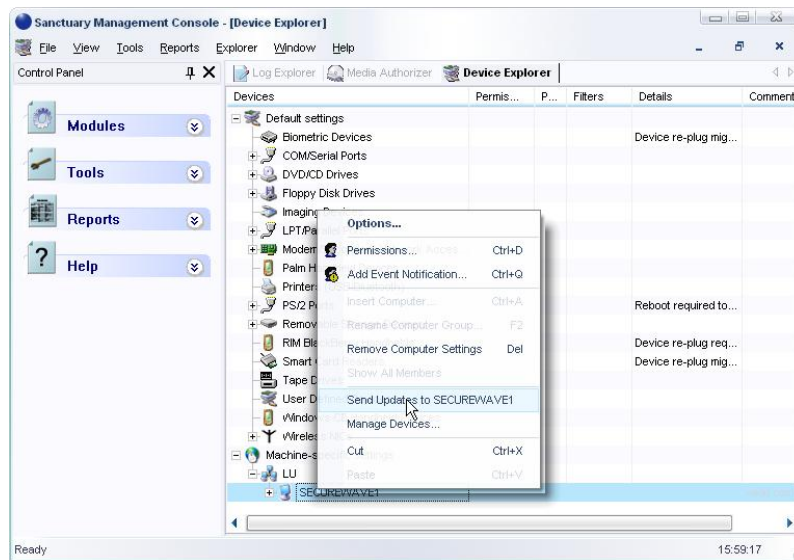
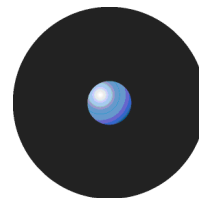


Figure 92: The send update item from the contextual menu

You do not need to use the *Send* command when you set *Temporary Permissions*. This type of permission is sent out automatically as soon as it is set.

Any computer that is switched off or disconnected from the network receives the updates next time it is connected or booted.

*✍ If a computer does not receive updates when you select 'Send Updates to All Computers' or 'Send Updates To', open the 'Online Machines Report' and check if the machine is present in the list. See Online Machines report on page 187. A machine that is not in the list will never receive updates when you select to send them. You can ask the user to select the 'Refresh settings' command in the right-click (contextual) menu of the Sanctuary Client Driver icon located on the system tray. If the user does not get the latest permissions, you should try rebooting the client computer. After rebooting, it should appear in the online table. If not, check the connectivity between the client machine and the SecureWave Application Server. You can use the pingsxs.exe utility on the client machine to check the communication. This tool is located under the BINTools directory of your Sanctuary Device Control Media.*

*✍ Your users can request the latest permissions from the SecureWave Application Server by using the 'Refresh Settings' command from the right-click (contextual) menu of the Sanctuary Client Driver icon located in the system tray.*



---

## Chapter 5: Using the Log Explorer

### Introduction

The Log Explorer module is used by Sanctuary Device Control for three distinct purposes:

- > To view information about input/output device actions that users have attempted to, or actually, carried out. For example, you can review attempts to access or connect unauthorized devices, or view records of files copied to authorized devices.
- > To view audit information about the actions carried out by administrators, including changing user access rights and device permissions.



*In previous versions of Sanctuary this second function, to audit administrator actions, was carried out using the Audit Log Viewer module. The functionality of this module has been incorporated into the Log Explorer module. The Audit Log Viewer module no longer exists.*

- > To generate automatic reports containing either details of input/output device actions or administrator actions. These can be scheduled to run at regular intervals between specified start and end dates.

You can set up templates in the Log Explorer module that enable you to generate customized reports quickly and easily. These templates contain the criteria you want to use to select the results in the report. They also contain details of what information is displayed for each result in your report.

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


### Monitoring user input/output device actions

There are four main types of information that you typically focus on when reviewing the input/output actions of users. These are:

- > Unsuccessful attempts to access I/O devices on the client machines: When a user tries to read from, or write to, a device for which no permissions are defined, the operation is traced. Other user actions such as reaching a data transfer quota, attaching a device to the computer or trying to use a protected WLAN interface are also traced. By default, central device logging is turned off. It can be enabled for all computers (*Tools*→*Default Options*→*Device Log*) or for a specific machine, by means of the detailed options of that computer.
- > When a device is connected or disconnected from a computer: This information is always logged. It is reported as *Device Attached*, you can then choose to add the device immediately by selecting the device register and then clicking on the ADD DEVICE button located on the lower right part of the screen. (If the log file was generated using a previous version of the client driver, this option might not be available.) Please see *Managing devices* on page 92 for a full description on how to add specific devices.
- > Client errors: Log entries are generated by events such as failure to burn a DVD/CD in an unsupported format, or failure to communicate with the application server because of a mismatch between the server private key and a client public key. By default, device logging is turned off. It can be enabled for all computers (*Tools*→*Default Options*→*Device Log*) or for a specific one by means of the detailed options of that computer.
- > Files copied from a PC to an authorized device: Sanctuary uses shadowing to record either the names or contents of the copied files. By default, shadowing is turned off. You can enable it for either all users or a





particular user. To do this, go to the Device Explorer module, right-click on the device you want to shadow and select *Shadow*. (Alternatively, use the shortcut key CTRL+W). Typically, you should monitor what authorized end-users copy or read, to or from a floppy, recordable DVD/CD, or removable drives. You may also want to extend such control over LPT and COM ports.

 *Shadowing is available for files copied/read to/from the following device types: Floppy disk, DVD/CD-ROM, Removable Media (depending on the shadowing rules defined, encrypted media can also be shadowed), Modem, LPT and COM. Shadowing a Modem or the LPT or COM ports results in a raw binary data shadow file. In some of these devices, you can only activate the 'name' option, not the full copy.*

*See Appendix A: DVD/CD Shadowing on page 191 for details of what can and cannot be shadowed when writing or reading, to or from a recordable CD/DVD.*

*Shadowing and Device logging rules are defined per-device and per-user. You can define different settings for users logging on the same machine.*

 *If the 'Log (Device Control)' access of the Sanctuary Management Console Administrator User Access is set to 'No', the currently logged administrator cannot use the Log Explorer module. Furthermore, if the 'Logs w/o File Access (Device Control)' is set to 'No', the administrator cannot see the contents of the file (even when enabling full shadowing). See *Defining Sanctuary administrators on page 32* for more details.*


 *If the 'Attachment' field of a file is set to 'true', then the content file has been shadowed. This only happens if full shadowing is active. You may or may not have access to this entry, depending on the role assigned to you by the 'Enterprise Administrator'.*

*The administrator has the option of explicitly requesting the log files from any client computer to display them using the 'Log Explorer' module. Although this is a very practical way of analyzing log entries of a specific machine, it can also cause some file operations to fail at the client side. Use this command cautiously and privilege the criteria settings (computer field) or change the log options in the 'Default Options' dialog (see *Chapter 8: Setting and changing options on page 169* for more details).*

*Some external WiFi cards are reported twice in the Log Explorer records. This is because they are first classified as Modem/Secondary Network Access Devices and then as Wireless NICs.*

Sanctuary Device Control monitors data as it is generated by the client application. For instance, shadowing a USB memory stick fetches the files copied/read — name or name and content, depending on the selected shadowing option — and places an entry in the log.

The files are automatically transferred from the client to the SecureWave Application Server according to the transfer options. By default, files are transferred every sixty minutes. You can also retrieve the latest shadow and log files from the client computers by selecting *Fetch Log* in the *Explorer* menu, by clicking **FETCH LOG**, or the **QUERY** button.

 *If you choose 'Fetch Log' while a user is copying data to a media, or if the automatic transfer of shadow files occurs while the user is copying data, the copy may fail.*

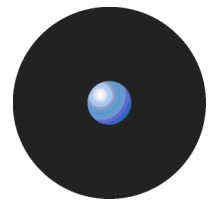
In addition to using the Log Explorer module to view user input/output actions, you can also use it to add specific, uniquely identified devices and afterwards assign them permissions using the Device Explorer module (see *Chapter 3: Using the Device Explorer on page 47*).

## Monitoring administrator actions


Sanctuary Device Control provides full auditing of all administrator actions including changes of user and/or system access rights to certain devices. You can also use the Log Explorer module to display the changes made to device permissions as well as any DVD/CD/Encrypted media added or removed from the database and any DVD/CD/Encrypted media assignment done.

You can, for example, view the following information about administrator actions:






- > Dates and times when changes were made.
- > Domains and usernames of the people who made the changes.
- > Domains and users/user groups to which the changes apply.
- > Names of target computers, where rules are applied to specific computers.
- > Devices to which the changes apply.
- > Permissions applied to the devices.

 If the 'Audit (Device Control)' option of the Sanctuary Management Console Administrator User Access is set to 'No', the currently logged-in administrator is not able to see or use the Log Explorer module to view administrator actions. Please refer to the Defining Sanctuary administrators section on page 32 for more details.

 Comments (added in the Device Explorer module) are not shown in the Log Explorer.

## Accessing the Log Explorer

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

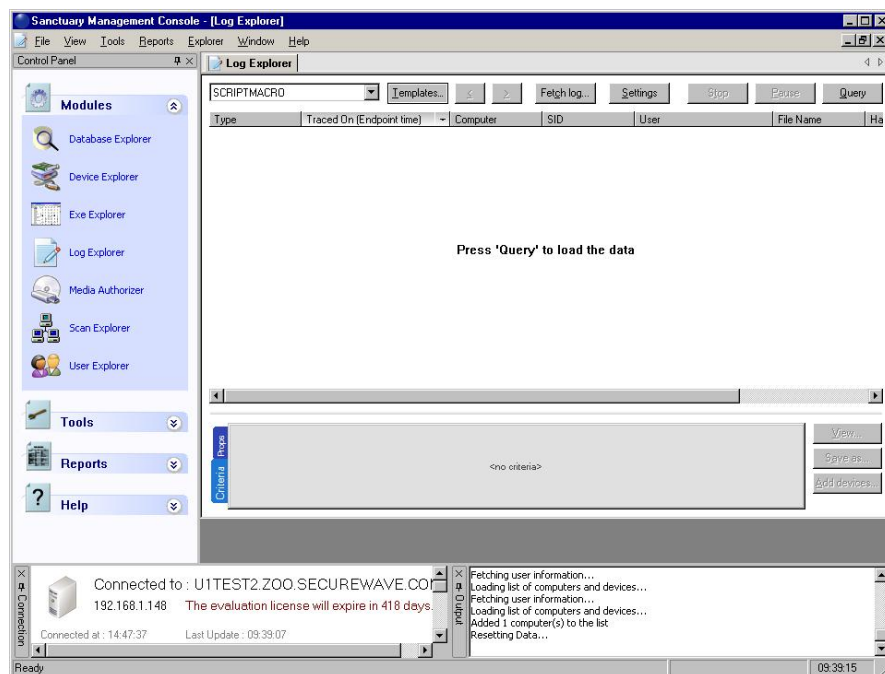
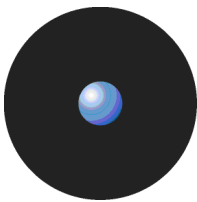


Figure 93: The Log Explorer main window



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

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

\* Current User means that you have logged in to Windows and Sanctuary Management Console as the same user. See *Log in as a different user* on page 20.  
 \*\*A user needs to have both permissions on machine wide DCOM security, and the permissions set in DCOMCNFG to successfully use DCOM. See [www.microsoft.com/technet/prodtechnol/winxppro/maintain/mangxpsp2/mngsecps.mspx](http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/mangxpsp2/mngsecps.mspx).

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

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

To correctly configure DCOM (dcomcnfg.exe):

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

Table 30: Limitations while using the Log Explorer module under other user/domain account



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

## Log Explorer templates

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

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

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



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

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

### To use an existing template

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

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

*The query only returns results if you have appropriate access rights to view it. See Defining Sanctuary administrators on page 32 for more details.*

### To create and use a new template

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

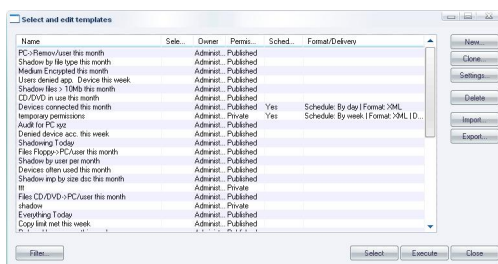


Figure 94: The Select and edit templates window

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

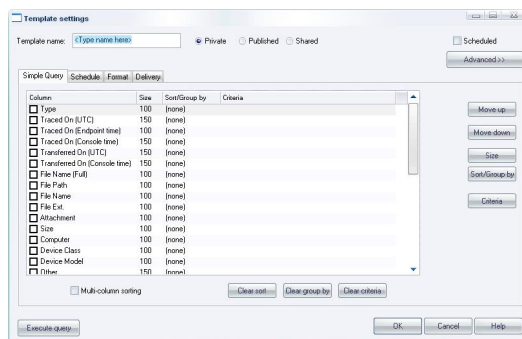



Figure 95: The Templates settings window



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

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


To select log entries that match certain criteria, select the Column to which the criteria apply, by clicking on the appropriate box, clicking  in the Criteria column, and specifying what you want to match entry details to. See *Table 33* on page 116 for instructions on how to define query criteria.

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

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

For more information, see *Schedule tab* on page 118.

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

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

 *The template is stored when you execute the query.*

If there are any records that match your query criteria, they appear in the Results panel list of the Log Explorer window (and your custom reports). The query only returns results if you have appropriate access rights to view it. See *Defining Sanctuary administrators* on page 32 for more details.

## Log Explorer window

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

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

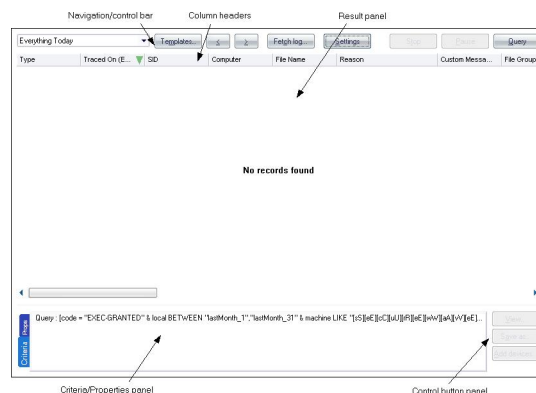
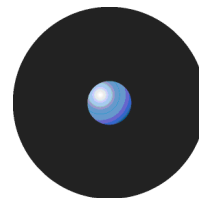


Figure 96: Components of the Log Explorer window

## Navigation/Control bar

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



Figure 97: Navigation/Control bar

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



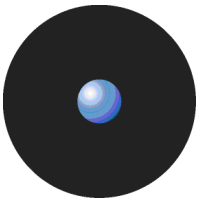
*In previous versions of Sanctuary the templates list included all templates created by you or by SecureWave. All templates can be accessed by clicking on the TEMPLATES button.*

- > TEMPLATES button — used to create a new template or select an existing one from the list in the Select and edit templates window.
- > ⏪ (Previous) button — navigates to the preceding result list from the ones internally stored, if you are carrying out multiple queries.
- > ⏩ (Next) button — navigates to the following result list, if you are carrying out multiple queries.
- > FETCH LOG button — retrieves logs and shadow files from a computer or a list of computers running the Sanctuary Client Driver. The Select Computer window is displayed. See *Forcing the latest log files to upload* on page 124.
- > SETTINGS button — goes directly to the advanced settings dialog for the template you are currently using. Here you can select columns and define criteria. See *Template settings window* on page 113.
- > STOP button — cancels the current query. This is used if you want to interrupt a lengthy sorting operation involving a large number of log entries.
- > PAUSE button — cancels the screen output, with any sorting processes continuing in the background. To resume the screen display, click on this button again.
- > QUERY button — retrieves all log entries that match the criteria defined in the current template.

## Column headers

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

- > Sort results — classify the results and display them in a specified depending on the value for the log entry (or log entries) in one or more columns.
- > Show/hide columns — determine what information is displayed for each result in the report.
- > Change the size of the displayed columns — by dragging the column header dividers to the left or right.



- > Change the order in which the columns are displayed — by dragging and dropping the column titles in the column headers.
- > Group log entries — display a single report row corresponding to multiple log entries grouped according to the values in one column.
- > Display computed columns — display calculated values such as a count of the number of log entries in a grouped result, the maximum value, minimum value, sum of values, or average value.



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



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



*You can also use the column context menu to access the advanced query settings for the template. For more information about defining complex queries see *Query & Output* tab on page 116.*

## Sorting results

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

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



Figure 98: Column headers showing multiple classifications



### Show/hide columns

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

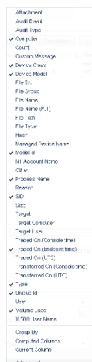


Figure 99: Columns context menu

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

### Group log entries

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

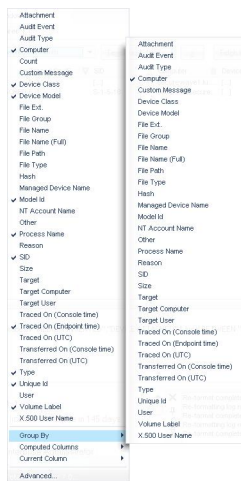


Figure 100: Group By option

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

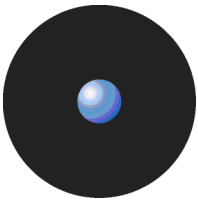


Figure 101: Column headers showing grouped results

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



Figure 102: Column headers showing sub groups



## Computed columns

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

The operations supported by computed columns are:

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

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

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

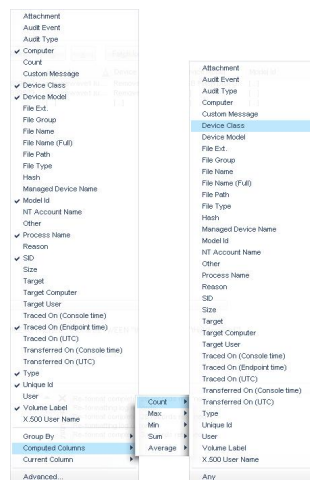


Figure 103: Computed columns

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

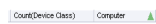


Figure 104: Column headers showing a computed and a sorted column

## Clear column settings

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

- > Proceed to the *Template settings* window. For more information see *Template settings window* on page 113.
- > Change the column settings of the currently selected column. To do this, select the Current Columns option in the Column context menu and select the relevant choices, for example Unsort or Ungroup.



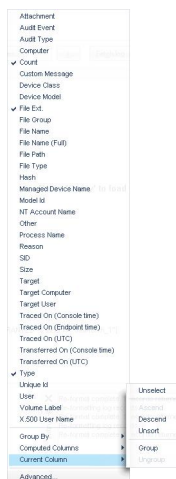


Figure 105: Resetting column headers

## Results panel / custom report contents

The Results panel is the main area of the *Log Explorer* window where the results are displayed and classified. You can save the information displayed as a CSV file using the **SAVE AS** button of the *Control button* panel (in the bottom right corner of the Log Explorer window).

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

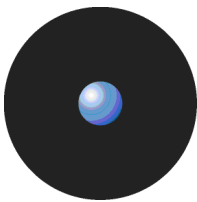
## Columns in Results panel / custom report

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

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

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

<b>Column</b>	<b>Description</b>	<b>Failed access attempt</b>	<b>Client Error report</b>	<b>Shadow -ing</b>	<b>Adminis -trator audit</b>
Attachment	If true, then a shadowed content can be visualized.	No	No	Yes	No
Audit Event	The nature of the event that triggered the audit log. See <i>Audit events</i> on page 126 for a description of the different audit events that can be recorded.	No	No	No	Yes
Audit Type	The type of action the administrator carried out. This can be 'Device Control' or 'Application Control'.	No	No	No	Yes
Computer	Machine name where the event was recorded.	Yes	Yes	Yes	No
Count	If grouping is active, shows how many log entries are hidden. Otherwise is a column of computed data.	Yes	Yes	Yes	Yes
Device Class	When available, device class. The device class can be Removable Storage Devices, Floppy, DVD/CD, etc.	Yes	No	Yes	No
Device Model	Manufacturer's device name.	If available (device-attached event)	No	No	No
File Ext	Contains the extension of the file involved in the access to the device, if any.	Yes	No	Yes	No
File Name	Contains the name of the file involved in the access to the device, if any.	Yes	No	Yes	No
File Name (Full)	Contains the full name (including path) of the file involved in the access to the device, if any.	Yes	No	Yes	No
File Path	When relevant, path to the file on the device.	If available	No	Yes	No



Column	Description	Failed access attempt	Client Error report	Shadow-ing	Adminis-trator audit
Hash	Unique identifier of the medium (DVD/CD or removable) inserted.	If available (DVD/CDs and encrypted media)	No	No	No
Managed Device Name	Device name as defined in the Device Explorer module. This is useful if you renamed devices, say replacing the standard names of some devices with say 'Sony key used by developers' in order to define a policy for them.	No	No	No	No
Model Id	Indicates the model of device on which the user performed some action.	Yes	Yes	Yes	No
NT Account Name	Domain user name of the person who triggered the event, for example 'MyDomain/MyUser' or LocalSystem.	Yes	Yes	Yes	Yes
Other	This may contain the access mask or DVD/CD serial number details, or additional information, in the case of an audit event, for example if an administrator erases a scheduled permission, this may contain its parameters.	Yes	No	No	Yes
Process Name	Process involved in the access to the device.	Yes	No	No	No
Reason	Indicates whether an action was granted or denied. This can have a value of 'NoPermission', 'Granted' or 'Denied'.	Yes	Yes	Yes	Yes
SID	The Secondary Identifier of the user. This is useful when attributing actions recorded in log files to users who have has left your organization.	Yes	Yes	Yes	Yes
Size	Size of the shadowed file.	N/A	N/A	Yes	No
Target	The device for which the permissions were modified.	No	No	No	Yes
Target Computer	Name of the computer that was the target of the administrator action.	No	No	No	Yes
Target User	Name of the user or group to which the administrator action was applied.	No	No	No	Yes
Traced On (Console time) *	Date the event occurred on the console computer.	Yes	Yes	Yes	Yes
Traced On (Endpoint time) *	Date the event occurred on the client computer.	Yes	Yes	Yes	Yes, if available.
Traced On (UTC)*	Date (Coordinated Universal Time) the event occurred on the client computer.	Yes	Yes	Yes	Yes
Transferred On (Console)*	Date the event record was transferred from the client computer to the SecureWave Application Server.	Yes	Yes	Yes	Yes, if available.
Transferred On (UTC)*	Date (Coordinated Universal Time) the event record was transferred from the client computer to the SecureWave Application Server.	Yes	Yes	Yes	Yes
Type	The nature of the event that triggered the log. For audit events see page 126.	No	No	Yes	Yes
Unique Id	The serial number of the device on which the user performed some action.	Yes	Yes	Yes	Yes
User	Name of the user who triggered the event, e.g. 'MARVIN/johns'. Also see note after table. The same information is displayed even if a user is removed from the Active Directory providing the log entries were generated by a Sanctuary 4.2 client. This enables the person who triggered an event to be identified after they have left your organisation.	If available	No	Yes	Yes
Volume Label	Tag of the volume for which an event was recorded.	If available	No	No	No
X.500 User Name	The username in Lightweight Directory Access Protocol format. This reflects the directory tree in which the user information is stored, for example, the X.500 user name may be 'CN=John Smith, CN=Users, DC=Marvin...'	Yes, if available.	Yes, if available.	Yes, if available.	Yes, if available.

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

Table 31: Log Explorer module column meaning



*If the 'User Name' column is empty for some shadow records, you must use the 'Synchronize Domain Names' command from the 'Tools' menu. If this does not display the user names, you could try to synchronize directly to the machine's domain where the shadow files were created (using the same command). It could be a local user who created the shadow files. If you are using a Novell environment, you should try running the synchronization script described in the Sanctuary's Setup Guide. You can also automate this script's execution for your convenience.*



- ✍ Columns with names starting 'Count', 'Min', 'Max', 'Sum' and 'Average' may also be displayed. These contain computed data based on the values in the specified columns. See *Computed columns* on page 108.
- ✍ Ellipses (...) in the Results panel indicate hidden log entries. For example, if you group a set of results using the value in one column, then the multiple values in some other columns for the results group are shown as [...].

## Criteria/Properties panel

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

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

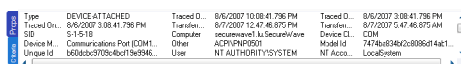


Figure 106: Props tab

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

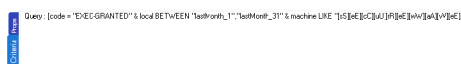


Figure 107: Criteria tab

## Control button panel

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

- > VIEW – to see shadow data. See *Viewing shadow files* on page 122.
- > SAVE AS – to save the information in the *Log Explorer Results panel* data as a CSV file.
- > ADD DEVICES – to directly manage and add those devices not recognized and shown in the *Log Explorer Results panel*.



Figure 108: Control button bar

## Select and edit templates window

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

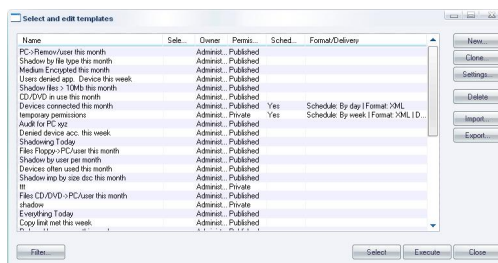





Figure 109: Select and edit templates window

The Select and edit templates window contains the following:



- > List of all the existing templates that you can access assuming this list is not filtered — see below). These may be created by yourself, one of your colleagues, or SecureWave. You can select a template and right-click to display a Templates context menu.
  -  *The asterisk (\*) in the Selected column indicates the template that is currently selected. You can either change the settings of this, or another highlighted template. To select a different template, highlight it in the list and click on the SELECT button.*
  -  *The Permissions column in the Select and edit templates window indicates whether the template can be viewed or changed by people other than the owner. The Scheduled and Format/Delivery columns indicate whether the template is used to create automatic reports periodically and, if so, who these are emailed to and/or where they are stored.*
  -  *You can click on the column headers to sort this list, or drag and drop the column titles to reorder the column information.*
- > NEW button — to create a template (see *To create and use a new template* on page 103).
- > CLONE button — to create a new template based on an existing template (with the Shared and Scheduled flags removed, if these were present in the original template).
- > SETTINGS button — go directly to the Template settings window for the selected template. Here you can define the criteria used to select results and choose how the results are displayed. For more information see *Template settings window* on page 113.
- > DELETE button — to remove a selected template.
- > IMPORT button — to import templates in XML format or to import legacy templates (\*.tmpl) from the registry.
- > EXPORT button — to export the highlighted template to an XML file.
- > FILTER button — to choose which templates are displayed in the Select and edit templates window. See below.
- > SELECT button — to select the highlighted template as the current template and return to the main Log Explorer window.
- > EXECUTE button — to retrieve all log entries that match the criteria defined in the current template and display these in the Log Explorer window.
- > CLOSE button — to return to the Log Explorer window without changing the current template.

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

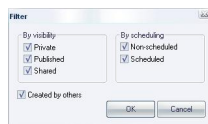
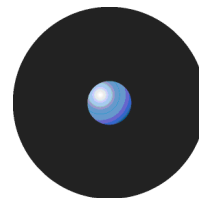


Figure 110: Filter templates dialog

The following template filters can be used:

Checkbox	Used to display...
Private	Templates that are only visible to the owner (and Enterprise Administrators).
Published	Templates that are visible to all Sanctuary Management Console users within your Sanctuary system, but can only be changed by the owner (and Enterprise Administrators).
Shared	Templates that can be seen and changed by all Sanctuary Management Console users within your Sanctuary system.
Non-Scheduled	Templates used to generate ad hoc reports.
Scheduled	Templates that are automatically executed periodically to generate regular reports. These are either saved in a shared folder on your Network or emailed to specified recipients.
Created by others	Templates created by other people. This is unchecked, for example, by Enterprise Administrators when they want to display only their own templates.

Table 32: Template Filter checkboxes



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

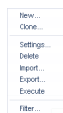


Figure 111: Templates context menu



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

You can use the Templates context menu to:

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



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

## Template settings window

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

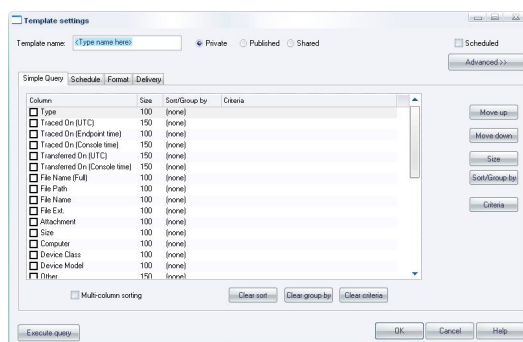
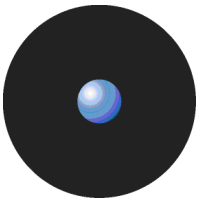


Figure 112: Template settings window – Simple Query tab

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

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



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

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

## Simple Query tab

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

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

File Type	Count(Type)	Computer	Traced On (En...
Executable	641 [1-]	[1-]	[1-]
Script	56 [1-]	[1-]	[1-]

Figure 113. Grouping results in the query

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

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



If you want to use specify a complex set of selection criteria or display settings, click on the ADVANCED button and enter information on the Query & Output tab. For more information see Query & Output tab on page 116.

- > Decide the column display order — using the MOVE UP and MOVE DOWN buttons located on the right of the window.



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

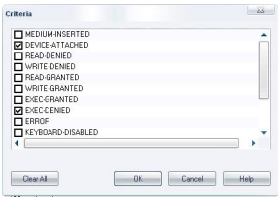
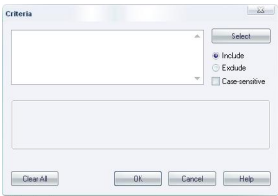
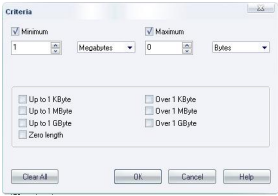
## Criteria

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

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

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

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

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



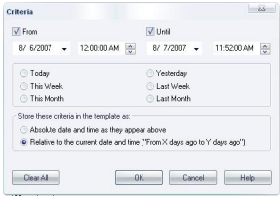
Criteria Dialog	Description
	<p><b>Time criteria</b></p> <p>This form of the Criteria dialog is used to search for log entries that were produced, or uploaded to the server, at a certain date/time.</p> <p>You can enter any period into the 'From' and 'Until' controls, or click one of the commonly used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

Table 33: How to use the available criteria dialogs

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

Column	Size	Sort/Group by	Criteria
<input checked="" type="checkbox"/> Type	100	(none)	MEDIA-INSERTED DEVICE-ATTACHED
<input checked="" type="checkbox"/> Traced On (Endpoint time)	100	Descending	Entries generated this week
<input checked="" type="checkbox"/> Computer	30	(none)	SECUREWAVE1
<input checked="" type="checkbox"/> Device Class	100	(none)	DVD/CD Drives Floppy Disk Drives Imaging Devices
<input checked="" type="checkbox"/> Model Id	150	(none)	
<input checked="" type="checkbox"/> Volume Label	100	(none)	
<input checked="" type="checkbox"/> Traced On (Console time)	150	(none)	From 8/7/2007 to 8/7/2007 11:58:52 AM
<input checked="" type="checkbox"/> Size	100	(none)	At least 1 Megabytes
<input checked="" type="checkbox"/> User	150	(none)	
<input checked="" type="checkbox"/> SID	100	(none)	
<input type="checkbox"/> Processor Name	150	(none)	
<input type="checkbox"/> Unique Id	150	(none)	
<input type="checkbox"/> Device Model	100	(none)	
<input type="checkbox"/> Traced On (BUTC)	150	(none)	
<input type="checkbox"/> Translated On (BUTC)	150	(none)	
<input type="checkbox"/> Translated On (Endpoint time)	150	(none)	

Figure 114: Example of criteria settings

## Query & Output tab

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

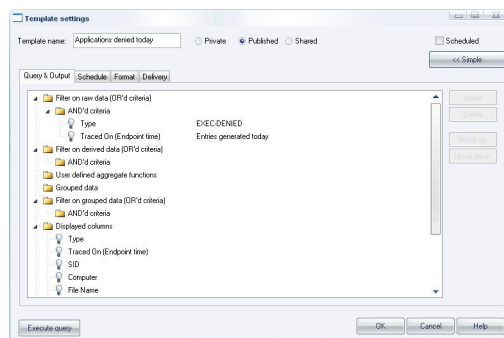


Figure 115: Query & Output tab

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

- > 'Filter on the raw data' — specify the criteria, based on information actually in the log entries, used to select results to be included in reports generated using the template. For example, if you specify an 'AND'd criteria' of Type and the criteria MEDIA-INSERTED the report includes events when a user inserts a DVD/CD in their computer's drive.





- > 'Filter on derived data' — specify the criteria, based on information derived from the Sanctuary Management Console, used to select results to be included in reports. For example, you can specify an 'AND'd criteria' of Traced On (Console time) or User.
- > 'Display user defined aggregate functions' — such as the sum, minimum, maximum, or average of values contained in the log entries.
- > 'Group the data' — produce a single result corresponding to multiple log entries with the same value for a particular field. You can, for example, group log entries by Type or Traced On (UTC) date.
- > 'Filter on grouped data' —determine whether the report generated using the template only displays results where the values for the computed columns match specified criteria.
- > Display columns — determine which columns are displayed and their order.
- > Sort the data — determine the order in which rows of results are displayed.




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

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

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

To set up and use a complex query:

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

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



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

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

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

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

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

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



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

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

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

## Schedule tab

The Schedule tab is used to define the following:

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



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

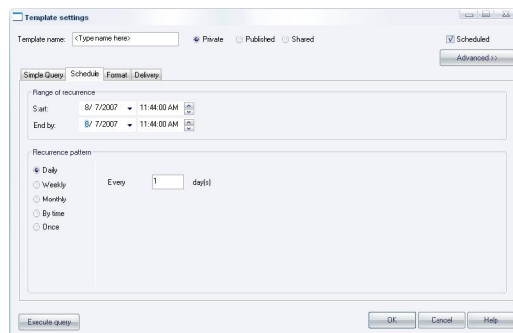


Figure 116: Schedule tab

## Format tab

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

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

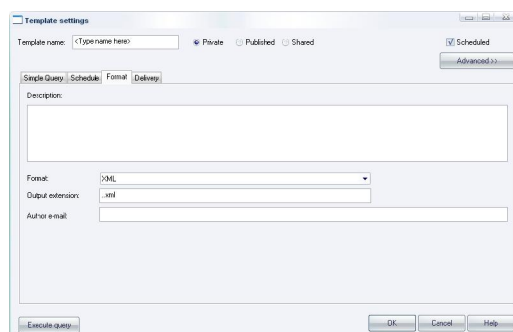


Figure 117: Format tab



## Delivery tab

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

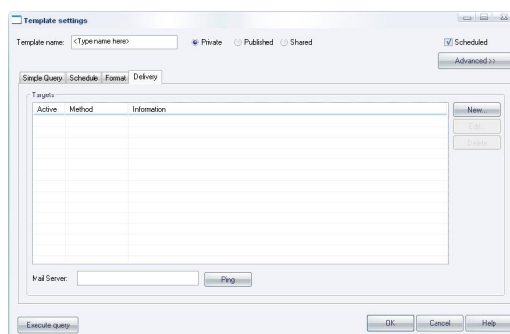


Figure 118: Delivery tab

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

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



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



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



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

To set up a new target:

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

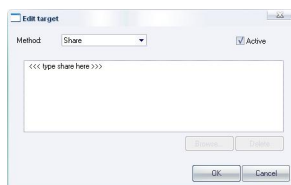


Figure 119: Edit target dialog

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



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

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

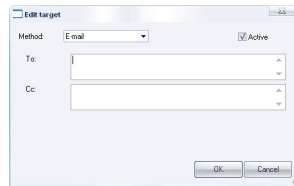


Figure 120: Edit target dialog (E-mail)

4. Click on the OK button.

## Viewing access attempts to devices

The *Computer*, *Traced On*, and *Transferred On* fields are always present in the logs for every event associated with input or output devices. You can list the following access event types when specifying the criteria for matching with log entry *Type* information:

- > **MEDIUM-INSERTED:** This event occurs when a user inserts a DVD/CD in their computer's drive or a media in a removable media reader, for example, this event is logged when a user inserts a Zip disk in a Zip drive . The following information is normally available:

- **Device type:** For example 'CD'.
- **Volume label:** Contains the medium tag. This is empty for encrypted media.
- **Medium hash:** Contains the hash number of the inserted medium (used by SecureWave technical support).
- **Other:** Contains the serial number of the medium (used by SecureWave technical support).



*This event can take place when no user is logged in or when several users are logged in at the same time (remote desktop). In Sanctuary 4.2 the user name provided for this event is the name of the currently logged on interactive user. If nobody is logged on when the device is inserted, the LocalSystem user is logged on.*

- > **DEVICE-ATTACHED:** This event occurs when a device is connected to a computer, for example a memory stick may be plugged into a USB port. The device name is logged.



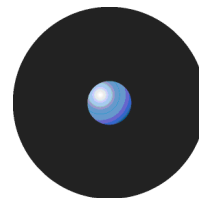
*This event can happen without any logged user or with several of them logged at the same time (remote desktop). In Sanctuary 4.2 the user name provided for this event is the name of the currently logged on interactive user. If nobody is logged on when the device is inserted, the LocalSystem user is logged on.*

- > **READ-DENIED:** This event occurs when a user tries to access an unauthorized device. The following information is normally available:

- **Device type:** For example, DVD/CD, floppy disk, removable storage devices, COM, LPT, etc.
- **Volume label:** The floppy disk, DVD/CD, or removable device label.
- **File Name:** The name of the file the user was attempting to read. A backslash indicates that the read attempt was carried out on the root folder of the medium.
- **User Name:** The name of the user who tried to access the protected device.
- **Process Name:** The application used by the user to try to access to the protected device.
- **Other:** The exact access mask, in hexadecimal format, used by the application to try to access the protected device (used by SecureWave technical support).



*Several identical log entries may appear as some applications, for example Windows File Explorer, retry automatically when there are unsuccessful access attempts to protected devices. An appropriate setting of the Device log throttling option significantly reduces the volume of redundant information logged. See the option description on page 173.*



*System or svchost can execute not impersonated mount requests for an encrypted media when the media encryption keys are not present on the client machine. As these requests are not identified, the User Name field cannot be retrieved and the corresponding field in the log is empty.*

> **WRITE-DENIED:** This event occurs when a user tries to write a file on a read-only device. The following information is normally available:

- **Device type:** For example, DVD/CD, floppy disk, removable storage devices, COM, LPT, etc.
- **Volume label:** The floppy disk, DVD/CD, or removable device label.
- **File Name:** The name of the file the user was attempting to write to the media.
- **User Name:** The name of the user who tried to access the protected device.
- **Process Name:** The application used by the user to try to access the protected device.
- **Other:** The exact access mask, in hexadecimal format, used by the application to try to access to the protected device (used by SecureWave technical support).



*Several identical log entries may appear as some applications, for example Windows File Explorer, retry automatically when there are unsuccessful access attempts to protected devices. An appropriate setting of the Device log throttling option significantly reduces the volume of redundant information logged. See the option description on page 173.*



*System or svchost can execute not impersonated mount requests for an encrypted media when the media encryption keys are not present on the client machine. As these requests are not identified, the User Name field cannot be retrieved and the corresponding field in the log is empty.*

> **KEYBOARD-DISABLED:** This event occurs when a user's keyboard is disabled because the Sanctuary client suspected the presence of a keylogger.

> **KEYLOGGER-DETECTED:** This event occurs when a Keylogger is detected. This is a device that captures all data typed at the keyboard, including passwords and other sensitive data.

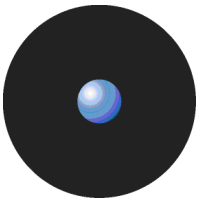
> **MEDIUM-ENCRYPTED:** This event occurs when a removable storage device is encrypted.



*MEDIUM-ENCRYPTED events are logged even if the Device Log option is set to 'Disabled'. They are required for the password recovery functionality, see Recovering a password for decentralized encryption when connected on page 143.*

> **ADMIN-AUDIT:** This event occurs when an administrator carries out an action such as changing permissions, adding or modifying users, user groups, file groups, accesses a shadow file and so on. The following information is normally available:

- **User Name:** The name of the administrator who carried out the action.
- **Audit Event:** The type of action that the administrator carried out. See *Audit events* on page 126.
- **Target:** The device for which the permissions were altered.
- **Target Computer:** The computer that was the target of the administrator's action.
- **Target User:** The name of the person or user group to which the administrator's action was applied.



## Viewing client error reports

The *Computer*, *Traced On*, and *Transferred On* fields are always present for every error logged. The other columns are populated when additional information is available. The following error types can be used as criteria:


- > **SHADOW-BAD-DIRECTORY:** This error occurs when the 'Shadow directory' cannot be created by the Sanctuary Client Driver, or when the shadow directory is not accessible. See *Shadow directory* on page 176 for information on how to set up the directory location.
- > **SHADOW-FILE-MALFUNCTION:** This type of error occurs when the Sanctuary Client Driver cannot proceed with the shadowing. Contact SecureWave Technical Support service to find out the cause of the problem.
- > **SHADOW-CD-R-MODE-UNSUPPORTED:** This error occurs when the Sanctuary Client Driver prevented the writing of a DVD/CD because the format used was unsupported. See *DVD/CD Supported formats* on page 194 for more details.
- > **SHADOW-CD-R-MALFUNCTION:** Sanctuary Client Driver generates this error when it was unable to carry out the shadowing of a DVD/CD. Contact SecureWave Technical Support service to find the cause of the problem.
- > **BAD-PUBLIC-KEY:** You get this error when default RSA (Ron Rivest, Adi Shamir, and Len Adleman) keys are used to protect the communication between the clients and the application server. See Sanctuary's Setup Guide for an explanation on how to create custom *sx-public.key* and *sx-private.key* and where to store them in the server and client machines.



*You should generate your own set of public and private keys before deploying the clients in the production network. It is recommended that you do not change the public and private keys in a production environment. Changing the keys in an environment where encrypted media are used, means they must be reformatted and encrypted using the Media Authorizer.*

## Viewing shadow files

When you want to view shadow files, we recommend that you first filter your data so that only log entries that have attachments are displayed. You can either use one of the predefined templates to do this, or you can:

1. Click on the **SETTINGS** button (or on the right part of any heading of any field).
2. Select the *Attachment* field.
3. Click on the **CRITERIA** or  button.
4. Select *With* and close the dialog by clicking the **OK** button.
5. Click on the **EXECUTE** button to close the Template settings window and execute the query.

The listed entries have attached files that are exact copies of the files copied or read by the users, from or to protected devices when the 'Shadow' rule was in effect. Depending on the selected fields, the date the files were copied/read to/from the media (*Traced On*) and the date the file was transferred to the SecureWave Sanctuary Database (*Transferred On*) are displayed. Sanctuary Device Control also tracks the name of the user that copied the file, the filename (and content), the computer where the copy took place, as well as the device.



*Sanctuary Device Control does not open big files (exceeding 350 MB) unless sufficient resources are available.*

Once you list the files, you can right-click on any of them that has an 'Attachment' value of 'True' (indicating that the full content has been shadowed), and carry out one of the following operations (by selecting the appropriate context menu option):

- > **Save as** — allows you to save the file to a local or network drive.
- > **View** — lets you view the contents of the file in a text or binary file internal viewer:

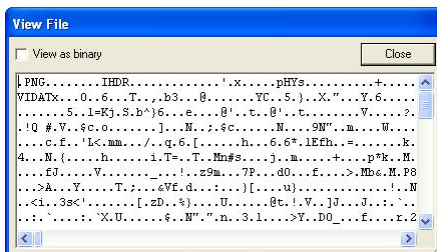


Figure 121: Viewing the content of a shadow file in text form

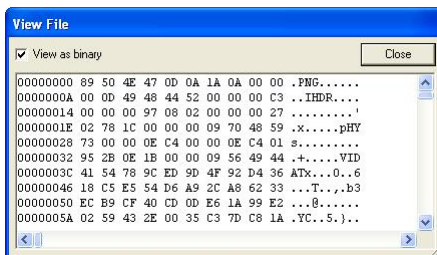


Figure 122: Viewing the content of a shadow file in binary form



*Sanctuary logs the file and administrator name each time a shadowed file is opened. This information is available in the Log Explorer module. (In previous versions of Sanctuary they were viewed using the Audit Logs Viewer module.)*

- > **Add device(s)** — using this option you can include the device(s) in the list of those administrated by Sanctuary Device Control and then grant it permissions.
- > **Open** — (only available for full shadow and when selecting one log registry) opens the file with the associated application (defined in Windows' Explorer). If there is no association, this command is equivalent to Open With.
- > **Open with** — (only available for full shadow and when selecting one log registry) lets you choose the application that opens the file.

You can also do some of these actions using the Control Button panel located on the lower right of the main Log Explorer window.

## When the Data File Directory is not available

There are some cases where the Application Server cannot find its associated Data File Directory, for example, when it resides in a different machine that is temporarily unavailable, or when the SecureWave Application Server account does not have rights over this directory. When this happens, a warning message indicates that the program has not found the shadow file for the log entry. The administrator can check for these events in Windows Event Viewer as shown in the following image:

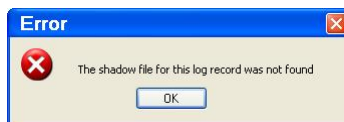


Figure 123: Error message when a shadow file is not found

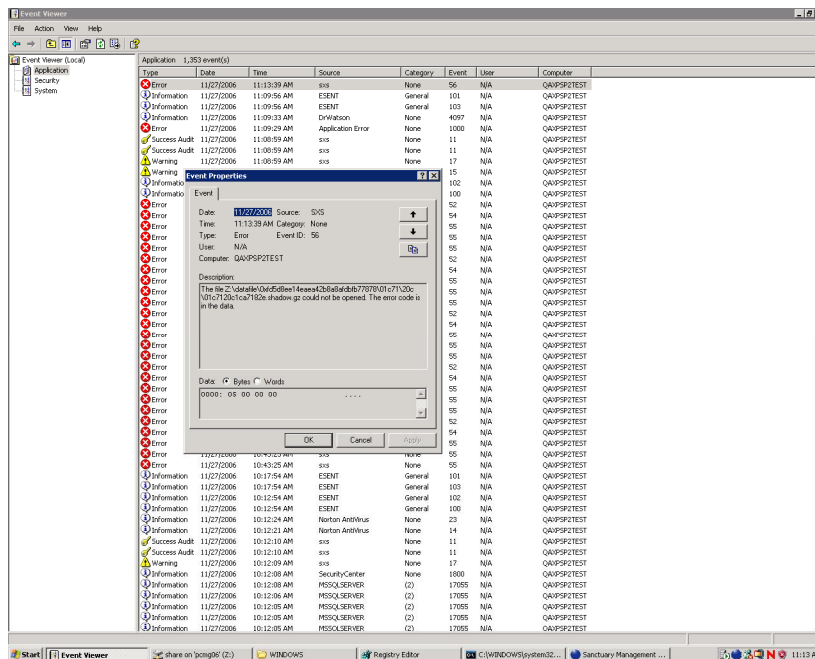


Figure 124: Windows' Event Viewer when a shadow file is not found

## Shadowing file names only

Files that have been shadowed specifying the option *File name* for the Removable Shadow Mode, DVD/CD Shadow Mode or Floppy Shadow Mode cannot be opened in the Log Explorer module. You only see the name of the file and the 'Attachment' value is shown as 'False' (indicating that there is no available content for the file).



*The full content of the file is always shadowed and compressed locally on the client-side. The entire file (or name, depending on the shadow rule) is transferred to the SecureWave Application Server during client synchronization. When the 'File name only' option is selected, only the name is transmitted to the server. This is particularly important for users connected to the company network occasionally or with a low-speed connection as sometimes (depending on the shadowing rule) the whole content of the shadow file has to be transferred to the server.*


## DVD/CD Shadowing

When CDs or DVDs are written or read, the CD image files are interpreted locally and sent to the server during synchronization. *Appendix A: DVD/CD Shadowing* provides details of how these shadowed files appear in the *Log Explorer* module.

## Forcing the latest log files to upload

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

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

1. Activate the *Log Explorer* module, if it is not already open. To do this, click on the Log Explorer icon  located in the Modules section of the *Control Panel* or use the *View*→*Modules* command.





- Click on the **FETCH LOG** button or select *Fetch Log* from the *Explorer* menu. The system prompts you to specify the machine from which you want to fetch all logs present on the client. You can only fetch logs from those computers that have the Sanctuary Client Driver installed.

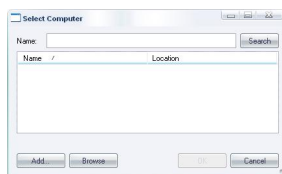


Figure 125. Fetching New Logs

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



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

## To manage devices using the Log Explorer module

Once the log entries are displayed in the Results panel, you can right-click on *Device –Attached* entries and use the context menu or the Control button panel to add device models or uniquely identified devices to the list of devices managed by the Device Explorer module.

To add a uniquely identified removable device:

- Traverse the list until you locate the device model or unique id of the device you want to add to the managed devices list.

Keep an eye on the **ADD DEVICES** button. If it is active, this means that the device can be integrated into the managed devices list.

- Right-click on the item or use the **ADD DEVICES** button.
- Select either the model of device or the specific device from the list by selecting the checkbox to the left of the entry (as shown below):

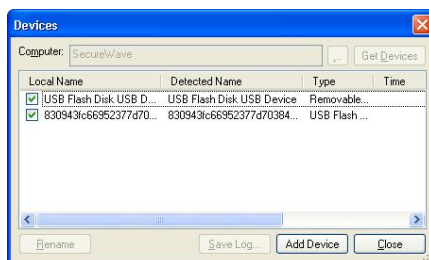
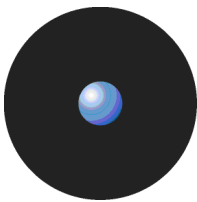


Figure 126. Adding devices to the managed devices list

- Click on the **ADD DEVICE** button.



## Viewing administrator activity

In addition to using the Log Explorer module to monitor the use of I/O devices, you can also use it to monitor the actions of your administrators including changing user access rights and device permissions. See *Monitoring administrator actions* on page 100 for more information.




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



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

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

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

## Audit events

Audit events describe the actions performed by administrators.

<b>Audit events</b>	<b>Description</b>
ACCESSED SHADOW FILE	This event is traced every time an administrator accesses a shadow file / Central logging file. The fields available are: User, machine, device, file name, copy date.
ACCESSED DEVICE LOG	When an administrator accesses a device log.
ADD COMPUTER GROUP	The administrator created a computer group.
ADD DEVICE GROUP	The administrator created a device group.
ADD MANAGED DEVICE	This event corresponds to the adding of a new device by an administrator with the Manage Devices functionality. The device name is logged.
ADDED MEDIA	Corresponds to the adding of a new device with the Media Authorizer; the label and description are logged.
ADDED TEMPORARY PERMISSION OFFLINE	When a temporary permission is added for devices used in computers that are temporarily not connected (offline) to your network.
ADDED PERMISSION	This action corresponds to the adding of a permission in the Device Explorer, the information available is user, machine, device, read/write, or priority.
ADDED SCHEDULED PERMISSION	The fields available are user, machine, device, read/write, begin time, end time, or weekdays.
ADDED TEMPORARY PERMISSION	The fields available are user, machine, device, read/write, begin time, or end time.
AUTHORIZED MEDIA	This action occurs every time a user is granted the right to use a specific media in the Media Authorizer. The user, label and description are logged.
AUTOMATIC USER ACCESS UPGRADE	Means that the <i>Sanctuary Management Console</i> user was implicitly a Sanctuary Enterprise Administrator, because no other Sanctuary Enterprise Administrator was defined. When the user creates an explicit Sanctuary Enterprise Administrator, he loses his implicit Enterprise Administrator privilege, which means he may block himself out. To prevent that from happening, the SecureWave Application Server makes this user an Enterprise Administrator explicitly, a message is displayed on screen and the user name and role will be traced. See also <i>Defining Sanctuary administrators</i> on page 32.
CHANGE COMPUTER GROUP	The administrator changed an existing computer group.
CHANGE DEVICE GROUP	The administrator changed an existing device group.
DELETED DEFAULT OPTION	Whenever a default option that applies to all the machines is deleted (in the <i>Tools→Default Options</i> menu), the option and the user/machine are traced.



<b>Audit events</b>	<b>Description</b>
DELETED OPTION	Whenever an option specific to a machine is deleted, the option and the user/machine are traced.
GENERATE MAINTENANCE TICKET	The administrator created a new maintenance ticket. See Endpoint Maintenance on page 27.
MODIFIED SCHEDULED PERMISSION	The available fields are user, machine, device, read/write, begin time, end time, or weekdays.
MODIFY USER ACCESS	When changes are made to the Sanctuary Administrator's roles, the user and role are logged.
PURGED DB AND FILE STORAGE	This action is recorded every time maintenance is performed on the system.
REMOVE COMPUTER GROUP	The administrator removed an existing computer group.
REMOVE DEVICE GROUP	The administrator removed an existing device group.
REMOVE MANAGED DEVICE	This event corresponds to the removal of a device from the list of managed devices, the device name is logged.
RENAME COMPUTER GROUP	The administrator renamed an existing computer group.
RENAME DEVICE GROUP	The administrator renamed an existing device group.
REMOVED MEDIA	When a media is suppressed from the database. The label and description are logged.
REVOKED PERMISSION	This corresponds to the removal of a permission in the Device Explorer; user, machine and device are traced.
REVOKED SCHEDULED PERMISSION	The available fields are user, machine, device, read/write, begin time, end time, or weekdays.
REVOKED TEMPORARY PERMISSION	The available fields are user, machine, device, read/write, begin time, or end time.
SET DEFAULT OPTION	A default option is one that applies to all the machines. Whenever a change is done by the administrator to one of these options (by using the <i>Tools</i> → <i>Default Options</i> menu), the option being changed and the user/machine are traced.
SET OPTION	This action is traced whenever a change to the system options is made, the option, user/machine are logged.
UNAUTHORIZED MEDIA	When a user is prevented from using a specific media in the Media Authorizer, the user, label and description are logged.
UPDATED MEDIA	When a media label or description is updated, the label and description are logged.
UPDATED PERMISSION	This action appears in the Audit Logs Viewer when a permission is modified in the Device Explorer, the information available is: user, machine, device, read/write, priority.
UPLOADED SHADOWS	This event is traced every time an administrator chooses to specifically retrieve the latest shadow files from a given machine. The <i>machine name</i> is logged.

Table 34. Audit events



---

## Chapter 6: Using the Media Authorizer

This chapter explains how you can use Media Authorizer to allow access to specific users for using individual CDs, DVDs, and encrypted removable media. 'Removable media' in this context means any device recognized as 'Removable Storage Devices' by Windows, including flash memory devices, zip drives, etc.

### Introduction

You can use the Media Authorizer for three main purposes:

- > To add individual CDs, DVDs and removable storage devices onto the system database and then grant permission to use them for users who would otherwise be barred by the defined policies. Each removable device is encrypted to suit your security preferences.
- > To carry out centralized data encryption for removable devices used outside the organization. This provides an effective way to protect your data in case the device is lost or stolen.
- > To do centralized data encryption for removable devices used in-house on computers which run Sanctuary Client Driver.



*Sanctuary Client must be installed on the machines where the Administration tools are used to perform encryption and authorization of multi-session DVDs/CDs.*

Although we recommend that you have a Microsoft Certificate Authority installed in your network for security reasons, a user can access the encrypted data without the need of one provided that he has the physical encrypted medium, its associated public key, password, and permission to access the removable device class.



*You may encounter problems decrypting keys that were encrypted using an older version of Sanctuary Device Control. Previous versions of the SecureWave Application Server did not store the media keys encrypted using user certificates. Instead, clients requested those of currently plugged media (which is not suitable for the new differential update schema available in recent versions) storing the media keys encrypted with user certificates and sending the encrypted media keys to all the clients differentially. SecureWave Application Server checks user's certificates published in AD at startup — and periodically — and, whenever it finds users' certificates for those user who have been authorized an encrypted media and that are NOT currently used to encrypt media keys, stores them. The periodicity of this verification is controlled by an optional registry value 'CertificateQueryPeriod' (in minutes; see Sanctuary's Setup Guide), defaulting to 180 minutes (three hours). This certificate 'refresh' mechanism ensures that when a Sanctuary installation is upgraded, media keys are created and communicated to clients. It also ensures that if some user certificate expires, SecureWave Application Server will detect them and use a new one when it becomes available.*

When doing central encryption you can choose one of a number of methods. You can use the *Easy Exchange* schema to encrypt a device and access it on computers that do not have the Sanctuary Client Driver installed. The user does not need to install any program or have administrative rights. See *Easy Exchange* on page 159 for more information. This schema is also used when doing decentralized encryption on removable storage devices. Please see *Decentralized encryption* on page 134 for more information.



## Creating a DVD/CD hash

A practical use of Sanctuary, besides defining all kinds of permissions for device I/O access, is to create a library of DVDs/CDs and assign each volume to a User(s)/Group(s). As an example, take an internal demo DVD that has to be used over and over again by marketing to show to your clients or an installation CD. You can also extend this to music DVDs/CDs.

When a DVD/CD is added to a library of available media, Sanctuary calculates a hash number based on the complete digest of its contents. If someone modifies even 1 bit of the content, the hash number changes radically and the DVD/CD is considered as a different one that is no longer in the library. This means that previously assigned users no longer have access to the modified medium.

Once this hash is created, the result is saved in the SecureWave Sanctuary Database.

## What happens when a user wants access to the DVD/CD

When a user wants to access a DVD/CD the following process applies:

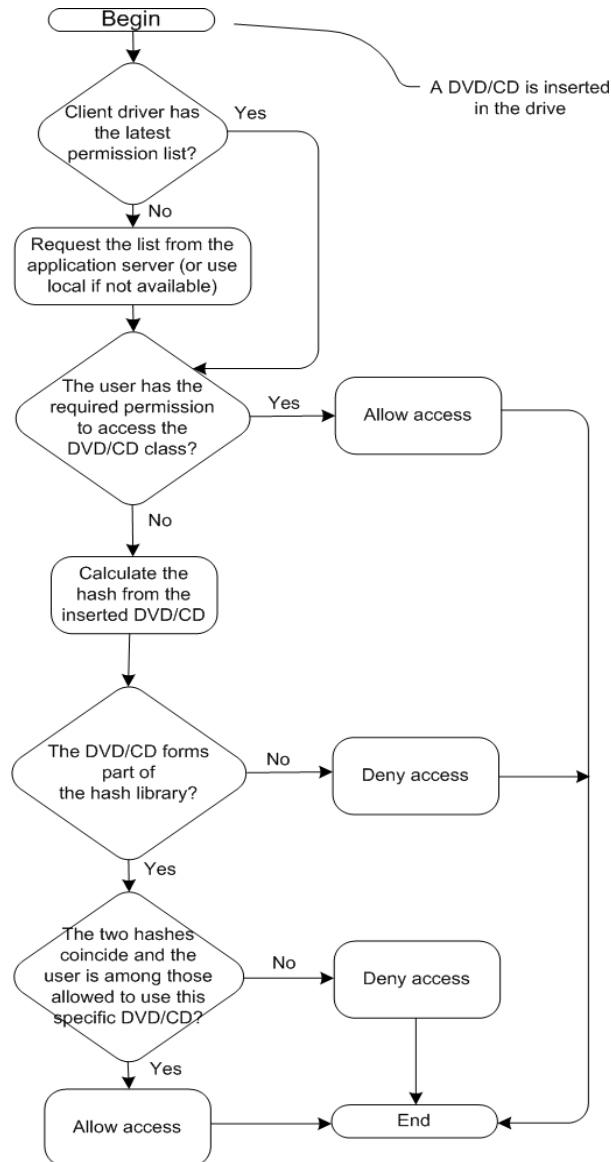


Figure 127: Using a DVD/CD from the library




The general process we recommend you follow when authorizing media is:

1. Set up as many CDs, DVDs, or removable storage devices as you want.
2. For each device, grant access to all appropriate users.



*You can grant access permissions to Novell accounts on CDs/DVDs, but you cannot grant access permissions to Novell accounts on centrally encrypted media. This limitation is caused by the lack of user certificates published in Active Directory for Novell users.*

## Accessing the Media Authorizer

You can access the *Media Authorizer* by clicking on the  icon located on the *Modules* section of the *Control Panel* in the main window.

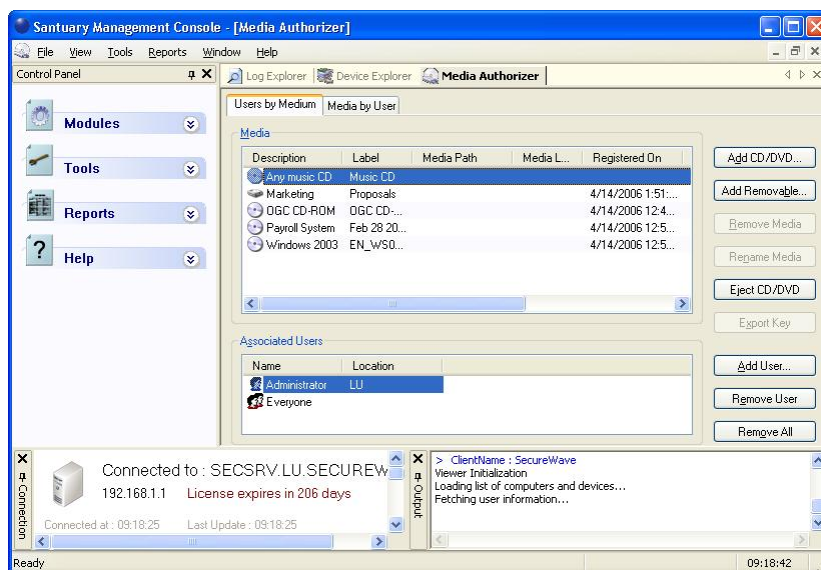


Figure 128: The Media Authorizer main window

*The Media Label column represents the actual media label as found in the medium properties dialog. The Media Label and the Label columns have the same content when the media has just been added. These labels may differ when a user with access to the encrypted device has changed it. In this case, an administrator connecting the media to his computer sees that the Label column has kept the original value while the Media Label column holds the modified one.*

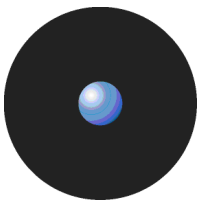
## Authorizing users to use specific DVDs/CDs

The default-installed configuration denies access to CDs and DVDs drives. You must grant the administrator permission to access the DVD/CD in Read or Read/Write mode. If not, the administrator cannot add them to the database. There is no need to modify your policies regarding the use of DVD/CD media for the users, just authorize them to use the individual DVD/CD the administrator adds to this 'library' (the only exception to this rule being generic Music CDs).

*Since Movie DVDs behave as DVD-ROMs, their treatment differs from the procedure used for Music CDs. You need to authorize each DVD separately.*



*You cannot authorize blank optical media.*



## Pre-requisites

Before adding multisession DVDs/CDs, you must install the Sanctuary Client on the machine where you are going to authorize them. If this is not done, the output window displays 'Error opening driver: please make sure that Sanctuary Client Driver is installed' and the ADD REMOVABLE button is disabled. It is not possible to calculate the signature of multisession DVDs/CDs when the Sanctuary Client is not installed on the Sanctuary Management Console machine. The Media Authorizer module is significantly slower when the Sanctuary Client Driver is not installed.

## To authorize the use of a specific DVD/CD

To authorize (add to the system database) the use of a specific DVD/CD, proceed as follows:

1. In the Sanctuary Management Console, switch to the Device Explorer module. Be sure to grant the Sanctuary administrator the required permissions to at least read the DVD/CD.
2. Switch to the Media Authorizer module.
3. Click the ADD CD/DVD button. You are prompted to insert a DVD/CD.
4. Insert the DVD/CD.

The Media Authorizer calculates a unique cryptographic signature of the DVD/CD and displays its label:

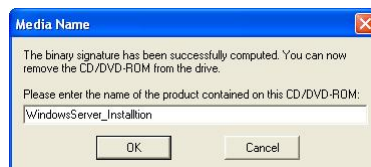


Figure 129: Adding an encrypted DVD or CD

This name is used to register this DVD/CD on the system. You can change it if you need to make it more meaningful.

5. Click the OK button.

The DVD/CD is included in the database so that permission to use it can be assigned to individual users/groups. Its details are shown on the *Media Authorizer* window.

Exact copies of the DVD/CD will also work on client machines if authorized, but the slightest modification (names, file sizes, number of sessions, number of files and directories, etc.) will require a new authorization.

*Adding a multisession CD may take several minutes.*

## Encrypting removable storage devices

Even though the general computing term 'removable media' may include any device that can be removed from your computer, such as floppy disks, Sanctuary Device Control refers to removable media as any device that declares itself to Windows in the class 'removable storage devices' through the Plug and Play mechanism. Therefore, removable storage devices include flash memory keys (USB sticks/pens), ZIP drives, Jaz drives, and some MP3 players and digital cameras. If you have a secondary internal ATA/IDE hard disk, it is recognized as a Removable Storage Device and you should define permissions for it.



*All non-system hard drives are treated as Removable Media and can be encrypted. If you have a secondary hard drive with multiple partitions, you will need to encrypt each partition independently.*






Sanctuary Device Control uses encryption to control the use of specific removable storage devices. Encryption achieves the following two goals:

- > It ensures tamper-proof device identification by associating the identifier of a device with its encryption key.
- > It prevents access to the data stored on the device when the device is attached to a computer not protected by Sanctuary Device Control.

Advanced Encryption Technology (AES) is the encryption algorithm used to cipher the media; Sanctuary Device Control uses disk encryption keys of 32 bytes (256 bits). The encryption process relies on the Microsoft Certificate Authority of the Active Directory domain for the delivery of encryption keys to the users, much in the same way as the NTFS file encryption does.

When a user has received the proper access rights to encrypted media, the Sanctuary Client Driver provides a transparent access to the media. Data copied to the media is encrypted/decrypted transparently when the media is accessed.

 *Users who have not received access to the encrypted media are not able to read its content (not even the Sanctuary Administrators).*

There are two steps required to authorize the use of a specific removable storage device:

1. Make the specific removable storage device unique through its encryption.
2. Grant rights to use the device to specific users.


Both of these steps are carried out using the *Media Authorizer* module.


In the event that access to a specific device is required on a computer where the Sanctuary Client is not installed, SecureWave provides the administrator with a tool to grant such access. See *Chapter 7: Accessing encrypted media outside of your organization* on page 149 for more details.

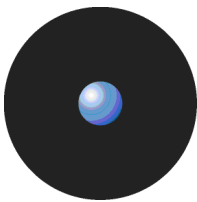
## Pre-requisites

In order for encryption to work properly, there are a number of pre-requisites that your system has to meet:

- > Encryption is available under Windows 2000, XP, and 2003 Active Directory Domains. This feature can be used, with difficulties, under non-Active Directory domains or Workgroups.
- > The Sanctuary Administrator must have administrative rights on the computer where the encryption is performed.
- > A Microsoft Certificate Authority must be available and published, and the DNS (Domain Name System) server must be properly configured. This can be avoided, but we do not recommend it. Please refer to Sanctuary's Setup Guide for more details.
- > The Sanctuary Client must be installed on the machines where the Administration tools are used to perform encryption.

 *You should ensure that the Sanctuary administrator has Read and Write and Encrypt access to the removable storage devices. Please refer to Using the Permissions dialog on page 57 for more details on how to set device permissions.*

 *When performing centralized encryption in a network with parent and child domains the child does not normally inherit the certification authority (CA) from the parent domain. See <http://support.microsoft.com/kb/281271> for more information.*



## Decentralized encryption

The Media Authorizer module is not used to carry out distributed encryption – only centralized encryption. Decentralized encryption is done using *Easy Exchange* (see *Removable device encryption methods comparison* on page 136 and *Easy Exchange* on page 159). Easy Exchange encryption can be used to do both centralized and decentralized encryption of media. See *Decentralized encryption* on page 163 for a full description of how to implement this option.

## Limitations

There are some limitations that you should be aware when encrypting removable storage devices:

- > Due to the nature of some devices and the way they are handled by Windows, there may be some limitations to the use of Zip media and certain types of Flash memory cards.

These specific types of removable storage devices are not always mounted when the media is plugged into the media reader. If a change has been made to the media permissions while the device is inserted in the reader, access may be denied when trying to read or write to an encrypted removable storage device. This occurs because media access rights are retrieved from the SecureWave Application Server and applied when the removable storage device is mounted by the operating system.

There are three possible ways to resolve this issue:

- The user logs off and logs on again, forcing the system to mount the device.
- The user unplugs and re-plugs the device.
- The user removes the media from the reader, tries to access the media with Windows Explorer and re-inserts the media after Windows displays the 'Please insert disk into drive' message.



*This limitation only affects devices where the media can be separated from the reader. USB DiskOnKey devices, for example, are not subject to this limitation.*

- > The Sanctuary Client Driver must be installed on the machine where the Sanctuary Management Console is installed.
- > Memory card readers integrated to cameras, printers, or scanners may not work properly if encrypted.



*The users do not need to be assigned permissions to the Removable Storage Devices class in the Device in order to use encrypted devices — Just assign the media to the user in the 'Media Authorizer' module.*



*By design, Windows assigns removable drives to the next free volume letter. Unfortunately, Novell clients may also map this volume letter to a Novell's server folder. When trying to access a removable device in a Novell system, you may need to assign another letter to it using the 'Disk Management' function of the 'Computer Management' dialog (using Windows Control Panel → Administrative Tools).*



*There is a 4 GB limit when encrypting with our Easy Exchange option. See Easy Exchange on page 159 for more information.*



*You cannot use our encryption methods on those keys that already offer their own 'embedded encryption' option (see next section).*



## To encrypt a specific removable storage device

Before an encrypted device can be assigned to the users, you (the administrator) must configure it. Attach the media to your computer and, using the Sanctuary Device Control Administration tool, add the device to the database. During this process, a unique identifier is written to the device and it is encrypted.


To add a removable storage device and encrypt it, follow these steps:


1. Attach the removable storage device to the computer. Check for the presence of any sensitive data that should be preserved during the encryption process.
2. In the Sanctuary Management Console, switch to the *Media Authorizer* module.
3. Click ADD REMOVABLE. The *Add Removable Media* dialog is displayed.



Figure 130: Adding a specific removable storage device

4. Select the letter corresponding to the *Drive* you want to encrypt.
5. Enter a free text *Description* for the device.
6. Enter a *Label*. This information is used to label the device after it is formatted. This information appears in the media properties and can be viewed by any user having proper access to the device. The *Label* text field can be a maximum of 11 alphanumeric characters (including upper and lower case letters, and digits).

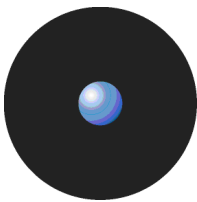
 *We strongly recommend that you apply a physical label (sticker, note, mark) to encrypted devices to distinguish them easily. Each sticker ideally has the label or part of the description on it. This is a safety precaution as the media properties cannot be read by users who do not have access to the device. If users complain they do not have access to an encrypted device, this reduces the administrator's work identifying why access is denied.*

 *Users cannot format an already centrally encrypted device unless the adequate permission is granted in the Device Explorer module (in the Removable Storage Devices' class). The 'Encryption' panel should be set to 'Both' and the Read/Write permissions activated.*

7. Choose the appropriate *Encryption* method as described in the following table:

Method	Description	Notes
Full & Slow (secure for existing data)	This method is used to encrypt the media while preserving any data already there. This operation can be time-consuming on high capacity removable media as all the sectors of the media are accessed during the encryption.	Encryption is applied to all free sectors of the device. All the data, including erased but still recoverable files, are encrypted. Therefore, in general, this option is recommended.
Quick Format (insecure for existing data)	Used to quickly encrypt the device while deleting all existing data.	All files written to the device are logically erased. However, the physical sectors of the device are not encrypted. A malicious user can use a data recovery tool to read the sectors and gain access to potentially sensitive data. This also applies when sensitive data has previously been deleted — it may still be recoverable. We therefore recommend that this encryption mode is only used when the device never contained sensitive data, or it has been securely wiped.
Easy Exchange (insecure for existing data):	A fast encryption method with the added advantage of being able to access the device in computers that do not have the Sanctuary Client Driver installed.	

Table 35: Available encryption methods



Although you can use our Stand-Alone Decryption/Encryption tool (SADEC) to install on a computer and access devices encrypted with the first two methods, the user needs administrative rights, not always a good choice. Using Easy Exchange, the user can use the encrypted device — with the password and the original encryption key used to encode the peripheral — without installing software and without requiring administrative rights. See *Table 36*, *Table 40*, *Table 41*, and next section for more details.

## Removable device encryption methods comparison

When you encrypt a removable device (add it to the database and then assign it to user(s)/groups(s)), you can choose among three proposed methods:

- > Quick format encryption.
- > Full format encryption.
- > Easy Exchange encryption.

Each of them has its own advantages and disadvantages as summarized in the following table:

<b>Method</b>	<b>Advantages</b>	<b>Disadvantages</b>	<b>Comments</b>	<b>Limitations</b>
Quick Format	<ul style="list-style-type: none"> <li>&gt; It is very fast.</li> </ul>	<ul style="list-style-type: none"> <li>&gt; Existing data is lost.</li> <li>&gt; The device's sectors are not encrypted.</li> <li>&gt; The user needs to use the device in a computer where the Sanctuary Client Driver is installed or where our SADEC tool can be installed.</li> <li>&gt; Should be used only in fully, wiped, formatted devices.</li> </ul>	<ul style="list-style-type: none"> <li>&gt; A malicious user can still recover the previously erased files.</li> <li>&gt; If the user is using the removable media in a machine where Sanctuary Client Driver is installed, the encryption key is not needed — only the password.</li> </ul>	<ul style="list-style-type: none"> <li>&gt; Is based on partitions.</li> <li>&gt; Limited to devices ≤32GB using FAT32 due to design restrictions of the Windows Format command (depending on the operating system you are using). Use NTFS if you need larger volumes.</li> </ul>
Full & Slow	<ul style="list-style-type: none"> <li>&gt; Data already stored in the device is not lost.</li> <li>&gt; All sectors are encrypted.</li> </ul>	<ul style="list-style-type: none"> <li>&gt; May take a long time to finish in large capacity devices.</li> <li>&gt; The user needs to use the device in a computer where the Sanctuary Client Driver is installed or where our SADEC tool can be installed.</li> </ul>	<ul style="list-style-type: none"> <li>Use on any kind of device that needs solid encryption; if the user is using the removable media in a machine where Sanctuary Client Driver is installed, the encryption key is not needed — only the password.</li> </ul>	<ul style="list-style-type: none"> <li>None; the format is not lost, only data is encrypted.</li> </ul>
Easy Exchange	<ul style="list-style-type: none"> <li>&gt; It is very fast.</li> <li>&gt; The user has access to the device's data even in computers where Sanctuary Client Driver is not installed.</li> <li>&gt; No need to install software to use the device.</li> </ul>	<ul style="list-style-type: none"> <li>&gt; Existing data is lost.</li> <li>&gt; Device's sectors are not encrypted.</li> </ul>	<ul style="list-style-type: none"> <li>The user does not need administrator's rights to use the device, only the password and the encryption key. If the device is used in a system that has the Sanctuary Client Driver installed, the administrator should also grant access to this device.</li> </ul>	<ul style="list-style-type: none"> <li>&gt; Limited to devices ≤4GB since FAT16 is used.</li> <li>&gt; Typically used for USB memory keys but can be used for any device recognized as a removable.</li> <li>&gt; Since the encryption is volume based, you can divide the whole available space in 4 GB partitions.</li> </ul>

Table 36: Encryption methods comparison

See *Table 40* and *Table 41* for further details.

## Problems encrypting a device

- > You need a Certificate Authority server installed before proceeding to encrypt a media (for an alternative method, please refer to *Encrypting devices without a Certificate Authority* on page 148). You can continue without installing the Certificate Authority, but the recommended procedure is to install it before proceeding to encrypt devices or media.
- > The device must not be in use. If there is a program accessing the device (e.g. a Flash drive when Windows Explorer is displaying the device's content), then the device cannot be encrypted. Close the program that is accessing the medium to make this error disappear.

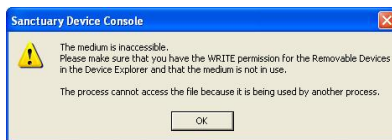
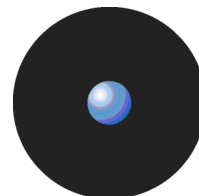


Figure 131: 'Inaccessible medium' error message

- > To encrypt a device, it must be attached to the Sanctuary administrator's computer; the administrator must have administrative rights on his machine and Read/Write and Encrypt access to the Removable Storage Devices class or to the sub class corresponding to the device model in the Device Explorer. Please refer to *Chapter 4: Managing permissions/rules* on page 57 for more details on how to set device permissions.

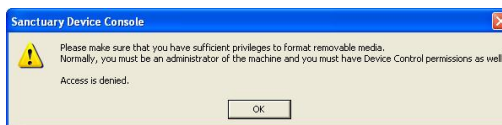


Figure 132: 'Not enough privileges' error message

- > If the device has already been encrypted, you get the following message.

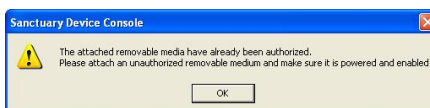


Figure 133: 'Already authorized' error message

Only non-encrypted media can be encrypted. If you are trying to re-encrypt a device, you should first remove it from the system database using the REMOVE MEDIA button.

- > If the device has previously been encrypted and then removed from the database while not physically attached to the administrator machine (perhaps because it was thought lost, and you try to encrypt it again using 'Quick Format') you are warned that any encrypted data on the device will be permanently deleted.



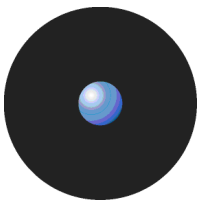
Figure 134: 'Already encrypted' error message

Select either YES to encrypt it again, and lose access to any previously encrypted data on the device, or NO cancel the operation. If you wish, you can import it to the database and re-encrypt again using the same key/password only if you previously exported its encryption key to the file or media itself, and remember the password.

- > Although the correct procedure to remove a device is to attach it to the administrator's computer before removing it, there are situations where an encrypted device must be removed from the database while it was not attached on the administrator's computer. The physical device remains encrypted. As there are no permissions anymore for these devices in the system, the Sanctuary Client Driver will consider them as encrypted media coming from other organizations and will prevent access to them unless the users has the media password, the media encryption key, and received proper permission access. See *Locally managed access to unauthorized encrypted media* on page 154.

When a device is in this particular state (still encrypted but removed from the database), the administrator can:

- Add the device back into the database without losing its content providing its encryption key had been exported before the device removal, either to the device or to a file, and that its password is known. In this case, you can use the *Import (secure for existing data)* command. The device will be inserted in the database again and its content preserved. See *Centrally managed access to unauthorized encrypted media* on page 153.



- Reuse the device and re-encrypt it. In this case, you can use the *Quick Format (insecure for existing data)* command. This operation will erase the device content.

If you remove the media when it is not connected to the computer, you get the following message:



Figure 135: 'Identification record cannot be deleted' error message

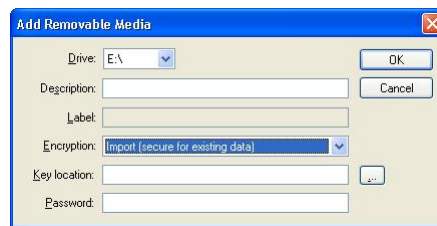


Figure 136: Importing back an already encrypted device

## Authorizing access

Once you have added CDs/DVDs/encrypted removable storage devices to the system database, you can authorize access to them for specific users to:

1. Grant permissions to use specific DVDs/CDs for those users who do not normally have access to the DVD/CD drive.
2. Allow specific users to access encrypted media.



*It is not possible to grant read-only access to encrypted media.*



*You cannot grant access permissions to Novell accounts.*

The process applies to DVDs/CDs/removable storage devices that have already been authorized using the Media Authorizer. In addition to these devices, there is a category — Any Music CD — that you can select to allow user access all audio CDs. This does not apply to removable devices encrypted using our *Easy Exchange* method.

## Selecting users for a device

You can select each of the CDs, DVDs, and removable storage devices that you have added to the system database to assign them permissions.

### To grant access to use DVDs/CDs/encrypted removable media

To assign permission to users to enable them to use a DVD/CD or removable media, proceed as follows:

1. Select the *Users by Medium* tab in the *Media Authorizer* module.
2. Select the DVD/CD/removable device for which you want to grant access.

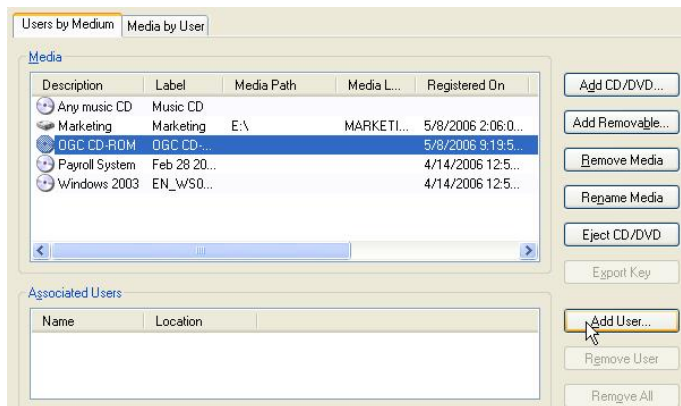


Figure 137: A specific medium with its related users and groups

3. Click the ADD USER button. The *Select Group, User, Local Group, Local User* dialog is displayed.



Figure 138: Adding a group or user to a selected medium

4. Select the users or groups you want. Type in the name or part of the name (or use wildcards, such as \* and ?), and then click SEARCH or BROWSE. In the list that appears, select one or several users or groups (using the CTRL or SHIFT keys), and then click OK.



*You cannot assign access for encrypted removable media to groups, only to users.*

### To deny access to DVDs/CDs/encrypted removable media

To remove the permission to use a DVD/CD/encrypted removable media from users or groups, proceed as follows:

1. Select the *Users by Medium* tab in the *Media Authorizer* module.
2. Select the DVD/CD/removable storage device to which you want to deny access.
3. In the *Associated Users* area, select the users (and/or groups) from who you want to remove access permission.

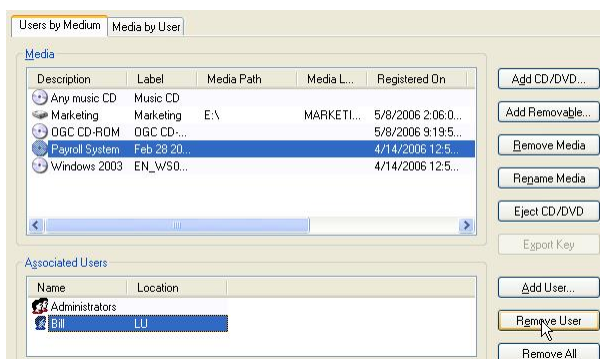
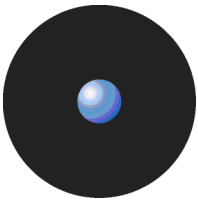


Figure 139: Denying access to DVDs/CDs/encrypted removable media



4. Click REMOVE USER.



*If you want to remove all users assigned to a medium, simply select the medium and click REMOVE ALL.*

Users are removed from the list of *Associated Users*, preventing them from accessing the selected media.



*The entire list of authorized DVDs/CDs/removable media is downloaded on the client. A disconnected user can only access the media permissions which were downloaded when the user's machine was last online. These may include media the user has never used, which become accessible to the user (permissions allowing). (This has changed since previous versions of the product, where the entire list of authorized DVDs/CDs/removable media was not downloaded on to the client.)*

## Selecting devices for a user

You can select each individual user on your system, and grant them access to the CDs, DVDs, and removable storage devices that you have added to the system database.

### To grant access to use DVDs/CDs/encrypted removable media

1. Select the *Media by User* tab in the *Media Authorizer* module.

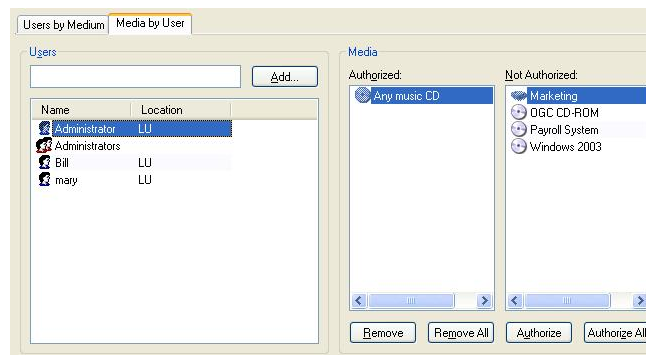


Figure 140: Media by user authorization

2. Click the ADD button. The *Select Group, User, Local Group, Local User* dialog is displayed.
3. Type in the name or part of the name and then click SEARCH or BROWSE. In the list that appears, select one or several users or groups (using the CTRL or SHIFT keys), and then click OK.
4. In the *Media by User* tab, select the user or group to which you want to assign permissions.



*You cannot assign access for encrypted removable media to groups, only to users.*

5. Select the DVDs/CDs/removable media that you want from the *Not Authorized* list (using the CTRL or SHIFT keys).
6. Click AUTHORIZE.



*If you want to authorize all devices in the 'Not Authorized' List, simply select the user and click AUTHORIZE ALL.*

The selected media is added to the Authorized list.

### To deny access to DVDs/CDs/encrypted removable media

To remove permission from a user or group to use one or more DVDs/CDs/ encrypted removable media, proceed as follows:





1. Select the *Media by User* tab in the *Media Authorizer* module.
2. Select the user or group that you want to remove permissions from.
3. Select the DVDs/CDs/removable media from the *Authorized* list (using the CTRL or SHIFT keys).
4. Click REMOVE.



*If you want to remove all media assigned to a user, simply select the user and click REMOVE ALL.*



*Changes in permissions to access DVDs/CDs/removable media are read by the client computer next time the DVD/CD/removable media is inserted. The entire list of authorized DVDs/CDs/removable media is downloaded at user logon (assuming you are using the client version 4.2). This means that a disconnected user can access the media permissions which were downloaded when the user's machine was last online. These can include media the user has never used. These will be accessible to the user (permissions allowing).*

## Removing media from the database

This section describes how to remove the following three categories of media from the system database:

- > CDs and DVDs.
- > Encrypted removable storage devices.
- > Lost or damaged media.

### To remove a DVD/CD

1. Select the *Users by Medium* tab in the *Media Authorizer* module.
2. Select the DVD/CD in the *Authorized* list on the *Media* panel.
3. Click REMOVE MEDIA.

The media is removed from the database. If there are users associated with the DVD/CD, a warning message is displayed:

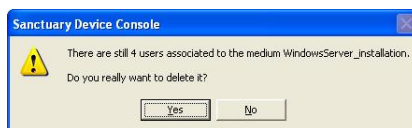


Figure 141: 'Users still associated with medium' warning message

You can click YES to proceed to remove the media from the database.

### To remove an encrypted removable storage device

1. Attach the device to your (the Sanctuary administrator) computer.
2. Select it from the *Authorized* list on the *Media* panel.
3. Click REMOVE MEDIA.

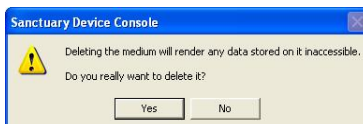
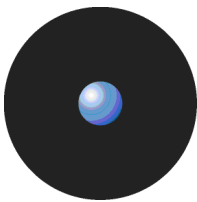


Figure 142: 'Deleting medium' warning message



*All encrypted data present on the device will be lost. The device is formatted after being removed from the database.*

## To remove lost or damaged media from the database

You may want to remove a media from the database if it is lost or damaged. Although you have no physical access to it, you can still delete it by selecting it and clicking on the REMOVE MEDIA button.



*Only delete lost or damaged devices that cannot be recovered.*

A warning message is displayed:



Figure 143: 'Cannot delete identification record' error message

The physical media remains encrypted. As there are no permissions anymore for these devices in the system, the Sanctuary Client Driver considers them as encrypted media coming from other organizations and prevents access to them. This happens unless the user has the password, encryption key, and has received proper access for using them in the Device Explorer module. See *Locally managed access to unauthorized encrypted media* on page 154.

When a device is in this particular state (still encrypted but removed from the database), the administrator can:

- > Add the device back into the database without losing its content. This is only possible if you import its encryption key before the device removal either to the device or to a file, and that you remember its password. In this case, you can use the *Import (secure for existing data)* command. The device is once more inserted into the database while preserving its content. See *Centrally managed access to unauthorized encrypted media* on page 153.
- > Reuse the device and re-encrypt it. This operation erases the device content. In this case, you can use the *Quick Format (insecure for existing data)* command.



*In case an encrypted device is no longer used for Device Control and you are unable to format it again in Windows Explorer (using the right-click format option), make sure you use the Disk Administrator on a computer without the Sanctuary Client Driver installed, to reformat the media (the standard FAT file system, not FAT32, is recommended). Other format methods may fail and render the media unusable until it has been reformatted properly. Alternatively, check it with the 'diskprobe.exe' tool found in the Windows resource kit if you are not sure that your media is working properly.*

## Other Media Authorizer utilities

In addition to the main utilities provided in the Media Authorizer to help you authorize and encrypt CDs, DVDs, and removable media, you can carry out a few more tasks:

- > Rename a DVD, CD, or removable storage device.
- > Export an encryption key.
- > Recover a password for decentralized encryption for an online user.
- > Eject a DVD/CD drive.

## To rename a DVD, CD, or removable storage device

1. Select the *Media by User* tab in the *Media Authorizer* module.



2. Select the DVD/CD/removable storage device you want to rename.
3. Click RENAME MEDIA. A dialog is displayed:

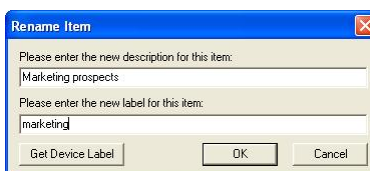


Figure 144: Renaming a DVD/CD/Removable storage device

4. Confirm or type a new description for the media. Use the GET DEVICE LABEL button to recover the information directly from the medium.
5. If the media is a removable storage device, confirm or type a new label, using up to 11 alphanumeric characters (upper and lower case and digits).
6. Click OK. The media is renamed.

## Exporting encryption keys

There are situations where encrypted removable storage devices need to be exchanged between people working in different organizations. Sanctuary Device Control allows you to export the media encryption key to permit its access outside of the company network.

The Media Authorizer allows an administrator to export the encryption key of an encrypted device. Although this is summarized below, for full details please refer to the *Centrally managed access to unauthorized encrypted media* section on page 153. Note that a user can also be allowed to export the encryption key when doing decentralized encryption (see *Forcing users to encrypt removable storage devices* on page 87).

1. On the *Users by Medium* tab, select an encrypted removable storage device.
2. Click EXPORT KEY. A dialog is displayed.

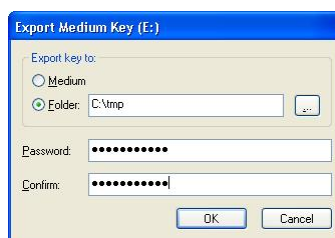


Figure 145: Exporting a medium key

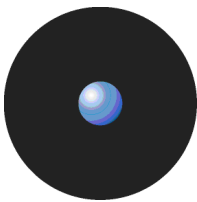
3. Choose either *Medium* to export the key to the device itself or select a *Folder* to export the key to a folder on your computer or network.
4. Type a *Password* and then *Confirm* it.
5. Click OK to export the device key.

## Ejecting a CD or DVD

To eject a CD or DVD from the drive attached to your computer, simply click the EJECT CD/DVD button. It is immediately ejected.

## Recovering a password for decentralized encryption when connected

Sometimes a user forgets the password they have set up to access an encrypted removable storage device that they want to attach to their computer, or fails to enter this password correctly after a specified number of attempts. The user must then contact a Sanctuary administrator with the identity of the device and a security code. Using this information the Administrator, if she approves access, can generate a passphrase. The device that the user needs to access is decrypted using the passphrase and re-encrypted using a new password.



*To provide the passphrase required to access the encrypted device without the password the administrator needs the appropriate access rights; The Sanctuary Management Console administrator's User Access must have 'Key Recovery (Device Control)' set to 'Yes'. See Defining Sanctuary administrators on page 32 for more information.*

*If the user forgets their encryption password when they do not have access to Sanctuary Client see Recovering a decentralized encryption password without Sanctuary Client on page 163.*

The procedure for recovering a password for decentralized encryption when you have access to Sanctuary Client involves a number of steps carried out by the user who wants to access the encrypted removable storage device, denoted [User] below, and a number of steps carried out by the administrator authorizing the decryption and re-encryption, denoted [Administrator]. To recover an encryption password:

1. [User] Click on the RECOVER PASSWORD button in the Unlock Medium window (in which the user normally enters the password required to access their encrypted device).



Figure 146: Unlock Medium window

*If the user attempts to guess their password more than the allowed number of times then the following message is displayed. In this case, he must click on the OK button before he can click on the RECOVER PASSWORD button.*

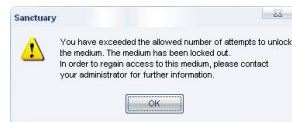


Figure 147: User exceeded allowed number of attempts to unlock medium message

The Recover Password dialog is displayed:

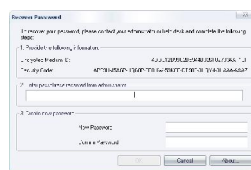
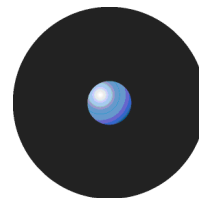


Figure 148: Recover Password dialog

2. [User] Telephone a Sanctuary administrator (with 'Key Recovery' access rights), explain your problem, and read out the 32-character Encrypted Medium ID (such as E34553B6F4C036488212AF4F1DE45E17).
3. [Administrator] If you need to check whether the person on the telephone is allowed to access the encryption media (rather than trusting their word for it), recover information about the user and computer from when the removable storage device was originally encrypted. To do this, carry out the following steps:
  - > Activate the *Log Explorer* module, if it is not already open.
  - > If the media has only recently been encrypted, force an upload of the latest log files. See *Forcing the latest log files to upload* on page 124.
  - > Select and run a template that generates a report of encrypted media. See *Log Explorer templates* on page 102.
  - > Identify the log entry in the report that corresponds to the original encryption event, using the first characters of the hash number that the caller read out.



- > Check the user and computer details and compare these with the details of the individual who is on the telephone, if required.

You can click on the Props tab in the Criteria/Properties panel of the Log Explorer window to view all the details of the log entry. See Criteria/Properties panel on page 111 for more information.

- > Check the full hash number in the report corresponds with that you have been given over the phone.



You can 'cut and paste' the hash number from the log into the Encrypted Medium ID field the following step to save time.

- [Administrator] Open the Sanctuary Password Recovery wizard on the Sanctuary Management Console. To do this, select *Key Recovery* from the *Tools* menu (or from the *Control Panel*). The Sanctuary Password Recovery wizard is displayed:

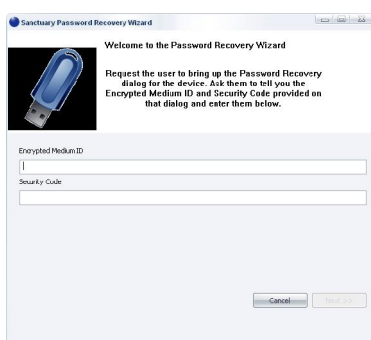


Figure 149: Sanctuary Password Recovery wizard - Encrypted Medium ID and Security Code page

- [Administrator] Enter the 32-character alphanumeric string provided by the user (or paste in the hash number from the previous step) in the Encrypted Medium ID field.
- [Administrator] Request a Security Code from the caller and, when this is read out to you, enter the 44-character alphanumeric string in the Security Code field.
- [Administrator] Click on the NEXT button.



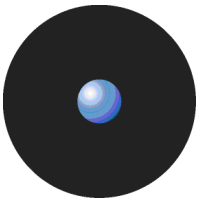
The NEXT button is only available if the Encrypted Medium ID and Security Code are the correct length.

If the Encrypted Medium ID and the Security Code were incorrectly entered, an error message is displayed explaining which one needs correcting. This can be edited and the NEXT button clicked on again.

If the Encrypted Medium ID and the Security Code were correctly entered, the Sanctuary Password Recovery wizard displays the Passphrase page. This provides details of the device and the person who originally encrypted the device, along with a Passphrase that can be used to decrypt the encrypted medium.



Figure 150: Sanctuary Password Recovery wizard - Passphrase page



8. [Administrator] If you approve the user's rights to access the encrypted removable storage device, read out the 52-character Passphrase (such as 8354Z-05DEP-M1ZGY-KKMCJ-AFLPR-8U773-C6ZQ7-Y5TUW-DP49Y-3Z5A7-7U).
9. [User] Enter the alphanumeric string provided by the administrator in the text field in the middle section of the Recover Password dialog.

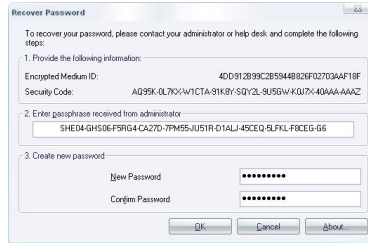


Figure 151: Recover Password dialog – entering passphrase

10. [User] Enter a New Password, retype this in the Confirm Password field, and click on the OK button. The following messages are displayed:



Figure 152: Sanctuary password recovered message



Figure 153: Sanctuary medium unlocked message

11. [Administrator] Once the user has confirmed that these messages are displayed, click on FINISH.

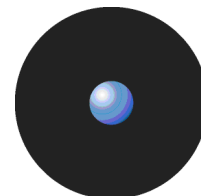
## Permissions Priority

Permissions to access DVD, CD and Removable Storage Devices can be defined in the Device Explorer and the Media Authorizer modules. This section explains how the Sanctuary Client Driver controls access when permissions are defined in both modules.

### Example 1:

In this first example, you have authorized the 'OfficeXP' DVD/CD using the Media Authorizer. The next table summarizes the resulting access when permissions are defined at the Device Explorer and Media Authorizer module levels. Note that in this example, permissions can be assigned directly to user Bill or to the user groups he belongs to.

<b>Device Explorer DVD/CD access defined for user Bill</b>	<b>Permission defined in Media Authorizer for user Bill to 'OfficeXP'</b>	<b>Resulting access when Bill inserts 'OfficeXP' in his drive</b>	<b>Resulting access when Bill inserts any other CD in his drive</b>	<b>Comments</b>
No access is defined (default)	Access granted to 'OfficeXP'	Yes	Denied	When nothing is defined in the Device Explorer, Bill can only access the DVDs/CDs granted to him in Media Authorizer.
	No access to 'OfficeXP'	Denied	Denied	
Read-Only	Access granted to 'OfficeXP'	Read-Only	Read-Only	The permissions defined in the Device Explorer take precedence.
	No access to 'OfficeXP'	Read-Only	Read-Only	
Read/Write	Access granted to 'OfficeXP'	Read/Write	Read/Write	
	No access to 'OfficeXP'	Read/Write	Read/Write	
'None'	Access granted to 'OfficeXP'	Denied	Denied	A 'negative' permission, with High or Low priority takes always



	No access to 'OfficeXP'	Denied	Denied	precedence on Media Authorizer permissions, the access to the DVD/CD drive has been specifically denied.
--	-------------------------	--------	--------	--

Table 37: Resulting access when permissions are defined at the Device Explorer and Media Authorizer levels (Example 1)

If a user already has permission to use the DVD/CD-ROM drive assigned in the Device Explorer module, assigning permission to use specific DVDs/CDs in the Media Authorizer has no further effect.

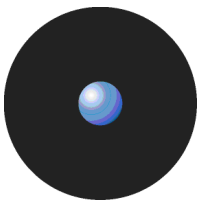
**Example 2:**

In this second example, you have encrypted the 'DiskOnKey8' removable storage device using the Media Authorizer. The table summarizes the resulting access when permissions are defined at the Device Explorer and Media Authorizer module levels:

<b>Device Explorer Removable Storage Devices access defined for user Bill</b>	<b>Permission defined in Media Authorizer for user Bill to 'DiskOnKey8'</b>	<b>Resulting access when Bill connects 'DiskOnKey8' to his computer</b>	<b>Resulting access when Bill connects any unencrypted storage device</b>	<b>Comments</b>
No access is defined (default)	Access granted to 'DiskOnKey8'.	Read/Write	Denied	Even though nothing is defined in the Device Explorer, Bill (as an example user) can read and write to the encrypted media he has been granted access.
	No access to 'DiskOnKey8'.	Denied	Denied	
Read-Only	Access granted to 'DiskOnKey8'.	Read/Write	Read-Only	When an access is granted in the Media Authorizer, it allows read and write operations even if there is a read only permission defined in the Device Explorer.
	No access to 'DiskOnKey8'. The user does not have the encryption key nor the password.	Denied	Read-Only	
	No access to 'DiskOnKey8'. The user has the encryption key and password.	Read/Write	Read-Only	
Read/Write	Access granted to 'DiskOnKey8'.	Read/Write	Read/Write	The Read/Write permission defined in the Device Explorer, does not allow access to an encrypted media, this operation is done solely by the Media Authorizer.
	No access to 'DiskOnKey8'. The user does not have the encryption key nor the password.	Denied	Read/Write	
	No access to 'DiskOnKey8'. The user has the encryption key and password.	Read/Write	Read-Only	
'None'	Access granted to 'DiskOnKey8'.	Denied	Denied	A 'negative' permission takes always precedence on any other permission, the access to a removable storage device has been specifically denied.
	No access to 'DiskOnKey8'. The user does not have the encryption key nor the password.	Denied	Denied	
	No access to 'DiskOnKey8'. The user has the encryption key and password.	Denied	Denied	

Table 38: Resulting access when permissions are defined at Device Explorer and Media Authorizer levels (Example 2)

The access to an encrypted media is controlled in the *Device Manager* module and the *Media Authorizer* module. The 'No access' ('None' in the Permissions column) rule defined in the Device Manager module always take precedence over the 'Media Authorizer' rule. Likewise, device rules alone may grant access to encrypted media even when no rules are defined in the *Media Authorizer* module; in this last case, however, media access is not transparent and the user must have the media key and password. While this scenario



may be useful in certain situations, it should generally be avoided since it is difficult to control and because password-protected keys are inherently weak.

If you specifically denied access to the DVD/CD Drives class, the Removable Storage Devices class, or one of their respective sub classes using a 'None' permission in the Device Explorer, whatever its priority, then the permission granted with the Media Authorizer is ignored. When a permission has been set with no Read nor Write access in the Device Explorer, it takes precedence and prevents access to the media whatever other permissions set. Please refer to *Priority of default permissions* on page 69 for more details on how permission priorities are applied.

Rights defined in Media Authorizer are cumulative. If a user is member of ten different groups, he has access to all CDs authorized to the groups from which he is a member. Please note that Encrypted media cannot be granted to groups.

## Encrypting devices without a Certificate Authority

Sometimes there is no Certificate Authority present and you are not willing to install one on your computer. You can still benefit from the encryption of removable media using the procedure described on the following section.

### To encrypt a removable media without installing a Certificate Authority

1. Proceed to a machine that has both the Sanctuary Management Console and the client installed. Open the console and plug an USB memory key to the machine. You should have previously given access to the memory key —activate the *Export to Media* option. Please see *Chapter 4: Managing permissions/rules* on page 57 for more information.
2. Close all programs that might use the media, including Windows Explorer. You are now ready to encrypt the device.
3. Encrypt the device in the normal way. See the procedure on page 132.
4. Export the media encryption keys on the media itself and provide a password. Check the permissions to be sure that you have the right to do this.
5. **IMPORTANT STEP:** Remove the USB key from the machine
6. Delete the newly created encrypted key from the list. You are deleting all traces of this key.
7. At this stage, you have an encrypted memory key with a password-controlled access containing an encryption key. This is equivalent to a key encrypted by another company using Sanctuary Device Control.
8. Define Read/Write and Import permissions on the *Encrypted removable media* class using the *Device Explorer* module so that your users can access this key. Users with permissions defined in this class can access the encrypted device, providing they also know the appropriate password.
9. Limitation: You can also access other devices that come from other companies and were encrypted by Sanctuary Device Control.



*If you plan to use this feature, please remember to 'Disable' the 'Certificate Generation' option for the client machine. Otherwise, a new one is created because it does not exist and you end up with unused client certificates. Please refer to Chapter 8: Setting and changing options on page 169 for more information on how to do this.*



---

## Chapter 7: Accessing encrypted media outside of your organization

There may be situations when data on a specifically authorized (encrypted) device would need to be accessed from a machine that is not part of your organization. This machine may or may not be protected by Sanctuary Device Control.

### Exporting encryption keys

In order to make a device accessible its encryption key must be imported. Before an encryption key may be imported, it must be exported from Sanctuary Device Control.

The Sanctuary administrators can export device encryption keys centrally or grant users the right to export the encryption keys of their devices locally.

There are two different ways to export encryption keys:

- > The most secure way is to export the media encryption key to a file and send it via a different channel (email for example) to the person that needs to access the encrypted media outside the organization.
- > The second way is to export the key to the encrypted media itself. This method is significantly less secure as the level of difficulty to access the data is directly linked to the media password complexity.

### Exporting encryption keys centrally

With Sanctuary Device Control, the administrator can export encryption keys for any device in the system.

In the Media Authorizer, it is easy to select a device and export its encryption key. You can export the encryption key, either by creating a password-protected encryption key file that can be sent to another computer or user, or by writing the encryption key to the media, where it will also be password-protected. See *To export the encryption key to a file* on page 151 and *To export the encryption key to the device itself* on page 152 respectively for details.

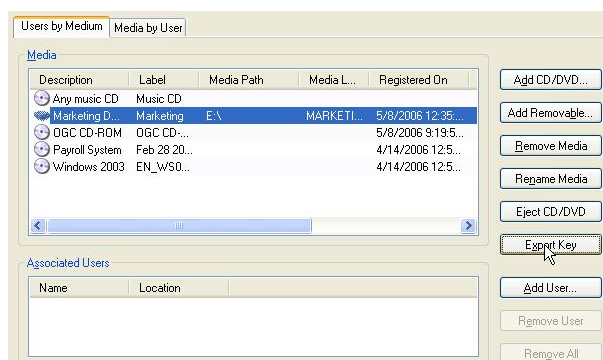


Figure 154: Exporting encryption keys



## Exporting encryption keys locally

Using Sanctuary Device Control, the administrator can give users the option to export an encryption key. A user may only export encryption keys locally if he has been given the rights to do so (using the Permissions dialog - see *Using the Permissions dialog* on page 57 for more details).

There are three conditions that must be met before a user to export a medium encryption key locally:

- > The user must have received proper access to the media. Please refer to *Chapter 6: Using the Media Authorizer* on page 129 for more details on granting user access to encrypted media.
- > The user must be logged on a computer with the permissions set to *Export To file* or *Export to media*. Please refer to *Special case: Working with Removable Storage Devices* on page 59 for more details.
- > The media must be attached to the user's computer.

If those three requirements are met, the *Export medium key* option is available in the context menu of the encrypted drive in Windows Explorer. (This option is not available if the key was exported to a file and its location given to the user.) The user can then export the encryption key, either by:

- > Creating a password-protected encryption key file that can be sent to another computer or user. See *To export the encryption key to a file* on page 151.

-or-

- > Writing the encryption key to the media, where it is password-protected. See *To export the encryption key to the device itself* on page 152 for details.

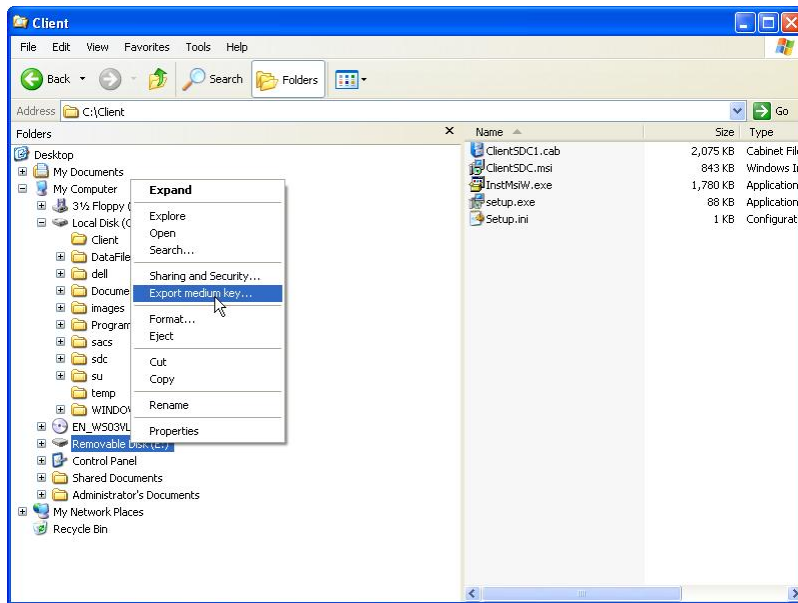


Figure 155: Exporting encryption keys (by the user)



## To export the encryption key to a file

Exporting the encryption key to a file is the most secure way to export the medium encryption key. You can send it via a different channel (email for example) to the person that needs to access the encrypted media outside the organization.

In the case of a central encryption key export, it is the Sanctuary administrator who does this (see *Exporting encryption keys centrally* on page 149 for more details). On the other hand, in the case of a local encryption key export, it is the user who does this (see *Exporting encryption keys locally* on page 150 for more details).


1. Either:
  - > For an administrator, centrally, select the device in the *Media Authorizer*, and click EXPORT KEY.
  - or–
  - > For a user, locally, right-click the device in the Windows Explorer, and select *Export medium key*.


The *Export Medium Key* dialog is displayed.



Figure 156: Export Medium Key dialog - to export the encryption key to a file

2. Select the *Folder* option.
3. Type the folder location or click the ellipsis button (...) to find the location, to which you want to export the keys.
4. Type a password in the *Password* and *Confirm* fields.

 *In the case of a local export, password complexity checks may be performed to guarantee that a secure password is chosen by the user. The check performed on the password strength depends on the settings of the Encrypted media password option as described on page 173. This option **does not** apply for administrators performing central export.*

 *If the Sanctuary administrator has set the Encrypted media password option (see page 173) to 'Require Password complexity', the password chosen by the user when doing a local export must meet certain requirements. It must:*

- > *Be at least eight characters long.*
- > *Contain upper and lower case letters.*
- > *Contain digits.*
- > *Contain at least one non-alphabetical character (!@#%\*...).*

5. Click OK.
6. Communicate the password and send the key file and the encrypted device to the person who needs to access the encrypted media from outside the organization. We recommend you use separate channels to send the encryption key, the medium and the password. For example, you could send the device by post, the encryption key by email and communicate the password by phone.



## To export the encryption key to the device itself

You can also export the encryption key directly to the encrypted device itself. This second method is significantly less secure as the level of difficulty required to access the data is directly linked to the device password complexity.

In the case of a central encryption key export, it is the Sanctuary administrator who does this (see *Exporting encryption keys centrally* on page 149 for more details). For local encryption key export, it is the user who does this (see *Exporting encryption keys locally* on page 150 for more details).

1. Either:
  - > For an administrator, centrally, select the device in the *Media Authorizer*, and click EXPORT KEY.
  - or–
  - > For a user, locally, right-click the device in the Windows Explorer, and select *Export medium key*.

The *Export Medium Key* dialog is displayed.

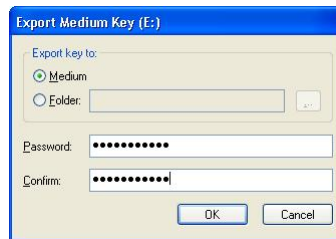


Figure 157: Export Medium Key dialog - to export the encryption key on the device itself

2. Select the *Medium* option.
3. Type a password in the *Password* and *Confirm* fields.



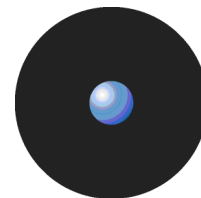
*Password complexity checks may be performed to guarantee that a secure password is chosen. The check performed on the password strength depends on the settings of the Encrypted media password option as described on page 173. This option **does not** apply for administrators performing central export.*



*If the Sanctuary administrator has set the Encrypted media password option (see page 173) to 'Require Password complexity', the password chosen by the user when doing a local export must meet certain requirements. It must:*


- > *Be at least eight characters long.*
- > *Contain upper and lower case letters.*
- > *Contain digits.*
- > *Contain at least one non-alphabetical character (!@#%\*...).*

4. Click on OK.
5. The user must communicate the password and send the encrypted device to the person who needs to access the encrypted device from outside the organization. If the device is lost or stolen, the password strength is the only barrier to access the data.



## Accessing encrypted media outside your organization

This section explains various scenarios and options for accessing media outside of your organization.

 *Users cannot use the encrypted medium outside of the company network if they do not have the medium encryption keys and password. The exporting of media encryption keys is controlled by the organization through the means of the local and central export of encryption keys.*

### Accessing media on a machine with Sanctuary Client Driver installed

You typically access media on a machine with Sanctuary Client Driver when two separated organizations protected by Sanctuary Device Control want to exchange data on Sanctuary Device Control encrypted media.

We define *Unauthorized Encrypted Media* as media encrypted using Sanctuary in another organization with a separate implementation of Sanctuary Device Control.

You can let your Sanctuary Administrators centrally control and authorize devices that come from other organizations or grant trusted users the right to use them.

### Centrally managed access to unauthorized encrypted media

You should follow this procedure when you want your Sanctuary Administrator to manage the access to the devices coming from other organizations.

With this method, users, even if they have the unauthorized encrypted media, its encryption key, and password, cannot use 'foreign' keys unless the administrator has authorized the device and granted them the right to use it with the Media Authorizer module.

The central authorization is done in two steps. The administrator first adds the device in the Media Authorizer module, and then grants users access to it.

### To add a device in the Media Authorizer

1. Attach the device to the administrator computer. This must have installed the Device Control Client and Console, and have read/write access to the Removable Storage Devices category. See *Encrypting removable storage devices* on page 132 for more details.
2. Using the Media Authorizer, click ADD REMOVABLE. The following dialog appears:

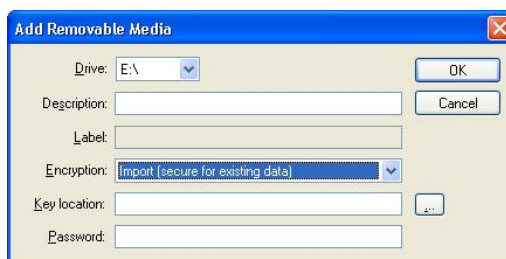


Figure 158: Adding a device with an external key

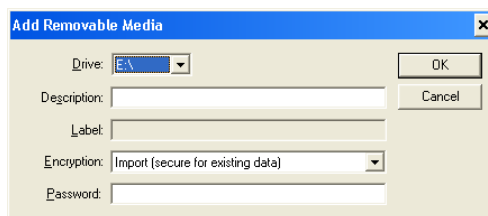
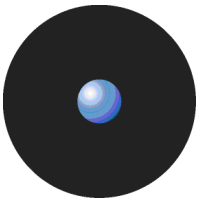


Figure 159: Adding a device where the key resides on the medium



3. Type the media *Description*. We strongly recommend that a physical label is stuck to the device identify it in the future.
4. In the *Encryption* field, choose to import the encrypted device (the default option). All information on the device is kept. Alternatively, you can choose to format the device when you want to re-use it while losing its information.
5. In the *Key location* field, browse for the file using the ellipsis button (...). This field is not available when the key was exported to the medium itself.
6. Type the media password in the *Password* field.
7. Click OK. Provided you have entered the right key and password, the device appears in the list of encrypted media in the Media Authorizer.

The encrypted medium is now included in the database and can be assigned to the required user(s).

### Granting user access to the device

After adding the media, you can use the Media Authorizer to grant users the right to access the media. See *To grant access to use DVDs/CDs/encrypted removable media* on page 138 for details.

### Locally managed access to unauthorized encrypted media

You may want to delegate to trusted users the right to access Sanctuary Device Control encrypted media coming from other organizations. This permission is controlled using the *Removable Storage Devices* class of the Device Explorer. See *Chapter 4: Managing permissions/rules* on page 57 and *To assign computer-specific permissions to users and groups* on page 71 for more information about setting up permissions.

You can set the following permissions:

- > Scheduled and temporary permissions – to restrict access to the *Removable Storage Devices* for a given time period.
- > Offline and online permissions – to assign Read or Read/Write permissions applying when the user is directly connect or not to the network.
- > Permissions for the *Removable Storage Devices* class – to restrict access to these devices. These can be defined as a Global permission (Default Settings section) or at the computer-specific level (Machine-Specific Settings section).
- > Read-only or Read/Write permissions. If a permission is read-only, your users can only read the content of the unauthorized encrypted media, not right to them.
- > Negative permissions ('None'). You can use these to specifically deny access to unauthorized encrypted media to a user or group.
- > You can add File Filtering to the *Removable Storage Devices* to further control access.

The priorities that apply for the *Removable Storage Devices* class are the same as the ones described in *Priority of default permissions* on page 69.

To access unauthorized encrypted media from other organizations, your user needs the following:

- > Appropriate permissions in the *Removable Storage Devices* class. This must include the right to Import on encrypted media devices.



*If a medium has an exported key, for example if it was encrypted using decentralized encryption, then a user with 'Import' permission can 'unlock' and import that medium.*

- > The encrypted device to be attached to his computer.
- > The encryption key file, if the disk encryption key is not stored on the device.
- > The password to access the device.



Providing these conditions are met, the users can access the unauthorized encrypted media.

### To access unauthorized encrypted media

Users can access unauthorized encrypted media using the following steps:

1. Attach the device to the computer.
2. In Windows Explorer, select the *Unlock medium* option from the right-click (contextual) menu of the encrypted drive.

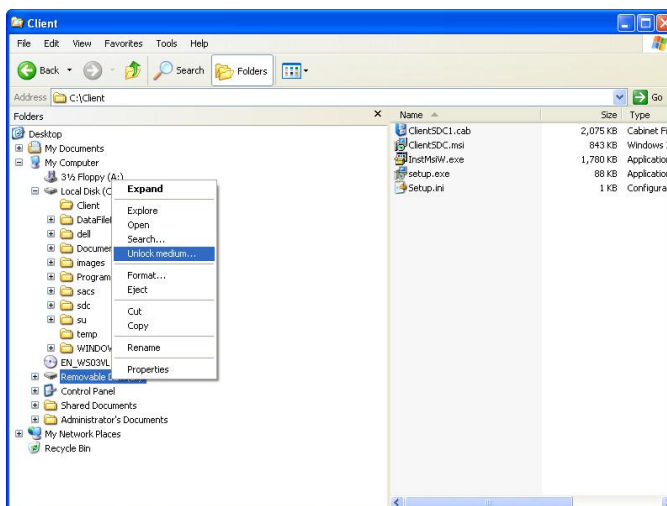


Figure 160: Accessing unauthorized encrypted media

The *Import Medium Key* dialog is displayed.

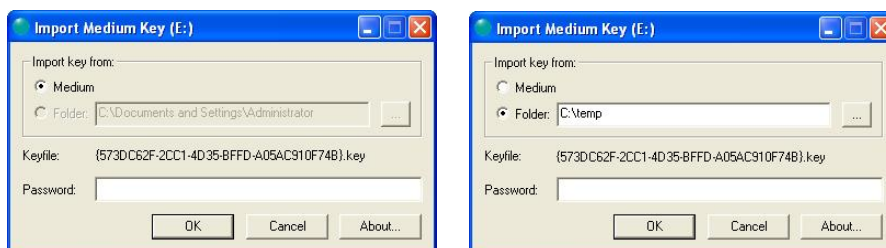
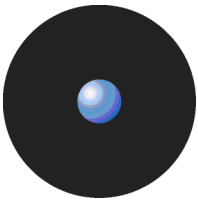


Figure 161: The Import Medium Key dialog (importing from the medium or a folder)

3. If the disk encryption key was exported on the encrypted media, select *Medium*. If the key was exported to a file, select *Folder* and browse for it using the ellipsis button (...).
4. Type in the media password in the *Password* field.
5. Click OK. Provided you have entered the right key and media password, the media is now unlocked and accessible using Windows Explorer.



*All data copied from the media to the computer's hard drive is decrypted during the copy operation and will be copied on the hard disk drive unencrypted. Make sure you store the copied files in a secure location. All data copied from the hard drive to the media will be encrypted during the copy operation.*



### To format an encrypted device

Once a key is encrypted, the user can use it, if the appropriate rights are given. However, they cannot format it as Windows Format command needs the key to be unlocked with the correct password. To format an encrypted key, the user must right-click on the device and select the **DECRYPT MEDIUM** menu option.



*Take care not to click this option if you know the password unless, of course, you need to format the disk.*

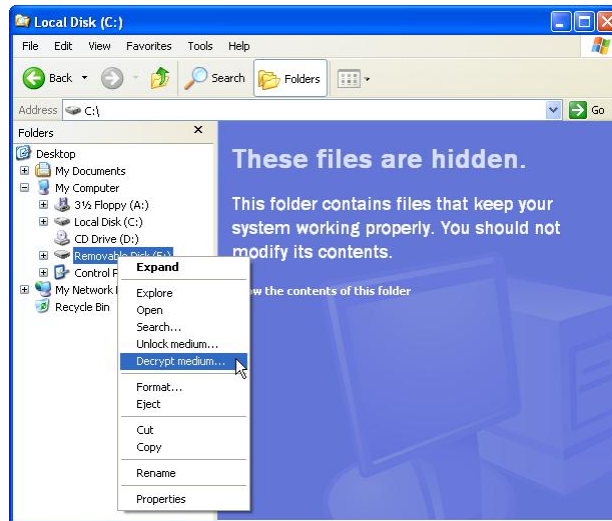


Figure 162: Formatting an encrypted key using the Decrypt Medium command

### Differences between locally and centrally managed access to Unauthorized Encrypted Media

**Centrally** managed access to unauthorized devices has the following characteristics:

- > The media, its encryption key, and password have to be provided to the Sanctuary Administrator. The password and encryption key file are only required when adding the media to the list of encrypted ones.
- > The administrator cannot grant read-only access, because the *Media Authorizer* only allows read/write access.
- > The administrator cannot grant user groups access to a specific device. Access has to be granted to each user individually.
- > The administrator controls the access to each encrypted device individually. It is not possible for the users to use a device that is not specifically authorized.
- > The access cannot be restricted to a given computer (except if the permission was given to the local user of a computer).

The **locally** managed access to unauthorized devices has the following characteristics:

- > The media, its encryption key, and password have to be directly provided to the user. The user needs to specify the encryption key location and password every time the media is inserted.
- > The password and encryption key file are required only by the user. The administrator has no control over the unauthorized encrypted media origin.
- > The administrator can grant read-only / read-write and temporary / scheduled / permanent access to Encrypted Removable devices. He can control when and how unauthorized encrypted media is accessed, but he has no control over which device is accessed. This control is delegated to the user.
- > The administrator can grant users or user groups access to Encrypted Removable devices, allowing them to use any unauthorized encrypted media. This permission can be set at the default permissions





level (Default Settings section) or at the computer-specific level (Machine-Specific Settings section). Therefore, allowing access to such devices on a specific computer is possible.

- > The administrator can grant Offline and Online permissions to the user. He can assign Read or Read/Write permissions depending if the user is directly connect or not to the network.

**To import an externally encrypted device to the database**

1. Plug the device in a computer that has the client and the Sanctuary Management Console. The Sanctuary Administrator also needs the encryption key file (on the device or externally) and the password.
2. Select the *Media Authorizer* module from the *Control Panel* or the *View* menu
3. Click the **ADD REMOVABLE** button. The following dialog appears:

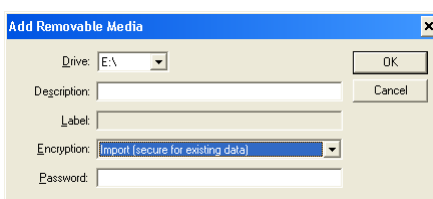


Figure 163: Importing an external device

4. Select the *Import (secure for existing data)* option from the list. Type the password.

The medium is added to the database and is displayed in the upper panel:

Description	Label	Media Path	Media Label	Registered On	Registered By	Comments
Any music CD	Music CD					
Imported media	DK03PH	E:\	DK03PH	7/25/2006 4:18:...	LU\Administrator	

Figure 164: Importing an external device

5. Select the medium in the upper panel and click on **ADD USER**.
6. Choose the user(s) that will be using this device (either by typing the name or using the **SEARCH** or **BROWSE** button) and click on **OK**.

The user is now associated with the device and can use it directly on its computer. The following image shows a user (Bill) assigned to an imported medium:

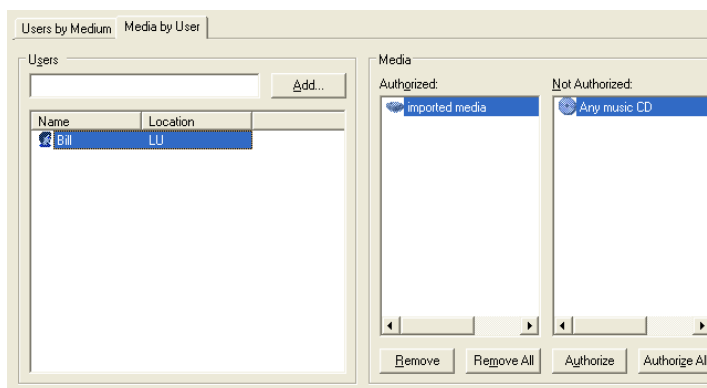


Figure 165: Importing an external device



## Accessing media without using Sanctuary Client Driver

You typically want to access encrypted media from a computer that does not have Sanctuary Client Driver installed on it when encrypted devices are exchanged between a company protected by Sanctuary Device Control and an organization that is not.

To access a device encrypted by Sanctuary from a machine where the Sanctuary Client Driver is not installed, a user can either:

- > Use the Sanctuary Device Control *Stand-Alone Decryption Tool (SADEC)*.

-or-

- > Encrypt using the *Easy Exchange* encryption option.

## Sanctuary Device Control Stand-Alone Decryption Tool (SADEC)

Before using the Sanctuary Device Control Stand-Alone Decryption Tool, a user requires the following:

- > The Sanctuary Device Control Stand-Alone Decryption Tool installed on his computer. This tool can be found on the Sanctuary CD under the SADEC folder, or downloaded from the SecureWave web site ([www.securewave.com](http://www.securewave.com)).



*The Sanctuary Device Control Stand-Alone Decryption Tool cannot be installed on computers protected by the Sanctuary Client Driver.*



*The Sanctuary Device Control Stand-Alone Decryption Tool can only be installed on Windows 2000, Windows XP Professional, Windows XP Home Edition, Windows 2003, and Vista (32- and 64-bit).*

Please refer to the SADEC.pdf guide on the Sanctuary distribution media for details on how to install the Sanctuary Device Control Stand-Alone Decryption Tool.

- > The encrypted device attached to his computer.
- > If the disk encryption key is not stored on the device, the encryption key file is needed.
- > The password to access the device.

## To use Sanctuary Device Control Stand-Alone Decryption Tool

Providing the requirements described in the previous section are met, you can use this procedure to access the encrypted device using the Sanctuary Device Control Stand-Alone Decryption Tool:

1. Check that the Sanctuary Device Control Stand-Alone Decryption Tool is installed on the computer.
2. Attach the device to the computer, if this has not already been done.
3. In Windows Explorer, select the *Unlock medium* option from the right-click (contextual) menu of the encrypted drive.

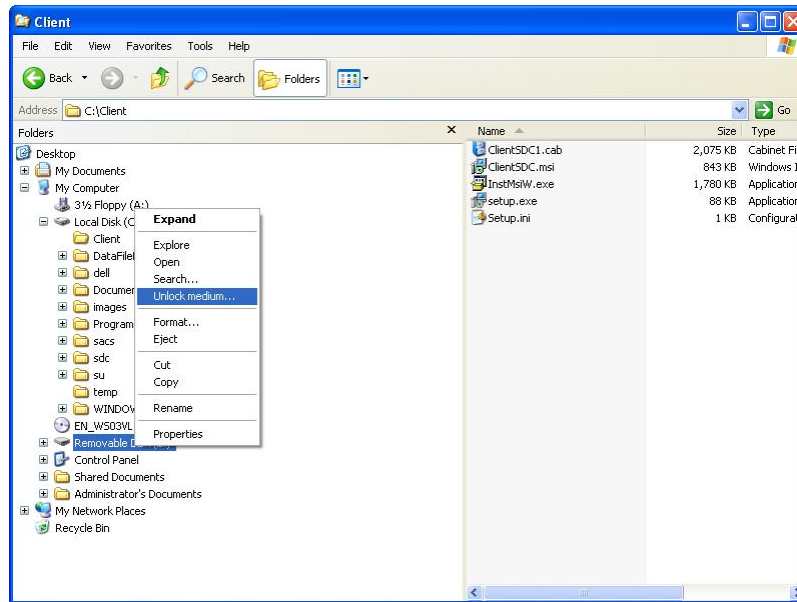
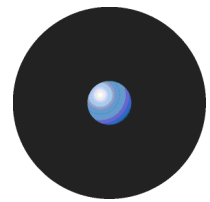


Figure 166: Using the Sanctuary Device Control Stand-Alone Decryption Tool

The *Import Medium Key* dialog is displayed:

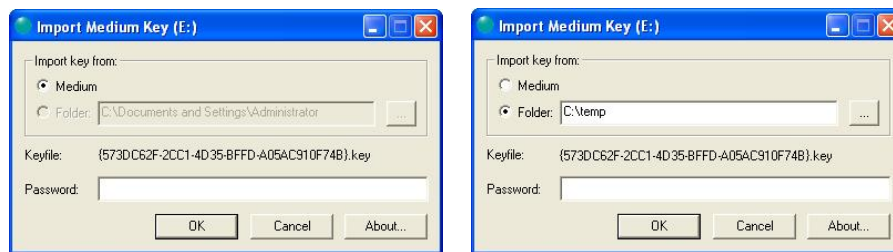



Figure 167: The Import Medium Key dialog when using the Stand-alone decryption tool

4. If the disk encryption key was exported on the encrypted media, select *Medium*. If the key was exported to a file select *Folder* and browse for it using the  button.
5. Type in the media password in the *Password* field.
6. Click OK. Provided you have entered the right key and media password, the media is now unlocked and accessible using Windows Explorer.



*All data copied from the media to the computer's hard drive is decrypted during the copy operation and will be copied on the hard disk drive unencrypted. Make sure you store the copied files in a secure location. All data copied from the hard drive to the media will be encrypted during the copy operation.*

## Easy Exchange

As an alternative to the Sanctuary Device Control Stand-Alone Decryption Tool for using data outside your company, you can use the *Easy Exchange* encryption option during the removable media encryption. Please see *To encrypt a specific removable storage device* on page 135 for more information.

### To encrypt a medium using Easy Exchange

1. Connect the medium to a computer that has the console and click the ADD REMOVABLE button.
2. Type-in the description and label. Select the *Easy Exchange (insecure for existing data)* option from the pull-down list.



- 3. Once the removable media has been encrypted, you can export the encryption key to the media or to a file, using the EXPORT KEY button.

Once you encrypt the medium this way, you can transport it safely to another machine. When inserting the medium and running the included Sanctuary Volume Browser application (SVolBro.exe), there are two possible cases:

- > The key is located in the medium itself: in this case, the program only asks for a valid password.
- > The key was exported to a folder: you should first import the key and then provide a valid password to unblock the medium.

The following table summarizes these settings:

Key's action	Key's location	To access the medium the user must	Notes
Key Exported	On the media	Know the password (the key is available in the medium itself).	A good compromise between security and safety. Try using a strong password schema.
	In a folder	Know the password and have the key.	Best security setting since the user has to have two elements to access the media's data.
Key not exported	n/a	Know the password and have the key.	The administrator must eventually export the key so that the user can access the medium.

Table 39: Easy Exchange encryption options

In both cases, and only if the user has the correct elements (password plus key), an explorer is shown in the Sanctuary Volume Browser from where all file extract, add, or remove operations are done:

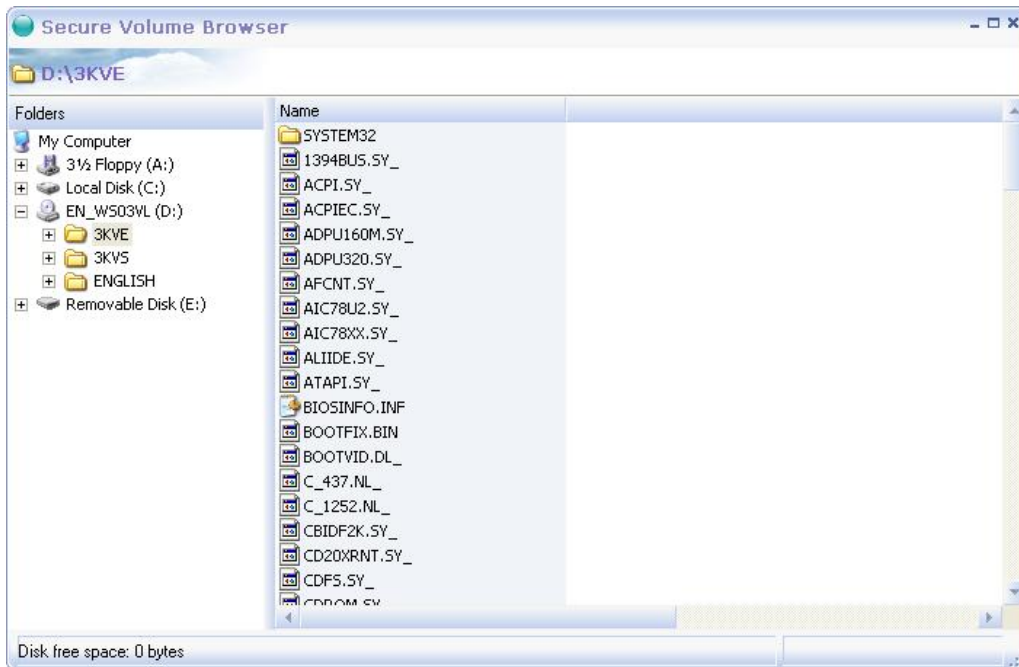
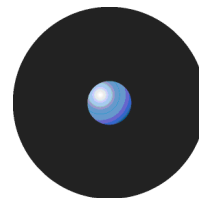


Figure 168: Sanctuary Volume Browser

The behavior and functionality of this browser is similar to Windows Explorer. You can:

- > Copy & paste.
- > Select multiple files.
- > Use a context menu with the most common file operations.
- > Double-click to save a file to your local hard disk and modify it.
- > Rename a file.



- > Create and erase folders.
- > Move files within the same volume.
- > Drag & drop internally or externally to the desktop, Windows Explorer, or any other application as per Windows' rules (see notes at the end of this section).

The user can use his data without needing to install any kind of software whatsoever, and without having administrative privileges. Sanctuary Volume Browser can also be run manually or automatically from the command line using different parameters:

```
SVolBro.exe [-p password] [-t target] [-k exported key]
```

Where:

- > -p is the password for the medium.
- > -t is the path where the encrypted folder is located (for example, d:\).
- > -k is the path where the exported encryption key is located. If not specified, the program looks on the path specified by the -t parameter.

If Sanctuary Volume Browser is called using another program, all required parameters (password, path of the encrypted folder, and encryption key location) are transparently interchanged, if provided.



*You should tell users not to remove USB devices directly without using the 'Safely Remove Hardware' icon (double or single click) located on the System Tray. If the user removes the device without warning, some files may be lost as Windows may not have written them from temporary memory to the volume. You should also insist that users close the Sanctuary Volume Browser window **before** unplugging the device.*



*Strong password policy is always enforced for the 'Easy Exchange' schema — unless you use it in the Media Authorizer module and change the Encrypted Media Password option (as described in Encrypted media password on page 173). The password is at least eight characters that shall include at least one letter, digit and one symbol.*



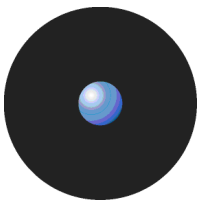
*You cannot use Windows' 'Send to' command (right-click menu) to directly copy files to a Sanctuary-encrypted medium (encrypted using the Easy Exchange method) — it must first be cipher using the proper algorithm, password, and key — this is only done using Sanctuary Volume Browser interface. Any of the other methods proposed by Sanctuary Volume Browser are valid (copy and paste, drag and drop, etc.).*



*Associated file icon images are lost inside Sanctuary Volume Browser since Windows does not have access to extract file resources inside an encrypted medium (or folder).*



*The combined file + path name should not exceed 256 characters.*



## Using encryption inside and outside your organization

The following two tables summarize encryption using the Full Encryption or Easy Exchange methods inside and outside your company, and depending whether Microsoft Certification Authority (MS Enterprise CA) is installed or not.

	<b>Full Encryption</b>			
	<b>(MS Enterprise CA is installed)</b>		<b>(MS Enterprise CA is not installed)</b>	
	<b>Access to the medium</b>			
	<b>Granted</b>	<b>Not granted</b>	<b>Granted</b>	<b>Not granted</b>
<b>Used within the organization's network</b> (Sanctuary Client Driver is installed)	Transparent access for the user, i.e. directly read and write from/to the removable storage device is possible without the need of a password or public encryption key.	A message informs the user that the device is not accessible.	A message informs the user that the device is not accessible. The medium can be unlocked using the right-click menu if the user knows the password and has the public encryption key.	A message informs the user that the device is not accessible.
<b>Used outside the organization's network</b> (Sanctuary Client Driver is not installed)	The user cannot read data — only garbled information is seen.			
<b>Measures for accessing data outside of the network</b>	The user must install the Stand Alone Encryption Tool (SADEC) and have the password/public encryption key — administrator rights are needed to install the software.			

Table 40: Full Encryption method inside and outside your company

	<b>Easy Exchange</b>			
	<b>(MS Enterprise CA is installed)</b>		<b>(MS Enterprise CA is not installed)</b>	
	<b>Access to the medium</b>			
	<b>Granted</b>	<b>Not granted</b>	<b>Granted</b>	<b>Not granted</b>
<b>Used within the organization's network</b> (Sanctuary Client Driver is installed)	Transparent access for the user, i.e. directly read and write from/to the removable storage device is possible without the need of a password.	A message informs the user that the device is not accessible.	A message informs the user that the device is not accessible. The medium can be unlocked using the right-click menu if the user knows the password and has the public encryption key. The user can also format the key using the Decrypt Medium option available in the right-click menu.	A message informs the user that the device is not accessible.
<b>Used outside the organization's network</b> (Sanctuary Client Driver is not installed)	The device includes a copy of SVolBro.exe (Sanctuary Volume Browser), no data is available.			
<b>Measures for accessing data outside of the network</b>	The user must start Sanctuary Volume Browser and provide a password. If the public encryption key is available, the user is given full access to the device's data using Sanctuary Volume Browser — no software to install, no administrator rights needed.			

Table 41: Easy Exchange encryption method inside and outside your company



## Decentralized encryption

Decentralized encryption is an alternative schema used when the organization does not need or want to control device encryption centrally using the Media Authorizer module.

Users can directly encrypt devices following the policies that Sanctuary administrators set. Administrators are not the only ones that can set encrypted devices for users' usage — users themselves or a designated agent can alternatively do this.



*Data recorded on a removable storage device before it is encrypted can be read following encryption. To enable this the user should select the appropriate checkbox when encrypting the removable storage device.*

Once administrators have set the rules, users are now on their own. The rules can be defined at the following different levels:

- > Class level — all data that a user copies to a removable device must be encrypted.
- > Model level — the data a user copies to certain types of devices must be encrypted.
- > Device level — anything a user writes to a specific, uniquely identified device, i.e. a particular serialized removable media, must be encrypted.

Decentralized encryption is backed-up by the Sanctuary Volume Browser tool (SVolBro.exe) allowing access to the device on unprotected machines. There are several important points regarding Sanctuary Volume Browser:

- > It is stored on the removable media itself.
- > It does not require any drivers.
- > It does not require administrative rights.
- > It does not mean that the USB key is recognized as a CD or floppy for authentication, as most of the external USB keys with embedded encryption do.

The size of the Sanctuary Volume Browser application is only 300KB, small enough considering the high capacity of most modern USB removable media.

The encryption process itself uses our 'Easy Exchange' method to cipher the medium. See *Easy Exchange* on page 159 for more information.

### How to configure Sanctuary so that users can encrypt their own devices

Please refer to *Forcing users to encrypt removable storage devices* on page 87 for more information, examples, and a step-by-step guide on how to set up decentralized encryption.

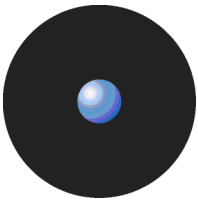
### Recovering a decentralized encryption password without Sanctuary Client

Sometimes users who are working on computers that do not have Sanctuary Device Control installed on them forget their encryption passwords for decentralized encrypted devices, or they fail to enter an encryption password correctly after a specified number of attempts.

In such a case, the user needs to use Sanctuary Volume Browser (since they do not have Sanctuary Device Control) and contact a Sanctuary administrator with the identity of the device and a security code. Using this information the Administrator, if she approves access, can generate a passphrase. The device that the user needs to access is decrypted using the passphrase and re-encrypted using a new password.



*To provide the passphrase required to access the encrypted device without the password the administrator needs the appropriate access rights; The Sanctuary Management Console administrator's User Access must have 'Key Recovery (Device Control)' set to 'Yes'. See *Defining Sanctuary administrators* on page 32 for more information.*



*If the user forgets their encryption password when connected to the network see Recovering a password for decentralized encryption when connected on page 143.*

The procedure for recovering a password for decentralized encryption without Sanctuary Client involves steps carried out by the user who wants to access the encrypted removable storage device, denoted [User] below, and the administrator authorizing the decryption and re-encryption, denoted [Administrator]. You can recover an encryption password without Sanctuary Client using the following steps:

1. [User] From Windows Explorer, launch the Sanctuary Volume Browser application (SVolBro.exe) that is stored on the encrypted device.

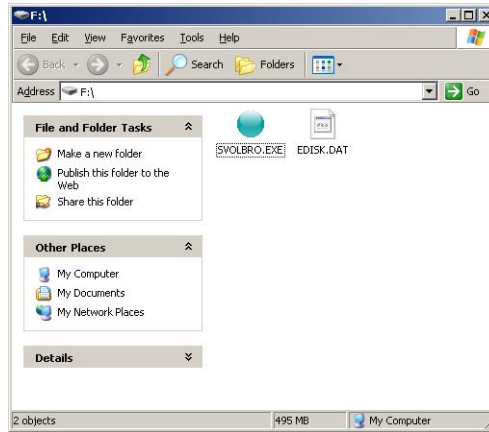


Figure 169: Accessing the Sanctuary Volume Browser application on the encrypted media

The Sanctuary Volume Browser window is displayed:

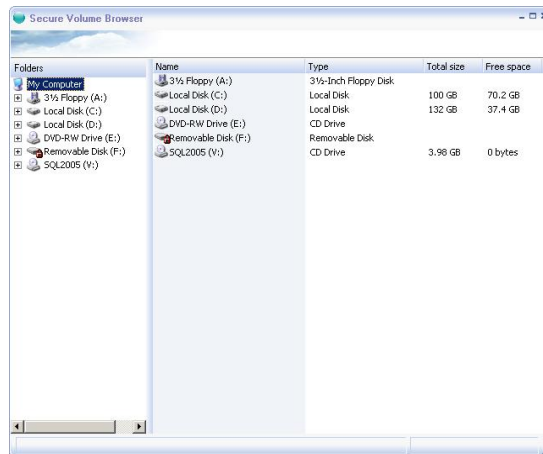



Figure 170: Sanctuary Volume Browser

2. [User] Highlight the encrypted medium that you want to access. To do this, click on the appropriate  icon in the Folders list.



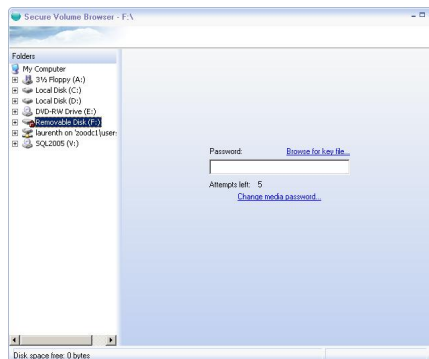


Figure 171: Sanctuary Volume Browser – encrypted medium selected

3. [User] Attempt to enter a Password five times.

*If the user has forgotten their password they must press their keyboard Enter key five times to display the Recover key link.*

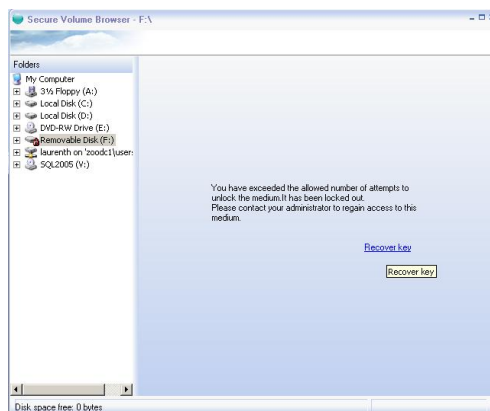


Figure 172: Sanctuary Volume Browser - Allowed attempts to unlock medium exceeded message

4. [User] Click on the Recover key link.

The Recover Password dialog is displayed:

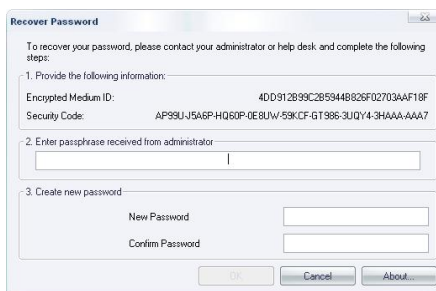


Figure 173: Recover Password dialog

5. [User] Telephone a Sanctuary administrator (with 'Key Recovery' access rights), explain your problem and read out the 32-character Encrypted Medium ID (such as 2CDB38A65A0694448805ABF17EB7F13B).
6. [Administrator] If you need to check whether the person on the telephone is allowed to access the encryption media (rather than trusting their word for it), recover information about the user and computer from when the removable storage device was originally encrypted. To do this, carry out the following steps:
  - > Activate the *Log Explorer* module, if it is not already open.



- > Select and run a template that generates a report of encrypted media. See *Log Explorer templates* on page 102.
- > Identify the log entry in the report that corresponds to the original encryption event, using the first characters of the hash number that the caller read out.
- > Check the user and computer details and compare these with the details of the individual who is on the telephone, if required.

You can click on the Props tab in the Criteria/Properties panel of the Log Explorer window to view all the details of the log entry. See *Criteria/Properties panel* on page 111 for more information.

- > Check the full hash number in the report corresponds with that you have been given over the phone.



You can 'cut and paste' the hash number from the log into the Encrypted Medium ID field the following step to save time.

7. [Administrator] Open the Sanctuary Password Recovery wizard on the Sanctuary Management Console. To do this, select *Key Recovery* from the *Tools* menu (or from the *Control Panel*). The Sanctuary Password Recovery wizard is displayed:



Figure 174: Sanctuary Password Recovery wizard - Encrypted Medium ID and Security Code page

8. [Administrator] Enter the 32-character alphanumeric string provided by the user (or paste in the hash number from the previous step) in the Encrypted Medium ID field.
9. [Administrator] Request a Security Code from the caller and, when this is read out to you, enter the 14-character alphanumeric string in the Security Code field.



The Security Code is shorter for a user wanting to recover a password for encrypted media outside your network than for a user connected to your network. This is due to the fact that Sanctuary Volume Browser does not have the public key required for tighter security.

A message is displayed notifying the administrator about the potential security risk involved in recovering a password for encrypted media when not connected to the network.

10. [Administrator] Confirm that you want to continue to provide the caller with access to the encrypted media despite the potential security risk.
11. [Administrator] Click on the NEXT button.

If the Encrypted Medium ID and the Security Code were incorrectly entered, an error message is displayed explaining which one needs correcting. This can be edited and the NEXT button clicked on again.

If the Encrypted Medium ID and the Security Code were correctly entered, the Sanctuary Password Recovery wizard displays the Passphrase page. This provides details of the device and the person who originally encrypted the device, along with a Passphrase that can be used to decrypt the encrypted medium.



Figure 175: Sanctuary Password Recovery wizard - Passphrase page

12. [Administrator] If you approve the user’s rights to access the encrypted removable storage device, read out the 52-character Passphrase (such as 8354Z-05DEP-M1ZGY-KKMCJ-AFLPR-8U773-C6ZQ7-Y5TUW-DP49Y-3Z5A7-7U).
13. [User] Enter the alphanumeric string provided by the administrator in the text field in the middle section of the Recover Password dialog.

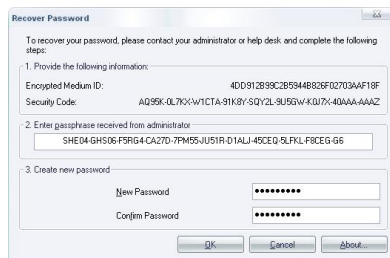


Figure 176: Recover Password dialog – entering passphrase

14. [User] Enter a New Password, retype this in the Confirm Password field, and click on the OK button. The following messages are displayed:



Figure 177: Sanctuary password recovered message



Figure 178: Sanctuary medium unlocked message

15. [Administrator] Once the user has confirmed that the above messages are displayed, click on the FINISH button.



---

## Chapter 8: Setting and changing options

There are various options that you would not want to change very often but which let you tailor Sanctuary Device Control to suit you and your organization.

You can change options either for all computers using Sanctuary Client Driver or a specific computer using it. These options can be used to:

- > Define rules governing USB KeyLoggers detection and notification.
- > Control if the user can see or not the client icon.
- > Decide if users are notified or not when updates are done.
- > Define the Shadow Directory.
- > Change or add SecureWave Application Server addresses.
- > Define the complexity of the password needed to encrypt media.
- > Choose if the client generates a certificate if none exists.
- > If unauthorized access to devices are logged or not.
- > Discard similar log events or not.
- > Send endpoint maintenance 'tickets' to selected computers/users.
- > Select how the online/offline state is detected.

You can find a detailed description of each option and instructions for changing them in the following sections.



*Changing options does not generate a popup window on the client icon informing the user of these modifications.*

### Options set in old Sanctuary versions

If you are upgrading from a previous version of Sanctuary Device Control you can find complete details in the readme file located in your installation CD.

The following table summarizes these changes:

<b>New name</b>	<b>Old name (version 3.x or previous)</b>
Device Log	Centralized Device Control Log
Device Log Throttling	Suppress Recurring Log Events
eDirectory translation	**
Encrypted Media Password	Encrypted Media Export Password
Endpoint Status	Device Control Status Window, Sanctuary Status
Log Upload Delay	**
Log Upload Interval	**
Log Upload Threshold	**
Log Upload Time	**
Offline/Online state detection	**
Server Address	SecureWave Application Server Address
*	Shadow File Upload Delay
*	Encrypted Media Key Export



\* discontinued \*\* new

Table 42: Option name comparison

## Default options

Sanctuary Device Control allows you to set default options for various aspects of the Sanctuary Client Driver behavior. You do this using the *Default Options* dialog.

You can access the *Default Options* dialog by selecting *Default Options* from the *Tools* menu (or from the *Control Panel*).

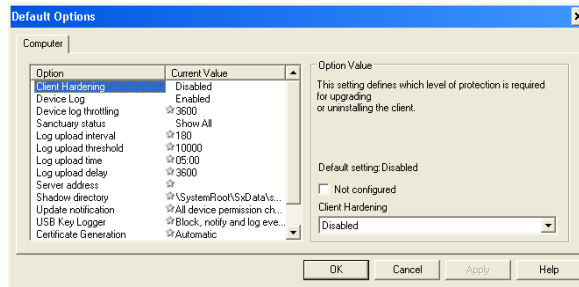



Figure 179: The Default Options dialog

The tab label is simply 'Computer' indicating that the options are not specific to a particular machine, but are the defaults for all computers in Sanctuary Device Control. If you do not override these default options for a specific machine, then these are applied to all computers in Sanctuary Device Control.

For each option, if the *Not configured* checkbox has a tick mark, 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 Device Control default is still in use.

If you change an option, the client computers need to be informed. You can do this by selecting *Send Updates to All Computers* or *Send Updates to* on the *Tools* menu (or from the *Control Panel*), or you can right-click on the computer in the Device Explorer module and select *Send Updates to <computername>* from the popup menu.

## Computer-specific options

You can override the default options for a specific computer. You can access the *Options* dialog for a specific computer by right-clicking on the computer in the Device Explorer module, and selecting *Options*.

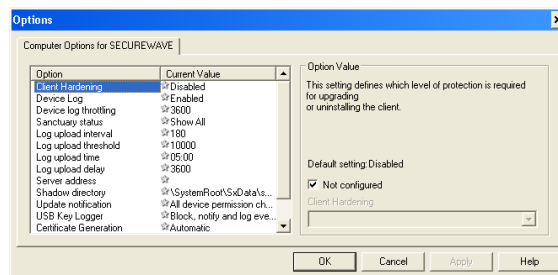



Figure 180: Setting computer-specific options

Notice that the tab label is *Computer Options for <computername>*, to show for which computer you are changing options.

If there is a star symbol  shown in the current value column of the option, this indicates that the Sanctuary Device Control default is still in use. If there is a tick mark  in the *Not configured* checkbox, then the default setting applies for that option.



## To change an option setting

1. Do either of the following:

To change default options for all computers, select *Tools* → *Default Options* (or use the *Control Panel*).

–or–

To change an option for a specific computer, right-click on the computer in the Device Explorer module, and then select *Options*.

The *Options* dialog is displayed, with the tab name indicating whether you are changing default settings for all computers or computer-specific settings.

2. Select the option you want to change in the list of option.
3. Uncheck the *Not configured* checkbox.
4. In the drop down list or field, set the option to the required value.
5. Click the OK button to save the setting and close the dialog, or the APPLY button to save the setting and keep the dialog open.

## Sending updates to client computers

After you have made changes, you can update the client computers by doing either of the following:

- > Selecting *Send Updates to All Computers* or *Send Updates to* on the *Tools* menu (or from the *Control Panel*), to update every computer with the changes.

–or–

- > Right-clicking on the computer in the Device Explorer module and selecting *Send Updates to <computername>* from the popup menu, to update a specific computer with the changes.

## Individual option settings

The remaining sections in this chapter describe the settings available for each option.

### Certificate generation

Windows Certificates are a prerequisite for using Sanctuary Device Control when centrally encrypting media — using the *Media Authorizer* module. See Sanctuary's Setup Guide for instructions on how to install it. If a user has no certificate, the Sanctuary Client Driver automatically creates one — using *rnotify.exe*. This option allows you to disable this automatic behavior.

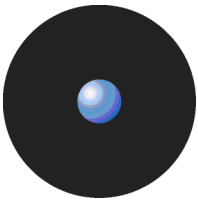
The possible settings are:

- > *Automatic* — (default value) The Sanctuary Client Driver automatically creates a certificate for those users that do not have one.
- > *Disabled* — The Sanctuary Client Driver does not create a user certificate.

You should set this option to 'disabled' if your Windows Certificate Authority is not published.



*If this option is disabled and the user does not have a certificate available, access to an encrypted media is not possible — even if the permission has been granted. This does not apply when using the Easy Exchange method.*



## Client hardening

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

You can choose from these settings:

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

Use the *Endpoint Maintenance* command to send maintenance 'tickets' to selected computers/users (see *Endpoint Maintenance* on page 27 for more information).

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



*You must disable client hardening before you can run a 'check disk' (chkdsk) on a client machine.*



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



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

## Device log

The device log determines what is recorded in the log system when the user attempts to access a protected device. The possible settings are:

- > *Disabled* — (default value) Nothing is written to the log.
- > *Enabled* — Attempts to access prohibited devices and client driver errors are written to the log system and can be viewed in the Log Explorer module. See *Chapter 5: Using the Log Explorer* on page 99 for more details.



*Some programs like Windows Explorer or some anti-virus programs may attempt repeatedly devices access. The Sanctuary Client Driver can filter out similar access occurrences; see *Device log throttling* on the next section for more details.*



*Even if the Device Log option is set to 'Disabled' MEDIUM-ENCRYPTED events, which are generated when a user encrypts a device, are always logged. These events are required for the password recovery functionality, see *Recovering a password for decentralized encryption when connected* on page 143.*





While you are reviewing the entries in the Log Explorer module, you may see a 'Write deny' or 'Read deny' record for removable drives or the floppy disk drive, for the 'NT AUTHORITY\SYSTEM' user. This is caused by the 'LocalSystem' account trying to access these devices — to 'block' them temporarily while the log is uploaded to make sure the user is not copying data — and not having the right permissions set. You should assign Read/Write permissions for the LocalSystem account of the machine where the 'Device Log' option is active so that this account can mount/dismount these types of devices.

## Device log throttling

When the device logging option is enabled, the Sanctuary Client Driver logs all access attempts to protected devices. Some programs, like Windows Explorer or some antivirus, may try to access devices repeatedly, causing massive volume of **similar** information to be logged in the system with this Read/Write-Denied operation. The *Device log throttling* option allows you to define a time period during which all similar occurrences of an already logged-on event are ignored.

The default setting is sixty minutes (3600 seconds). If you clear the *Not configured* checkbox, you can type in another value. You should increase this value if you see repetitive occurrences of similar events in the Log Explorer module.



This setting applies only to Read/Write denied events. Every time another event occurs, such as when a device is plugged in, an error is reported, the logging of one read/write event is allowed and the logging history period is reset. You can use this feature to your advantage to see if a read/write event occurred after a new device has been connected to the computer.

## eDirectory translation

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

- > Enabled (default value) — The eDirectory account information is shown along with the Windows account information.
- > Disabled — eDirectory account information is not shown, only Windows accounts are shown.

## Encrypted media password

The Encrypted media password option defines the strength of the password used to protect encryption keys when authorized users export them.

The possible settings are:

- > *Require password complexity* — (default value). The password needs to meet the following requirements:
  - Be at least eight characters long.
  - Contain upper and lower case letters.
  - Contain digits.
  - Contain at least one non alphabetical character (!@#%\*...).
- > *Allow weak password* — Any password except a blank field is accepted



The Encrypted media password option only applies when the 'Export to File' and/or 'Export to Media' option of the removable class permissions is also used.



## Endpoint status

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

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



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

## Log upload interval

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

## Log upload threshold

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

## Log upload time

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

## Log upload delay

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

## Online state detection

The Online state detection option is used to define the criteria that prevail to determine if a machine is online/offline.

There are two possible settings for this option:

- > *Server connectivity*: State is determined whether the client driver can communicate or not with a SecureWave Application Server.



- > **Wired connectivity:** State is determined whether the network cable is plugged or not.

The Online state detection option works in conjunction with the Offline/Online permissions that should already be defined for the required device class(es) — see *To assign online and offline permissions* on page 80. As an example, you may want to use this option when the client machine uses several network cards (NICs) — one of them wireless — to apply the following scenario:

1. User 'EndPointClient' logs on to the corporate network at his desk in the office (through a wired connection) - online wireless permissions applied: wireless card is disabled.
2. User 'EndPointClient' unplugs his laptop from the corporate network to go to a meeting in a conference room (no system boot) - offline wireless permissions apply: wireless card is now enabled.
3. User 'EndPointClient' logs into a wireless network in the conference room and uses a VPN connection to the corporate network (no system boot) - offline wireless permissions continue to apply: wireless card is now enabled.
4. User 'EndPointClient' returns to his office after the meeting and plugs back into the corporate network at his desk (through a wired connection) (no system boot) - online wireless permissions applied: wireless card is now disabled.

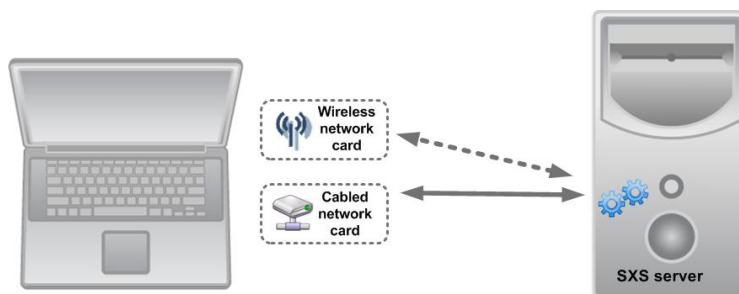


Figure 181: Online/Offline state detection option as applied to Wireless NICs

The objective here is to let the user use his wireless NIC when the cabled one is unplugged from the network and vice versa. The following table clarifies this point (taking the Wireless NICs class as an example):

Offline/Online state detection setting	Wireless NIC permission	Resulting permission
Server connectivity	Offline R/W	User can use his wireless connection only when SecureWave Application Server is not detected (even when there is a physical cable plugged to the machine's network card).
	Online disabled	User cannot use his wireless connection when a SecureWave Application Server is detected (through the cable or wireless network card).
Wired connectivity	Offline R/W	User can use his wireless connection only when there is no physical cable connected to the other computer's network card or no communication can be established with a SecureWave Application Server.
	Online disabled	User cannot use his wireless connection when there is a physical cable connected to the other computer's network card (even when the SecureWave Application Server cannot be detected).

Table 43: Offline/Online state detection configuration as applied to Wireless NICs

## Server address

The Server address option defines the IP address of the SecureWave Application Server(s) to which the Sanctuary Client Driver should connect. You normally use this option when:

- > A new server is placed in the working environment.
- > You change the IP address or name of the SecureWave Application Server.



- > You want to specify more than three servers for your clients (done during the client installation — see Sanctuary's Setup Guide for more information).

When no default setting or computer-specific settings are defined, the client uses the server addresses provided when the Sanctuary Client was installed. If you clear the *Not configured* checkbox, you can type in one or more alternative addresses. Separate multiple servers by a space. Each IP address and port combination must be entered in the form 1.2.3.4:5001. You can also use the NetBIOS name or the Fully Qualified Domain Name (FQDN) — compulsory if you are using TLS protocol (see *Sanctuary's Setup Guide*).

## Shadow directory

The shadow directory is the temporary folder where shadow and log files are stored before being uploaded to the SecureWave Application Server. The default setting for this folder is `\SystemRoot\sxdata\shadow\`. If you clear the *Not configured* checkbox, you can type in an alternative shadow directory.



*Changing this option requires extreme care. You must ensure that the directory, and its subdirectories, exists. The driver reverts to the previous directory if the path provided is not valid. You must also be sure that the Shadow directory is set to a fixed, writable hard-drive. DVD/CD-ROM, removable media (even large external Firewire/USB hard disks), etc., will cause Shadow to misbehave. The shadow directory can NEVER be a UNC path or a directory on a mapped drive. Furthermore, folders not included under %Windows%\sxdata are not protected by the Client Hardening feature — you should provide other methods to protect these folders.*

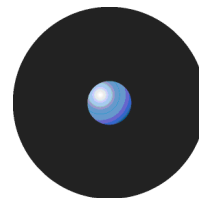
## Update notification

The Update notification option allows you to determine which messages are shown to the end-user when permissions change in one way or another. The possible settings are:

- > *No messages* — No warnings are displayed to the user.
- > *Temporary permission changes* — Display a message when temporary permissions are changed. This also sends a message three minutes before the permission expires and, finally, when the permission is no longer valid.
- > *All device permission changes* — (default value) A message is displayed when any change is made to permissions that affect the user, including permanent, scheduled, offline, online, and temporary ones.

## USB Keylogger

As the PS/2, the standard port to connect a keyboard and/or mouse, is being rapidly superseded by the USB port, these devices are using alternative ones. The hardware Keylogger™ is a device that captures all data typed at the keyboard, including passwords and other sensitive data. There is also a software version of the Keylogger. You can check the presence of software Keyloggers using a commercially available program and block it using our Sanctuary Application Control Suite. The USB hardware version of this device can be blocked, either as a general option or as a computer specific one.



The possible settings are:

Option	Description	Notify user	Block keyboard	Log event
Disabled	Default value. Do not react in any way to the detection of a Keylogger.	x	x	x
Notify user	Only inform the user of the presence of a Keylogger. This does not notify the use when the keylogger is attached to a computer using Vista.	✓	x	x
Log event	Only log the event if a Keylogger is detected. The keyboard is not disabled.	x	x	✓
Notify user and log event	If a Keylogger is detected, log the event and inform the user. The keyboard is not disabled. This does not notify the use when the keylogger is attached to a computer using Vista.	✓	x	✓
Block keyboard and notify user	Hinder the keyboard and notify the user if a Keylogger is detected. This does not notify the use when the keylogger is attached to a computer using Vista.	✓	✓	x
Block keyboard and log event	Hinder the keyboard and log the event if a Keylogger is detected.	x	✓	✓
Block keyboard, notify, and log event	Hinder the keyboard, log the event, and notify the user if a Keylogger is detected. This does not notify the use when the keylogger is attached to a computer using Vista.	✓	✓	✓

Table 44: USB Keylogger options



Changing from one setting to another requires a client reboot.

## Checking settings on a client machine

As long as the Endpoint status option is not set to 'Do not Show' then a user on the client computer can double-click on the icon located in the system tray to see the current status settings for the machine.

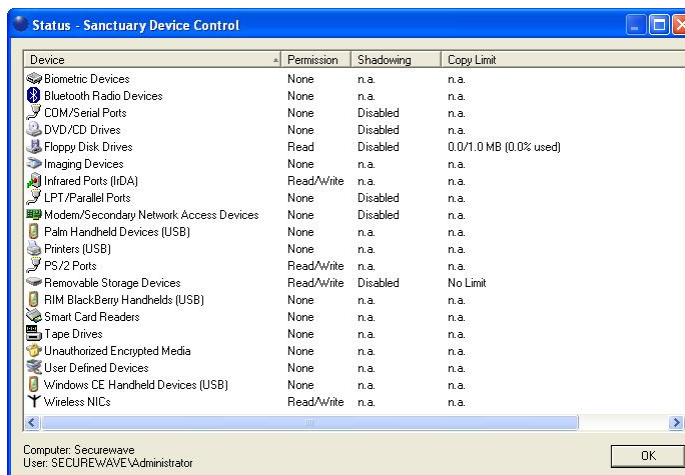



Figure 182: Checking the settings on a client machine


Depending on the settings you define, the client user can see all details, all details but without the *Shadowing* column, or just the allowed permission rules without the *Shadowing* column. The *Copy Limit* column only shows details if a permission of this type has been assigned to a device, including how much has already been consumed from the assigned quota.



## Chapter 9: Generating Sanctuary Reports

The *Reports* menu (or module in the *Control Panel*) allows you to generate a variety of reports about Sanctuary Device Control information including permissions, shadowing, options, and media. The generated reports are HTML files displayed in an internal window. Simply select the *Reports* menu item or module and choose the required one. Once saved, the Sanctuary Reports 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 provisionally created and saved in the Report folder located in your temporary directory — %TEMP%.


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

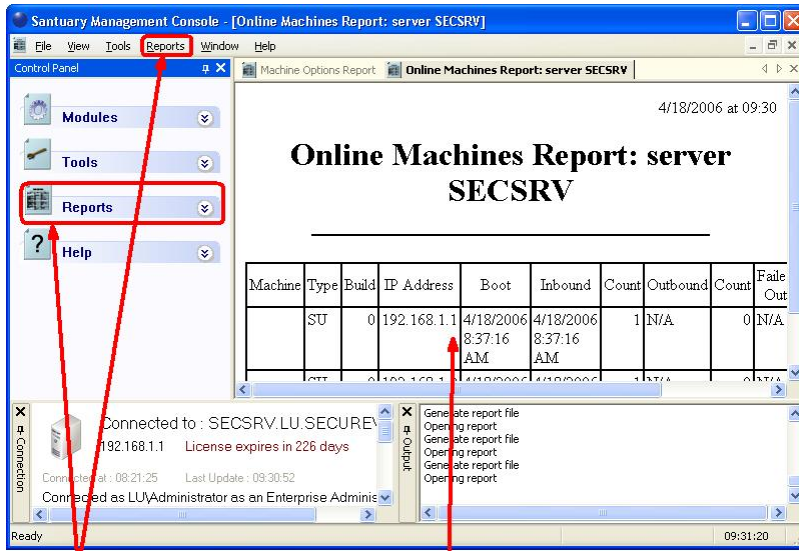
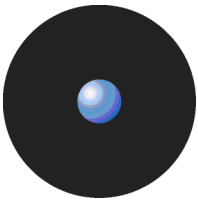
 You can change the way the date is formatted in a Sanctuary Report by using the 'Regional and Language' options of the 'Control Panel' of your Windows system. Consult Windows Help for details.

The following table summarizes the types of reports that can be obtained by a user (controlled in the 'User Access Manager' dialog):

<b>Type of user access</b>	<b>Available Reports</b>
Enterprise Administrator	All of them.
Administrator with no other options set in the 'User Access Manager' dialog. These are the 'default' options for all Administrators.	'Users Permissions', 'Device permissions', 'Computer permissions', 'Online Machines', 'User Options', and 'Machine Options'.
Administrators with 'Media (Device Control)' setting of the 'User Access Manager' dialog set to 'Yes' or 'Compatible'.	All those of the 'default' Administrator plus the 'Media by User' and 'Users by Medium' reports.
Administrators with 'Logs (Device Control)' setting of the 'User Access Manager' dialog set to 'Yes' or 'Compatible'.	All those of the 'default' Administrator plus the 'Shadowing by Device' and 'Shadowing by User' reports.
Administrators with 'Scheduled Reports' setting of the 'User Access Manager' dialog set to 'Yes' or 'Compatible'.	All custom reports that are scheduled to run automatically using templates you have created or updated. See <i>Chapter 5: Using the Log Explorer</i> on page 99.

Table 45: Reports that can be obtained by Administrator type

 In addition to the standard reports that are available through the Reports menu, you can define your own criteria for selecting log entries and producing custom reports using the Log Explorer module. See *Chapter 5: Using the Log Explorer* on page 99 for more information.



Select the desired report from the menu or Control Panel

You get the selected report in the main window panel

Figure 183. Obtaining a report

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

## User Permissions report

The User Permissions report displays all permissions rules defined for a specific user(s). To generate this report:

1. Select *User Permissions* from the *Reports* menu (or the *Control Panel*).
2. Select one or more users in the *Select Domain User or Group* dialog. You can use wildcards (\*, ?) in the name field. Use the **SHIFT** key to select consecutive items or **CTRL** for nonconsecutive ones.

An example of the User Permissions report is shown below:

25/05/07 at 07:31

### User Permissions

#### SECURE\Bill (Domain User)

Devices	Computer	Permissions/Priority/Details	User Name / Group Name
<b>CD/DVD-ROM</b>	SECURE\CLIENT	<b>Permissions:</b> FileName <b>Priority:</b> High <b>Details:</b> Shadow option	Via Everyone
<b>Modem</b>	SECURE\CLIENT	<b>Permissions:</b> None <b>Priority:</b> High <b>Details:</b>	SECURE\Bill
<b>SanDisk Cruzer Mini USB Device</b>	<i>Default settings</i>	<b>Permissions:</b> Read/Write <b>Priority:</b> High <b>Details:</b>	SECURE\Bill
<b>Scanner</b>	<i>Default settings</i>	<b>Permissions:</b> Read/Write <b>Priority:</b> High <b>Details:</b>	Via SECURE\Domain Users
<b>Windows CE Devices (USB)</b>	SECURE\CLIENT	<b>Permissions:</b> Read/Write <b>Priority:</b> High <b>Details:</b>	Via LUMarketing

Figure 184: User Permissions report





## Device Permissions report

The Device Permissions report displays all permissions rules for the devices defined in the Device Explorer module. To generate this report, select *Device Permissions* from the *Reports* menu (or the *Control Panel*).

An example of the Device Permissions report is shown below:

25/05/07 at 07:31

### Device Permissions

Devices	Default Settings / Computers	User Name / Group Name	Permissions/ Priority / Details
<b>RIM BlackBerry Handhelds</b>	Default Settings	SECURE\user13	<b>Permissions:</b> Read/Write/Encrypt <b>Priority:</b> High <b>Details:</b> Microsoft Office (import/export)
<b>CD/DVD drives</b>	Default Settings	SECURE\Bill	<b>Permissions:</b> Read/Write <b>Priority:</b> High <b>Details:</b>
		SECURE\Cert Publishers	<b>Permissions:</b> Read <b>Priority:</b> High <b>Details:</b> Online
		SECURE\Cert Publishers	<b>Permissions:</b> Read/Write <b>Priority:</b> High <b>Details:</b> Offline
	SECURE\CLIENT	SECURE\Bill	<b>Permissions:</b> Read/Write <b>Priority:</b> High <b>Details:</b>
<b>COM/Serial Ports</b>	>>> No users and/or computers you may manage have permissions for this device <<<		
<b>Floppy Disk Drives</b>	Default Settings	Administrators	<b>Permissions:</b> Read/Write <b>Priority:</b> Low <b>Details:</b>
		SECURE\Todd	<b>Permissions:</b> W:Filename R:Enabled <b>Priority:</b> High <b>Details:</b> Shadow option
			<b>Permissions:</b> 1 MB <b>Priority:</b> High <b>Details:</b> Copy Limit
<b>LPT/Parallel Ports</b>	>>> No users and/or computers you may manage have permissions for this device <<<		
<b>Modem /Secondary Network Access Devices</b>	Default Settings	SECURE\GG_MANAGEMENT	<b>Permissions:</b> Read/Write <b>Priority:</b> High <b>Details:</b>
	SECURE\CLIENT	SECURE\Bill	<b>Permissions:</b> None <b>Priority:</b> High <b>Details:</b>
<b>Palm Handheld Devices</b>	>>> No users and/or computers you may manage have permissions for this device <<<		
<b>Removable storage devices</b>	Default Settings	SECURE\Fred	<b>Permissions:</b> Read/Write <b>Priority:</b> High <b>Details:</b> File Filters: Adobe Acrobat (import/export)
<b>SanDisk Cruzer Mini USB Device</b>	>>> No users and/or computers you may manage have permissions for this device <<<		
<b>Smart Card Reader</b>	>>> No users and/or computers you may manage have permissions for this device <<<		
<b>Tape Drives</b>	Default Settings	SECURE\Domain Admins	<b>Permissions:</b> Read/Write <b>Priority:</b> High <b>Details:</b>
<b>TwinMOS Mobile Disk USB Device</b>	>>> No users and/or computers you may manage have permissions for this device <<<		
<b>User Defined Devices</b>	>>> No users and/or computers you may manage have permissions for this device <<<		
<b>Windows CE Devices (USB)</b>	SECURE\CLIENT	SECURE\Bill	<b>Permissions:</b> Read/Write <b>Priority:</b> High <b>Details:</b>

Figure 185: Device Permissions report



## Computer Permissions report

The Computer Permissions report displays all permissions rules defined for a specific computer(s). To generate this report, proceed as follows:

1. Select *Computer Permissions* from the *Reports* menu (or the *Control Panel*).
2. Select one or more computers in the *Select Computer(s)* dialog. You can use wildcards (\*, ?) in the name field. Use the **SHIFT** key to select consecutive items or **CTRL** for nonconsecutive ones.

An example of the Computer Permissions report is shown below:

25/05/07 at 07:31

### Computer Permissions

Computer	User Name / Group Name	Devices	Permissions/Priority Details
SECURE\CLIENT	SECURE\Bill	CD/DVD-ROM	<b>Permissions:</b> Read/Write <b>Priority:</b> High <b>Details:</b>
		Modem	<b>Permissions:</b> None <b>Priority:</b> High <b>Details:</b>
		Windows CE Devices (USB)	<b>Permissions:</b> Read/Write <b>Priority:</b> High <b>Details:</b>
	SECURE\John	Modem	<b>Permissions:</b> Read/Write <b>Priority:</b> High <b>Details:</b> 06:00 - 20:00 every Mon, Tue, Wed, Thu, Fri
Lu\Sales	Everyone	Removable Storage Devices	<b>Permissions:</b> Read/Write <b>Priority:</b> High <b>Details:</b> File filters: Adobe Acrobat (import/export)

Figure 186: Computer Permissions report



## Media by User report

The Media by User report displays all permissions rules defined for a user(s) classified by medium. To generate this report, proceed as follows:

1. Select *Media by User* from the *Reports* menu (or from the *Control Panel*).
2. Select one or more users in the *Select User(s) and/or Group(s)* dialog. You can use wildcards (\*, ?) in the name field. Use the **SHIFT** key to select consecutive items or **CTRL** for nonconsecutive ones.



*The 'Media by User' report does not list the DVD/CDs indirectly authorized when a User is a member of a Group.*



*Since Movie DVDs behave as DVD-ROMs, their treatment differs from the procedure used for Music CDs. You need to authorize every DVD separately.*

An example of the Media by User report is shown below:

25/05/07 at 07:31

### Media by User Report

1. **SECURE\Bill** (*Domain User*)

CD/DVD Label	Description	Registered On	Registered By
Music CD	Any music CD		
O9PRMCD01	Office XP	3-02-2006	SECURE\Chuck
V2KEE_IE	Visio	1-01-2005	SECURE\Administrator
vsentd2	Visual Studio .Net	2-02-2006	SECURE\Administrator
X05-69971	Microsoft Project	2-22-2006	SECURE\Emily
Encrypted Media Label	Description	Registered On	Registered By
DK09	Mobile Disk DK09	2-15-2006	SECURE\Administrator
DK12	Mini Cruzer 128 Mb DK12	12-30-2005	SECURE\Administrator

Figure 187: Media by User report



## Users by Medium report

The Users by Medium report displays all permissions rules defined for removable media — using the Media Authorizer module — classified by user(s). To generate this report, select *Users by Medium* from the *Reports* menu (or from the *Control Panel*).

An example of the Users by Medium report is shown below:

25/05/07 at 07:31

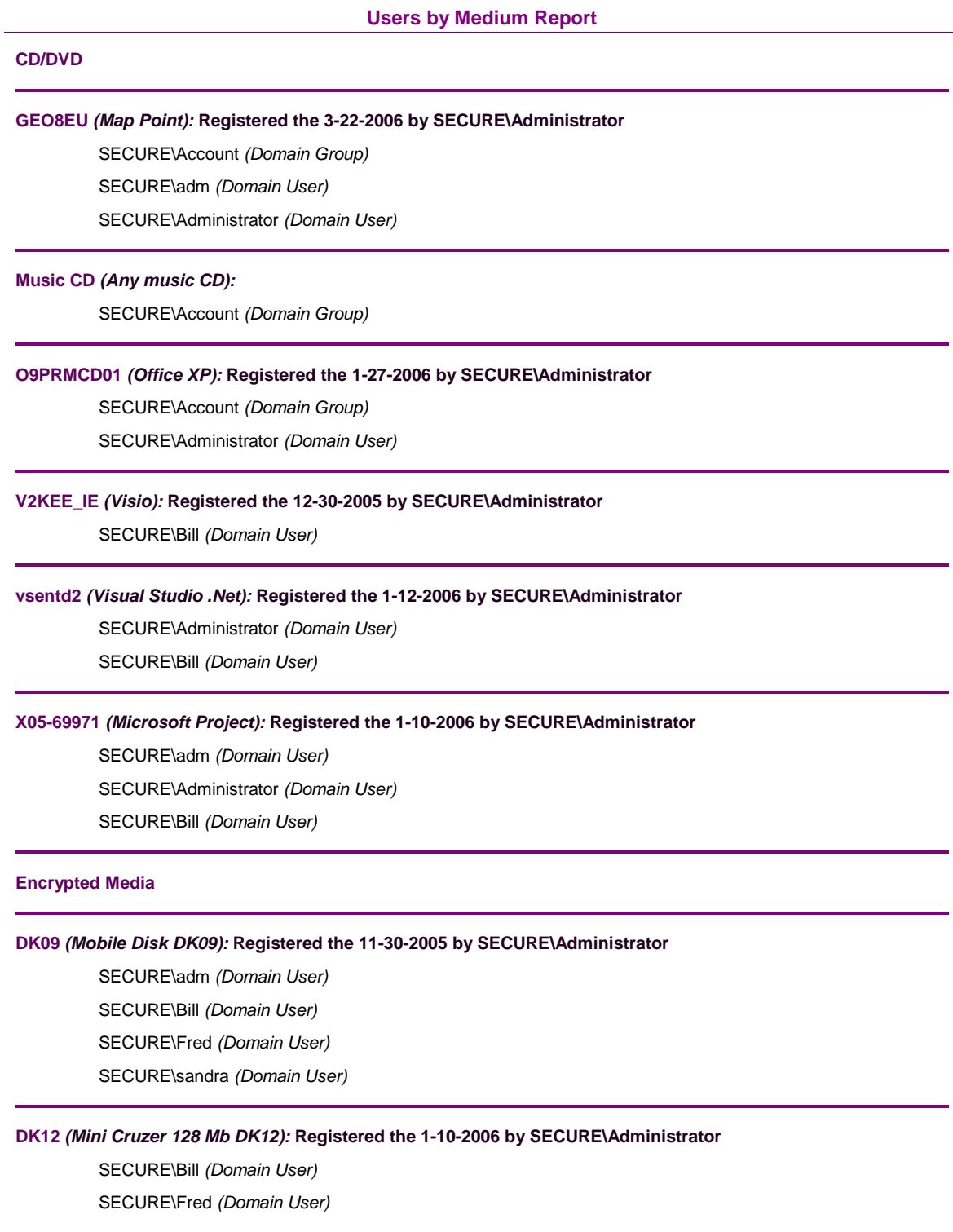
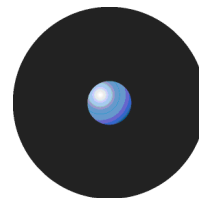


Figure 188: Users by Medium report



## Shadowing by Device report

The Shadowing by Device report displays a summary of all data being copied/read by user. It is sorted in ascending order in the device section. To generate this report, select *Shadowing by Device* from the *Reports* menu (or the *Control Panel*) and then the dates from the dialog.

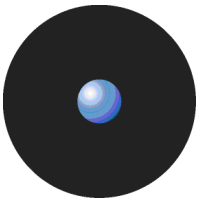
An example of the Shadowing by Device report is shown below:

25/05/07 at 07:31

### Shadowing by Device between 12-12-2005 and 1-30-2006

Device	User Name	Computer Name	Total Size (Mb)
<b>CD/DVD</b>	SECURE\Administrator	CLIENT	980.730118
	SECURE\Bill	CLIENT	123.359511
		SECSRV	532.046730
	SECURE\Farida	CLIENT	14.199219
SECSRV		85.147934	
<b>Floppy</b>	SECURE\Bill	CLIENT	0.438139
		SECSRV	0.441463
<b>Removable storage devices</b>	SECURE\Bill	CLIENT	3.113281
		SECSRV	1.117001
	SECURE\Ann	CLIENT	0.906691
	SECURE\Jennifer	SECSRV	10.101629
	SECURE\Marilyn	SECSRV	0.175781

Figure 189: Shadowing by Device report



## Shadowing by User report

The Shadowing by User report displays the total size of data copied/read by user and device class. It is sorted in ascending order by quantity. To generate this report, select *Shadowing by User* from the *Reports* menu (or the *Control Panel*) and then the dates in the dialog.

An example of the Shadowing by User report is shown below:

25/05/07 at 07:31

### Shadowing by User between 12-26-2005 and 2-06-2006

User	Computer Name	Device	Total Size (Mb)
SECURE\Farida(2.613680 Mb)	CLIENT	CD/DVD	0.199219
		Floppy	1.050115
	SECSRV	CD/DVD	1.147934
		Floppy	0.192587
		Removable	0.023826
	SECURE\Ann(0.906845 Mb)	CLIENT	Removable
SECSRV		Floppy	0.000154
SECURE\Marilyne(0.175781 Mb)	SECSRV	Removable	0.175781
SECURE\Jennifer(0.111960 Mb)	SECSRV	CD/DVD	0.010331
		Removable	0.101629
SECURE\Sandy(0.060682 Mb)	SECSRV	CD/DVD	0.027414
		Floppy	0.033268

Figure 190: Shadowing by User report



## Online Machines report

The Online Machines report displays all machines that are online when the report is generated. It also serves as a troubleshooting help: You can find why a machine is not receiving updates when you send them. If the machine is not in the list, it does not receive updates. If the machine is in the list but its Failed Out counter is different from 'N/A', it can indicate a communication problem, misconfiguration, networking problems, misconfigured network timeouts, etc. To generate this report, select *Online Machines* from the *Reports* menu (or the *Control Panel*).

An example of the Online Machines report is shown below:

25/05/07 at 07:31

### Online Machines Report: server Company

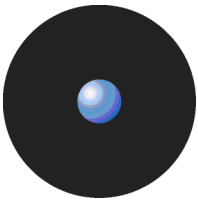
Machine	Type	Build	IP Address	Boot	Inbound	Count	Outbound	Count	Failed Out	Count	Consecutive
SecSrv	SN	0	192.168.1.15	N/A	2006-08-10 13:35:45 PM	1	2006-08-10 14:49:01 PM	16	N/A	0	0
Company	SU	0	127.0.0.1	2006-08-10 15:00:15 PM	2006-08-10 15:00:31 PM	6	2006-08-10 16:21:47 PM	3	2006-08-10 16:36:31 PM	2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

Figure 191: Online Machines report

Below is an explanation of the columns:

Column	Description
Machine	This column holds the computer's name of the machine found in the online table. A machine not listed in this table does not receive updates when using the <i>Send Updates to All Computers</i> or <i>Send Updates to</i> command on the <i>Tools</i> menu. The table updates when the client machine reboots or logs.
Type	This column holds the kind of client driver installed on the client computer: <i>SN</i> for Sanctuary Client Driver version 3.1 or older; <i>SX</i> for Sanctuary Client Driver version 2.1; <i>SU</i> for Sanctuary Client Driver version 3.2 or later.
Build	This column holds the IP address of the machine as registered in the online table.
IP Address	This column holds the IP address of the machine as registered in the online table.
Boot	The date and time the SecureWave Application Server last received a boot notification from the client machine. A value of 'N/A' indicates that the SecureWave Application Server did not receive a boot notification but did receive a logon or unlock notification. This notification applies for machines that could not contact a SecureWave Application Server at boot. When the user selects the <i>Refresh settings</i> , all modifications done by the administrator to his machine/profile are updated.
Inbound	This field contains the date and time the SecureWave Application Server last accepted a connection from the client computer.
Count	(Referring to the Inbound connection) Contains the number of connections accepted from the client computer by the SecureWave Application Server.
Outbound	This field contains the date and time of the last connection initiated from the SecureWave Application Server towards the client computer.
Count	(Referring to the Outbound connection) Contains the number of connections that the SecureWave Application Server initiated with the client computer.
Failed out	This field contains the date and time of the last unsuccessful connection between the SecureWave Application Server and the client computer.
Count	(Referring to the failed out connection) Contains the total number of connections that failed between the SecureWave Application Server and the client computer. This number increases 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 46: Columns of the 'Online Machines' Report



## Machine Options report

The Machine Options report displays how the default program's option changed. To generate this report, select *Machine Options* from the *Reports* menu (or the *Control Panel*). Please refer to *Chapter 8: Setting and changing options* on page 169 for more details on the meaning of each option.

An example of the Machine Options report is shown below:

25/05/07 at 07:31

### Machine Options Report

Option	Machine	Setting
USB Key Logger	default	(*) Block, notify and Log Event to Sanctuary Management Console
Sanctuary Status	default	(*) Show All
	SECURE\CLIENT	Show allowed
Update Notification	default	(*) All device permissions changes
Shadow Directory	default	(*) \SystemRoot\SxData\shadow
Encrypted Media password	default	Allow weak password
Certificate Generation	default	(*) Automatic
Device Log	default	Enabled
Device log throttling	default	(*) 3600
Client Hardening	default	(*) Disabled
Log upload interval	default	(*) 180
Log upload threshold	default	(*) 10000
Log upload time	default	(*) 05:00
Log upload delay	default	(*) 3600
Server address	default	(*)
eDirectory translation	Default	(*) Enabled
Online state definition	Default	(*) Server connectivity

Figure 192: Machine options report

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





## Server Settings Report

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

An example of the Server Settings report is shown below:

25/05/07 at 07:31

### Server Settings Report

Setting	Machine	Value
<b>CommVer</b>	secsrv.lu.company	2
	secsrv1.lu.company	3
<b>DataFileDirectory</b>	secsrv.lu.company	\\lu\DataFileDirectory
	secsrv1.lu.company	\\lu1\DataFileDirectory1
<b>DBConnectionCount</b>	secsrv.lu.company	20
	secsrv1.lu.company	30
<b>DBConnectionString</b>	secsrv.lu.company	Provider=sqloledb; Data source=SECSRV\SQLEXPRESS; Initial Catalog=sx; Trusted_Connection=yes
	secsrv1.lu.company	Provider=sqloledb; Data source=SECSRV\CPMPANY; Initial Catalog=sx; Trusted_Connection=yes
<b>DBConnectionTimeout</b>	secsrv.lu.company	(*) 5
	secsrv1.lu.company	(*) 5
<b>Log file name</b>	secsrv.lu.company	Sxs.log
	secsrv1.lu.company	Sxs.log
<b>Log to console</b>	secsrv.lu.company	No
	secsrv1.lu.company	No
<b>Log to dbwin</b>	secsrv.lu.company	No
	secsrv1.lu.company	No
<b>Log to file</b>	secsrv.lu.company	No
	secsrv1.lu.company	No
<b>MaxRPCCalls</b>	secsrv.lu.company	(*) 50
	secsrv1.lu.company	(*) 50
<b>MaxSockets</b>	secsrv.lu.company	5000
	secsrv1.lu.company	5000
<b>Port</b>	secsrv.lu.company	65129
	secsrv1.lu.company	65129
<b>Protocols</b>	secsrv.lu.company	(*) ncacn_ip_tcp
	secsrv1.lu.company	(*) ncacn_ip_tcp
<b>RegProtectionLevel</b>	secsrv.lu.company	6
	secsrv1.lu.company	6
<b>SecureInterSXS</b>	secsrv.lu.company	No
	secsrv1.lu.company	No
<b>SecureCertSerial</b>	secsrv.lu.company	(*)
	secsrv1.lu.company	(*)
<b>ServerName</b>	secsrv.lu.company	(*)
	secsrv1.lu.company	(*)
<b>SndPort</b>	secsrv.lu.company	33115
	secsrv1.lu.company	33115
<b>SxdConnectAttempts</b>	secsrv.lu.company	(*) 10



	secsrv1.lu.company	(*) 10
<b>SxdConnectDelayBeforeRetray</b>	secsrv.lu.company	(*) 500
	secsrv1.lu.company	(*) 500
<b>SxdConnectTimeoutMsec</b>	secsrv.lu.company	5000
	secsrv1.lu.company	5000
<b>SxdPort</b>	secsrv.lu.company	33115
	secsrv1.lu.company	33115
<b>TLSCertFriendlyName</b>	secsrv.lu.company	Lux Server
	secsrv1.lu.company	USA Server
<b>TLSCertID</b>	secsrv.lu.company	611CF237000000000002
	secsrv1.lu.company	711DE216000000000011
<b>TLSCertIssuer</b>	secsrv.lu.company	DC=company, DC=LU, CN=Company
	secsrv1.lu.company	DC=company, DC=LU, CN=Company
<b>TLSCertName</b>	secsrv.lu.company	CN=secsrv.lu.company
	secsrv1.lu.company	CN=secsrv.lu.company
<b>TLSCertMaxSockets</b>	secsrv.lu.company	5000
	secsrv1.lu.company	5000
<b>TLSPort</b>	secsrv.lu.company	65229
	secsrv1.lu.company	65229

Figure 193: SecureWave Application Server Settings report

Note the asterisk (\*) that indicates that the option has not been configured explicitly and has its default value.

## **Part III: Additional information**



---

## Appendix A: DVD/CD Shadowing

### Introduction

DVD/CD shadowing is the term used to describe the capture of data written/read to/from CD-R, CD-RW, DVD-R, DVD+R, DVD-RW, DVD+RW and DVD-RAM media, its analysis, and extraction. The information is stored by the SecureWave Application Server and can be retrieved in summary form or with full file data using the Log Explorer module of the Sanctuary Management Console.

### Operation of the Sanctuary Client Driver

If you enable the Shadowing option for the client computer and the user attempts to write (read) data to a CD-R or similar device, a local copy of the entire data stream is normally saved to a file in the temporary shadow files folder on the client computer. This file is submitted to a special component of client driver (SCC) for parsing purposes and submitted to an available SecureWave Application Server during the next available upload time-frame operation.

Additionally, one or two log files are added describing progress and problems encountered during this phase.

If a serious error is found, the entire image is added to the shadow files list under a special file name. If necessary, you can easily retrieve this file for manual analysis using third party tools.

If the analysis failed altogether for a reason such as lack of disk space or memory, the Sanctuary Client Driver keeps the file and resubmits it during the next upload window. In either case, the analysis logs detailing the problems found are created.

There are two cases while transmitting this data:

1. A full shadow mode is in effect and all data must be transmitted to the server for archive and, possible, further analysis. The file is deleted once successfully sent.
2. A file name only shadow mode is active. Only the name and size of the file(s) is transmitted before deleting it. If the written/read data is in a format that cannot be decoded with reasonable effort, the attempt to write to the medium is denied.

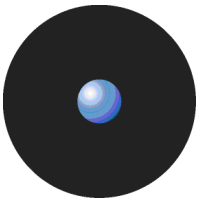
Individual files embedded in the data stream are extracted by the SecureWave Application Server and added to the 'shadow files' list.



*The priority of shadowing options has changed for Sanctuary Device Control version 4.x: In previous versions the 'Filename only' and 'Enabled' options took priority over 'Disabled'. In version 4.x the 'Disabled' option takes priority over the other options. User upgrading from a previous version of Sanctuary Device Control should modify their permissions accordingly, especially if there is a shadowing 'Disabled' rule defined in their policy set.*

### Disk space requirements

The analysis of CD and DVD images can, by its nature, consume huge amounts of disk space. For filename shadowing — where the files themselves are not stored — the temporary space needed is the same size as that of the image being analyzed. If 'full' shadowing is enabled (i.e., the contents of files recorded onto CD or DVD media are stored), the Sanctuary client requires three times the space of the file, or even more if there are many small files. With current DVD recorders storing up to 8.5 GB on a single disc and higher-capacity solutions (Blu-Ray, HD-DVD) on the horizon, it is necessary to carefully monitor disk space.



## Supported formats when shadowing

Current CD recording standards allow for a bewildering array of formats, ranging from plain user data in a simplified ISO file system to a UDF/ISO+Joliet bridge DVD with interleaving, extended attributes, security descriptors, and associated files.

Common recording software uses only a small subset of those combinations, and Sanctuary Device Control concentrates on those; the following table offers an overview of what is and what is not supported in each of the two possible shadow modes.

<i>Format</i>	<i>Full shadow mode</i>	<i>File name only shadow mode</i>
Audio tracks (not interpretable)	○	×
Scrambled tracks (not interpretable)	○	×
Raw-mode data (not interpretable)	○	×
Packet writing, Mount Rainier	○	×
ISO, ISO/Joliet	●	●
UDF	○	×
UDF+ISO/Joliet bridge	◐	◐
ISO+EI Torito bootable CDs	◐	◐
ISO+Rock Ridge extensions	◐	◐
High Sierra Group format	○	×
Apple HFS	◐	◐
Legend:		
× Not supported, writing blocked by the Sanctuary Client Driver		
● Shadowed and fully supported; individual files are extracted and made available		
◐ Shadowed, partially supported; individual files are extracted and made available		
○ Shadowed, but individual files not extracted		

Table 47: Supported formats for the full shadow or file name only shadow modes

## Handling of unsupported shadowing formats

Sometimes the SecureWave Application Server stores an entire image of a recording session, for instance. Administrators may want to look at such images immediately. To do so, an image can be retrieved from the Shadow File Explorer in the Sanctuary Management Console and recorded onto a suitable medium. As an alternative, there are other commercially available products that can 'mount' an image, making it appear as a virtual CD-ROM or DVD-ROM drive.

Among those programs simulating virtual media we can find ImageDrive (a utility that is part of Ahead Software's Nero recording software: <http://www.nero.com>), Daemon Tools (<http://www.daemon-tools.cc>), and Microsoft's VirtualCD (not available on-line; distributed usually to Beta customers and to Premier support accounts on request).

There are three technical limitations caused by the peculiarities of recording; the information needed to determine whether they apply to a particular recording session is included in the header of the analysis log file.

1. For multi-session CDs, only the first session can be used without further conditioning.

A recording that starts at, let's say, block number 10,000 cannot be read correctly if it does not have exactly 10,000 blocks preceding it (otherwise, all the block numbers within the session would be off). Therefore, such a recording cannot be used in a virtual disk drive. If you need to write again to the same medium, you must first create a session with the proper number of blocks (9,999 in our example).

2. Only Track-At-Once recordings can be used.

Recordings in Disc-At-Once mode carry a 'pre-gap' sequence of 150 blocks before the start of the actual data for the session. This has the same effect as a session that is not the first one on the medium (i.e., that does not start at the very first block). This case, technically speaking, is just a special case of the previous limitation.

3. Only recordings with a data block size of 2048 bytes can be used.

Virtual disk drives and recording software expect an image to process having 2048 bytes per block, at least for data recordings. Yet they often use block sizes different from this quantity when actually writing information to a medium. This behavior has also been noticed when copying discs using hybrid CD-RW/DVD reader drives.



## CD image analysis

The analysis of a CD or DVD image always creates at least one file: the analysis log file. This file is discussed in the following sections.

All files added to the database, including the log files, an eventual image file, and any data files extracted from the image, have a number prefixed to their names; for example, the file 'foo.dat' that was written to a CD-R would, thus, appear as '[000055394] foo.dat'. All files created from the same recording session have the same ID number, and distinct recording sessions are guaranteed to be assigned distinct numbers. This allows for easy grouping of related files. This prefixed ID number shall be represented as '[#####]' in the remaining part of this document.

### Files

The files in the recorded session are stored in the database and, if full shadowing is enabled for the analysis, their contents are copied to the Data File Directory used by the SecureWave Application Server. Files whose data is absent (see *Multi-session media*) are logged but not added to the database as individual entries.

### Logs

The Sanctuary Client Driver always produces a shadow file named '[#####] CD-or-DVD-analysis-log.txt', a Unicode text file that can be read with Notepad or any other Unicode-enabled editor or viewer. This file contains information on the write settings, additional file systems (e.g., the ISO file system accompanying a Joliet file system), any errors encountered, and the full list of directory entries found, including files with data residing in an earlier recording session. We recommend reviewing this log file as it contains, near the end, any non-zero and unused portions of the image that might be use as a covert channel.

If any errors are encountered, the Sanctuary Client Driver also creates an error log ('[#####] CD-or-DVD-error-log.txt') containing just the error messages. We strongly recommend reviewing this file if it does appear.

### Saved image

Should a fatal error be encountered during the analysis (e.g. unreadable directory, invalid image format), the entire image file is added as a shadow file '[#####] Unparsed-CD-or-DVD-image.iso'. You can record this file onto a suitable medium for manual analysis. To record such a file, it is essential to get the write mode right – the log header shows you that information. For more details, see *Handling of unsupported shadowing formats* on page 194.

## Sample analysis log

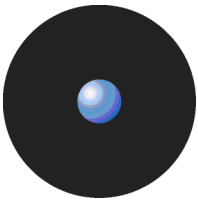
The following is an actual analysis log of a small recording (two directories with six nearly empty files using a Joliet file system). Comments are mingled with actual log entries.

```
Image parsing started:
copydate ..... Thu 29-May-2003 16:05:04
device ..... 1
user SID ..... S-1-5-21-725345543-1275210071-1644491937-1106
computer ..... FTA
image size ..... 1224704 bytes (approx. 2 MB)
first sector ..... 0
write type ..... 1 (track-at-once)
data block type ... 8 (2048 bytes -- mode 1 (ISO 10149))
multi-session .... 3 (B0 pointer indicates next PMA -- next session allowed)
block size ..... 2048 bytes
```

In this first stage, the Sanctuary Client Driver just received the initial message of an intercepted recording. Note the write parameters.

At this stage, the client parses the entire image data and sends it to the SecureWave Application Server that stores it in a temporary file.

```
Image blocksize is 2048 bytes, logical block size is 2048 bytes.
```



The logical block size for data recordings must be 2048 bytes, but the size of a physical block may vary with the recording mode:

```
Analysing volume descriptors.
Primary Volume Descriptor found at block 16.
Supplemental Volume Descriptor found at block 17.
Supplemental Volume Descriptor type: Joliet.
Volume Descriptor Set Terminator found at block 18.
```

On a pure ISO or ISO+Joliet recording, the Primary Volume Descriptor always points to the ISO file system. Joliet file systems are always referenced through a Secondary Volume Descriptor. There are other arrangements, for example a bootable CD or DVD shows a Boot Volume Descriptor in the first position, followed by PVD and any SVD entries.

On an ISO+Joliet recording, the client driver prioritizes Joliet over ISO. If the ISO file system structure is not read, some blocks are considered 'unused'. To avoid this, the client driver reads unused file system structures:

```
Touching directory tree for VD #2.
<ROOT>: touching subtree.
Found subdir: THIS_IS2
Found subdir: THIS_IS_
THIS_IS2: touching subtree.
THIS_IS_: touching subtree.
```

Having done that, the Joliet directories are read to build a list of files, subdirectories, their lengths, and their location in the image:

```
Building directory tree.
<ROOT>: building subtree.
Found file: This is the first file in the root directory
Found subdir: This is the first subdirectory
Found file: This is the second file in the root directory
Found subdir: This is the second subdirectory
This is the first subdirectory: building subtree.
Found file: This is the first file in the first subdirectory
Found file: This is the second file in the first subdirectory
This is the second subdirectory: building subtree.
Found file: This is the first file in the second subdirectory
Found file: This is the second file in the second subdirectory
```

The next stage adds those files to the shadow files known to the client and, if full-contents shadowing is enabled, extracts the actual data for those files:

```
Extracting files from image.
<ROOT>: extracting files from directory.
[000000004]This is the first file in the root directory:
Added file name and data (path "\", shadowid 10823,
location 1;0;3;cdshadow;000\000\00000003.cdshadow)
```

The above entry (all this data is in only one line in the original log) shows the file 'This is the first file in the root directory' being added to the list of shadow files. Had the file been imported from an earlier recording session on the same disc, the entry would have read '[000000004] This is the first file in the root directory: file data are in an earlier session (LBA NNN) -- skipping this file.', where 12345 would have given the block number of the file's data on the disc itself.

```
[000000005] This is the second file in the root directory:
Added file name and data (path "\", shadowid 10824,
location 1;0;4;cdshadow;000\000\00000004.cdshadow)
<ROOT>: extracting files from subdirs.
This is the first subdirectory: extracting files from directory.
```

Having processed all the files in the root directory, the first of the subdirectories (in this case 'This is the first subdirectory') is examined in the same way. We omit here all other entries of this type to save space, but they do appear fully in the analysis log.

The final stage consists in checking any block that contains data (i.e., not filled with zeros) but is not part of any file or subdirectory, and to check for partially-unused blocks, in whose unused portions data may be hidden. Since this image has not been manually falsified, no such blocks exist:

```
Verifying that unused blocks do not contain any data.
0 hidden blocks with data were dumped to the log.
0 partial blocks with extra data were dumped to the log.
Image analysis completed.
Image parsing ended (result 0).
Log closed.
```





Once this is done, the analysis of the image is now complete. If a fatal error occurs (one for which the client cannot guarantee that the shadow files and the log contain all data recorded to the disc), the image file itself would also have been added as a shadow file. You can easily verify this condition, since the name of these files in the shadow files list is deliberately chosen to be distinctive.

## Supported and unsupported CD formats

### Summary

A track-at-once (TAO) recording for data generally works fine. Ahead's Nero (we tested from 5.5.10.15a onwards) data CDs written in disc-at-once mode (DAO, but not DAO/96!) is also compatible with CD shadowing. Roxio's Easy CD Creator 5.2 and 5.3 often decide to use raw mode for SAO recordings, which is unsupported and is not allowed by the Sanctuary Kernel (client kernel driver). The same applies for Roxio's CD Copier, which is a part of Easy CD Creator. The IMAPI built-in CD-recording of Windows XP is compatible with Sanctuary Device Control.

Audio recordings are generally blocked, as they could be abused as a large-capacity covert channel to hide data.

UDF recordings cannot be analyzed (UDF/ISO bridge sessions can and will be analyzed), but CD shadowing will at the very least provide an image that can be inspected for further information.

### Supported data block formats and recording modes

In TAO mode, most recording applications use data block types 8, 10, or 13, all of which are acceptable to Sanctuary Device Control. In SAO mode, recording applications sometimes use data block type 0 for non-audio data. The details of a session's track mode, write type, and data block type are logged at the beginning of the analysis log.

Supported: ISO and Joliet

ISO 9660:1988 defines the simplest of all supported file systems. File names are restricted to eight characters, file name extensions to three; subdirectory names are also limited to eight characters and cannot have an extension; allowed characters are uppercase characters, digits, and the underscore (plus the dot to separate a file name from its extension). A less restrictive version (standard 'level 2 compliance') allows thirty-one characters in filenames including extensions, but maintains all other limitations. Sanctuary Device Control is level 2 compliant.

Joliet is, from the analysis point-of-view, a trivial extension to ISO and is not discussed separately; any noticeable differences are mentioned in the text. As mentioned above, Joliet supports the full Unicode character set, file and directory names of up to 64 characters, multiple dots in a file or subdirectory label, and a much deeper directory hierarchy.

### Supported and unsupported file system features

Sanctuary Device Control supports all basic file system features of the ISO and Joliet file systems. Interleaving and extended attributes are unsupported; neither of them is used by recording software today. If used, they show up among the unused blocks dumped to the analysis log. Associated files (akin to NTFS streams or Macintosh data and resource forks) show up as separate files of the same name.

If a Joliet file system is present, it takes precedence over the accompanying ISO file system.

#### UDF/ISO Bridge

A 'bridge' CD is one that unifies features of two normally separate media or file system types. In this case, it is a CD or DVD with a UDF file system as its primary directory structure, but the files are reflected in an additional ISO (or ISO+Joliet) file system, which UDF allows for, and which Sanctuary Device Control *can* read.

Sanctuary Device Control performs the analysis for this type of medium, considering it as a regular ISO or ISO + Joliet one. The data blocks containing the UDF file system information (subdirectories, path tables, etc.) are dumped as 'unused blocks': Sanctuary Device Control regards them as unused because the ISO or Joliet file systems do not reference them in any way.



## Multi-session media

Multi-session recordings have a special property: Earlier recording sessions on the same disc may be 'imported'; the files in such an imported session show up in the new session being recorded, but their data blocks continue to reside in the original session. In short, for an imported file, the filename is part of the new session but not the file data, and the same applies to the image.

The analysis reports such files in both the main and the error logs, but they will not be entered as shadow files into the database. No security problem arises from this behavior: The file name is logged and traceable, and since the file data is already on the disc, Sanctuary Device Control report it when the old session was recorded.

The exception is a media recorded before Sanctuary Device Control was installed, and which allows adding additional sessions. In such a case, it is possible (but difficult) to force the recording application to create a local image file, manually modify it to disguise the older files' names, and record that in a medium. The log shows the false name and the data is absent. The countermeasure is to finalize such media with the installation of Sanctuary Device Control. This ensures that no further sessions can be written, making it impossible to disguise the name of a sensitive file.

## Unsupported: UDF-only recordings

UDF is generally unsupported. Since the Sanctuary Client Driver has no way to determine, at recording time, the type of file system contained within the data stream, such an image is submitted to SecureWave Application Server. The client analysis will have failed, as UDF does not even have a 'Primary Volume Descriptor' (the hook off which, in an ISO/Joliet file system, all other data structures hang). SecureWave Application Server then adds the image file in its entirety to the shadow files and makes appropriate notations in the main and error logs.

Usually, such images can be recorded to a suitable medium or mounted as a virtual disk volume.

## Unsupported: Audio tracks

Audio tracks are not permitted since Sanctuary Device Control cannot interpret them. The raw track format allows writing completely unstructured data in any format a user might choose and would thus circumvent monitoring or shadowing the information recorded to disc.

## Partially supported: Disc-At-Once recordings

Depending on the make and version of the recording software used and on the version and service pack of the underlying operating system, some recording software uses data block type zero to write data media in DAO mode. These recordings are indistinguishable from audio recordings and, for the same reasons, are not permitted by Sanctuary Kernel (client kernel driver).

## Unsupported: Scrambled tracks

Data tracks can be recorded in the same mode as audio tracks. To do so, a recording application calculates the error-correcting CIRC and shuffles the data appropriately. These are the same steps that a CD recorder performs internally when instructed to write a normal data block.

Data tracks recorded in such a mode are not permitted by Sanctuary Kernel (client kernel driver).

## Unsupported: Packet writing, Mount Rainier

Packet writing does not record an image as such. Rather than that, it writes a block here, a few more over there, and so on in a more or less random fashion. This mode and any software implementing it are, therefore, unsupported.

## Unsupported: ISO interleaving, associated files

The ISO file system was originally designed to support interleaving – instead of occupying a number of consecutive blocks according to its length, a file would be spread out to every second, third, or, generally, Nth block. It was intended to allow delay-free playback on drives that cannot handle two data blocks without a pause. The feature was proposed even before the first CD-ROM drives were marketed. To the best of our knowledge, there is no recording software using this feature, and analyzing an image recorded in this manner causes SecureWave Application Server to log an error and store the entire image file.



### Unsupported: 'El Torito' bootable CDs

'El Torito' is a specification that builds on and expands the ISO 9660:1988 standard to accommodate bootable media. Generally speaking, 'El Torito' media can either provide an embedded image of some other media (for example, of a bootable floppy disk) with the computer's BIOS emulating a floppy disk drive using the contents of this embedded image. It can also provide a boot loader that then proceeds to read additional files from the medium, just as the computer's hard disk boot does.

In the former case, the embedded image is separate from, and unreferenced by, the ISO or Joliet file system and are therefore considered as consisting of 'unused blocks' by Sanctuary Device Control; these blocks are dumped to the analysis log as usual. Since the format and file system of the embedded bootable image are not standardized, no attempt is made to interpret the contents.

In the latter case (simple boot loader without emulation of a bootable floppy disk), the files read by the loader must be referenced like any other file in the ISO or ISO+Joliet file systems and will be analyzed like any other file.

### Unsupported: Rock Ridge extensions

Rock Ridge extensions provide several Unix-like capabilities for ISO-formatted media (hard links & file attributes used for soft links). The files themselves are accessible normally and are listed as shadow files; the control blocks used by the Rock Ridge extensions show up in the main log as 'unused blocks'.

### Unsupported: HSG (High Sierra Group) format

The High Sierra Group format was the predecessor and basis for the ISO 9660:1988 standard; the latter is a superset of the former. There is no current application that records media in High Sierra Group format; in the worst case, Sanctuary will simply file the entire image.

### Partially supported: HFS

HFS refers to Apple's Hierarchical File System. It uses the System Use Sharing Protocol to set aside a part of each directory entry for Macintosh-specific information (flags, Mac file type, and Mac file creator); these fields are ignored. Macintosh CD-ROMs also use associated files, which are not allowed for level 2 compliance; this ISO mechanism is intended to let a file have multiple 'sub-files', like NTFS streams. Associated files are recorded as multiple files bearing the same name and special flags. In particular, the 'resource fork' of a Macintosh-file is represented by such an associated file, while the main portion ('data fork') corresponds to the main entry for that file on the disc. Associated files are added to the shadow files list as separate files with the same name as the main file.



*In case the write process fails even before starting ('SCSI command aborted' or 'ASPI failing'), check the log files of the CD writer software and also the Windows Event Log to see if the write mode the drive used (if logged) is compatible with Shadowing. Some drives will automatically switch from hardware-wise to a raw write mode when copying on the fly CDs. This is often the case with hybrid 'combo' units, which support CD-RW writing and DVD reading in a single unit. A workaround in such a case is disabling shadowing completely, use a different dedicated CD or DVD burner, or copy the individual files first to the local hard disk and recreate the disc with your recording software.*



### Supported DVD/CD burning software

As DVD/CD burning operations depend heavily on the software used to do the writing, we are only currently supporting these programs when blocking DVD/CD devices:

<b>Company</b>	<b>Name of the Software</b>
NERO AG	Nero burning ROM
Sonic Roxio	Easy Media Creator
Microsoft Corp.	Windows XP built-in CD burning software

Table 48: Supported DVD/CD burning software

Other programs may cause some issues when the user tries to burn a DVD/CD. The reason for this is that some of them use 'non standard' drivers that interact directly with the hardware bypassing the 'normal' Windows channel.

You can avoid this situation if you take care on not allowing the user to be Administrator of his own machine. You can also use other cost-effective solutions, like Sanctuary Application Control Suite, to prevent the execution of non-authorized software. In this way, you avoid two potential dangers: jeopardizing the system security and avoiding the installation of non-approved, non-licensed software.



*Windows' CD recording capacity is controlled by a service called Image Mastering Applications Programming Interface (IMAPI; run by LocalSystem). If you give R/W access to LocalSystem for the 'DVD/CD Drive' class in the 'Default Settings' or 'Machine-Specific Settings' using the 'Device Explorer' module or add LocalSystem to the users of a music CD using the 'Media Authorizer' module and the service is running, then the user can create CD/DVD copies — using Windows Media Player, Windows Explorer, or any other program that uses this service — of any file from the hard disk, including private data, proprietary information, music, etc. See details in Chapter 3: Using the Device Explorer on page 47 and Chapter 6: Using the Media Authorizer on page 129. Some third-party burning software do not need the IMAPI service and can be controlled using our Sanctuary Application Control Suite.*



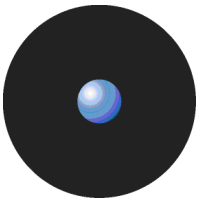
*When setting read-only permissions on the DVD/CD Drives class, some applications, notably CD-R applications, may not notice that access was denied by Sanctuary and erroneously report to the user that a CD has been burned properly when it has not. In this case, we recommend that you use Sanctuary event notification to warn users of this.*

---

## Appendix B: Important notes

In this appendix, you will find the most common difficulties that you will encounter when using Sanctuary Device Control.

- > If you define a copy limit rule for a specific user that is lower than that set for Everyone, then the ruling one will be that specified for the user. If, on the other hand, the specified copy limit rule for the user is greater than that of Everyone, the prevailing rule will be that of Everyone.
- > Be aware if you modify or create a new permission rule for the PS/2 port. The PS/2 port permission rule is enabled (Read/Write) by default for Everyone. If you define a new rule for a client, send the update, and reboot (to apply the rule) the PS/2 port is blocked for everybody until the login sequence is finished.
- > If you have too many rules in the *Media Authorizer* module or SX database, reports may take too long to be generated.
- > If you need an access to external modems, depending on your brand, you may also need to allow access to the COM port.
- > Some cashier workstations use a COM-connected printer running as a service under LocalSystem context. You will have to define explicit permissions rule for Local Systems and COM ports to make them work.
- > If you are using computers in different time zones, be aware that when using Date filter settings in the *Reports* and *Log Explorer* modules you may 'lose' some of the records where the day has not changed yet.
- > Some users may find poor performance in their server machines when servicing a large number of users. This occurs when using standard desktop machines as servers and, normally, this is traced down to a slow hard disk system. We recommend using a server-grade machine with a fast disk system, and a dedicated SQL machine.
- > If a remote user logs off incorrectly, by simply turning the machine off or closing the terminal service (remote desktop connection), those devices for which the user identity cannot be determined with 100% certainty are blocked. You should try to persuade all users to logoff correctly to prevent this kind of problems.
- > Sometimes the Sanctuary Management Console will block when the Device Explorer is open. This problem has been tracked down to machines running Windows 2000 Professional edition with Service Pack 4 installed. As stated on Microsoft's Web site:  
<http://support.microsoft.com/default.aspx?scid=kb;en-us;318731>, removing Clbcatq.dll will fix the problem.
- > Occasionally the installation of some COM+ products corrupts. Microsoft COM (Component Object Model) technology enables software components to communicate between them, for example, Word and Excel. You should consult Microsoft's Web site for instructions on how to reinstall the COM+ component (<http://support.microsoft.com/default.aspx?scid=kb;en-us;318731> removing Clbcatq.dll).
- > Scanners can only be blocked if they are connected using TWAIN or WIA COM interfaces. You can normally find those scanners listed in the Windows' *Control Panel* → *Scanners and Cameras* dialog. Direct access scanners (not using TWAIN or WIA interfaces) cannot be blocked during remote sessions.
- > If you are trying to connect a HP Omnibook notebook to your system, you should assign LocalSystem Read/Write permission rule on the LPT/Parallel port because there is a bug in the OMNI97.sys driver that controls the device. Otherwise, your system could block. Since the LPT class controls the machine, you cannot assign shadow and copy limits rules.



- > The Sanctuary Command & Control can now dismount volumes without any explicit permissions. However, volumes are dismounted *only* when the Sanctuary Command & Control receives an explicit request from SecureWave Application Server to upload current shadow/log files. When Sanctuary Command & Control uploads files in the normal course of operations, volumes are never dismounted.

Take into account that in some special cases you will not get the latest shadow files for your administrators to review. This happens, particularly, when the client uploads files in the normal course of operations (as governed by the Log Upload Interval, Log Upload threshold, Log Upload Time, Log upload Delay option). In order to upload shadow files, the client needs to dismount the drive (this will force all information in Windows caches to be committed to the drive). Dismounting drives during a lengthy copy operation would interrupt the copy and disrupt the user. This is why, in the case of normal course operation, volumes are never dismounted and the files are transmitted as soon as the media is removed. However, volumes *are* dismounted when the client receives an explicit request from the server to upload current shadow/log files (i.e. the administrator clicks on the **FETCH LOG** button in Log Explorer and selects the client machine). This means that using the Fetch Log functionality while users are busy copying data can interrupt the copy.

- > When the Media Authorizer exports a key to a file, it does not use *Sanctuary Kernel* to do so — it obtains the key directly from the server. This is done for administrative purposes. However, it still has to use Sanctuary Kernel to export the key to the medium — but Sanctuary Kernel does not know about the administration status of the user and refuses to export it if the Export permissions on the Removable Device class is not configured properly. See *Special case: Working with Removable Storage Devices* on page 59 for more information.
- > If a *Copy Limit* rule (see page 84) exists for a device and this quota is exceeded during a file copy, the *Shadow* system only sends those bytes established under that rule, not the complete file.
- > You can experiment some 'strange' behavior when connecting some hardware not recognized as removable device but as a 'hard drives'. The Sanctuary Client Driver does not dismount hard drives to avoid interference with applications already using the device. Some shadow files may be unavailable until the device is unplugged (dismounted). When multiple files are copied, only the most recent are not transmitted, older files become transmittable. Please notice that if the hard drive is unplugged, it is dismounted and does not represent a security hole: as soon as the files **TRULY** leave the machine, they will be made available for the Log Explorer module. The only problem arises when the machine is **SWITCHED OFF** without notifying first the OS (some files are not transmitted). If a full shadow rule is defined, there is no information loss. However, if only the file name is requested, file size info will not be available.
- > Notes on the *Removable Storage Devices* class:

The shadow rule applies, among others to the *Removable Storage Devices* class. It cannot be activated for the *User Defined Device* class.

The removable memory of those Smart Phones that use Windows CE as OS is included on the *Removable Storage Devices* class — the internal device memory can be treated and acceded with alternative methods. Therefore, what is copied to this removable memory can be shadowed and controlled with the same flexibility and granularity as for all those devices included in this class.

Smart Phones that do not use Windows CE as their operating system are sometimes defined on the *User Defined Devices* class. Consequently, only 'R/W' or 'No Permission' can be assigned to their memory and I/O data transfer cannot be shadowed. Recent models, however, adhere to the 'standard' schema of declaring their memory to the *Removable Storage Device* class (ex. Sony Ericsson W800).

Please see *Managing devices* on page 92 for more details.

- > A practical example for the *User Defined Devices* class:

A user buys a mobile phone with a non Windows CE OS. As these devices have high memory capacity (going into the GB), they can be a potential data leakage hole in your security system.

Windows, when installing these devices through the PnP mechanism, proposes up to eight (or more, depending on the functionalities offer by the device: MP3, photo, radio, USB memory stick, etc.) internal drivers, ranging from modems to USB generic drives passing through generic phones.

No direct connection is allowed for this kind of devices since no default permissions is set. Sanctuary Device Control is denying access to this (yet) unknown peripheral.



To grant permissions for using all/some of the device's functionalities, you must first add it — and all its internal drivers, as recognized by the PnP mechanism — using the *Manage Device* dialog.

The memory of these peripherals, since they do not use Windows CE as OS, is not included on the *Removable Storage Devices* class not allowing the definition of a *Shadow* rule. If you only define permissions for one type of class — for example, the memory included on the *Removable Storage Devices* class —, the device will not connect or have a partial functionality. The same is true if you grant permissions for the part included in the *Modem/Secondary Network Access Devices* and *Wireless NICs* class.

To have a complete access to this kind of device, you must define permissions for all those classes where the drivers that Windows recognized for this peripheral belongs — for example, one permission on the *Modem/Secondary Network Access Devices* class, one for the *Wireless NICs* class, and one for the *Removable Storage Devices* class.

Conclusion: Although there is no shadow rule for the memory of those devices that do not use Windows CE as their OS, you can grant them full/partial functionality when defining permissions on those classes where the proposed Windows' drivers belong. Please see *Managing devices* on page 92 for more details on how to do this. You can rest assured that you are protected for those future devices not yet on the market place.





---

## Glossary

### ADSI

**Active Directory Service Interface.** Previously known as OLE Directory Services, ADSI makes it easy to create directory management applications using high-level tools such as Basic, Java, or C/C++ without having to worry about the underlying differences between the dissimilar namespaces.

### AES

**Advanced Encryption Standard.** A symmetric key encryption technique that is replacing the commonly used DES standard. It is the result of a worldwide call for submissions of encryption algorithms issued by NIST in 1997 and completed in 2000.

### CAB

File extension for **cabinet** files. They 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

A computer on your network that is supervised by the Sanctuary Device Control.

### Cscript.exe

A command prompt-based version of WSH that sends its output to the command window in which it was started.

### CSV

**Comma Separated Value.** A file format that allows easy data table retrieval into a variety of applications. It is often used to exchange data between disparate applications. The file format has become a pseudo standard throughout the industry, even among non-Microsoft platforms. Common examples of applications that use this format are spreadsheets and databases. You can also see and edit these files using an ASCII text editor (Notepad, Word, WordPad, Excel, etc.).

### DAO

**Disc-At-Once.** A method of recording data on a CD that consists in a single write operation without turning the laser light off.

### DCOM

**Distributed Component Object Model.** A set of Microsoft concepts and interfaces built into Windows operating system in which client program objects can request services from server program objects on other computers in a network. The first versions of DCOM were exploited to introduce worms and Trojans into networks. Windows XP SP2 and Windows Server 2003 SP1 and later include many changes that enhanced security. Although these resolved problems present in earlier versions of Windows, they also changed some DCOM properties that must be fine-tuned.

### Delegation

The act of assign responsibilities for management and administration of a portion of the resources or items used in a shared computing environment to another user, group, or organization.



### Direct cable connection (DCC)

A RAS (**R**emote **A**ccess **S**ervice) networking connection between two computers, or between a computer and a Windows CE–based device, which uses a serial or parallel cable directly connected between the systems instead of a modem and a phone line.

### DN

**Distinguish Name.** A name that uniquely identifies an object in the Directory Information Tree.

### Executable program

A program that can be interpreted by itself directly on a computer. The term usually applies to a compiled program translated into machine code in a format that can be loaded in memory and run by a computer's processor.

### GUID

A **G**lobal **U**nique **I**dentifier number generated when the NDS object is created. It is simply an object's NDS attribute. In order to ensure data consistency, Novell eDirectory implements a globally unique ID (GUID) for all objects within the directory. The total number of unique keys (2128 or 3.4028 x 1038) is so large that the possibility of using the same number twice is nearly zero.

### iFolder

A Novell client that runs on Windows-based computers. It allows a user to work on his files anywhere —online or offline. iFolder integrates encryption and file synchronization services.

### IMAPI

**Image Mastering Applications Programming Interface.** A Windows' operating system service assigned to LocalSystem used by some CD/DVD burning software. It should be disabled so that users cannot — using Windows Explorer, Windows Media Player or other programs that rely in this service — create CD/DVD copies in Windows XP & above.

### IOCP

**I/O (Input/Output) Completion Port.**

### MAPI

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

### MDAC

**Microsoft Data Access Components.** A component required by computers using Windows to connect to SQL Server, MSDE, or SQL Server 2005 Express Edition databases.

### MSDE

**Microsoft Data Engine** (also known as Microsoft SQL Server Desktop Engine), is a SQL Server compatible database server, suitable for small and medium size organizations. MSDE databases can subsequently be migrated to SQL Server 2000/2005. SQL Server 2005 Express Edition now supersedes MSDE.

### NDAP

**Novell Directory Access Protocol.** The NDAP component gives Windows applications full access to the Novell eDirectory and administration capabilities for NetWare servers, and volumes.

### NDS

Novell's eDirectory previously called **Novell Directory Services.** eDirectory is a hierarchical, object oriented database that represents all the assets in an organization in a logical tree. Assets can include users, positions, servers, workstations, applications, printers, services, groups, etc.



## Negative permission

It is important to make a distinction between the absence of permission and a negative permission — 'None':

- > In the first case, if no permission has been defined, the driver applies the most restrictive access.
- > In the second case, when creating a permission for which neither the read nor the write flags are selected, you deny the user access to the device even if the group he is member of grants him this access. You specifically deny the access to a device for the user.

## NICI

**Novell International Cryptographic Infrastructure.** NICI is a base set of cryptographic services available for Novell. NICI provides an API set that offers a consistent interface for application developers to use and deploy cryptography within their applications.

## OU

**Organizational Units.** A part of the Active Directory (AD) structure inherited from Novell's NDS structure. Within Novell's NDS/eDirectory there are three classes of objects in the NDS database: Roots, Containers, and Leafs. There are three supported types of container objects: Country (C=), Organizations (O=), and Organizational Units (OU=).

## Private Key

One of the two keys used in public key encryption. In our case, the server keeps the private key secret and uses it to encrypt digital signatures and to decrypt received messages.

## Public Key

One of the two keys used in public key encryption. In our case, the server releases this key to the client drivers. It is used to encrypt messages sent to the client and to decrypt his digital signature.

## RPC

**Remote Procedure Call.** A protocol that allows a computer program running on one host to run a subroutine on another host. RPC is used to implement the client-server model of distributed computing.

## RSA Encryption

In 1977, Ron Rivest, Adi Shamir, and Len Adleman developed the public key encryption scheme that is now known as RSA, after their initials. The method uses modular exponentiation, which can be performed efficiently by a computer, even when the module and exponent are hundreds of digits long.

## SAO

**Session-At-Once.**

## 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.

## SQL Server

Microsoft's industry standard database server. You will need it, or the SQL Server 2005 Express Edition component, to run Sanctuary Device Control.

## 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 Sanctuary Client Driver.

## TAO

**Track-At-Once.**



## TCP/IP

**Transmission Control Protocol/Internet Protocol.** The protocol used by the client computers to communicate with the SecureWave Application Server.

## VBScript

A scripting language created by Microsoft embedded in many applications used in Windows. Although it allows for powerful interoperability and functionality, it also creates a great deal of security risks unless it is tightly controlled.

## Well-Known Security Identifiers

A security identifier (SID) is a unique value used to identify a security principal or security group. The values of certain SIDs remain constant across all installations of Windows systems and for this reason are termed well-known SIDs. Everybody, Local, Guest, Domain Guest, etc. are some examples of SIDs.

## WMI

**Windows Management Instrumentation.** WMI is a standard technology to access management information in an enterprise environment. WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components. You can use WMI to automate administrative tasks in an enterprise environment. WMI improves administrative control by allowing administrators to correlate data and events from multiple sources and vendors on a local or enterprise basis. It is used as a complement to ADSI.

## WSH

**Windows Script Host.** Application provided with Windows operating systems to interpret plain text files containing a series of valid commands called scripts. It is language-independent, meaning that it will work with any modern scripting language. It has built-in support for JavaScript, XML, and VBScript, but can be extended to use almost any other language, such as Perl and Python. There are two versions of the Windows Script Host: a windows-based version (wscript.exe) dialog for setting script properties, and a command prompt-based version (cscript.exe). WScript.exe generates windowed output, while CScript.exe sends its output to the command window in which it was started.

## Z.E.N.works

**Zero Effort Networks.** This lets you create a Workstation Policy Package and edit the Novell client configuration parameters, including the preferred tree and default print-capture settings, as well as client parameters, like opportunistic locking.

---

## Index of Figures

Figure 1: Connecting to the server .....	20
Figure 2: Connection / Output window.....	20
Figure 3: The Sanctuary Management Console screen.....	21
Figure 4: License status warning.....	21
Figure 5: Docked Control Panel .....	22
Figure 6: Docked window.....	22
Figure 7: Floating Control Panel.....	22
Figure 8: Floating windows.....	23
Figure 9: Minimized windows .....	23
Figure 10: Endpoint maintenance.....	28
Figure 11: The Default Options dialog .....	30
Figure 12: The Synchronizing Domains dialog .....	31
Figure 13: Adding workgroup computers.....	31
Figure 14: The Connect As dialog.....	31
Figure 15: Performing database maintenance.....	32
Figure 16: Searching for users .....	33
Figure 17: Defining the administrators' roles.....	33
Figure 18: The four level removable device class structure .....	37
Figure 19: The four level removable device class structure with permission examples .....	38
Figure 20: Computers and computer groups .....	39
Figure 21: Device Explorer main window.....	47
Figure 22: The Device Explorer module two main sections .....	48
Figure 23: Contextual menu.....	50
Figure 24: Show all members.....	52
Figure 25: Event notification: selecting the users/groups.....	53
Figure 26: Event notification: options.....	53
Figure 27: Event notification: finish the rule definition.....	54
Figure 28: Event notification: new permission rule as shown for the device class.....	54
Figure 29: Using Drag & Drop to move devices to a newly created group .....	55
Figure 30: Main permissions dialog.....	57
Figure 31: Bus dialog used for Shadow.....	58
Figure 32: General Permissions dialog exceptions.....	58
Figure 33: Removable permissions settings example 1 .....	59
Figure 34: Removable permissions settings example 2.....	60
Figure 35: Removable permissions settings example 3 – Encrypted.....	60
Figure 36: Removable permissions settings example 3 - Unencrypted.....	60
Figure 37: Removable permissions settings example 4.....	60

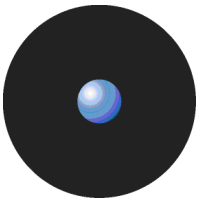


Figure 38: Defining a file filter..... 62

Figure 39: The Select Group, User, Local Group or Local User dialog ..... 66

Figure 40: Assigning default permissions to users and groups ..... 68

Figure 41: The Permissions dialog ..... 68

Figure 42: The Select Group, User, Local Group or Local User dialog when adding default permissions ..... 68

Figure 43: The Select Computer dialog showing multiple selection in action ..... 71

Figure 44: Assigning permissions in the Device Explorer module..... 71

Figure 45: Defining Read, Read/Write, or None permissions when adding permissions ..... 72

Figure 46: The Select Group, User, Local Group or Local User dialog ..... 72

Figure 47: Modifying permissions..... 72

Figure 48: Removing permissions ..... 73

Figure 49: Add a Scheduled permission..... 73

Figure 50: The Choose User dialog when adding a scheduled permission ..... 73

Figure 51: Defining Read or Read/Write permissions when adding scheduled permissions ..... 74

Figure 52: The Choose Timeframe dialog when adding a scheduled permission..... 74

Figure 53: Modifying a scheduled permission..... 74

Figure 54: Adding a Temporary permission..... 75

Figure 55: The Choose User dialog when adding a temporary permission ..... 75

Figure 56: Defining Read or Read/Write permissions when adding a temporary permission ..... 76

Figure 57: The Choose Period dialog when adding a temporary permission ..... 76

Figure 58: Sanctuary Client's Request Temporary Access Offline dialog – Introduction page ..... 77

Figure 59: Sanctuary Client's Request Temporary Access Offline dialog – Input page ..... 77

Figure 60: Sanctuary Management Console's Authorize Temporary Access Offline dialog ..... 77

Figure 61: Sanctuary Client's Request Temporary Access Offline dialog - Unlock page..... 78

Figure 62: Sanctuary Client's Request Temporary Access Offline dialog – Finish page ..... 79

Figure 63: Temporary Access Offline reminder to administrators ..... 80

Figure 64: Defining Read, Read/Write, or None permissions when adding online/offline permission ..... 81

Figure 65: Importing permission settings..... 82

Figure 66: The Choose User dialog when adding a shadow rule ..... 83

Figure 67: Selecting the bus when adding temporary permissions ..... 83

Figure 68: Defining the type of shadow for a device ..... 84

Figure 69: Finishing the shadow rule definition..... 84

Figure 70: The Choose User dialog when adding a copy limit rule ..... 85

Figure 71: Defining a copy limit ..... 85

Figure 72: The status screen on the client's side: copied/remaining bytes..... 85

Figure 73: Decentralized encryption: The Access Denied message and inviting the user to encrypt it..... 89

Figure 74: Password complexity is required to encrypt the device..... 89

Figure 75: Decentralized encryption: The Encryption option of the contextual menu ..... 89

Figure 76: Decentralized encryption: Encryption begins ..... 89

Figure 77: Decentralized encryption for a group defined at a device group level (1/2) ..... 89

Figure 78: Decentralized encryption for a group defined at a device group level (2/2) ..... 89

Figure 79: Decentralized encryption at the unique device level (1/2) ..... 90

Figure 80: Decentralized encryption at the unique device level (2/2) ..... 90

Figure 81: Decentralized encryption at the class level (1/2)..... 91

Figure 82: Decentralized encryption at the class level (2/2)..... 91

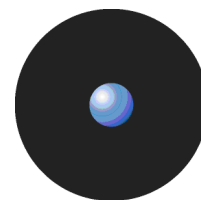


Figure 83: Decentralized encryption using a 'delegated' user (1/2).....	92
Figure 84: Decentralized encryption using a 'delegated' user (2/2).....	92
Figure 85: Managing devices .....	93
Figure 86: Managing devices - selecting the computer.....	93
Figure 87: Managing devices - choosing the devices from the selected computer.....	93
Figure 88: Removing devices.....	94
Figure 89: Confirming the removal of a device .....	94
Figure 90: Priority setting .....	95
Figure 91: Sending updates to client computers.....	96
Figure 92: The send update item from the contextual menu.....	97
Figure 93: The Log Explorer main window .....	101
Figure 94: The Select and edit templates window .....	103
Figure 95: The Templates settings window .....	103
Figure 96: Components of the Log Explorer window .....	105
Figure 97: Navigation/Control bar.....	105
Figure 98: Column headers showing multiple classifications .....	106
Figure 99: Columns context menu.....	107
Figure 100: Group By option .....	107
Figure 101: Column headers showing grouped results.....	107
Figure 102: Column headers showing sub groups.....	107
Figure 103: Computed columns .....	108
Figure 104: Column headers showing a computed and a sorted column.....	108
Figure 105: Resetting column headers.....	109
Figure 106: Props tab.....	111
Figure 107: Criteria tab .....	111
Figure 108: Control button bar.....	111
Figure 109: Select and edit templates window .....	111
Figure 110: Filter templates dialog .....	112
Figure 111: Templates context menu .....	113
Figure 112: Template settings window – Simple Query tab .....	113
Figure 113. Grouping results in the query.....	114
Figure 114: Example of criteria settings .....	116
Figure 115: Query & Output tab .....	116
Figure 116: Schedule tab .....	118
Figure 117: Format tab.....	118
Figure 118: Delivery tab .....	119
Figure 119: Edit target dialog .....	119
Figure 120: Edit target dialog (E-mail) .....	120
Figure 121: Viewing the content of a shadow file in text form .....	123
Figure 122: Viewing the content of a shadow file in binary form .....	123
Figure 123: Error message when a shadow file is not found.....	123
Figure 124: Windows' Event Viewer when a shadow file is not found.....	124
Figure 125. Fetching New Logs.....	125
Figure 126. Adding devices to the managed devices list .....	125

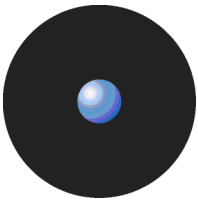


Figure 127: Using a DVD/CD from the library .....	130
Figure 128: The Media Authorizer main window .....	131
Figure 129: Adding an encrypted DVD or CD .....	132
Figure 130: Adding a specific removable storage device .....	135
Figure 131: 'Inaccessible medium' error message .....	137
Figure 132: 'Not enough privileges' error message .....	137
Figure 133: 'Already authorized' error message .....	137
Figure 134: 'Already encrypted' error message .....	137
Figure 135: 'Identification record cannot be deleted' error message .....	138
Figure 136: Importing back an already encrypted device .....	138
Figure 137: A specific medium with its related users and groups .....	139
Figure 138: Adding a group or user to a selected medium .....	139
Figure 139: Denying access to DVDs/CDs/encrypted removable media .....	139
Figure 140: Media by user authorization .....	140
Figure 141: 'Users still associated with medium' warning message .....	141
Figure 142: 'Deleting medium' warning message .....	141
Figure 143: 'Cannot delete identification record' error message .....	142
Figure 144: Renaming a DVD/CD/Removable storage device .....	143
Figure 145: Exporting a medium key .....	143
Figure 146: Unlock Medium window .....	144
Figure 147: User exceeded allowed number of attempts to unlock medium message .....	144
Figure 148: Recover Password dialog .....	144
Figure 149: Sanctuary Password Recovery wizard - Encrypted Medium ID and Security Code page .....	145
Figure 150: Sanctuary Password Recovery wizard - Passphrase page .....	145
Figure 151: Recover Password dialog – entering passphrase .....	146
Figure 152: Sanctuary password recovered message .....	146
Figure 153: Sanctuary medium unlocked message .....	146
Figure 154: Exporting encryption keys .....	149
Figure 155: Exporting encryption keys (by the user) .....	150
Figure 156: Export Medium Key dialog - to export the encryption key to a file .....	151
Figure 157: Export Medium Key dialog - to export the encryption key on the device itself .....	152
Figure 158: Adding a device with an external key .....	153
Figure 159: Adding a device where the key resides on the medium .....	153
Figure 160: Accessing unauthorized encrypted media .....	155
Figure 161: The Import Medium Key dialog (importing from the medium or a folder) .....	155
Figure 162: Formatting an encrypted key using the Decrypt Medium command .....	156
Figure 163: Importing an external device .....	157
Figure 164: Importing an external device .....	157
Figure 165: Importing an external device .....	157
Figure 166: Using the Sanctuary Device Control Stand-Alone Decryption Tool .....	159
Figure 167: The Import Medium Key dialog when using the Stand-alone decryption tool .....	159
Figure 168: Sanctuary Volume Browser .....	160
Figure 169: Accessing the Sanctuary Volume Browser application on the encrypted media .....	164
Figure 170: Sanctuary Volume Browser .....	164
Figure 171: Sanctuary Volume Browser – encrypted medium selected .....	165



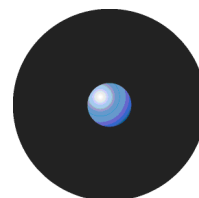


Figure 172: Sanctuary Volume Browser - Allowed attempts to unlock medium exceeded message .....	165
Figure 173: Recover Password dialog.....	165
Figure 174: Sanctuary Password Recovery wizard - Encrypted Medium ID and Security Code page.....	166
Figure 175: Sanctuary Password Recovery wizard - Passphrase page.....	167
Figure 176: Recover Password dialog – entering passphrase .....	167
Figure 177: Sanctuary password recovered message.....	167
Figure 178: Sanctuary medium unlocked message .....	167
Figure 179: The Default Options dialog.....	170
Figure 180: Setting computer-specific options.....	170
Figure 181: Online/Offline state detection option as applied to Wireless NICs.....	175
Figure 182: Checking the settings on a client machine.....	177
Figure 183. Obtaining a report.....	180
Figure 184: User Permissions report.....	180
Figure 185: Device Permissions report.....	181
Figure 186: Computer Permissions report.....	182
Figure 187: Media by User report.....	183
Figure 188: Users by Medium report .....	184
Figure 189: Shadowing by Device report.....	185
Figure 190: Shadowing by User report.....	186
Figure 191: Online Machines report .....	187
Figure 192: Machine options report.....	188
Figure 193: SecureWave Application Server Settings report .....	190



---

## Index of Tables

Table 1: The Sanctuary Device Control modules.....	24
Table 2: File menu options.....	26
Table 3: View menu options.....	26
Table 4: Tools menu options.....	27
Table 5: Report menu options.....	29
Table 6: Explorer Menu options.....	29
Table 7: Window menu options.....	30
Table 8: Help menu options.....	30
Table 9: Administrator's prerogatives.....	33
Table 10: Administrator's roles.....	34
Table 11: Standard Windows' device classes as seen on the Device Explorer module in the Default Settings section.....	36
Table 12: Managing unique individual removable devices.....	37
Table 13: Simultaneous permissions definitions for all Windows' standard device classes in the Device Explorer module.....	40
Table 14: Shadow permissions priorities.....	43
Table 15: Default settings following installation (these apply to 'Everyone').....	49
Table 16: Possible assignments by device.....	50
Table 17: Keyboard shortcuts in the Device Explorer module.....	51
Table 18: Device classes that can have Device Groups.....	55
Table 19: Allowed settings when working with the Removable Storage Devices class.....	59
Table 20: File type filtering options.....	61
Table 21: File types for filtering.....	63
Table 22: File filter settings and permission relation.....	63
Table 23: File filter settings examples.....	65
Table 24: Add user/group dialog options.....	66
Table 25: Applied permissions.....	70
Table 26: Temporary Access Offline dialog settings.....	78
Table 27: Permissions example.....	87
Table 28: Resulting access.....	96
Table 29: Permission settings priority.....	96
Table 30: Limitations while using the Log Explorer module under other user/domain account.....	102
Table 31: Log Explorer module column meaning.....	110
Table 32: Template Filter checkboxes.....	112
Table 33: How to use the available criteria dialogs.....	116
Table 34: Audit events.....	127
Table 35: Available encryption methods.....	135



Table 36: Encryption methods comparison..... 136

Table 37: Resulting access when permissions are defined at the Device Explorer and Media Authorizer levels (Example 1) ..... 147

Table 38: Resulting access when permissions are defined at Device Explorer and Media Authorizer levels (Example 2)147

Table 39: Easy Exchange encryption options..... 160

Table 40: Full Encryption method inside and outside your company ..... 162

Table 41: Easy Exchange encryption method inside and outside your company ..... 162

Table 42: Option name comparison ..... 170

Table 43: Offline/Online state detection configuration as applied to Wireless NICs ..... 175

Table 44: USB Keylogger options ..... 177

Table 45: Reports that can be obtained by Administrator type..... 179

Table 46: Columns of the 'Online Machines' Report..... 187

Table 47: Supported formats for the full shadow or file name only shadow modes ..... 194

Table 48: Supported DVD/CD burning software ..... 200

---

# Index

## A

Access rights  
  Monitoring; 99, 100, 126  
Accessing encrypted media outside of your organization; 149, 153  
Active directory; 33, 71, 126, 133  
  Delegation; 33  
  Service Interface; 205  
Add  
  A specific removable device; 135  
  Managed device; 126  
  Removable; 135  
Adding DVD/CD; 131, 132  
  Pre-requisites; 132  
Administrator; 32, 33, 126  
  Monitoring; 99, 100, 126  
  Roles; 14  
ADSI; 205  
Advanced Encryption Standard; 133, 205  
Advanced queries; 116  
AES; 133, 205  
Analysis of a CD image; 195  
Assigning permissions to use DVD/CDs/Encrypted Media; 138, 140  
Attachment; 109  
Audit events; 109, 126  
  Accessed device log; 126  
  Accessed shadow file; 126  
  Add computer group; 126  
  Add device group; 126  
  Add managed device; 126  
  Added media; 126  
  Added permission; 126  
  Added scheduled permission; 126  
  Added temporary permission; 126  
  Authorized media; 126  
  Automatic user access upgrade; 126  
  Change computer group; 126  
  Change device group; 126  
  Deleted default option; 126  
  Deleted option; 127  
  Generate maintenance ticket; 127  
  Modified scheduled permission; 127  
  Modify user access role; 127  
  Purged DB and file storage; 127  
  Remove computer group; 127  
  Remove device group; 127  
  Remove managed device; 127  
  Removed media; 127  
  Rename computer group; 127  
  Rename device group; 127  
  Revoked permission; 127

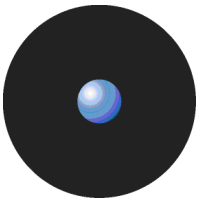
  Revoked scheduled permission; 127  
  Revoked temporary permission; 127  
  Set default option; 127  
  Set option; 127  
  Unauthorized media; 127  
  Updated Media; 127  
  Updated permission; 127  
  Uploaded shadows; 127  
Audit logs; 99, 100, 109, 126

## B

Biometric devices; 16

## C

CAB; 205  
Calculated values; 108  
Centralized device control log; 169  
Centralized encryption; 14  
Certificate generation  
  Disabled; 171  
Certificates; 133  
CIM; 208  
Client computer; 69, 72, 73, 74, 81, 84, 94, 96, 100, 141, 170, 174, 193, 205  
Client hardening; 172  
Client Hardening; 27  
Client ticket; 27  
  Create; 28  
  Rules; 27  
Column headers; 105  
COM; 16  
  Printers; 201  
  Serial ports; 16  
COM+; 201  
Comments; 51  
Common Information Model; 208  
Compatible mode; 34  
Computed columns; 108  
Computer groups; 51  
Computer-specific  
  Options; 170  
  Permissions; 71, 154  
Connect  
  As; 31  
  Events; 99  
  To the SecureWave Application Server; 19  
Contact details; 8  
Context-sensitive permissions; 13  
Copy limit; 13, 84, 201  
Criteria; 111, 115  
Criteria dialog; 115  
Cscript.exe; 205, 208



CSV; 205  
Custom reports; 102, 116

## D

DAO; 205  
Data file directory; 32  
Database  
    Maintenance; 26  
Database maintenance; 32  
DCC; 206  
Decentralized encryption; 14, 40, 129  
Decrypt medium; 156  
Default  
    Options; 170  
    Permissions; 68  
    Settings; 68, 71  
Default Permissions; 67  
Delegation; 205  
Device  
    Import; 157  
    Management, Log Explorer; 125  
    Monitoring; 99  
Device Attached; 120  
Device class; 109  
Device control status window; 169  
Device Explorer; 24, 47, 57, 96, 146, 147, 170, 171  
Device groups; 55  
    Add; 55  
Device log; 92, 99, 100, 172  
    Disabled; 172  
    Enabled; 172  
    throttling; 173  
Device Model; 109  
Devices in logical groups; 38  
DN; 206  
DNS; 133  
DVD/CD  
    Drives; 16  
    Shadowing; 14, 124, 193  
    Supported formats; 194, 197  
    Unsupported formats; 194, 197  
DVD/CD hash; 130

## E

Easy Exchange; 159  
Encrypted media  
    Key recovery; 143  
Encrypted Media; 138  
    Import; 157  
Encrypted media export password; 169  
Encrypted media key export; 169  
Encrypting media; 40  
Encryption; 129  
    Adding removable drives; 132  
    Centralized; 14  
    Decentralized; 14, 40  
    Examples; 41  
  
    Easy exchange (insecure for existing data); 135  
    Encrypt Removable; 135  
    Error messages; 136  
    Export key on medium; 152

    Export key to file; 151  
    Full & Slow (secure for existing data); 135  
    Import (secure for existing data); 137, 142  
    Import a device; 157  
    Key Length; 133  
    Limitations; 134  
    Lost or broken media; 142  
    Method; 135  
    Password; 154, 155, 159  
    Password strength; 151, 152  
    Pre-requisites; 133  
    Quick Format (insecure for existing data); 135  
    Users by medium; 138, 140

Endpoint; 177  
Endpoint Maintenance; 27, 172  
Enterprise Administrators; 33  
Errors  
    on client machines; 99  
Event Log; 172  
Executable program; 206  
Explicitly deny; 48, 86  
Explorer menu; 29  
Export  
    Encryption key; 143, 149  
    Key  
        To file; 150  
  
        To media or file; 150  
    Medium key; 150

## F

Fetch Latest Log Files; 100  
File filters; 14, 60  
    Examples; 64  
    Remove; 63  
File Menu; 25  
File shadowing; 13, 100  
File type filtering; 14, 60  
    Examples; 64  
    Remove; 63  
Floppy disk drives; 16  
Format custom reports; 118

## G

Grouping log entries; 107  
GUID; 206

## H

Hash; 110  
Help menu; 30

## I

Identifying devices; 35  
Identifying users and user groups; 35  
iFolder; 206  
Imaging devices; 16  
IMAPI; 206  
Import; 157  
Important notes; 201  
Incorrect logoff; 201  
Individual option settings; 171  
Informing client computers; 96



Insert Computer; 71  
IOCP; 206

## K

Key logger; *See* Keylogger  
Key recovery; 143, 145  
Keyboard shortcuts; 51  
Keylogger; 176

## L

Label; 135  
Log entries; 99, 111  
Log entry fields; 109  
Log Explorer; 24, 25, 99, 101, 104  
    Force latest log; 124  
    Limitations; 102  
Log system; 172  
LPT/Parallel ports; 16

## M

Machine-Specific Settings; 71  
Managing specific computers; 39  
MAP; 206  
MDAC; 206  
Media  
    By user; 140  
    Label; 135  
    Label column; 131  
    Media Authorizer; 24, 25, 129, 132, 133, 138, 146, 150  
    Media Description; 135  
    Media-inserted; 120  
Microsoft Certificate Authority; 129, 133  
Modem; 16  
Monitoring  
    Administrators; 99, 100, 126  
    Devices; 99  
MSDE; 206  
Multiple permissions; 86

## N

Navigation/Control bar; 105  
NDAP; 206  
NDS; 206  
Negative permission; 48, 50, 69, 86, 146, 147, 148, 154, 207  
NIC; 207  
None; 48, 50, 51, 69, 86, 146, 147, 148  
Novell support; 13

## O

Offline updates; 14  
Omnibook; 201  
Online/Offline permissions; 80  
Options; 30, 169, 170  
    Centralized device control log; 169  
    Certificate generation; 171  
    Change; 171  
    Changes; 169  
    Client hardening; 172  
    Device control status window; 169

Device log; 169, 172  
Device log throttling; 169, 173  
eDirectory translation; 169, 173  
Encrypted media export password; 169  
Encrypted media key export; 169  
Encrypted media password; 169, 173  
Endpoint; 169  
Individual options; 171  
Log upload delay; 169, 174  
Log upload interval; 169, 174  
Log upload threshold; 169, 174  
Log upload time; 169, 174  
Offline/Online state detection; 169, 174  
Sanctuary status; 174  
SecureWave Application Server address; 169  
Server address; 169, 175  
Shadow directory; 176  
Shadow file upload delay; 169  
Suppress recurring log events; 169  
Update notification; 176  
USB Keylogger; 176  
Organizational Units; 33  
OU; 207  
Out of band permissions; 76

## P

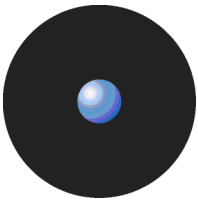
Palm Handheld Devices; 17  
Passphrase; 146, 167  
Password recovery; 143  
PCMCIA; 13, 17  
Per-device  
    Encryption; 14  
    Permissions; 14, 95  
Permissions; 68, 71  
    Dialog; 57  
    Monitoring changes; 99, 100, 126  
    None; 207  
    Online/Offline; 80  
    Priority; 69, 146  
    Send to client; 34  
    Temporary; 75  
    Temporary offline; 76  
    Types; 39  
Plug & Play; 17, 132  
Poor performance; 201  
Pre-defined device classes; 36  
Private Key; 207  
PS/2  
    Ports; 17, 201  
Public Key; 207  
Purge Online Table; 26

## Q

Queries  
    Complex; 116  
    Simple; 114  
Quick Format (insecure for existing data); 129, 138, 142

## R

Read denied; 120  
Read-only; 13  
Recover password; 144, 165



- Removable; 17, 132
  - Storage devices; 17
- Remove
  - Copy limit; 86
  - DVD/CD/Encrypted Media; 140, 141
  - DVD/CDs; 141
  - Encrypted media; 141
  - Offline and online permissions; 81
  - Permissions to DVD/CD/Encrypted Media; 139, 140
  - Scheduled permissions; 75
  - Shadow; 84
  - Temporary permissions; 76
- Reports; 102, 179, 201
  - Computer permissions; 28, 182
  - Device permissions; 28, 181
  - Machine options; 29, 188, 189
  - Media by user; 28
  - Media by user; 183
  - Menu; 28, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189
  - Online machines; 29, 187
  - Shadowing by device; 29, 185
  - Shadowing by user; 29, 186
  - User options; 29
  - User permissions; 28, 180
  - Users by medium; 28, 184
- RIM BlackBerry handhelds; 17
- Root-level permissions; 67
- RPC; 207
- RSA; 122
  - Definition; 207
- S**
- SADEC; 149, 158
- Salt; 27
- Sanctuary Device Control
  - Advantages; 12
  - Controlling your environment; 11
  - Description; 11
  - Features; 12
  - Introduction; 11
- Sanctuary Management Console
  - Connection window; 21, 22
  - Control panel; 21
  - Main window*; 21
  - Menu; 21
  - Modules; 24
  - Screen; 21
  - Status bar; 21
- Sanctuary status; 174
- Sanctuary Volume Browser; 160
- SAO; 207
- Scanners; 201
- Scheduled custom reports; 118
- Scheduled permissions; 13, 36, 73, 74
- Secondary hard disks; 17
- Secondary hard drives; 132
- Secondary network access devices; 16
- SecureWave Application Server; 25, 207
- SecureWave Application Server address; 169
- Send updates; 96
  - To a specific computer; 26
  - To all computers; 26, 69, 72, 73, 74, 81, 84, 94, 96, 170, 171
- SHA-1; 207
- Shadow
  - Bad directory; 122
  - Bad public key; 122
  - CD R malfunction; 122
  - CD R mode unsupported; 122
  - File malfunction; 122
  - Files; 100
- Shadow file upload delay; 169
- Shadowing; 99, 109
  - a device; 83
  - Devices; 82
  - File Name; 124
- Show all members; 52
- Show/hide columns; 107
- SID; 110
- Smart Card readers; 17
- Sorting results; 106
- Specifically deny access; 50, 69, 146, 147, 148, 154, 207
- SQL Server; 206, 207
- Supported devices; 16
  - Types; 56
- Supported DVD/CD burning software; 200
- Suppress recurring log events; 169
- SVolBro.exe; 160
- Synchronize Domain; 26, 27, 30, 31, 35, 47
- Synchronizing
  - Novell eDirectory; 31
- T**
- TAO; 207
- Tape drives; 18
- Target; 110
- TCP/IP; 208
- Technical support; 8
- Templates; 102, 116
  - Adding; 103
  - Columns; 109
  - Filtering; 112
  - Queries; 114
  - Select and edit templates; 111
  - Settings; 113
  - Using; 103
- Temporary
  - Access; 13
  - Permissions; 75, 176
  - Permissions offline; 76
- Ticket; 28
- Time zones; 201
- Tools menu; 26, 97
- Traced; 110
- Traced on; 122
- Transferred on; 122
- U**
- Unable to communicate with WLD driver; 132
- Unauthorized Encrypted Media; 153, 154, 155, 156
- Unique devices; 14, 37
- Unlock medium; 144, 155, 158
- Unsuccessful attempts to access devices; 99





USB; 16  
    Printer support; 17  
User  
    Access; 26, 32  
    defined classes; 36  
    Defined devices; 13, 18, 92  
User names; 110

**V**

**VBScript**; 208  
View menu; 26  
Viewing  
    Access attempts to devices; 120  
    Client error reports; 122  
    Shadow files; 122

**W**

Well-Known Security Identifiers; 208  
Window menu; 30  
Windows CE handheld devices; 18  
Windows Management Instrumentation; 208  
Windows NT4; 206  
Windows Script Host; 208  
Wireless NICs; 18  
WMI; 208  
Workgroup; 133  
    Computers; 31  
Write denied; 121  
WScript.exe; 208  
WSH; 208

**Z**

ZENworks; 208