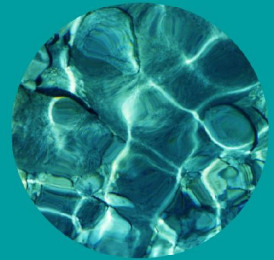




SecureWave
Sanctuary[®]
Device Control



Administrator's Guide

Liability Notice

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

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

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

SecureWave claims copyright in this program and documentation as an unpublished work, revisions of which were first licensed on the date indicated in the foregoing notice.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

Copyright 2000–2006© SecureWave S. A.
All rights reserved.

Trademarks

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

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

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

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

You can contact our technical support team by calling:

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

or by sending an email to support@securewave.com

Published on: October 2006

Sanctuary Device Control – Version v4.0.0



Contents

About this guide	9
Introduction	9
A complete portfolio of security solutions	9
What do you find in this guide	11
For more information	12
Conventions used in this guide	13
Notational conventions	13
Typographic conventions	13
Keyboard conventions	13
To contact us	14
1 st Part – Step by step guide to administrate your installation	15
Chapter 1: Introducing Sanctuary Device Control	17
Welcome to Sanctuary Device Control	17
What is Sanctuary Device Control	17
What can you do with Sanctuary Device Control	18
What do you gain using Sanctuary Device Control	19
Overview of system architecture and connectivity	20
The SecureWave Sanctuary Database	21
The SecureWave Application Server	21
Administration Tools	21
The Sanctuary Management Console	22
The Key Pair Generator	22
The SXDomain command-line tool	23
The Sanctuary Client	23
How does the Sanctuary Device Control solution works	23
What happens when a user uses his computer?	25
What happens if a computer is taken off the network?	26
Major features	27
Device types supported	31
Conclusions	34
Chapter 2: Knowing your Way Around: the Administrator's Console	35
Novelties & changes from previous versions	36
Starting up Sanctuary Management Console	37
Connecting to the Server	37
Log in as a different user	38
The Sanctuary Device Control screen	39
Controlling your workspace	40
Sanctuary modules, menus and tools	42
The four control modules	43
The Audit Logs Viewer	43
The Device Explorer	44



- The Log Explorer45
- The Media Authorizer45
- The File menu46
- The View menu47
- The Window menu47
- The Tools menu48
- Endpoint Maintenance.....49
 - Client ticket rules49
 - To create and save maintenance "tickets" for endpoint machines/users50
- The Reports menu 51
- The Explorer menu 52
- The Help menu..... 53
- Other administrative functions..... 53
 - Setting and changing options 53
 - Synchronizing domain members 54
 - Adding workgroup computers54
 - Performing database maintenance 56
 - Defining the Sanctuary Device Control administrators 57
 - Sending updated permissions to client computers 61
- Everyday work..... 61
 - Identifying and organizing users and user groups 61
 - Identifying the devices to be managed 62
 - Working with the Sanctuary system's pre-defined device classes 63
 - Adding your own, user-defined devices to the system..... 64
 - Identifying specific, unique, removable devices64
 - Organizing devices into logical groups66
 - Identifying specific computers to be managed 67
 - Defining different types or permissions.....67
 - Encrypting removable media & authorizing specific DVDs/CDs70
 - Forcing users to encrypt removable media 70
- Practical setup examples71
 - DVD/CD burner permissions assignments.....71
 - Removable permissions assignments.....72
 - Assigning permissions to groups instead of users 72
 - Shadowing notes..... 73
- 2nd Part: The modules and functions in detail..... 74
- Chapter 3: Using the Device Explorer 75
 - Introduction 76
 - How does the Device Explorer works? 77
 - Restricted and not restricted devices 78
 - Optimizing the way you use Device Explorer 80
 - Context menu and drag & drop..... 80
 - Keyboard shortcuts 81
 - Adding comments to an entry..... 82
 - Computer groups 82
 - Renaming Computer Groups/Device Groups/Devices..... 82
 - Show All Members..... 83
 - Event notification84
 - To create an Event Notification84
 - To delete an Event Notification..... 86



- To modify an Event Notification 86
- Some practical examples 86
- Device Groups 87
 - To add a device group 87
- Supported devices types 88
- Managing permissions 92
- Chapter 4: Managing permissions/rules 93**
 - Using the permissions dialog 93
 - Special case: working with the Removable Storage Devices class 96
 - Examples 97
 - Using file filters 98
 - File Filtering examples 102
 - To assign default permissions 106
 - Root-level permissions 106
 - Where can you apply default permissions? 106
 - How do you assign default permissions to a node? 107
 - To assign default permissions to users and groups 107
 - Default Permission priority 110
 - Read/Write permissions 112
 - To assign computer-specific permissions to users and groups 112
 - To modify permissions 115
 - To remove permissions 116
 - To assign scheduled permissions to users and groups 116
 - To modify scheduled permissions 119
 - To remove scheduled permissions 119
 - To assign temporary permissions to users 120
 - To remove temporary permissions 122
 - To assign online and offline permissions 123
 - To remove offline or online permissions 125
 - To export and import permission settings 125
 - Shadowing devices 126
 - To shadow a device 127
 - To remove the shadow 129
 - Copy limit 130
 - To add a copy limit 130
 - To remove a copy limit 132
 - Applying multiple permissions to the same user 132
 - Forcing users to encrypt removable storage devices 134
 - To define permissions that force users to encrypt removable storage devices 135
 - To force decentralized encryption 135
 - Concrete examples 137
 - Managing devices 141
 - To add a new device 142
 - To remove a device 145
 - Specific, unique, removable devices 145
 - Changing permissions mode 146
 - Priority options when defining permissions 147
 - Informing client computers of changes 148
- Chapter 5: Using the Log Explorer 151**
 - Introduction 151



- Basic operation155
 - To use an already defined template155
 - Managing templates.....155
 - What is a template155
 - To create a template155
 - To delete, save with another name, rename, import, and export a template ..156
- The Log Explorer window in detail 157
 - Navigation/Control bar157
 - Column Headers158
 - The Settings dialog159
 - Results window164
 - Criteria/Properties panel164
 - Control buttons panel164
 - Sorting and applying criteria to specific fields164
- Available columns165
- Viewing access attempts to devices167
- Viewing client error reports170
- Viewing Shadowed files.....171
- Shadowing file names only173
- DVD/CD Shadowing173
- Forcing an upload of the latest log files173
 - To force the immediate retrieval of the latest logs from any client173
- Saving application execution logs to a CSV (comma-separated values) file.....174

Chapter 6: Using the Audit Logs Viewer 175

- To view system administrator activity176
- Search options176
- Actions178

Chapter 7: Using the Media Authorizer183

- Introduction183
- Authorizing users to use specific DVDs/CDs.....186
 - Pre-requisites186
 - To authorize the use of a specific DVD/CD186
- Encrypting removable storage devices187
 - Introduction187
 - Pre-requisites188
 - Decentralized encryption189
 - Limitations.....189
 - To encrypt a specific removable storage device190
 - Removable device encryption methods comparison193
 - Possible error messages when encrypting a device194
- Authorizing access197
 - Selecting users for a device197
 - To grant access to use DVDs/CDs/encrypted removable media197
 - To deny access to DVDs/CDs/encrypted removable media199
 - Selecting devices for a user200
 - To grant access to use DVDs/CDs/encrypted removable media200
 - To deny access to DVDs/CDs/encrypted removable media201
- Removing media from the database.....202
 - To remove a DVD/CD202
 - To remove an encrypted removable storage device202



- To remove lost or damaged media from the database203
- More utilities 204
 - To rename a DVD/CD/removable storage device 204
 - Exporting encryption keys.....205
 - Ejecting a CD or DVD 206
- Permissions Priority..... 206
- Encrypting devices without having a Certificate Authority installed 209
 - To encrypt a removable media without installing a Certificate Authority:..... 209

Chapter 8: Accessing encrypted media outside of your organization 211

- Exporting encryption keys.....211
 - Exporting encryption keys centrally (by the administrator)211
 - Exporting encryption keys locally (by the user) 212
 - To export the encryption key to a file 213
 - To export the encryption key to the device itself 215
- Scenarios for accessing encrypted media from outside your organization..... 216
 - Accessing media on a machine that has Sanctuary Client installed 216
 - Centrally managed access to unauthorized encrypted media.....217
 - Locally managed access to 'unauthorized encrypted media' 218
 - Differences between locally and centrally managed access to Unauthorized Encrypted Media..... 221
 - Accessing media in a machine that does not has the Sanctuary Client installed.. 223
 - Sanctuary Device Control Stand-Alone Decryption Tool.....224
 - Easy Exchange.....226
 - Using encryption within and outside your organization230
- Decentralized encryption.....231
 - How to configure Sanctuary so that users can encrypt their own devices 232

Chapter 9: Setting and changing options 233

- Changes from previous versions234
- Default options 234
- Computer-specific options.....235
- To change an option setting.....236
 - Sending updates to client computers 236
- Individual option settings..... 237
 - Certificate generation 237
 - Client hardening 237
 - Device log..... 238
 - Device log throttling..... 238
 - Encrypted media password 239
 - Log upload threshold 239
 - Log upload delay..... 239
 - Log upload interval 240
 - Log upload time 240
 - Sanctuary status..... 240
 - Server address 241
 - Shadow directory 241
 - Update notification 241
 - USB Keylogger..... 242
- Checking settings on a client machine 243



Chapter 10: Reports	245
User Permissions report.....	247
Device Permissions report.....	248
Computer Permissions report.....	250
Media by User report.....	251
Users by Medium report.....	252
Shadowing by Device report.....	254
Shadowing by User report.....	255
Online Machines report.....	256
Machine Options report.....	258
Chapter 11: Using Sanctuary Device Control on a Novell network	259
What components are required?.....	259
How does the Novell interface works?.....	259
Synchronization Script parameters.....	260
How to use the Synchronization Script for Novell.....	261
Script examples.....	262
What can go wrong and how do I fix it?.....	262
3rd Part: Useful additional information	265
Appendix A: DVD/CD Shadowing	267
Introduction.....	267
Operation of the Sanctuary Client.....	267
Disk space requirements.....	268
Supported formats when shadowing.....	268
Handling of unsupported shadowing formats.....	269
CD image analysis.....	270
Files.....	270
Logs.....	270
Saved image.....	270
Sample analysis log.....	271
Supported and unsupported CD formats.....	273
Summary.....	273
Supported data block formats and recording modes.....	273
Supported and unsupported file system features.....	274
Supported DVD/CD burning software.....	278
Appendix B: Installing a Certificate Authority for Encryption	279
Requirements.....	279
Active Directory.....	279
Integrate DNS with Active Directory.....	279
Installing the Certificate Services.....	280
Checking that certificates are correctly issued to the users.....	284



Appendix C: Important Notes..... 287

Appendix D: Controlling administrative rights for Sanctuary's administrators 293

 VBScript Tools..... 293

 Ctrlacx.vbs 293

 Introduction..... 293

 Requirements 294

 Usage 294

 Examples..... 295

 What to do after running the script..... 295

Glossary 299

Index of Figures..... 305

Index of Tables 311

Index 313



About this guide

Introduction

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

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

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

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

A complete portfolio of security solutions

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

- > Sanctuary Standard Edition enables you to define a group of files that can be run on the organization's computers. Nothing else will run
- > Sanctuary Custom Edition lets you create multiple File Groups and User Groups, so you can control application execution at any level of granularity
- > Sanctuary Terminal Services Edition extends application control to Citrix or Microsoft Terminal Services environments, which share applications among multiple users
- > Sanctuary Server Edition extends application control to protect the organization's servers, such as its Web-hosting server, email server, file servers, database servers, etc.



- > Sanctuary Device Control – described in this Administrator's Guide – prevents unauthorized transfer of data by controlling access to input/output devices, such as memory sticks, modems, and PDAs



What do you find in this guide

This guide explains how to use the Sanctuary Device Control to restrict and manage data copied to physical devices on your computer.

We have divided this manual in three distinctive sections.

In the first part, you will find a general introduction to the program. You can find detailed information on part two (chapters 3 through 11). This is a must read part:

- > *Chapter 1: Introducing Sanctuary Device Control* provides a high-level overview of the solution, how it works and how it benefits your organization
- > *Chapter 2: Knowing your Way Around: the Administrator's Console* describes the basic principles of how to use Sanctuary Device Control

The second part of the manual, the reference part, explains in detail all Sanctuary Device Control modules and functionality.

- > *Chapter 3: Using the Device Explorer* explains how to set the Access Control List permissions on I/O devices
- > *Chapter 4: Managing permissions* shows you how to administrate – create, delete, modify, organize, group – permissions and rules and force a user to encrypt removable storage devices
- > *Chapter 5: Using the Log Explorer* provides information on how to view a copy of traced files, errors, and access attempts on client computers
- > *Chapter 6: Using the Audit Logs Viewer* explains how to view administrative logs and copies of files ('shadow files') users have written/read to/from certain devices
- > *Chapter 7: 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 8: Accessing encrypted media outside of your organization* explains how to use encrypted media outside the company
- > *Chapter 9: Setting and changing options* describes how to tailor the Default and Computer-specific options to suit you and your organization
- > *Chapter 10: Reports* explains how to obtain the various HTML reports generated by Sanctuary Device Control



- > *Chapter 11: Using Sanctuary Device Control on a Novell network* introduces the use of Sanctuary Device Control on a eDirectory structure

In the third and last part, you can find extra material that will help you in your everyday work. There is also a handy glossary and index section.

- > *Appendix A: DVD/CD Shadowing* describes the operation of copying 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
- > *Appendix B: Installing a Certificate Authority for Encryption* describes how to install a Microsoft Certificate Authority
- > *Appendix C: Important Notes* shows some key comments you should take into account when working with the program
- > *Appendix D: Controlling administrative rights for Sanctuary's administrators* shows you how to set and control the rights to administrate Organizational Units/Users/Computers/Groups
- > The *Glossary* provides definitions of standard concepts used throughout the guide
- > The several indexes (*Index of Figures*, *Index of Tables*, *Index*) provides 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:

<http://www.securewave.com>

This regularly updated Web site provides you with:

- > The latest software upgrades and patches
- > Troubleshooting tips and answers to FAQ
- > Other general support material that you may find useful
- > New information about Sanctuary Device Control



Conventions used in this guide

Notational conventions

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



Special note. This symbol indicates further information about the topic you are working on. These may relate to other parts of the system or points that need particular attention.



Time. Used in a paragraph describing a 'short-cut' or tip that may save you time.



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

Typographic conventions

The following typefaces are used throughout this guide:

- > This typeface (*italic*) is used to represent fields, menu commands, and cross-references
- > This typeface (`fixed width`) is used to represent messages or commands typed at a command prompt
- > This typeface (`SMALL CAPS`) is used to represent 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 USA.

You can contact our technical support team by calling:

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

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

Alternatively, you can write to customer support at:

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

1st Part – Step by step guide to administrate your installation



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. You will also find here an overview of the whole system and an explanation of the inner works of the program.

Welcome to Sanctuary Device Control

Sanctuary Device Control eliminates the majority of dangers associated with insiders 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 drain & electronic theft of intellectual property and proprietary information.

On the other hand, Sanctuary Device Control also hinders the introduction of malicious code, unlicensed software, and other counterproductive applications that promote inappropriate use of corporate resources and create unnecessary expenses.

In this way, 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 devices by applying an Access Control List (ACL) to each device type. Access to any device is prohibited by default for all users. The designed administrators then assign access and permissions to specific users or groups of users for those devices that they require in their everyday work. You are in control, always. These permissions can be temporary, online/offline, scheduled, copy limit, shadow (a copy of transferred data), read, read/write, etc.

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* say the word.

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.

Using Sanctuary Device Control you can:

- > Define user/group based permissions
- > Define user/group permissions on all/specific machines
- > Prevent the installation of unknown devices
- > Authorize only specific device types within a class
- > Uniquely identify one specific device
- > Scheduled 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 rules (a copy of transferred data) for all data written/read to/from external devices or specific ports (file names only or full copy of transferred files)
- > 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 25.

What do you gain using Sanctuary Device Control

When first using Sanctuary Device Control you immediately gain:

- > A strict user policy enforcement: 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: a panoply of useful information to keep everything under the strictest control
- > 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
- > A complete event notification when a user attempts to access an unauthorized device
- > Limit or hinder copied data: you have the choice between establishing a daily limit or simply impeding data to be 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



Overview of system architecture and connectivity

The Sanctuary Device Control solution features four main components:

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

The following image shows this relation:

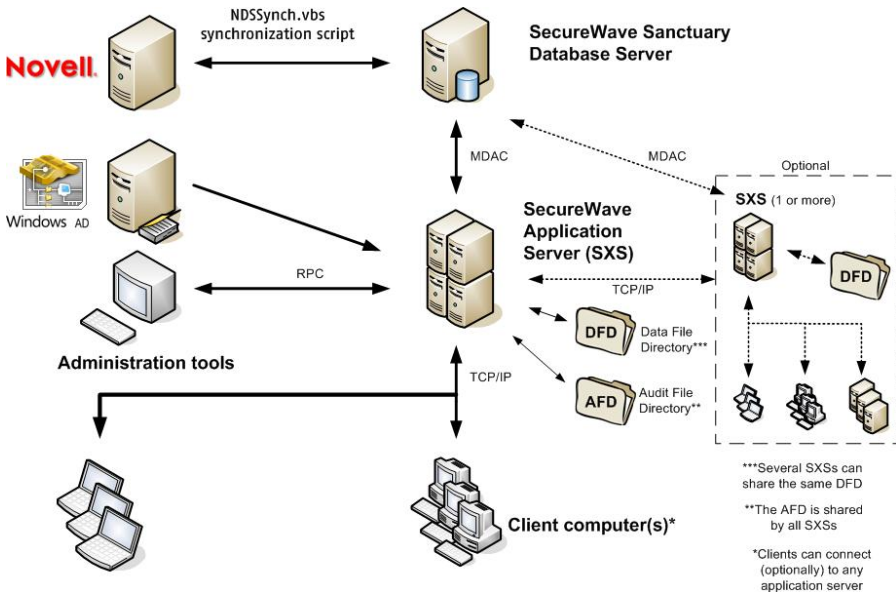


Figure 1: SecureWave Device Control components



The SecureWave Sanctuary Database

Each Sanctuary Device Control site must have one database. This is the master storage point for the user policies and permissions.

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

The SecureWave Application Server

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

The SecureWave Application Server is a Windows Service and runs under an account capable of reading Domain users/groups/computers accounts from the Domain Controller.

The application server is used to:

- > Get the latest information about device I/O permissions from the database and store it in its cache
- > Sign, compress, and pass this permissions information to client computers, where it is also stored locally
- > Save a log of administrators and, optionally, users actions.

Administration Tools

Administrators use the Sanctuary Management Console (part of the Administration tools on *Figure 1*) to configure the software and carry out a range of day-to-day administrative tasks. These include managing the I/O device access policies, auditing, generating the device and user reports, encrypting, and authorizing media.

Among these administration tools you have:

- > The Sanctuary Management Console – or SMC. Described in this guide
- > The Key Pair Generation. See a complete description in the *Setup Guide*



- > The *SXDomain* command-line tool. See a complete description in the *Setup Guide*
- > The *Client Deployment Tool*: to install the Sanctuary Client in your protected computers & servers. It uses standard MSI technology and can also be used to find out which computers already have the client and its status. See a complete description in the *Setup Guide*

The Sanctuary Management Console

The Sanctuary Device Management Console is used to configure Sanctuary Device Control and to perform day-to-day administrative functions. These include:

- > Managing access to I/O devices
- > Authorizing specific DVDs/CDs to be used in DVD/CD drives
- > Encrypting removable media
- > Granting users' permission to use specific authorized DVDs/CDs or encrypted media
- > Use the Sanctuary Device Control to configure the options that modify the way the client computers operate
- > Viewing lists of files transferred using authorized I/O
- > Viewing the content of files transferred using authorized I/O
- > Viewing the attempts to access or connect to unauthorized devices

The Sanctuary Management Console may be installed on several computers if required.

The Key Pair Generator

The Key Pair Generator is used to create a unique set of private and public keys. The SecureWave Application Server is authenticated when communicating with the Sanctuary Client driver. See a complete description in the *Setup Guide*.



You should always generate your own set of keys before deploying the product in a working environment.



The SXDomain command-line tool

The SXDomain command-line tool is used to store in the database the changes done to the domains, users, groups, and workstations within your network. See a complete description in the *Setup Guide*.

The Sanctuary Client

The Sanctuary Client, installed on the client machines, ensures that only those I/O devices that the user has been authorized to use can be accessed on the computer. Any attempt to access an unauthorized device is barred, regardless of the computer the user logs on to.

End-users cannot interact with the Sanctuary Client, except to receive notifications when their permissions changes or to update them using the *Refresh Settings* command of the system tray icon. The user cannot change in any way its settings or permissions.

The administrator can also ask the user to show the "salt" value used to do endpoint maintenance when the computer is not connected to the network and this value cannot be obtained by alternative methods. See *Endpoint Maintenance* on page 49 for more details.

The client is installed on each computer you want to control. The setup also installs an application that provides (optionally) device status information to the end-user.

How does the Sanctuary Device Control solution works

When first installing Sanctuary Device Control, default permission rules are created and configured with their default settings. Besides that, devices are automatically assigned to predefined device classes according to Windows classification. The predefined permissions include Copy Limit restrictions and Read/Write permissions for some of the devices.

Even though some users may already be satisfied with these settings, the majority will prefer to change them accordingly to reflect the device policy they want to attain. One of the first tasks of an administrator will be to change and define new permissions for users, groups, computers, or devices in their network.

Administrators can also manage specific devices by type or brand if needed. They just needs to assign rights and attributes by device class, specific device, or specific media to user(s) / user group(s) or to a specific computer.



You do not have to worry about adding new permissions every time an unknown device is connected to a computer in your network. Most devices are declared in one of the Sanctuary Device Control predefined classes during the plug and play discovery phase. Sanctuary Device Control will apply existing device class permissions to the device. If a device is unknown and does not belong to a predefined device class, the most restrictive permission rule is applied and the access is denied until specifically told otherwise. These permissions can even be extended to a specific model installed on a precise computer.

Every time a user wants to access a device, the Sanctuary Device Control driver intercepts the Operating System request at the kernel level. If the device is not in the list of authorized classes and/or specific devices, Sanctuary Device Control will deny its use. If the device is known (e.g., it is in the device class list), the driver checks the user rights in the Access Control List (ACL). In this case, if a user has the right to access a device (for instance a CD burner drive), either Read or Read/Write access is granted. If a user does not have rights on the device, an 'access denied' notification pops up to inform the user – the administrator can optionally define custom messages. The program can log this action, optionally, for the Administrators to analyze.

The following schema summarizes these steps:

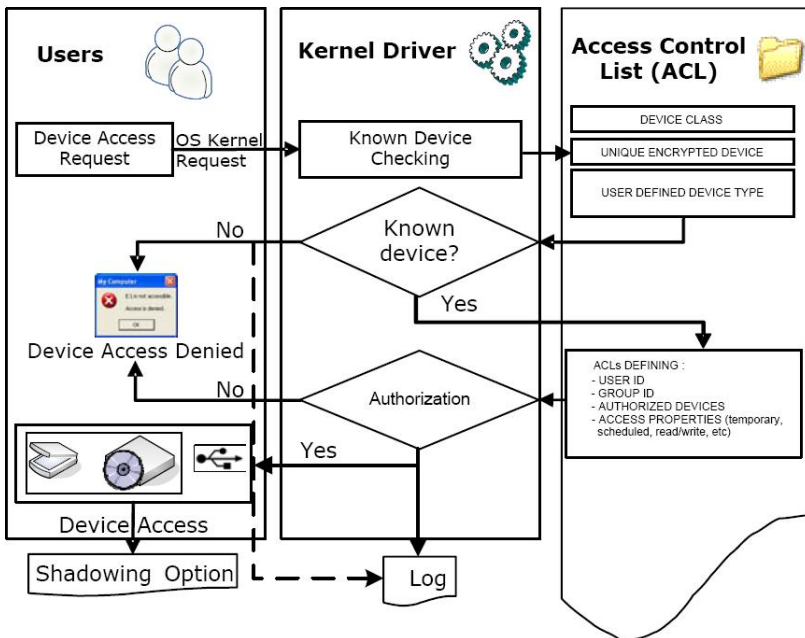


Figure 2: Client driver – internal works



Communication between the Sanctuary Management Console and the Application Server is set to RPC (Remote Procedure Call) level 6. The messages interchanged between them are fully encrypted.

The Sanctuary Management Console connects to the Application Server to carry out administrative changes. Therefore, at no time does the Sanctuary Management Console connect directly to the Database. All communication with the Database is through and by the Application Server(s).

Traffic between the Client and Application Server is authenticated based on Private/Public key technology.

What happens when a user uses his computer?

All computers equipped with the *Sanctuary Client* receive an administrator created permissions list of those known devices reported by the *Console*. Forwarded by the *SecureWave Application Server* to the machine, this permissions list is delivered in several possible ways depending on whether the computer is or not connected to the network:

<i>Network connection</i>	<i>Permission updates are done:</i>
Not available	By importing them from a file
	Are kept internally on the computer's memory
Available	When the user logs in
	When the user asks for them using the client's tray icon (using the <i>Refresh settings</i> item)
	When the administrator makes changes and explicitly sends them to a specific computer or all on-line machines
	If another user logs in
	Every 60 minutes
	When communication starts between the Application Server and the client Before triggering a shadow file transfer (please see <i>Shadowing devices</i> on page 126 for a complete explanation)

Table 1: Permissions list updates depending on network connection status

The *SecureWave Application Server*, in turn, communicates with the *Database* to retrieve the whole list – only when its cache is empty. The *SecureWave Application Server* then cryptographically signs the list, compresses it, select only those parts that have changed, and forward it to the *client computer*.



The process is summarized in the following diagram.

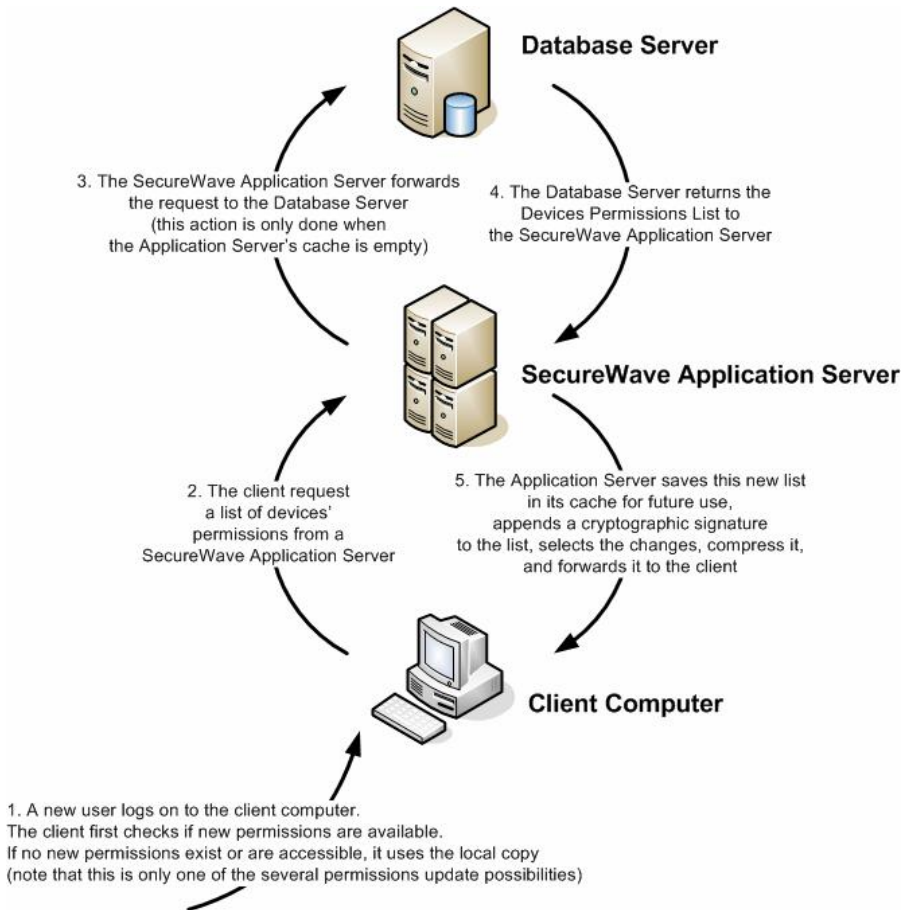


Figure 3: Obtaining a List of Accessible Devices

What happens if a computer is taken off the network?

Sanctuary Device Control protects all computers, at all times, using the Sanctuary Client. Whenever a computer is disconnected from the network, it is still protected by the permissions that were downloaded from the Sanctuary system when it was last connected. This could be the case with laptop computers. The computer



simply accesses its local copy until it is reconnected to the network and able to receive automatic updates once again. You can create 'online' and 'offline' permissions for any computer or device on your network, to be applied automatically, as appropriate. There is no problem if users try to delete or tamper the list: they would not have access at all.

Major features

Designed for large organizations with complex needs, Sanctuary Device Control 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.

Novell support

Full support to Novell's eDirectory/NDS structure. The Novell's eDirectory trees are synchronized using an external script. These objects will appear on the Device Explorer structure so that permissions and rules can be assigned to them explicitly. The administrator can schedule this script using Windows's scheduler task manager. You can see an example in the Setup Guide.

Intuitive user interface

Device access is controlled by means of a native Access Control List, exactly the same way as when navigating through files and folders. Permissions can apply at different levels: users, user groups, all machines, machine groups, specific machines, groups of devices, or even specific devices.

Native support for Plug & Play devices

All types of buses, such as PCMCIA (or Cardbus), FireWire and USB are supported and all Plug and Play devices are detected and policies enforced.

Read-only access

Sanctuary Device Control makes it possible to set the access to a particular device to be read-only. This option is valid for all file-system based devices such as the floppy drive, DVD/CD writer, PCMCIA hard drives, etc.



Copy limit

Afraid of letting your users abuse their writing permissions? Limit the quantity of data they can write to each device on a per-day basis.

Scheduled access

Scheduled device access lets you grant or deny permissions to use a device during a specific period. You can use this feature to develop sophisticated security policies where certain devices can only be used from, for example, 9 am to 5 pm, Monday to Friday.

Temporary access

Grant users with a temporary access to their devices. This feature lets you 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.

Context-sensitive permissions

Different permissions can be applied depending on the context. 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.

Offline updates

It is possible to 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.

File shadowing

Sanctuary Device Control's patent pending 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.



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 or group of users also incorporates an encryption process to ensure that sensitive data is not inadvertently exposed to those without authorized access.

Centralized and/or decentralized encryption

Not only can administrators 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 3 or later) and later only. Windows NT4 is no longer supported by Sanctuary Device Control.



Enhanced infrared control

Infrared ports offer, through IrDA (Infrared Data Association), an extremely easy way to connect peripherals or other computers to a PC; it will even supply a network interface, completely bypassing any access restrictions defined in a regular corporate network. Sanctuary Device Control allows disabling infrared ports through permissions.

Wireless network interface cards

When installing the Sanctuary Client, 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.

USB printer support

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

Bluetooth Radio Devices

Bluetooth, a very popular standard in the mobile phone and PDA world, offers an extremely easy way to connect peripherals to a PC. It completely bypasses any access restrictions defined in a regular corporate network. Sanctuary Device Control now allows disabling Bluetooth through a simple permission definition.

PS/2 ports

PS/2, the standard port to connect a keyboard, is being rapidly superseded by the USB port. You will probably like to limit permissions if you only use USB keyboards or if you suspect the use of a hardware Keylogger™. This device 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. The USB version of the Keylogger is also blocked, either as a general option or as a computer specific one. Please consult *Chapter 9: Setting and changing options* on page 233 for more information.

Administrators' roles

The 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 *Appendix D: Controlling administrative rights for Sanctuary's administrators* on page 293 to learn how to set rights to control Organizational Units/Users/Computers/Groups.

Tamper-proof client component

Sanctuary Device Control depends on the installed client to do its work. Since this is a critical part of the installation, the client is protected against uninstalling – even for authorized administrators. Sanctuary Administrators may emit an "endpoint maintenance ticket" (see *Client hardening* on page 237 and *Endpoint Maintenance* on page 49) or explicitly deactivate this protection.

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.

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.

Bluetooth radio devices

The Bluetooth standard offers an extremely easy way to connect peripherals and other devices to a PC. You can control permissions to these devices quickly and easily. See *Chapter 3: Using the Device Explorer* on page 75 for more information.

COM/Serial ports and LPT/Parallel ports

By securing the serial and parallel ports, Sanctuary Device Control is able to control whether the user can use devices such as printers, modems and PDAs attached to these types of ports.

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.

Imaging devices

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.

Infrared ports (IrDA)

Keyboards and mice are examples of devices that you can connect using an infrared port, but also are printers, personal digital assistants, and even computers. You can control these devices with a simple permission that enables or disables them (user/user group/device/class/computer and combinations).

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 (ex. ISDN).

Palm handheld devices

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

Printers (USB)

Access to USB printers connected to the computer can be controlled with Sanctuary Device Control.

PS/2 Ports

If you are only using USB keyboards and USB mice in your network, you can opt to block definitely all PS/2 ports.

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 Disk on Key, memory stick, ZIP, as well as USB-connected MP3 players and digital cameras.



RIM BlackBerry handhelds

Access to these PDA/GSM devices can be managed with Sanctuary Device Control.

Scanners

Access to these devices can be managed with Sanctuary Device Control whether they are USB or SCSI.

Smart Card readers

Access to these devices 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.

Unauthorized encrypted media

This category of devices represents devices that have been encrypted by Sanctuary Device Control in a separated environment. A user receiving permission for this class of devices will be able to access devices that were encrypted by Sanctuary Device Control in another organization.

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).

Wireless NICs (network interface controllers)

You can enable or disable this kind of network adapter with one simple option in the Sanctuary Device Control. Please check the *Appendix C: Important Notes* on page 287 for a list of all the Wireless NICs that can be blocked.



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 mechanism, 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.

USB, FireWire, PCMCIA, ATA/IDE, SCSI, Bluetooth, and IrDA

Since USB, FireWire, PCMCIA, ATA/IDE, SCSI, Bluetooth, and IrDA are bus types, and not true ports, devices attached using these bus systems are 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, will be recognized as device type DVD/CD-ROM and will, therefore, be controlled using the same mechanism and settings as an internal DVD/CD-ROM drive.

Conclusions

Sanctuary Device Control eliminates the majority of the dangers associated with insiders abusing their access to network resources and mission critical information. It will significantly increase 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: Knowing your Way Around: the Administrator's Console

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

When you first install Sanctuary Device Control, default permission rules are created and configured with their default settings. These rules include Copy Limit restrictions and Read/Write permissions for some of the devices. Even though some users may already be satisfied with these settings, the majority will prefer to change them accordingly to reflect the device policy they want to attain. One of the first tasks of an administrator will be to change and define new permissions rules for users, groups, computers, or devices in their network.

Using the Sanctuary Management Console you can:

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



Novelties & changes from previous versions

New to this version we have:

<i>Category</i>	<i>Feature</i>
New design	The management console has been completely redesigned.
Unified Management Console	Each one of the programs that form our Sanctuary solution previously required an independent console component. We have designed a unified console component that now works with our entire software suite, depending on those modules that you have purchased.
Advanced administrative protection	More control of who can uninstall/modify the client driver.
Decentralized encryption	Users are now allowed/enforced to encrypt their own removable devices.
Differential updates	Instead of sending a complete permission list, the application server now sends only those permissions that changed.
Unified Logging	All our products now share the same log structure.
Upload and Storage Enhancements	<p>You can now have several 'data file directories' (DFD, see <i>Figure 1</i>) defined and spread over your network to be used by the SecureWave Application Server(s). The previous limitation of all servers using the same, single, shared, DFD has been removed. Now it is possible for each server to use its own, distinct, one. This improves performance in multi-server installations as each server can be configured to store its data files in a location that is physically closer, or reachable through a high-speed network connection. It also helps spread disk load, as each defined directory only contains part of the files.</p> <p>Note that:</p> <ul style="list-style-type: none"> - It is still possible for more than one server to use the same DFD - All servers can still access all data files; it does not matter if only one or multiple directories are used. When a server does not find a file in its defined directory, it requests a copy from a server having access to it. <p>There is also an extra, unique and common, Audit File Directory (AFD). This is the place where all audit and history files are stored.</p>
More client localizations	The client is now available in several other languages beside English, French, German, and Spanish.
Two way shadowing	"Shadowing" (a copy of data written by users) was previously only done on write operations. Now it may be done during read and/or write processes.
File filtering	Certain kind of permissions can now be set for specific file types.

Table 2: Novelties in this version

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

Starting up 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.

Type the name of the SXS Server you want to connect to, or select one from the list, and then click the OK button.



Figure 4: Connecting to the server

To connect to the server, follow these steps:

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

secsrv.secure.com[1234]



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



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

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

If the Sanctuary Management Console screen does not appear, an error message is displayed. This indicates that there were problems when all internal tests were carried out. Check that you have the required permissions to connect to that server, on domain rights and Sanctuary Management Console rights level. See *Defining the Sanctuary Device Control administrators* on page 57.

Log in as a different user

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

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

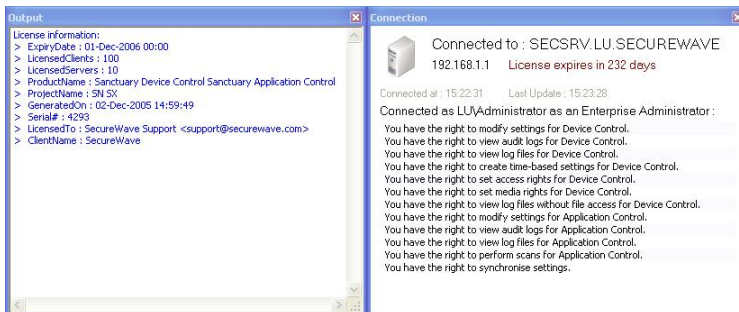


Figure 5: Connection / Output window

The Sanctuary Device Control screen

When you begin a Sanctuary Management Console session, the *Sanctuary Management Console* screen is displayed. This console adopts a Microsoft Outlook-style interface, which is easy to use and is one that most users are familiar with.

The following illustration identifies the various areas of the screen.

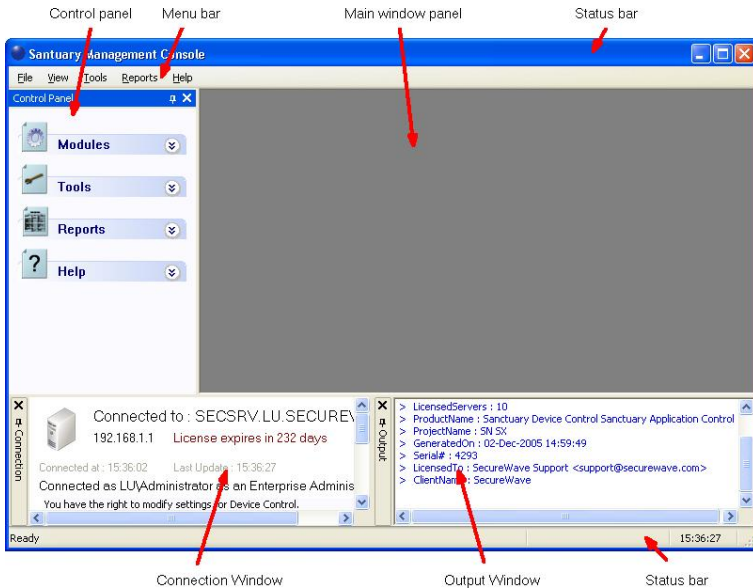


Figure 6: The Sanctuary Device Control screen

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

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

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



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

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

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

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



Figure 7: License status warning

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

Controlling your workspace

Use the Pin icon to "pin down" – Park (the icon changes to) – or "float" () the *Control Panel*, *Connection*, or *Output* window. In the *Dock* mode, the panel hides itself as a tab next to the program's window border leaving more space for the main window panel. In the *Floating* mode, the windows can be moved to any position in the screen, sharing the working area with whatever module is opened.



Figure 8: Docked Control Panel



Figure 9: Docked window

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

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

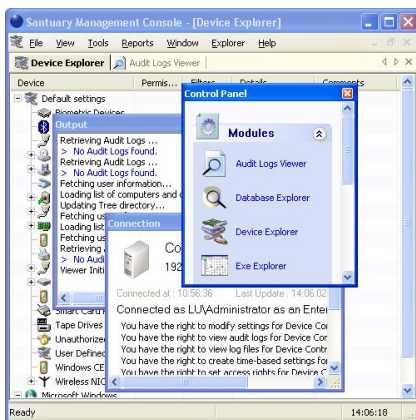


Figure 10: Floating Control Panel

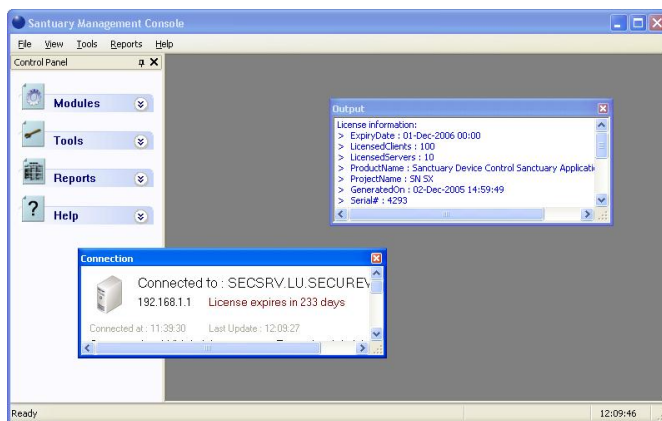


Figure 11: Floating windows

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

All open modules occupy the main window area and can be "floated" or "docked" at will. You can use the *Window* menu to arrange those opened module's windows in a tile, cascade, or iconize mode. Each window can also be close, maximize, or iconize independently as needed. If several modules are already open (as shown in *Figure 10*), 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.

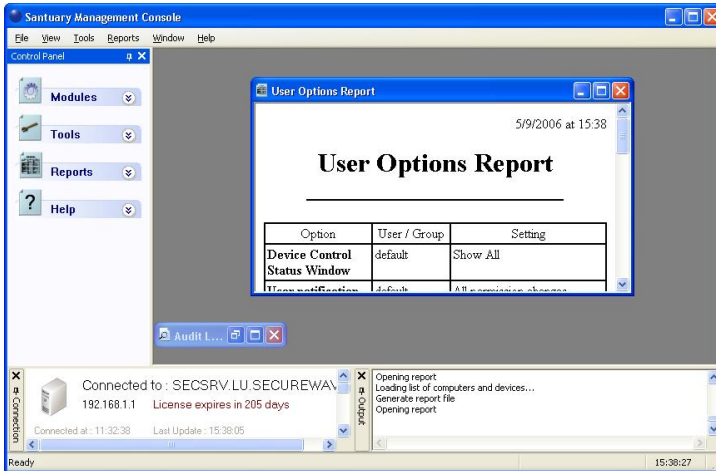


Figure 12: Minimized windows

Sanctuary modules, menus and tools

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

The four control modules

The Sanctuary Management Console consists of four control modules summarized in the following table:





<i>Module</i>	<i>Icon</i>	<i>Used to ...</i>	<i>In-depth description</i>
<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"> > View records of files copied from any PC to authorized I/O devices, and view the contents of the files themselves (two way "Shadowing") > View attempts to access or connect unauthorized devices 	<i>Chapter 5: Using the Log Explorer</i>
<i>Audit Logs Viewer</i>		View records of all operations made by Sanctuary's administrators.	<i>Chapter 6: Using the Audit Logs Viewer</i>
<i>Media Authorizer</i>		<ul style="list-style-type: none"> > 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 > Give permission to use specific DVD/CDs for users who have been barred from using the DVD/CD drive > Establish permission to use specific (encrypted) media > Centrally encrypt removable devices 	<i>Chapter 7: Using the Media Authorizer</i>

Table 3: The four available modules in the Sanctuary Device Control

You will find a brief description of each of the four modules in the next sections.

The Audit Logs Viewer

Sanctuary Device Control provides full auditing of all Administrator actions including changes of user and/or system access rights to certain devices. You will find the following information in the Audit Logs Viewer module:

- > Date and time of the change done
- > The Domain and User Name of the author of the change
- > The Domain and User Name or Group to who the change applies
- > Name of the Target Computer if there was a specific computer specified in the rule setting



- > The device(s) to which the changes apply
- > Permission(s) applied to the device

You can find more information on *Chapter 6: Using the Audit Logs Viewer* on page 175.

The Device Explorer

The Device Explorer module is the main nucleus of the Sanctuary Management Console program. 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 on *Chapter 3: Using the Device Explorer*.

The Log Explorer

The auditing of user actions – for example, users accessing floppy drives or other device types – is accessible from the Log Explorer module.

This module forms the core housekeeping control routine that should be done by Sanctuary administrators. 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.

The Log Explorer has four different purposes:

- > You can view unsuccessful access attempts to available devices on the client machines: Actions like attempting to read or write to a device for which a user has no permission, reaching a data transfer quota, attaching a device to the computer or trying to use a protected WLAN interface
- > You can see client error reports: The log entries are generated by events such as failure to burn a DVD/CD in an unsupported format, failure to communicate with the application server because of a mismatch between encryption keys
- > You can investigate which files have been copied from a PC to an authorized device (shadowing; you can also find out what has been read from the device): Typically, you will want to monitor what authorized end-users copy to a floppy, recordable DVD/CD, or removable drives but you may also want to extend such control to cover LPT and COM ports – only data streams, not files
- > Use the list of attached devices to (possibly) add them to the list of managed ones and then apply the required permissions. The device can be uniquely identified if needed (only removable memory keys)

You can find in this log several fields that will help you identify possible policies violations. You can find more information on *Chapter 5: Using the Log Explorer* on page 151.

The Media Authorizer

Administrators can use the Sanctuary Management Console's Media Authorizer 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 CD is made available. If the checksum and label do not correspond, access will be denied, thus preventing the use of unauthorized DVDs/CDs.

You can find more information in *Chapter 7: Using the Media Authorizer* on page 183.

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/user group 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.

You can find more information in *Chapter 8: Accessing encrypted media outside of your organization* on page 211.

The 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.

You can choose between the following items:

<i>Use this option</i>	<i>to</i>
<i>Connect</i>	Communicate with another SecureWave Application Server in other server or/a different user name in order to carry out administrative tasks.
<i>Disconnect</i>	Detach from the current server SecureWave Application Server. You need to do this in order to reconnect using a different user or server or to change license information.
<i>Save As</i>	Save the contents of the main page in CSV format (only available for specific modules). You can use it to export data to any CSV compliant program, for example Excel.

<i>Use this option</i>	<i>to</i>
<i>Print</i>	Print the active report window. You get the standard Internet Explorer print dialog where you can choose the printer and select several printer options.
<i>Exit</i>	Exit from the Sanctuary Management Console application. Note that this command does not stop the Sanctuary Application Server, just your administrative session.

Table 4: The File menu items

The View menu

The *View* menu controls the navigation and display of various elements of the Sanctuary Device Control window:

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

Table 5: The View menu items

The Window menu

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

<i>Use this option</i>	<i>to</i>
<i>Cascade</i>	Place all open windows in an overlapping arrangement.
<i>Tile</i>	Lay all open windows side by side in a non-overlapping fashion.
<i>Arrange Icons</i>	Position your iconize windows in orderly rows.

Table 6: The Window menu items



The Tools menu

You can synchronize domains, do database maintenance, define administrators' roles, change default options, send updates to all clients, and flush the online computer's list using the Tools menu:

<i>Use this option</i>	<i>to</i>
<i>Synchronize Domain members</i>	Update the database with the current list of users and groups of a domain or a local workstation.
<i>Database Maintenance</i>	Delete the shadow files and central event logging entries created before a given date from the database and data file directory.
<i>User Access</i>	Define Sanctuary Device Control Enterprise Administrators and Sanctuary Device Control Administrators. It will allow you to restrict the right to set permissions, view the audit log or the shadowing information. You should also consult <i>Appendix D: Controlling administrative rights for Sanctuary's administrators</i> on page 293 to learn how to set rights to control Organizational Units/Users/Computers/Groups
<i>Default Options</i>	Change the default computer options settings. You can find more information on <i>Chapter 9: Setting and changing options</i> on page 233.
<i>Send Updates to all computers</i>	Dispatch the latest changes to all computers on the network. Changes can be sent in synchronous or asynchronous mode.
<i>Send Updates to</i>	Transmit the latest changes to a specific computer on the network.
<i>Purge Online Table</i>	SecureWave Application Servers keep a record of the connected clients. Sometimes, clients are disconnected without notifying their server that they are not available anymore. In this case orphan entries are left in the online table affecting the performance of the 'Send Updates' functionality. When you purge the online table, the application server erases all information it has regarding connected clients. Every time a user logs on/off or unlocks his station the online table is modified.
<i>Endpoint Maintenance</i>	Create and save maintenance "tickets" for computers/computer groups allowing protected files and/or registries to be modified. See next section for an explanation.

Table 7: The Tools menu items



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

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

Endpoint Maintenance

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

This key value works in conjunction with the *Client Hardening* value established in the *Default Options* dialog (see *Chapter 9: Setting and changing options* on page 233). If "Extended" or "Basic" is used, the client protection mechanism can only be deactivated using the endpoint maintenance. The generated "ticket" can be saved and transported to the client computer(s) by any available 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's icon – located on the system bar – and selecting 'Endpoint Maintenance' from the contextual menu.

Client ticket rules

The client ticket follows these rules:

1. The maintenance ticket is unique and per machine. You cannot generate the same ticket for several computers (even though you are allowed to do so).
2. The time options are only valid to accept the corresponding maintenance ticket. Once the ticket is accepted, there is no time limit for it. To deactivate the ticket you will need to reboot the machine.
3. If the maintenance ticket is generated for a specific user, this user must be logged to accept it. If this is not the case, the ticket is rejected.
4. If you choose to "relax" the client hardening value by creating and using a maintenance ticket for a computer without choosing a user and another user logs into the same machine, the computer continues in a "relaxed" state until the next reboot.
5. Your comments will appear on the audit log. You can review them by using the Audit Logs Viewer module (see *Chapter 6: Using the Audit Logs Viewer* on page 175)



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

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

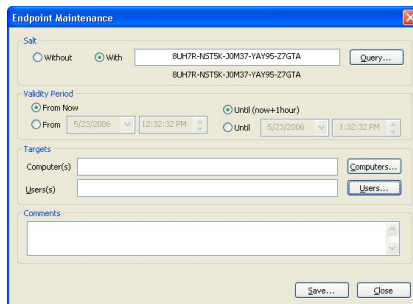


Figure 13: Endpoint maintenance

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. You can also save directly to the “ticket” directory of the necessary online machine. This “maintenance ticket” must then be copied to the predefined ticket directory in the client computer(s). See the *Setup Guide* for a description of the registry keys. As previously explained, this ticket also depends of the *Client Hardening* option value.

The Reports menu

Use the *Reports* menu to obtain a plethora of resummed information that you can save or print:

<i>Use this option</i>	<i>to</i>
<i>User Permissions</i>	Select one or more users and generate a report of their device permissions.
<i>Device Permissions</i>	Generate a report of users' permissions for each device.
<i>Computer Permissions</i>	Select a computer and generate a report of the permissions assigned to the user for the use of the different devices of that machine.
<i>Media by User</i>	Select a User or Group and generate a report of the DVDs/CDs they are allowed to use. <i>⚡ DVDs/CDs authorized as a result of a User being a member of a Group are not listed.</i> Specific (encrypted) media that users are allowed to use will also be listed in this report.
<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 access a specific encrypted media will also be listed in this report.
<i>Shadowing by Device</i>	Create a device grouped report of users copying/reading data to/from devices.
<i>Shadowing by User</i>	Obtain a report for all users with the total amount of data copied/read to/from different devices.
<i>User Options</i>	Select a user and see a report with all related permissions and settings
<i>Machine Options</i>	See a report including all computers' options as currently defined in the system. These can be changed using the command <i>Tools</i> → <i>Define Options</i> (or from the <i>Control Panel</i>)
<i>Online Machines</i>	SecureWave Application Servers 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.

Table 8: The Report menu items

Please refer to *Chapter 10: Reports* on page 245 for more detailed information.



The Explorer menu

The *Explorer* menu contains different items depending on which module you are currently using. We describe each item available in the *Explorer* menu in detail in the corresponding section of each module.

<i>Use this option</i>	<i>To</i>
In the Audit Logs Viewer module	
<i>Clear all filters</i>	Clean the searching info fields.
In the Device Explorer module	
<i>Manage Devices</i>	Add/remove devices that can be administrated directly using permissions.
<i>Insert Computer</i>	Add a machine to the Microsoft Windows Network section or to a computer group.
<i>Add/Modify Permissions</i>	Define/change general permissions.
<i>Add/Modify Online Permissions</i>	Define/change permissions to apply when a computer is not connected to the network.
<i>Add/Modify Offline Permissions</i>	Define/change to apply when a computer is connected to the network.
<i>Add/Modify Scheduled Permissions</i>	Define/change programmed permissions.
<i>Add/Modify Shadow Settings</i>	Create/modify a rule 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/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.
In the Log Explorer module	
<i>Fetch log</i>	Obtain the latest log from a client computer.

Table 9. The Explorer Menu

The Help menu

This menu, *Help*, is primarily used to access the help file menu. It also gives you information about the program's version and access to SecureWave's Web site:

<i>Use this option</i>	<i>to</i>
<i>Contents</i>	Use this command to go directly to the contents tab of the help file.
<i>Search...</i>	Use this item to lookup information in the help file.
<i>Index...</i>	Show the help index.
<i>About...</i>	This item displays information about the current version of Sanctuary Device Control. This is useful when contacting SecureWave technical support staff.
<i>SecureWave on the Web</i>	You can go to the SecureWave home page from here. There you can find updated information about all Sanctuary products.

Table 10: The Help menu items

Other administrative functions

This section explains the use of other administrative functions.

Setting and changing options

Sanctuary Device Control allows you to set default options for various aspects of the Sanctuary Client 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*):

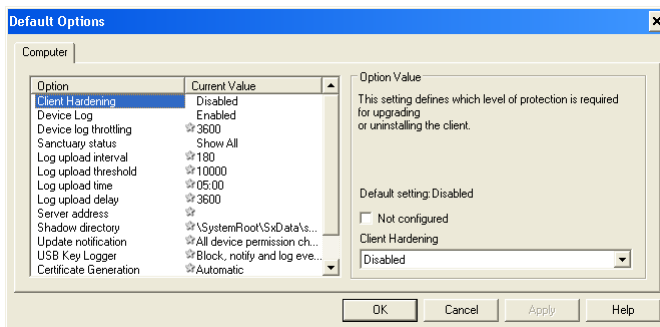



Figure 14: The Default Options dialog

The tab label is simply named 'Computer', indicating that the options are not specific to a particular machine, but are the defaults for all machines in Sanctuary Device Control. If you do not override these default options for a specific computer, then these are applied to all computers in Sanctuary Device Control.



For each option, if the *Not configured* checkbox is selected, 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. The predefined default setting is also indicated for each individual option in this chapter.

If you change an option, the client computers need to be 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 Device Explorer and select *Send Updates to <computername>* from the popup menu.

This same dialog applies when you are changing computer-specific options.

Please refer to *Chapter 9: Setting and changing options* on page 233 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.

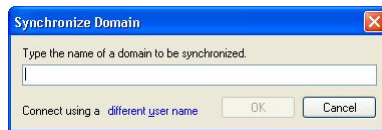


Figure 15: The Synchronizing Domains dialog

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 are updated.



If a machine name is used instead of a domain name, and the machine is a domain controller, this particular domain controller will be 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.

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 of the workgroup individually.

To do this, select *Synchronize Domain members* from the *Tools* menu (or from the *Control Panel*). The following dialog appears:

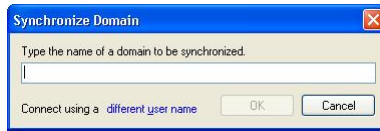


Figure 16: Adding workgroup computers

Type in the name of the computer you want to add, and then click on **DIFFERENT USER NAME**. You will see the following dialog:



Figure 17: 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 of 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

To delete all shadow files and central log files 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*):

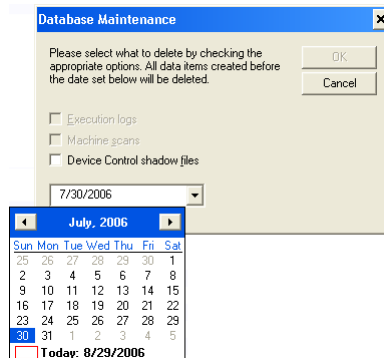


Figure 18: Performing database maintenance

You can click on the field's arrow to select the date visually from a calendar. The only type of maintenance you can do when using Sanctuary Device Control is Device Control Shadow Files (if they exist). Clicking the OK button will delete the selected files before the chosen date from the database tables and the Application Server data file directory.



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 a 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.



This maintenance operation does not clean the records of all operations done by the Sanctuary administrator (Audit logs). You can easily remove these files manually if absolutely required. They are stored in the history subfolder of the data file directory. The 'datafiledirectory' location can be determined from the

value of the registry parameter on the SecureWave Application Server computer:

HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\SXS\PARAMETERS\DATAFILEDIRECTORY

The naming of the audit log files follows the 'History SN (yyyy-mm-dd).log' scheme. Where yyyy represents the year, mm: the month and dd: the day in the month.

*You can remove all audit logs before a specific date by deleting all 'History SN *.log' files that are older than that date (use Windows File Search capabilities).*

Defining the Sanctuary Device Control 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 user cannot manage Sanctuary Management Console even if they are assigned as Enterprise Administrators. They cannot be authenticated at a domain level and, thus, Sanctuary Device Control refuses to run in order to protect the program from misuses.



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 SXS are Sanctuary Device Control 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.

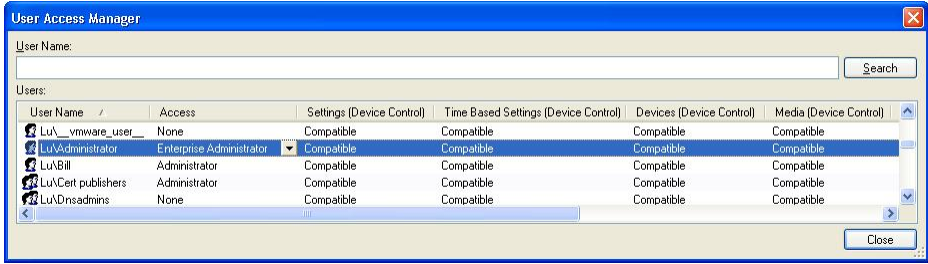


Figure 19: Defining the administrators' roles

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 (*,?) in the name.

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 will have the following prerogatives:

<i>Action</i>	<i>Type of Administrator</i>	<i>Comments</i>
View all permissions.	All Administrators	
Modify global-level permissions.	Enterprise Administrators	
	Members of the 'Manage Device Console Settings' role.	ONLY for the users the administrator is allowed to manage.
Modify machine-level permissions.	Enterprise Administrators (for ALL accounts, including the WELL-KNOWN accounts).	
	Members of the 'Manage DC Settings' role (for ALL accounts, including the WELL-KNOWN accounts).	ONLY for the machines the administrator is allowed to manage.
Modify machine-group permissions.	Enterprise Administrators (for ALL accounts, including the WELL-KNOWN accounts).	

<i>Action</i>	<i>Type of Administrator</i>	<i>Comments</i>
	Members of the 'Manage DC 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 11: Administrator's prerogatives



When you define at least one user as Enterprise Administrator, the members of local Administrators group (default setting) will no longer have access to SXS/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):

<i>Option</i>	<i>This Administrator can do these actions when selecting the 'Yes' option</i>	<i>Comments</i>
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. He 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 'Audit Logs Viewer' 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').



<i>Option</i>	<i>This Administrator can do these actions when selecting the 'Yes' option</i>	<i>Comments</i>
Logs without File Access (Device Control)	Same actions done by the Logs (Device Control) option but cannot see the content of a file.	This option is a sub-group of 'Logs (Device Control)'.
Endpoint maintenance	Create tickets to update, delete, and install the client driver	See <i>Endpoint Maintenance</i> on page 49

Table 12: 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 Sanctuary SecureWave 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 Appendix D: Controlling administrative rights for Sanctuary's administrators on page 293 to learn how to set rights to control Organizational Units/Users/Computers/Groups.

Sending updated permissions to client computers

Administrators use the Device Explorer in the Sanctuary Management Console to modify permissions and rules. When a policy changes, the Sanctuary Client will download 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 17*.

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 125 for more information.

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 will need to explicitly publish the Windows NT shared printers and those 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.

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 work since the most restrictive policy applies. Please see *Table 16* on page 78 and *Table 17* on page 80 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 computer or device, you will 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 only accessible if you are using the Device Explorer module (). You can access it directly 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. Please proceed to section *Managing devices* on page 141 for more details.

Remember, the important thing is that you DO NOT have to take any action if the 'No access' permission rule is OK for that computer or device.

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	Imaging Devices	Printers (USB)	Tape Drives
Bluetooth Radio Devices	Infrared ports (IrDA)	PS/2 Ports	User Defined Devices
COM/Serial ports	LPT/Parallel Ports	Removable Storage Devices	Windows CE Handheld Devices
DVD/CD Drives	Modem/Secondary Network Access Devices	RIM BlackBerry Handhelds	Wireless NICs
Floppy Disk Drives	Palm Handheld Devices	Smart Card Readers	

Table 13: 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 16* on page 78. 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 will like to add. Depending on the device type, you can add:

- > Read or Read/Write permissions; see *Read/Write permissions* on page 112 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 134.
- > Online/Offline permissions; see *To assign online and offline permissions* on page 123 for more information
- > Scheduled permissions; see *To assign scheduled permissions to users and groups* on page 116 for more information
- > Temporary permissions; see *To assign temporary permissions to users* on page 120 for more information
- > Shadow; see *Shadowing devices* on page 126 for more information
- > Copy limit; see *Copy limit* on page 130 for more information



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 141 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 Bluetooth Radio Devices, Wireless NICs, Infrared Ports (IrDA), and PS/2 Ports, since they already form part of the standard device classes you will 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 Microsoft Windows Network 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. Beware that these 'apparently' conflicting permissions will generate 'multiple' messages at the client side.

Identifying specific, unique, removable devices

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

<i>Level</i>	<i>Permissions applies to</i>	<i>Example</i>
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 66 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	For all devices belonging to	Offline permissions for a

<i>Level</i>	<i>Permissions applies to</i>	<i>Example</i>
included in the class itself or in a group.	the same, exclusive, model	device model "M-Sys Xkey 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 # 4352AB879920A
<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>		

Table 14: Managing unique individual removable devices

The following image shows this four level structure:



Figure 20: The four level removable device class structure

As an example of the permission structure depicted in *Table 14* (page 65), consider the following example:





Figure 21: 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 specific, unique, device 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 from the list, and click on the **ADD DEVICES** button.

As an alternative method, you can:

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 or manually traversing the list. Once the register located, right click on it. 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.
3. Follow steps 4–6 of the 1st method.

Organizing devices into logical groups

Sometimes you will need or want to organize your devices in logical units within a device class and assign them special permissions. 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 87 for more information.

Identifying specific computers to be managed

Sometimes you will need special rules for specific computers. In this case, you can add them directly on the Microsoft Windows Network section of the Device Explorer module. All computers added will 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 22: 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 Microsoft Windows Network sections, they apply depending on the priority selected. Please refer to *Priority options when defining permissions* on page 147 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 15* found on page 69).



To furthermore extend our example, we will like to do the following with user Emily of Sales Department for the Floppy Disk Drive she has on her company's laptop:

- > Have 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 will 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							Microsoft Windows Network						
	P	ON	OF	SC	TP	SH	CL	P	ON	OF	SC	TP	SH	CL
Biometric devices	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗
Bluetooth radio devices	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗
COM/Serial ports	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗
DVD/CD drives	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✗
Floppy disk drives	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓
Imaging devices	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗
Infrared Ports (IrDA)	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗
LPT/Parallel ports	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✗
Modem/Secondary Network Access Devices	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✗
Palm handheld devices	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗
Printers (USB)	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗
PS/2 Ports	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗
Removable storage devices	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
RIM BlackBerry handhelds	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗
Smart Card Readers	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗
Tape drives	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗
User defined devices	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗
Windows CE handheld devices	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗
Wireless NICs	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗

* Code used:
P=Permissions; ON=Online permissions; OF=Offline Permissions;
SC=Schedule; TE=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 15: 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 will not be 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 will be 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 Sanctuary's 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 will not correspond to what was initially encrypted and registered. The result is that the user will no longer have access to 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 231.

Practical setup examples

We will illustrate different common uses of Sanctuary Device Control in this section. We will learn, for example, 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 will 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 our Sanctuary) and access to DVD/CD drives has been defined, the administrator can move Bob's computer into this group. His machine will receive automatically 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 will take 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 will probably be 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 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.*




2nd Part: The modules and functions in detail



Chapter 3: Using the Device Explorer

The main purpose of the 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 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* by clicking on the  icon located on the *Modules* section of the *Control Panel* in the main window.

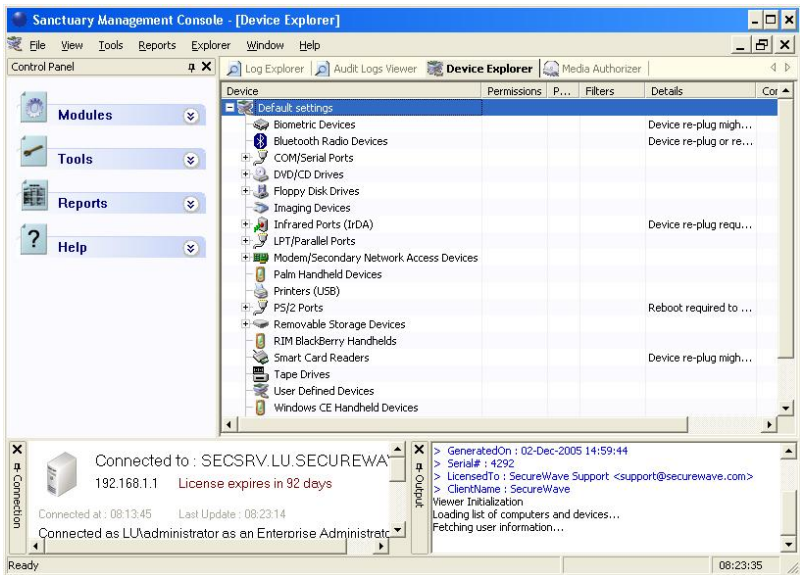


Figure 23: Device Explorer main window



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 Chapter 11: Using Sanctuary Device Control on a Novell network on page 259.



If the 'Settings (Device Control)' access of the Sanctuary Management Console Administrator User Access is set to No, this administrator will have limited access. See Table 11 and Table 12 on pages 59 & 60.



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



The administrator can also use this module to define permissions forcing users to do a decentralized encryption on removable storage devices.

Introduction

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

- > Grant read-only access to the DVD/CD-ROM to all members of the group 'Domain Users'
- > Make a floppy read-only to 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 will be denied (scheduled permission)
- > Add a temporary permission for using a device to a group/user



- > Deny access to a device when the user is online but allow it when offline (or vice versa)
- > Get a copy (shadow) of all data written/read to/from a device for a specific computer/user
- > Limit the quota written to a device for a user/group
- > Create an Event Notification rule that informs the user when trying to gain access to an otherwise unauthorized device
- > Force a user/group to do a decentralized removable storage device encryption

How does the Device Explorer works?

When first installing the software, all permissions are set to their default settings (see the following *Table 16*). It is now your main job 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:

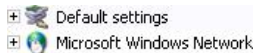


Figure 24: The Device Explorer two main sections

- > In the Default Settings section, you can find those 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 consideration 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 not restricted devices* section on page 78 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 147
- > The section Microsoft Windows Network, on the other hand, is used to define specific permissions to users/groups that will only apply to a specific computer or group of computers. These set of rules will override those located in the Default Settings section. Here you can also add a 'computer group' to reorganize some computers in a logical way that will allow 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 will only have restricted access to their floppy disk drive during working hours (from 8:00 AM to 5:00 PM)



<i>Device</i>	<i>Permissions</i>	<i>Shadow</i>	<i>Copy limit</i>
COM/serial port		Disable	
DVD/CD drives		Disable	
Floppy disk drive		Disable	1MB
Infrared port (IrDA)	Read/Write with Low priority		
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	5MB
Wireless Network Interface Cards	Read/Write with High priority		

Table 16: Default settings when first installing the program (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 will need to reinstall the client.

Restricted and not restricted devices

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

The following table shows the possible assignments by device.

<i>Device Class</i>	<i>Allowed Permissions</i>	<i>Applies to</i>	<i>Notes</i>
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
Bluetooth radio devices	Read-Write /None	Only the Local System or Everyone	Device re-plug or reboot required to enforce updated



<i>Device Class</i>	<i>Allowed Permissions</i>		<i>Applies to</i>	<i>Notes</i>
			group	permissions
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 (for example a Scanner)	Read-Write /None; Select bus type		Any user or group	-
Infrared Ports (IrDA)	Read-Write /None		Only to Local System or Everyone	Device re-plug required to grant access for an already blocked port
LPT/Parallel ports	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)	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
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	Device re-plug 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



<i>Device Class</i>	<i>Allowed Permissions</i>	<i>Applies to</i>	<i>Notes</i>
			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	Device re-plug or reboot required to enforce updated permissions

Table 17: Possible assignments by device



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

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 indirectly authorize 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 Device Explorer

This section describes how you can use your mouse and keyboard to full effect within the Device Explorer.

Context menu and drag & drop

You can use then right-click to get a contextual menu to assign permissions saving you considerable time and effort:

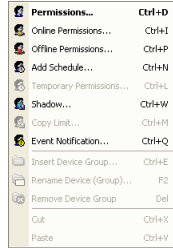


Figure 25: Context menu

Keyboard shortcuts


We have defined some quick access keys to save you time when using some of the features of the Device Explorer module of the Sanctuary Management Console.

For keyboard shortcuts in which you press two or more keys simultaneously, the keys to press are separated by a plus sign (+). The following table summarizes them:

<i>Shortcut</i>	<i>Description</i>
CTRL+D	Add/Modify permission for the selected item(s)
CTRL+P	Add/ Modify Offline permission for the selected item(s)
CTRL+I	Add/ Modify Online permission for the selected item(s)
CTRL+N	Add/ Modify a schedule for the selected item(s)
CTRL+L	Add/ Modify a temporary permission for the selected item(s)
CTRL+W	Add/ Modify Shadow settings
CTRL+M	Define the Copy limit for the selected item(s)
CTRL+E	Insert Device Group
F2	Rename Computer Group/Device
DELETE	Delete entry (see note below)
CTRL+A	Insert 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 18: Keyboard Shortcuts used on the Device Explorer module



 *If you use Delete on a computer entry, it will erase all permissions, shadow, copy limit, etc. for this machine. This computer will not be visible but still exist in the group; you can use the right click menu to show it again. See Show All Members on page 83 for more information.*

Adding comments to an entry


When you have dozens or hundreds of entries on your Device Explorer list, it is very 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' ones 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 will be to FIRST define as many 'Default Settings' as possible that apply to all computers and then define 'Computer groups' for the exceptions. You can then proceed to set permissions to specific machines. You use this kind of groups to make the same exceptions to a series of machines.

 *It is a good idea to add comments to the permission modifications you make. It will help you remember the purpose of each modification 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 will find that there are 'hidden' computers in a computer group inside the *Microsoft Windows Network* section of the *Device Explorer* module. This happens mainly when inserting computers and then 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 will all be moved back to their domain along with those that do 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 to a computer that has been '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).

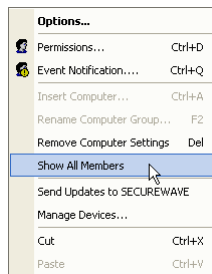


Figure 26: Show all members

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:


- > The root level: when selecting the *Default Setting* node. The notification applies to all devices for the user(s)/user group(s) defined
- > The 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
- > To a specific device in a device class: when selecting a 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
- > To a *Device Group* created within a device class: when selecting a group created within a device class, for example, the Marketing DVD Rewritable previously created in the *DVD/CD Drives* class
- > For a specific computer in the Microsoft Windows Network 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.

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 its 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 button. Click OK when you finish.

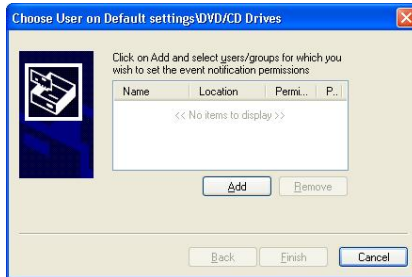


Figure 27: Event notification: selecting the users/groups

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

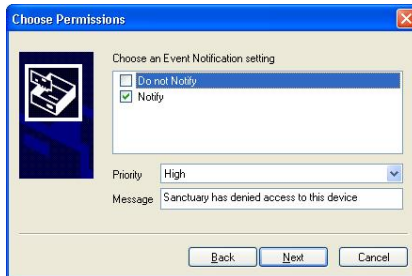


Figure 28: Event notification: options

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

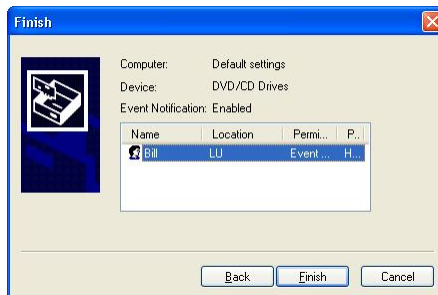


Figure 29: Event notification: finish the rule definition



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:

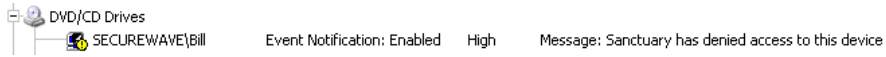


Figure 30: Event notification: new permission rule as shown for the device class



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), follow these steps:

1. Click on the permission and then press the DEL key.
– or –
2. 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), follow these steps:

1. Click on the permission and then press the Ctrl+Q shortcut key.
– or –
2. 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 in your advantage by carefully planning some rules. As an 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 *Microsoft Windows Network*, 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 this newly created device group.

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 **CTR+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)
Removable storage devices	RIM BlackBerry handhelds
Smart card readers	Tape drives
User defined devices	Windows CE handheld devices

Table 19: 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+C**), Copy (**CTRL+C**), and Paste (**CTRL+V**) for the same purpose. These commands are also available from the right-click context menu:



Figure 31: 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. The device types supported are:

Plug & Play devices

Sanctuary Device Control is able to detect Plug and Play devices, even when they are added on the fly.

Since USB, FireWire, ATA/IDE, SCSI, and PCMCIA are bus types, and not true ports, devices attached using these bus systems are recognized based on the device class they belong, not on the way they are connected. For example, an external CD-ROM attached to a PC using the USB port, will be recognized as being part of the 'DVD/CD drives' class and, therefore, receive the same permissions as any other DVD/CD drive. Nevertheless, permissions can also be defined for different devices types within a class, making it possible to assign dissimilar policies for an internal IDE DVD/CD reader or an external USB one.

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.



Bluetooth Radio Devices

You can either enable or disable the communication with Bluetooth devices

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, will only work if the COM port is also enabled. If you use a printer that is configured to use some particular COM port (even if this port is provided by a Bluetooth adapter), then you might have to give access to the COM port as well.

DVD/CD drives

CD-ROM drives, including CD-R and CD-RW drives, as well as DVD drives including DVD+-R, DVD+-RW, and DVD-RAM.

Floppy disk drives

These 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)

Document scanners connected to the computer. Some digital cameras declare themselves to Windows as scanners.



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.

Infrared Ports (IrDA)

Keyboards and mice are examples of devices that you can connect using the infrared port, but so are printers, personal digital assistants, and even computers. You can control these devices with a simple option to enable or disable them.



LPT/parallel ports

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

Modem/Secondary Network Access Devices

Modem devices, including ISDN cards.



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

Palm handhelds – and Compaq iPAQ's – using USB cradles are managed in a separate device class. For those cases where the cradle connects via a serial port, permissions are administrated through the COM port permissions.

Printer (USB)

All models of USB printers connected to the USB port of the computer.



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 is the standard port used to connect a keyboard and mouse to most “old” computers. You will probably like to block it if you use USB keyboards or if you suspect the use of a hardware Keylogger™. You can prevent the installation of software Keyloggers using any program of our Sanctuary Application Control Suit.

Removable Storage Devices

Removable disk drives of any kind not comprise in the Floppy class category, including the Iomega Zip drive (USB, SCSI, parallel or IDE), digital cameras, MP3 devices, and various USB connected memory devices such as DiskOnKey.



Secondary hard disks drives (including SCSI drives) are treated as Removable Storage Devices.

RIM BlackBerry handhelds

Handheld computers/mobile phones from the RIM (Research in Motion) BlackBerry range connected to the computer through a USB port.

Smart Card Readers

Readers for smart cards like eToken or fingerprint readers.

Tape drives

Tape drives attached to the PC.



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

User defined devices

Other devices not falling into the categories listed in this section, such as iPaq, Qtec, HTC, or webcams.

Windows CE handheld devices

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

Wireless NICs

You can enable or block this kind of network adapter using the available permissions rules of Sanctuary Device Control.



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

In this chapter, we analyze in depth the different type of permissions/rules that can be administrated using the Device Explorer module. Please refer to *Chapter 3: Using the Device Explorer* on page 75 for a detailed description on how to use the Device Explorer module.

As seen in the previous chapter, using the Device Explorer you can administrate the rules and permissions that determine which devices your users and user groups can use or not. Users (or groups of users) can only gain access to I/O devices if they have the appropriate permissions to do so.

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

To define permissions, you first select the appropriate section of the Device Explorer tree, *Default Settings* or *Microsoft Windows Network*, choose the desired device class and proceed to the Explorer menu or right click on the item. From there you can select all type of permissions and rules to assign to a device and associated user(s)/user group(s).



You should not use permissions other that Read and Read/Write when working on a system that uses older versions of the Sanctuary client. The client cannot interpret these types of permissions and the result will be "no permissions applied".

Using the permissions dialog

When defining all type of permissions you will see the same following dialog as the first screen (except for *Copy Limit* where there is a different screen and for *Scheduled Permissions* and *Shadow* where a subset is used as depicted in *Figure 33*):

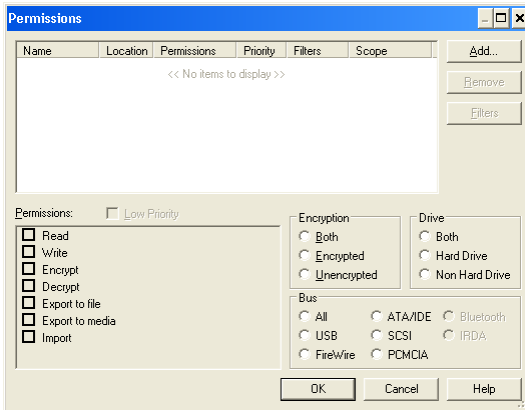


Figure 32: Main permissions dialog

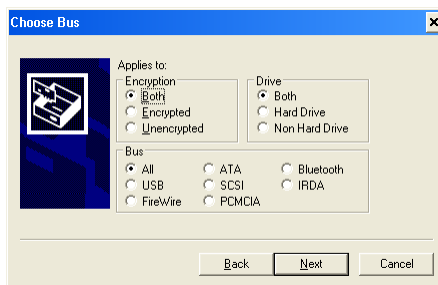


Figure 33: Bus dialog used for Scheduled Permissions and Shadow

Select 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 and are fully explained in the corresponding section of this chapter. Once the user(s)/group(s) selected – using the Add button – you can reselect them (all or some) to define Permissions, Encryption, Drive, and Bus type (if applicable) individually or globally.

You can add as much permissions to user(s)/user group(s) as you desire without closing the dialog: just click on the Add button.

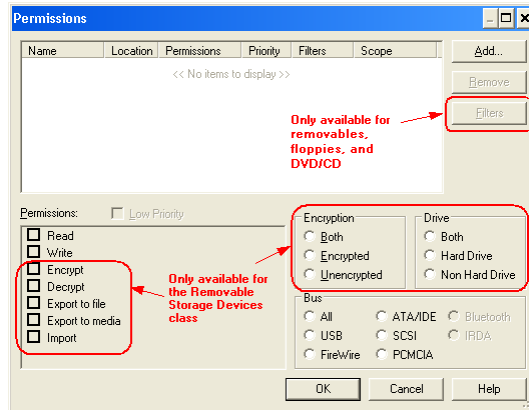


Figure 34: General Permissions dialog exceptions

If the class for which you are defining permissions is not the Removable Storage Devices class, you can select among Read Only, Read/Write, or None (not selecting any option). On the other hand, if working with others class, you can also choose the other options as explained in the following section.

The Bus panel has all 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).

In the user/group panel you can find the following fields:

- > The *Name* shows the user/group name.
- > The *Location* indicates the user domain or workgroup (if available). It is the same ones as that shown in the *Select User* dialog (opened with the *Add* button).
- > The *Permissions* field reflects those options selected on the *Permissions* panel (lower left side of the dialog).
- > The *Priority* exhibits if the permission is applied with a high or low priority (by selecting or not the *Low Priority* option). See a description of priorities and how do they apply in *Default Permission priority* on page 110.
- > The *Filters* field shows the type of files the user can access (or not).
- > The *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 continue to add all kind of permissions to as many different users/groups as you want without closing the dialog. 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 the Removable Storage Devices class

If defining permissions or a "Shadow" rule for this class, you can also choose to apply the permission(s) to encrypted and/or decrypted devices. To limit further the permission, you can choose from the *Encryption* and *Drive* panels the required scope options.



Note that some USB memory sticks are recognized as external hard disk drives. This could lead to confusions 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 since the "real" secondary hard disk drive(s) could be blocked/allowed/shadowed or force to be encrypted/decrypted without being noticed.

You can use the following settings when working with the removable class:

<i>Parameter</i>	<i>Description</i>
None (neither read nor write)	The user/group has no 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 be a secure channel. You must first choose the Encrypt setting.
Export to media	The public key that was use 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 20: 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.

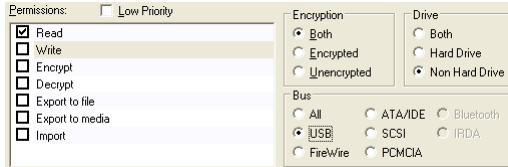


Figure 35: Removable permissions settings example 1

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

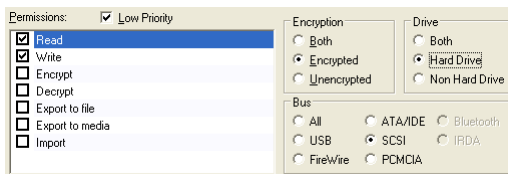


Figure 36: Removable permissions settings example 2

3. User have 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.

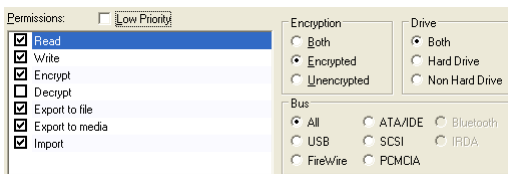


Figure 37: Removable permissions settings example 3

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.

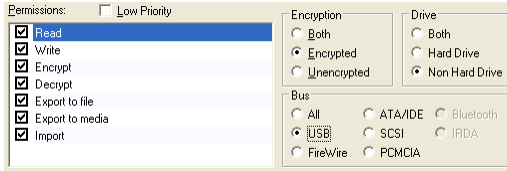


Figure 38: Removable permissions settings example 4

See *Decentralized encryption* on page 231 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 23*). 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 line.

Filters are ONLY available for the *Removable Storage Devices*, *Floppy Disk Drives*, and *DVD/CD Drives* classes.

Once the filter set, click on the OK button to accept or on CANCEL to close the dialog without selecting the filter. You should now see all the filter details in the corresponding field of the permission dialog. Once the permission defined, the details are also visible in the *Filters* column of the *Device Explorer* module window.

When using permissions that include File Filters you have the following possibilities:

<i>File type filtering</i>	<i>Result</i>				
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 removable devices to the local HDD
				<input type="checkbox"/> Import <input checked="" type="checkbox"/> Export	Deny file copy from the local HDD to removable devices
				<input type="checkbox"/> Import <input type="checkbox"/> Export	Resulting limitations depend of other permissions defined



<i>File type filtering</i>	<i>Result</i>				
					for the user/group
	<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 removable devices to the local HDD
				<input type="checkbox"/> Import <input checked="" type="checkbox"/> Export	Allow file copy from the local HDD to removable devices
	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	Read /Write		<input type="checkbox"/> Import <input type="checkbox"/> Export	Resulting limitations depend of other permissions defined for the user/group
<p>The</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> All Known files <input checked="" type="checkbox"/> All File Types <p>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.</p>					

Table 21: File type filtering possibilities

We have dedicated a whole section to explain its usage through examples. See *File Filtering examples* on page 102 for a complete set of examples.



You cannot copy files bigger than 1GB once a file filter is defined.



You can define different file filters for read, write, or read/write permissions.



The Filters button is disable 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.



In the 'File Type Filtering' dialog you can find two options: 'All Known Files' and 'All File Types'. These options control whether the filters apply solely to those files selected in the list panel or to all types of files (even those not included in the list).

If no filter is defined, the profiled permission applies to all type of files.

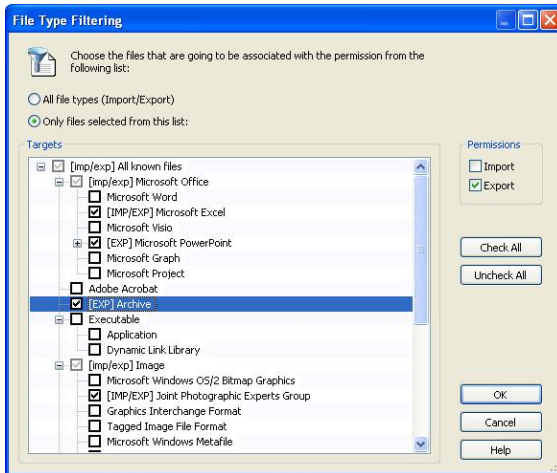


Figure 39: Defining a file filter

The extensions are referenced on the following table:

<i>Description</i>	<i>Extension(s)</i>
Microsoft Office	
Microsoft Word	doc;dot;wiz
Microsoft Excel	xls;xla;xlt
Microsoft Visio	vsd;vss;vst
Microsoft PowerPoint Slideshow	pps
Microsoft PowerPoint Presentation	ppt
Microsoft PowerPoint Template	pot
Microsoft Graph	gra
Microsoft Project	mpp



<i>Description</i>	<i>Extension(s)</i>
Adobe Acrobat	pdf , ai
Archive	zip;rar;cab;ace;msi;msm;pcp;wid
Executable	
Application	exe
Dynamic Link Library	dll;ocx:cpt
Image	
Microsoft Windows OS/2 Bitmap Graphics	bmp
Joint Photographic Experts Group	jpg;jpeg
Graphics Interchange Format	gif
Tagged Image File Format	tiff;tif
Microsoft Windows Metafile	wmf
Microsoft Windows Icon	ico
Microsoft Windows Cursor	cur
Enhanced Microsoft Windows Metafile Format	emf
Portable Network Graphic	png
Audio Video	
Moving Picture and Associated Audio/Video	
Moving Picture Experts Group	mpg;mpeg
MPEG Audio Stream Layer II	mp2
MPEG Audio Stream Layer III	mp3
Resource Interchange File Format	
Windows Animated Cursor	ani
Audio Video Interleave	avi
Downloadable Sounds	dls
Musical Instrument Digital Interface	rmi
DirectMusic Style	sty
WAVEform audio format	wav
Advanced Streaming Format	asf;wma;wmv
Standard MIDI File	mid;midi
RealNetworks Content	rm
Rich Text Format	rtf
Microsoft Windows Setup	
Microsoft Windows Installer File	msi;msm;pcp;wid
Microsoft Windows Installer Patch	msp
Microsoft Windows SDK Setup Transform Script	mst

Table 22: Filter type filtering extensions

File filters work in direct relation to the permission type being set:

<i>Permission type</i>	<i>File filter example</i>	<i>Description</i>
Device access set to "None"	*.doc, *.rtf	Access is denied for files with extension doc or rtf
Device access set to "Read"	*.mp3	Read access is allowed for files with extension mp3
Device access set to "Read/Write"	*.doc, *.txt	Read/Write access is allowed for all those files with extension doc and txt
All types	Not defined	The permission defined will apply to all type of files.

Table 23: File filter settings and permission relation



Once the filter assigned, you can modify it by editing the related permission, clicking the **FILTERS** button, and changing the required file type(s).

You can also choose these settings from the Import/Export Permissions panel:

- > *Export*: to allow copying from the system hard disk drive to the external device
- > *Import*: to allow copying from the external device to the system hard disk drive.



When defining File filters, you are not allowed to open the file directly from the external device. You must first copy it to your system – or authorized – hard disk drive.

File Filtering examples

In this section, we analyze several common cases where you can utilize File Filtering in your advantage by blocking or allowing user file access by type.

1. Allow "Marketing" users to access all kind of files with the exception of MP3.

We first need to define the two following rules:

- > Domain users have "Read/Write" access to removable devices (File Filtering rule with *All File Types* and *Import/Export* activated)
- > "Marketing" user group has a "None" permission for the Removable Storage Devices class with a File Filter defined for MP3 files. Activate the Import/Export settings

From these two rules, we infer that:

- > "Marketing" users can copy everything they want to removable devices except MP3 files since there is a "negative" permission defined from them, but there is also a "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.

2. Allow "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 PDF files 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 will be the only type of files that "Sales" can copy.

3. Allow "Marketing" users to 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 PDF files and *Import* permissions for Microsoft Word and Microsoft Excel files

User of the user group "Marketing" can now copy to their external devices PDF files (but not the other way around) and copy to their system hard disk drive (from their external devices) Microsoft Word and Microsoft Excel files. The file can be opened once it resides in the hard disk drive.

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

- > Define a Read/Write permission for domain user to the Removable Storage Devices class with a File Filter set for Microsoft Office, PDF, and Image files. Select the *Import* and *Export* checkboxes from the permissions panel in the File Type Filtering dialog.

Since MP3 files were not included in the File Filter, they will NOT be accessible.

In all cases:



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



If you define a file filter authorization, all those 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 will NOT be denied by this rule. They can be denied by default or by defining another rule.

The following table contains other examples to further clarify file filtering setup. User Jack and Jill belong to the user group "Marketing" and all permissions are defined for the Removable Storage Devices class.



<i>Example #</i>	<i>Permission type</i>	<i>User/Group</i>	<i>File filter</i>	<i>Import/export parameter</i>	<i>Resulting permission for the user</i>
1	Read	Jack	<input checked="" type="checkbox"/> Only files selected from this list; *.doc	<input checked="" type="checkbox"/> Import <input type="checkbox"/> Export	Jack can copy DOC files 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; *.pdf	<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 DOC files 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; *.doc	<input checked="" type="checkbox"/> Import <input type="checkbox"/> Export	
4	Read/Write	Marketing	<input checked="" type="checkbox"/> Only files selected from this list; *.doc	<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; *.pdf	<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



<i>Example #</i>	<i>Permission type</i>	<i>User/Group</i>	<i>File filter</i>	<i>Import/export parameter</i>	<i>Resulting permission for the user</i>
	None	Jack	Not defined	n/a	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.
7	Read/Write	Marketing	<input checked="" type="checkbox"/> Only files selected from this list; *.doc	<input checked="" type="checkbox"/> Import <input type="checkbox"/> Export	Jack and Jill – and all other users belonging to the user group Marketing – can only copy DOC files from removable devices to their local hard disk drive.
8	Read	Marketing	Not defined	n/a	Jack and Jill – and all other users belonging to the user group Marketing – can only read data from removable devices.
9	Read	Jack	<input checked="" type="checkbox"/> Only files selected from this list; *.doc	<input checked="" type="checkbox"/> Import <input type="checkbox"/> Export	Jack cannot copy DOC files to/from removable devices but can copy all other type of files from removable devices.
10	Read/Write	Jack	<input checked="" type="checkbox"/> All file types	<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	
	None	Jack	<input checked="" type="checkbox"/> Only files selected from this list; *.mp3	<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



Example #	Permission type	User/Group	File filter	Import/export parameter	Resulting permission for the user
	Read/Write	Jill	<input checked="" type="checkbox"/> Only files selected from this list; *.doc	<input type="checkbox"/> Import <input checked="" type="checkbox"/> Export	their removable devices to their local HDD, but Jill can also copy DOC files from her HDD to removable devices
*Auxiliary file groups created to serve as a "bridge" to define required permissions					

Table 24: File filter settings examples

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 Microsoft Windows Network tree) and, consequently, apply to all devices for a specific user(s)/user group(s). You can have, for example, 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 the access to certain devices (notably those connected to the PS/2 port) is performed on the context of the built-in 'LocalSystem' user, it is not recommended to use the built-in 'Administrators' group – that includes that user – for root-level permissions. By doing so, you may allow unexpected users to access certain devices (depending on the particular machine's configuration). It is preferable to define a specific group to assign 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 can you apply default permissions?

Default permissions can apply to:

- > 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 *Microsoft Windows Network* tree
- > A computer previously added to an existing domain or workgroup within the *Microsoft Windows Network* 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 151 for more details) without denying them access. You can combine this feature with a "Shadow" (see *Shadowing devices* on page 126 for more details) at device class level for a full log control.

How do you assign default permissions to a node?

To assign permissions, 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 Microsoft Windows Network 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 134.

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 *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.

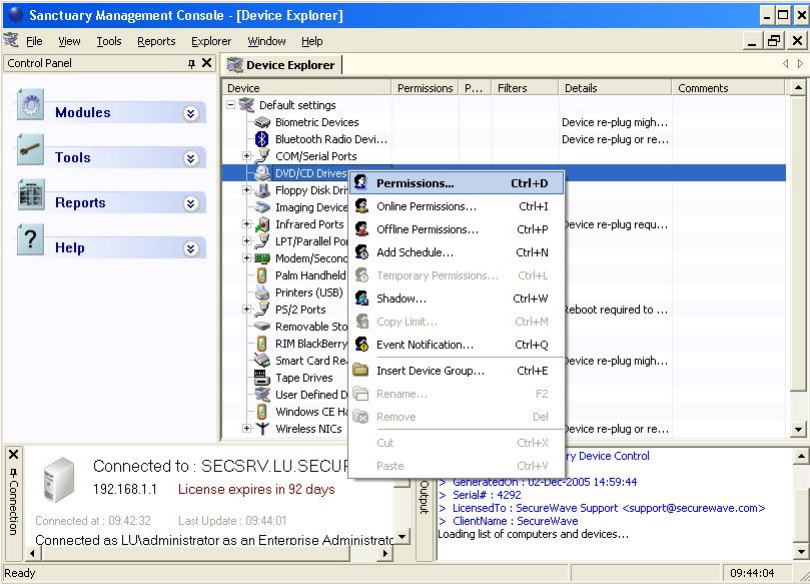


Figure 40: Assigning default permissions to users and groups

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

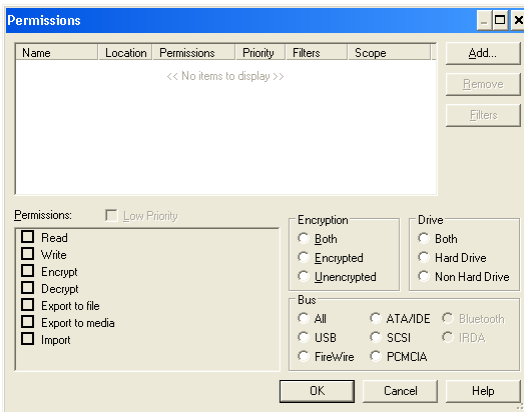


Figure 41: The Permissions dialog



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.

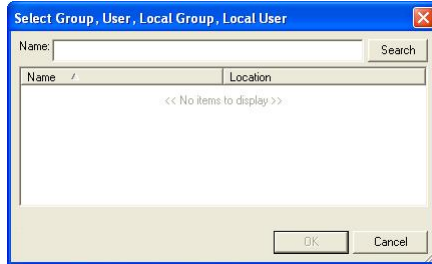


Figure 42: The *Select Group, User, Local Group or Local User* dialog when adding default permissions

3. Type the name of the user or group you want and press **ENTER**. You can use wildcards (*, ?) in the name. You can also use the **SEARCH** button. In the list that appears, select one or more users and groups, and then click **OK**. If the user/group you are looking for does not appear, please make sure you synchronize the domain and have the appropriate permissions on the object in the Active Directory (delegation) or Novell's eDirectory. You can use the **SHIFT** and **CTRL** keys to do a multiple selection on the user/group 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 93 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 98. This button is only active for those device classes where it is possible to define a *Shadow* rule.
6. Click **OK** to finish.

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



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 78 for those devices that will need a reboot.

Default Permission priority

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 make a distinction between the absence of permission (the most restrictive access) and a negative permission ('None').

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 indirectly authorize to use the device. You specifically deny the access to a device for the user and a negative permission ('None').

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:



<i>Default Setting</i>	<i>Default Permission Priority</i>	<i>Computer-specific permission</i>	<i>Computer Specific permission priority</i>	<i>Resulting permission</i>	<i>Explanation</i>			
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				
Rules: 1 Combine both permissions. 2 Sort them according to their priority. 3 The one with the highest one is applied. 4 In case both of them have the same priority, follow this precedence:				<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>None</td> <td rowspan="3" style="text-align: center;"> Highest Lowest </td> </tr> <tr> <td>Read/Write</td> </tr> <tr> <td>Read-only</td> </tr> </table>	None	Highest Lowest	Read/Write	Read-only
None	Highest Lowest							
Read/Write								
Read-only								

Table 25: Applied permissions



Please refer to Permissions Priority on page 206 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 17* on page 80 for device's restrictions.

To assign computer-specific permissions to users and groups

In a way similar to the assigning of default permissions, it is possible to assign permissions on a per-computer basis so the settings will overwrite those defined in the *Default Settings* section for a given machine. The procedure is very similar to assigning default permissions to users and groups.

1. If the computer is not listed in the *Microsoft Windows Network* 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:

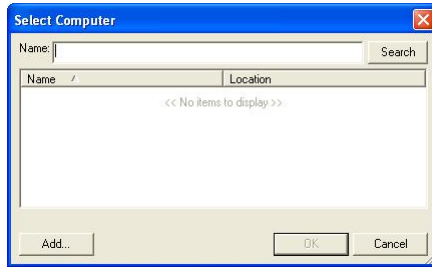


Figure 43: The Select Computer dialog showing multiple selection in action

2. Type the name (or part of it) of the computer you want to assign permissions to. You can use wildcards (*,?) in the name. Click the SEARCH button to get a list of computers. Select the computer(s) from the list and click OK. If the computer you are looking for does not appear, please make sure you synchronize the domain and have the appropriate permissions on the object in the Active Directory (delegation) or Novell's eDirectory. You can use the SHIFT and CTRL keys to do a multiple selection on the computer dialog.

You return to the Device Explorer.

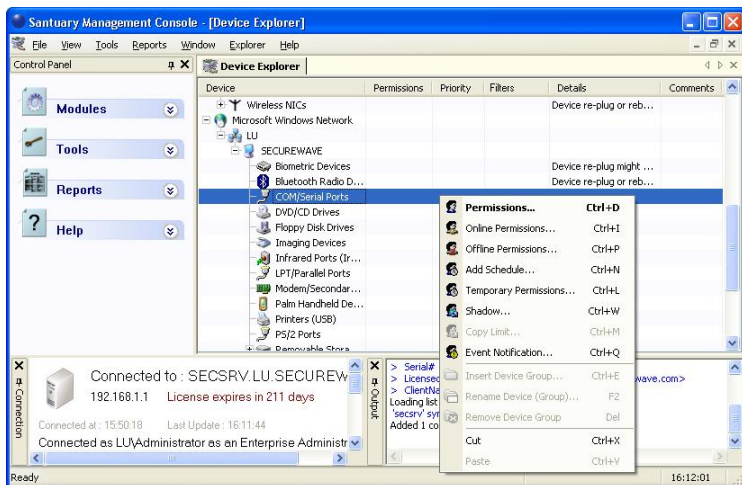


Figure 44: Assigning permissions in the Device Explorer module



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).

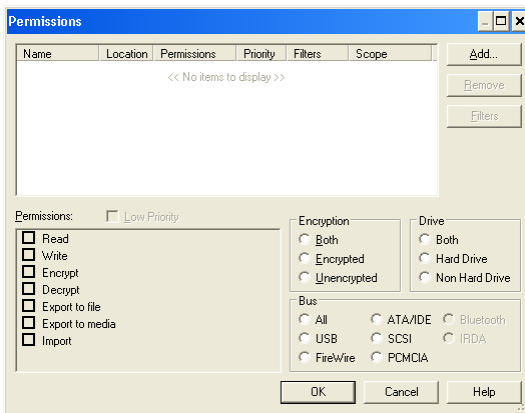


Figure 45: Defining Read, Read/Write, or None permissions when adding permissions

5. Click on Add.

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

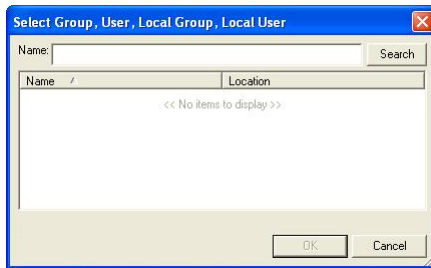


Figure 46: The Select Group, User, Local Group or Local User dialog



6. Select the user(s) or group(s) you want. Type in the name, or part of it, and then click the **SEARCH** button. In the list that appears, select one or more user and/or group (use the **SHIFT** or **CTRL** key), then click **Ok**. If the user/group you are looking for does not appear, please make sure you synchronize the domain and have the appropriate permissions on the object in the Active Directory (delegation) or Novell's eDirectory.
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 93 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

2. 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.

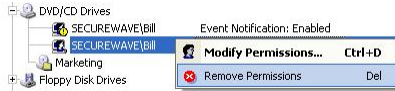


Figure 48: Removing permissions

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:

1. 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.

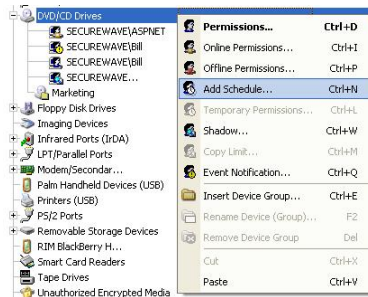


Figure 49: Add a Scheduled permission



The *Choose User* dialog is displayed.



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

2. Click **Add** to display the *Select Group, User, Local Group or Local User* dialog, and select the user(s) and/or group(s) you want to assign the scheduled permission. If the user/group you are looking for does not appear, please make sure you synchronize the domain and have the appropriate permissions on the object in the Active Directory (delegation) or Novell's eDirectory. Click on **Next** when you finish. The *Choose Bus* dialog opens:

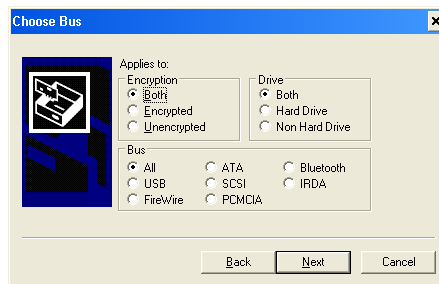


Figure 51: Selecting the bus when adding scheduled permissions

The first part of the dialog is only active when you are adding scheduled permissions for a removable device. It lets you select if the user has access to all type of devices or just encrypted or decrypted ones. The *Drive* panel lets you select between permissions 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 93* 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.



Figure 52: Defining Read, Read/Write, or None permissions when adding scheduled permissions

4. Choose the permissions that you want to apply to the schedule (None, Read, Read/Write) and then click NEXT. The *Choose Timeframe* dialog is displayed.

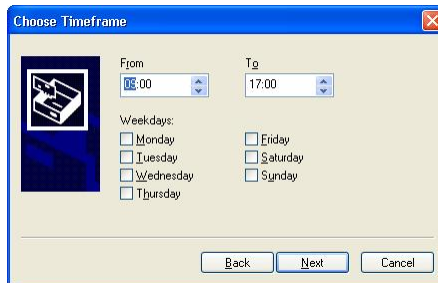


Figure 53: The Choose Timeframe dialog when adding a scheduled permission

5. 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.
6. 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, increasing call charges.



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.

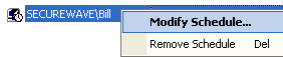


Figure 54: Modifying a scheduled permission

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 the administrator 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 SMC local time is converted to UTC (Coordinated Universal Time) and sent to the client who will convert his local time to UTC before comparing these values.

To assign a temporary permission:

1. Right-click on the device in the *Microsoft Windows Network* section and select *Temporary Permissions* from the pop-up menu. Alternatively, select the device and use the *Temporary Permissions* option on the *Explorer* menu, or use the CTRL +L shortcut key.

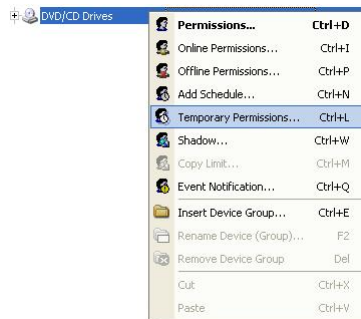


Figure 55: Adding a Temporary permission



The *Choose User* dialog is displayed.



Figure 56: The Choose User dialog when adding a temporary permission

2. Click on the **ADD** button. In the *Select Group, User, Local Group or Local User* dialog, select the user(s) and/or group(s) you want to assign the temporary permission. Click on the **NEXT** button. The *Choose Bus* dialog opens:

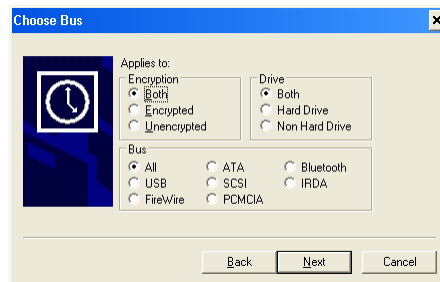


Figure 57: Selecting the bus when adding temporary permissions

The first part of the dialog is only active when you are adding temporary permissions for a removable device. It lets you select if the user has access to all type of devices or just encrypted or decrypted ones. The *Drive* panel lets you select between permissions 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 93 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.

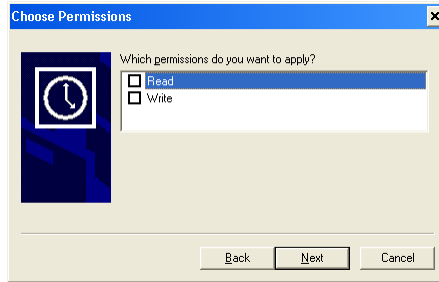


Figure 58: Defining Read, Read/Write, or None permissions when adding a temporary permission

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

The *Choose Period* dialog is displayed.

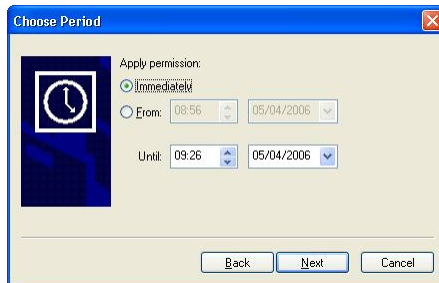


Figure 59: The Choose Period dialog when adding a temporary permission

5. 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.
6. 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 online and offline permissions

You assign this kind of permission when you want to control differently the use of certain devices when the user is online or offline. An example of this could be allowing the user to use his DVD/CD writer completely when at home but not when he is online at the company. Another example will be banning a user from establishing a WiFi/Modem connection to Internet when he is wired to the company network.

You should be aware that:

- > An 'online' state is when the client computer is under the control of your server or is connected to the computer network
- > An 'offline' state, contrary to the 'online' state, is when the client computer is not under the control of your server or is not connected to the computer network

The SecureWave Client Control 'discovers' when a computer is on-line or off-line when any of the following occurs:

- > The machine boots (and the SecureWave Control Client 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: a network cable is unplugged or plugged; a WiFi card connects or disconnects; a modem connects or disconnects; a VPN connection is established or terminated; an address (DHCP) is used or released; a network card is disabled, enabled, deleted or added
- > Every hour if none of the above happens before



If the SecureWave Application Server is stopped or disconnected and you defined different online and offline permissions, the clients that are already logged will stay with online permissions for a maximum of one hour. This happens because the SecureWave Control Client 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 will COMBINE with the regular ones, in full accordance with their mutual priorities.



WLAN adapters cannot be enabled/disabled on the fly; they require a reboot to enforce permissions. When rebooting a LAN/WLAN equipped machine with offline-only, read/write permissions for WLAN, and no LAN cable connected during the boot, the user can later plug in the LAN cable and subsequently use LAN and WLAN in parallel, as long as the machine is not rebooted.

Use the following procedure to assign online/offline permissions (is the same method for both of them):

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).

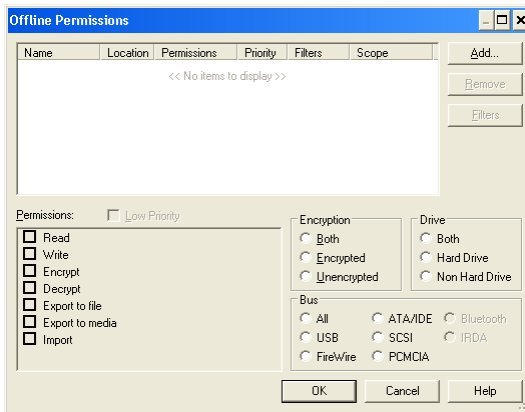


Figure 60: Defining Read, Read/Write, or None permissions when adding online/offline permission

2. Click on the Add button and select the user(s)/groups(s) from the *Select Group, User, Local Group or Local User* dialog.
3. Enable the desired options and accept by clicking on OK. See *Using the permissions dialog* on page 93 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 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 require a reboot in order to apply the new permissions.

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

With this feature, you can export a group of carefully crafted permissions for a range of devices and then import them onto a computer to synchronize them.

You can also use this feature when a computer is not connected to the network, and cannot be connected for the time being, and you need to change permissions. The rules will apply when you import them into the target computer.

There is also a special case when you export to a file called 'policies.dat'. Please consult the Setup Guide for more information.

To export/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 will be a network drive, floppy disk, or any other kind of removable media.
3. Go to the client computer where you want to import the permission settings and right-click on the Sanctuary Control Client icon to display a popup menu. This image may change depending on your license type and installed programs.

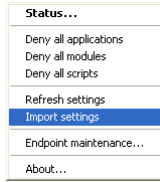


Figure 61: Importing permission settings

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. This rule is available for these classes:


- > COM/Serial ports
- > Modem/Secondary Network Access Devices
- > LPT/Parallel ports
- > Removable storage devices
- > DVD/CD drives
- > 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

 *Shadowing rules can be defined either at the device-type level or at the device class level (the topmost category of the device).*

 *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 need to choose the 'Encrypted' setting in the first dialog so that the Shadow rule applies to this kind of devices. Please see Chapter 7: Using the Media Authorizer on page 183 for more information*



You will see the setup details in the Permissions column of the Device Explorer module: an R means that the shadow is on for those file read from the device, a W when they are written to it and no letter means a read/write shadow setting.

✍ 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, thus, 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 the 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 62: 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:

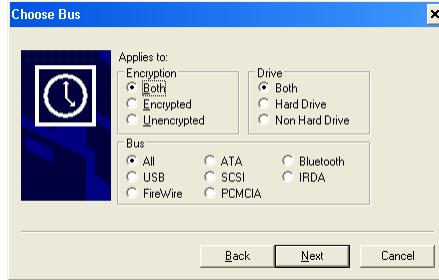


Figure 63: Selecting the bus when adding temporary permissions

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 decrypted 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 93 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 media but not the content. In this case, the "Attachment" field in the Log Explorer module is set to "True". 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 plus an exact copy of what is written. This content is stored on the local data file directory and then transmitted to the server. Please note that high capacity devices, such as DVDs, can consume a lot of 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.

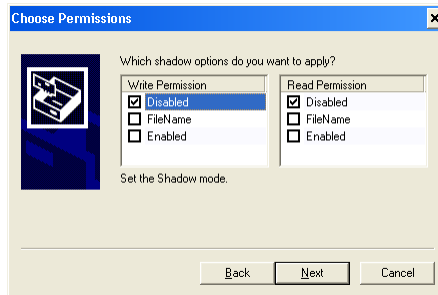


Figure 64: Defining the type of shadow for a device

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

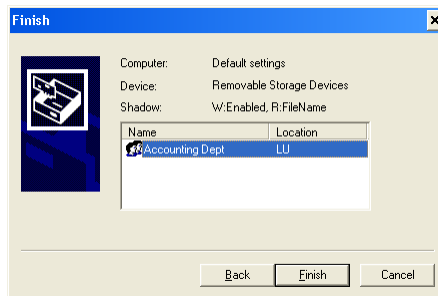


Figure 65: Finishing the shadow rule definition

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

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.



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 you first install the program, the data is limited to 1 MB for floppies and 5 MB for removable drives.

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 *Microsoft Windows Network* (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.

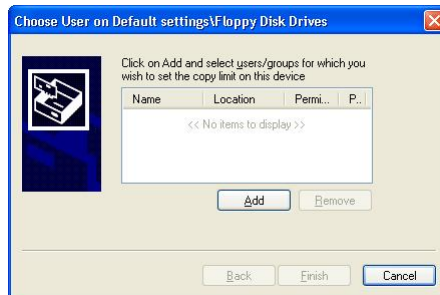


Figure 66: The Choose User dialog when adding a copy limit rule

2. Click on the **ADD** button and select the user(s)/groups(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 67: 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 68*.

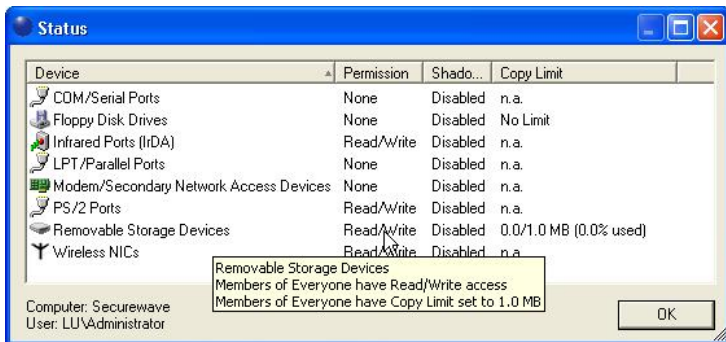


Figure 68: The status screen on the client's side: copied/remaining bytes



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 54 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 will be 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 111).

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 here that you will 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 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:

<i>Permission</i>	<i>Filter</i>	<i>Priority</i>	<i>User/User Group</i>
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 26: Permissions example

When Bill logs onto his laptop, he has the following permissions (refer to previous table and to *Table 25* on page 117):

- > 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 7: Using the Media*



Authorizer on page 183 and *Chapter 8: Accessing encrypted media outside of your organization* on page 211).

The encryption process itself uses our "Easy Exchange" method to cipher the medium. Please refer to the *Easy Exchange* section on page 226 for more information.

To define permissions that 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 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.

To force decentralized encryption

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

- > In the first one, you (the administrator) define Read/Write Encrypt/Decrypt permissions for the LocalSystem account. This is necessary since users are not normally administrators of the machine they work with but the encryption process itself requires formatting the device. This unique permission can be defined at several emplacements depending of the expected result as described in the *Concrete examples* section on page 137.
- > The second phase consists of defining permissions for the specific user that must do the encryption. There are two case 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 226), other users do not need to have Sanctuary's client installed nor have administration rights to use these, already, encrypted devices.
 - 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 permissions rules as you need and always two per use/group: one to define that the user must encrypt the device and the other one defining the mode (read/write, etc.).




- > The third and last, optional, phase consists of defining an *Event Notification* (see *Event Notification* on page 84) so that the user is informed of what must be done

In the most complex case, there should be three 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) or at the *Microsoft Windows Network* level (to activate decentralized encryption for a specific computer).

The following steps summarize this procedure (please refer to *Using the permissions dialog* on page 93 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. Define a permission for the LocalSystem user with the Read, Write, Encrypt, Decrypt, Import, and Export options activated. Select the type of bus (if any) and drive. Activate the Encrypted option of the Encryption panel. You can use a Low priority setting.
4. Proceed to define an encryption permission 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 force to encrypt all those unencrypted devices plugged to the computer.
5. Define Read/Write permissions as required. Do not forget to add the Encrypted option.
6. Optionally define an Event Notification for the user/group or class. Please see page 84 for a full description on how to define Event Notifications.
7. The user will now receive a Deny Access message along with an invitation to encrypt the device when trying to access the removable media. The encryption is done by using the *Encrypt* contextual menu option.



The following images show this process:



Figure 69: Decentralized encryption: the user receives an Access Denied message and an invitation to encrypt it

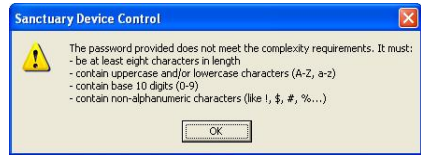


Figure 70: Password complexity is required to encrypt the device

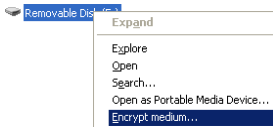


Figure 71: Decentralized encryption: the user proceeds to encrypt the device using the *Encryption* option of the contextual menu

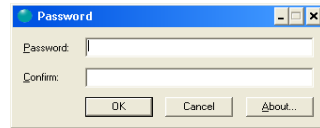


Figure 72: Decentralized encryption: the encryption process begins

Please see the next section for some examples.

Concrete examples

As described in the precedent section, you must first assign the LocalSystem account permissions to do encryption.

In this first example, we define a decentralized encryption rule for a group at the Removable Storage Devices class root level:

1. 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.

Procedure: 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. Define the LocalSystem permission at this device group level (if it is not going to be used elsewhere); Define an encryption permission for the group "Management" at the devices group level; Define a Read/Write permission for the group "Management" at the devices group level. Define an Event Notification for the group "Management" informing the need to encrypt removable devices and providing a help phone number.

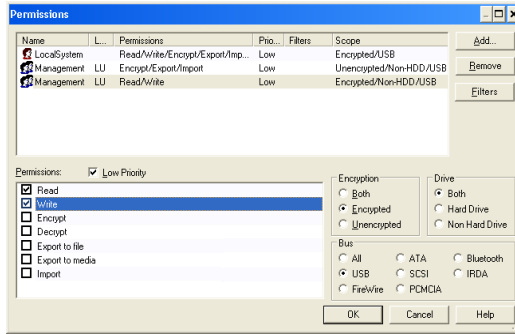


Figure 73: Decentralized encryption for a group defined at a device group level (1/2)

Removable Storage Devices	Permissions	Priority	Message
Management Devices			
LocalSystem	Encrypted/USB: Read/Write/Export (file)/Export (media)/Import	Low	
LU/Management	Unencrypted/Non-HDD/USB: Event Notification: Disabled	High	Message: MUST encrypt this kind of devices. Call 321 for help.
LU/Management	Encrypted/Non-HDD/USB: Read/Write	Low	
LU/Management	Unencrypted/Non-HDD/USB: Encrypt/Export (file)/Export (media)/Import	Low	

Figure 74: Decentralized encryption for a group defined at a device group level (2/2)

The second example deals with a particular user that MUST encrypt a unique device:

2. 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.

Procedure: Define the LocalSystem permission at the Removable Storage Devices class for the device model (can also be defined at the root level); Define an encryption permission for "Bill" for the specific model; Define a Read/Write permission for "Bill" for the specific model.

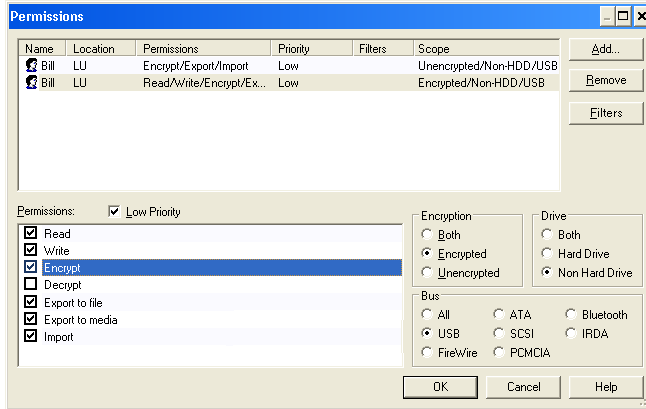


Figure 75: Decentralized encryption at the unique device level (1/2)

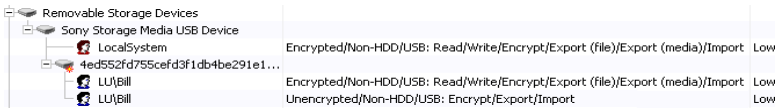


Figure 76: Decentralized encryption at the unique device level (2/2)

The next example shows how to force everyone to encrypt all devices recognized by the system in the Removable Storage Device class:

3. All users must encrypt their own USB keys and have Read/Write access to encrypted devices.

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

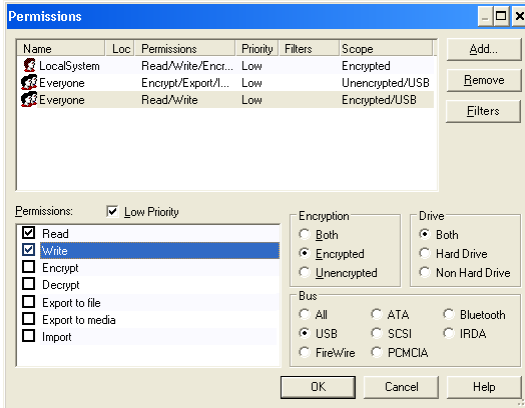


Figure 77: Decentralized encryption at the class level (1/2)



Figure 78: Decentralized encryption at the class level (2/2)

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:

4. 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.

Procedure:

- Define the LocalSystem permission at the Removable Storage Devices class for the “Sony USB devices” (can also be defined at the root level);
- Define an encryption permission for “Bill” at the “Sony USB devices” level;
- Define a Read/Write permission for “Marketing” at the “Sony USB devices” level.
- 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.

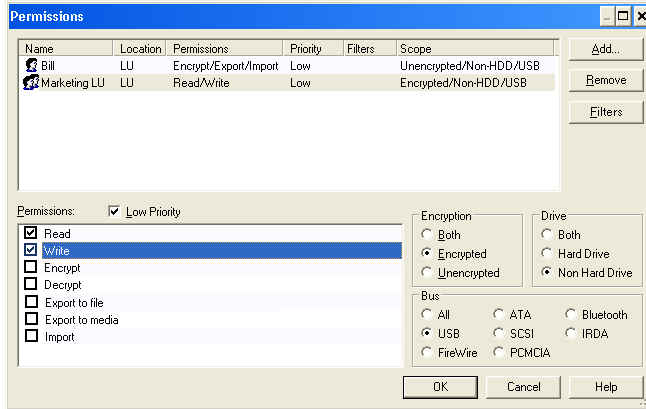


Figure 79: Decentralized encryption using a “delegated” user (1/2)

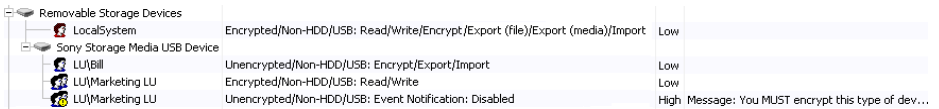


Figure 80: Decentralized encryption using a “delegated” user (2/2)



You must inform the user(s)/group(s) that they will receive a “Drive not accessible message” when trying to access a non-encrypted device. The user must do a right click on the device and choose ‘Encrypt medium’ to do the device ciphering. Once the device encrypted, all authorized user have direct access to its data as explained in the Easy Exchange method on page 226.

Managing devices

All kinds of devices can be attached to the computers that form 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 will 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 will not be able to use the device when it is plugged it into 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*→*Centralized Device Control Logging*) 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 you 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:

- > Bluetooth Radio Devices
- > Wireless NICs
- > Infrared Ports (IrDA)
- > PS/2 Ports

When you initially connect a new type of device (e.g. a webcam) to a computer controlled by Sanctuary Device Control, the Sanctuary Client 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. You will see the following dialog with all the already managed devices:

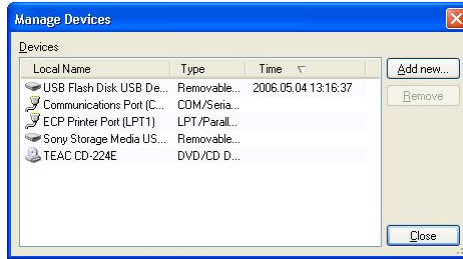



Figure 81: Managing devices

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  button to show all available computers logged on to the network:

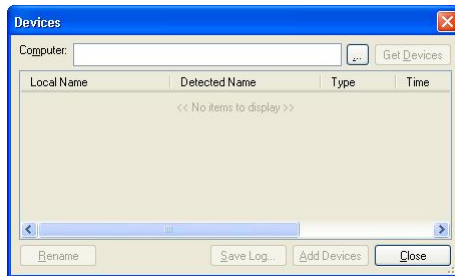


Figure 82: Managing devices – selecting the computer

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. You will see another dialog where you can select those 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.

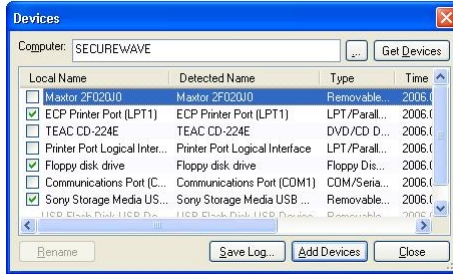


Figure 83: Managing devices – choosing the devices from the selected computer



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 those 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 will go back to the *Manage Device* window that 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.

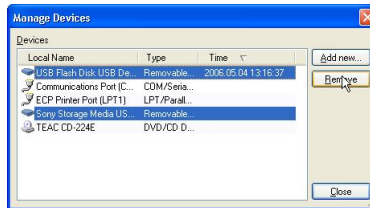


Figure 84: Removing devices

3. Click on the REMOVE button. You will get a warning message. Click the Yes button to close it.



Figure 85: Confirming the removal of a device

Sanctuary Device Control will revert 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 64 to add a particular removable device.



Changing permissions mode

Some devices you add will 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 and by Sanctuary Device Control. 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 will 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 130 for more information). You would ideally place all different models of Zip drive readers in a device group (see *Device Groups* on page 87 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):

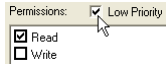


Figure 86: Priority setting

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 will 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 will not work UNLESS you define a 'None' permission (not Read nor Read/Write) at the Default Settings level with a Low priority, allowing the overwriting of the permission rule defined for the specific computer.

This 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 117).



<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
Type	Read/Write	Low	
Class	None	Low	Read/Write
Type	Read/Write	High	
Class	Read/Write	High	None
Type	None	High	
Class	None	Low	None
Type	Read/Write	Low	
Class	Read	High	Read/Write
Type	Read/Write	Low	
Class	Read	Low	Read/Write
Type	Read/Write	High	
Class	Read/Write	High	Read/Write
Type	Read	High	
Class	Read	Low	Read/Write
Type	Read/Write	Low	

Table 27: 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 28: Permission settings priority



We can distinguish between two removable devices of the same make by using the Media Authorizer module.

Informing client computers of changes

Whenever you make a change to the device permissions in the Device Explorer, 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 will show when you choose the *Send Updates to All Computers* command:

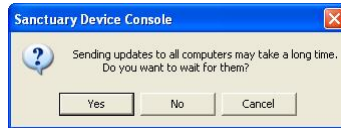


Figure 87: Sending updates to client computers

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

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*).

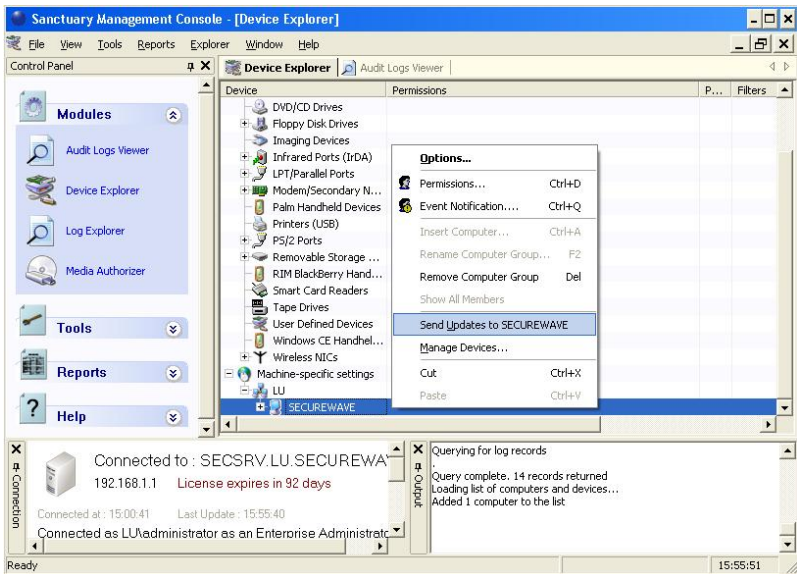


Figure 88: The send update item from the contextual menu



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 will receive 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 256. 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 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 icon located in the system tray.



Chapter 5: Using the Log Explorer

Introduction

The Log Explorer has four different purposes:

- > You can view unsuccessful access attempts to the available 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 and can be reviewed centrally by the administrator. Other user actions like 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 logging is turned off. It can be enabled either for all computers (*Tools*→*Default Options*→*Centralized Device Control Logging*; or from the *Control Panel*) or for a specific one by means of the detailed options of that computer
- > When a device is connected or disconnected from a computer, you can optionally activate a log for this type of event (see previous point for a guideline on how to activate central logging). The event is reported as *Device Attached*, you can choose to add the device immediately selecting the 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 141 for a full description on how to add specific devices
- > You can view client error reports: The log entries are generated by events such as failure to burn a DVD/CD in an unsupported format, failure to communicate with the application server because of a mismatch between the server *sx-private.key* and client *sx-public.key* (the private and public key are generated by the Administrator to control access to specific devices). By default, central error logging is turned off. It can be enabled either for all computers (*Tools*→*Default Options*→*Centralized Device Control Logging*) or for a specific one by means of the detailed options of that computer



See Appendix A: DVD/CD Shadowing on page 265 for details on what can and cannot be shadowed when writing/reading to/from a recordable CD or DVD.

- > You can see which files have been copied from a PC to an authorized device (shadowing: you can also control what was read from a device): By default, Shadowing is turned off. It can be enabled either for all users or a specific one (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 will want to monitor what authorized end-users copy/read to/from a floppy, recordable DVD/CD, or removable drives but 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 will result in a raw binary data shadow file. In some of these devices, you can only activate the 'name' option, not the full copy.



Shadowing and Central logging are a set of rules 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. Furthermore, if the 'Logs w/o File Access (Device Control)' is set to 'No', the administrator will not be able to see the contents of the file (even when enabling full shadowing). Please refer to the Defining the Sanctuary Device Control administrators section on page 57 for more details.



If the "Attachment" field of a file is set to "true", then the content file has been shadowed. This will only happen if the 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 Log Explorer can only show the first 32,000 records of a log. You can limit your search by selecting a suitable range in the available fields.



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, this may 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 9: Setting and changing options on page 233 for more details).

Sanctuary Device Control monitors data as it is generated by the client application. For instance, shadowing a USB memory stick will fetch the files copied/read – name or name and content, depending on the selected shadowing option – and place and entry on 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, but 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 to '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.

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

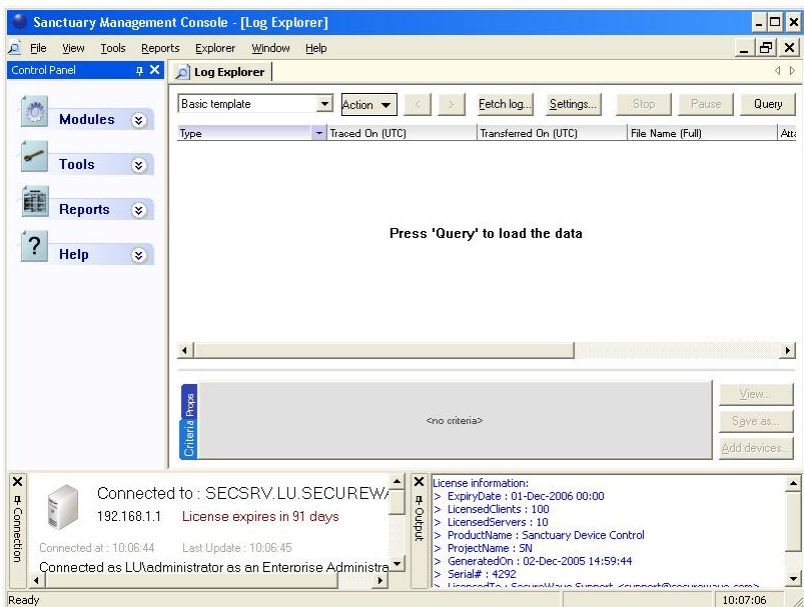


Figure 89: The Log Explorer main window



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

<i>Possible configurations</i>	<i>Domain type</i>	<i>Logged user*</i>	<i>Result</i>	<i>Notes</i>
SXS & SMC are running on the same machine	n/a	Current user	Works properly	If SXS and SMC are running on un-trusted domains, the configuration may not work
		Other user	Would not work	DCOM error when using the Log Explorer module
SXS & SMC are running on different machines	Trusted domain	Current user	Works properly	
		Other user	Works properly	Only if DCOM is configured correctly (if using Windows XP SP2 or later or Windows 2003 SP1 or SR2)
SXS & SMC are running on different machines	Un-trusted domain	Current user	Would not work	
		Other user	Would not work	
*Current User = the same user that logged to Windows is the one that logs to SMC. See <i>Log in as a different user</i> on page 38.				
To correctly configure DCOM:				
<ol style="list-style-type: none"> 1. Run dcomcnfg.exe (Start → Run) 2. Select 'Component Services' and open the 'Computer' branch 3. Right click on the desired computer on the right panel and select 'Properties'. 4. Select the 'COM Security' tab, click on 'Edit Limits' in the 'Launch and Activation Permissions' panel. 5. Select the user you want to define as the SMC administrator and activate the 'Remote Activation' option. 6. Verify that in the 'Access Permissions' panel the chosen user has 'Remote Access' activated. 				

Table 29: Limitations while using the Log Explorer module under other user/domain account



Basic operation

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



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

To use an already defined template

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

Managing templates

What is a template

As you work in the *Log Explorer* changing criteria options, column size and order, which columns must be show in the window, and the whole set of configurable options, you are creating a template. A template is, in this context, a set of rules to use when displaying data in the *Log Explorer module*. Once satisfied with your log report, you can always save this template for future use. Your templates can be reloaded, saved with another name, renamed, deleted, imported, and exported as needed.

To create a template

Click on the **ACTION** button and select *New* from the list. You will see the template name change to *New (0)** indicating that this is a new template and it has not been saved. After changing the required options, click once more on the **ACTION** button and select *Save As* from the list. Do not choose to save your template if you want to freely modify criteria and other parameters without overwriting your original one.

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



Figure 90: Saving your new template

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

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

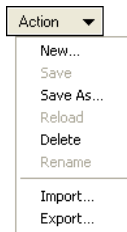


Figure 91: Managing your templates

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



The Log Explorer window in detail

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

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

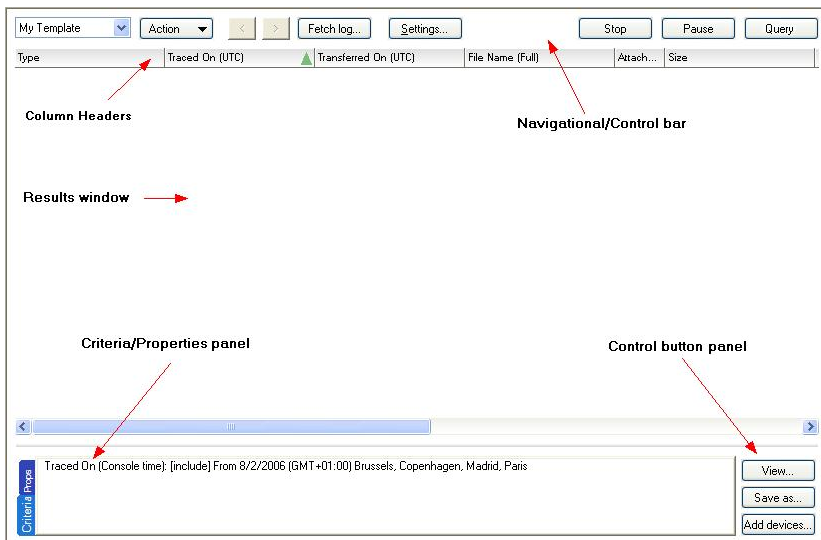


Figure 92: Components of the Log Explorer window

Navigation/Control bar

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



Figure 93: Navigation/Control bar



- > Template list – select a template from those created by you or by SecureWave. If you see an asterisk by the name [*], it means that the template needs to be saved since you recently modified a search or classifying parameter
- > Action – used to manage your templates (save, save as, create, delete, rename, reload, export, or import a template). See *To delete, save with another name, rename, import, and export a template on page 156*
- > Previous – navigate to the preceding result list from the ones internally stored
- > Next – navigate to the subsequent result list from the ones internally stored
- > Fetch log – retrieve all client's logs and shadow files
- > Settings – go directly to the advanced settings dialog where you can select columns and define criteria
- > Stop – cancels the current query, usually when you want to interrupt a long classifying operation – involving a large number of log entries
- > Pause – cancels the screen output but the classifying process continues in the background. Click again on this button to continue the screen display
- > Query – recuperates all log entries corresponding to defined criteria

Column Headers

The column headers, besides being used as a title of the chosen column, can also be used to classify results. To sort ascending by a column, click once on the header, click again to sort in descending order. Click on another heading to change the sorting order to that column. You can see the result as a green arrow in the column's title with the sorting order number.

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



Figure 94: Column Headers

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

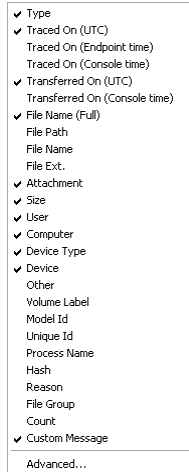


Figure 95: Show/hide columns

The options shown in *Figure 95* may be different depending on the installed license. If you want to clear the sorting filters, proceed to the *Settings* dialog as described in the next section.

The Settings dialog

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



Figure 96: How to open the Settings dialog

In all cases, the *Settings* dialog opens:

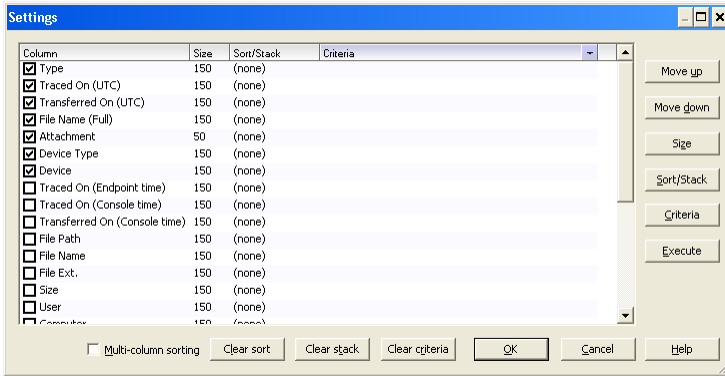


Figure 97: Settings dialog

In this dialog, you can:

- > Show/hide columns – simply check/uncheck the desired one(s)
- > Change the display size of a column – select the desired field, place the cursor over the size column, click, and change the size directly. You can also do it from the main window by dragging the heading divider
- > Sort ascending/descending and by several criteria – click on the sort/stack column and choose among the available options. If you want to do a multi-column sorting, select another classification from the Sort/stack column. You can sort using several columns by selecting first the *Multi-column sorting* option located on the lower left part of the dialog
- > Stack by any field by clicking on the Sort/Stack column and selecting the *Stacked* option. When selecting a stack, all log entries in the main result window will be 'pile' in single entries. You can also add a total by selecting the Count column

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

Figure 98. Stacking the query

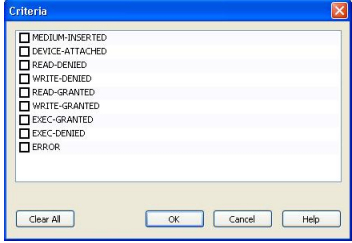
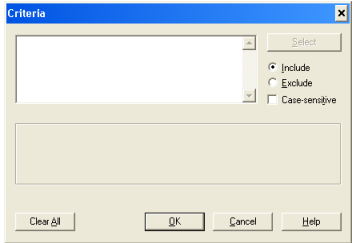
In the previous image, the Custom Message is stacked and you can see the ellipsis indicating hidden log entries and the count column indicating how many entries are present.



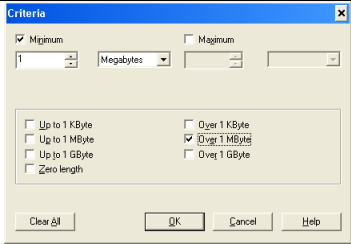
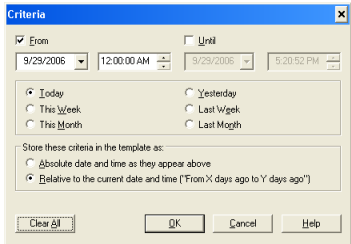
- > Decide the column displaying order – using the MOVE UP and MOVE DOWN buttons located on the right part of the dialog
- > Clear sorts, stacks, add or remove criteria, change the size of any column, and execute the query – using the corresponding buttons located on the lower and right part of the dialog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

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

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

<i>Criteria Dialog</i>	<i>Description</i>
	<p>Criteria List</p> <p>Dialog box displayed when log entry fields can only have a fixed set of values.</p> <p>Check or uncheck the boxes that correspond to the values you are looking for.</p> <p>Examples: (Using the "Type" column) if you are searching for log entries related to those devices being attached to your network, set the "Device-Attached" checkbox and clear all others. If you additionally want to see all read denied events, set this checkbox as well and the query will return log entries related to these two types of events.</p>
	<p>Free-text criteria</p> <p>This dialog is used to filter the query results based on any text that you type in.</p> <p>Enter the text you want to search in the field. You are allowed to use wildcards (? to match any single character and * to match any sequence of zero or more characters). If entering several strings, separate them by using semicolons (;) to get log entries matching any of the strings specified. You can further specify – by using the corresponding controls on the right part of the dialog – if the search should be case-sensitive, and whether the query should return entries that include or exclude the entered strings.</p> <p>Examples: to search all log entries that contain main executables run by users, enter "*.exe" (without the quotes). To additionally get results concerning XP Service Pack Message DLLs (xpspires.dll, xpsp2res.dll...), enter "*.exe;xpsp?res.dll" (without</p>



<i>Criteria Dialog</i>	<i>Description</i>
	<p>quotes)</p> <p>Size criteria</p> <p>This dialog is used to show event logs for shadow files based on their size.</p> <p>The query will return log entries concerning files with the size specified manually in the "minimum" and "maximum" controls. You can alternatively use one of the predefined commonly used sizes by clicking the corresponding checkboxes.</p>
	<p>Time criteria</p> <p>This dialog is used to search for log entries that were produced, or uploaded to the server, at a certain date/time.</p> <p>You can enter any period manually into the "from" and "until" controls, or click one of the most commonly used time ranges settings. You can further specify how these time criteria are stored in the template; this has an influence on how the time criteria you specify will be interpreted if you execute again this query.</p> <p>If you select to save your settings as absolute values, there are considered as unconditional parameters. As an example, a query for all log entries produced between May 21st 2006 and May 23rd 2006 will always return the log entries produced between these two dates.</p> <p>If, on the other hand, you select to store the values as relative ones, those values will be converted to a comparative time span relative to the current date and time.</p> <p>For example, if on May 23rd 2006 at 10:00 you query for entries generated after May 23rd 2006 9:00, and select "relative time", the criterion will be stored as "return all entries generated in the last hour". If you run again this query on June 12th 2006 at 11h30, you will get all entries generated during the last hour, i.e. after June 12th 2006 10h30.</p> <p>If you set the criteria to be stored as relative time and select one of the predefined periods, they are reevaluated each time you run again the query. For example, if on May 23rd 2006 you query for all entries generated "last month", you will get all entries</p>



<i>Criteria Dialog</i>	<i>Description</i>
	generated between April 1st and April 30th. If you set this criteria to be stored as relative time and run the query on August 17th, you will get all entries generated between July 1st and July 31st.

Table 30: How to use the available criteria dialogs

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

Some of them contain predefined settings, notably those related to dates or options; you only have to choose the required parameters from a list. Others are free context dialogs where you can type in what is needed using wildcards to delimit the criterion. For example, if you are using the “File Name” column criterion, you can directly type wind*.* to search for all files matching this pattern (beginning with ‘wind’ and with any extension).

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

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

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

Figure 99: Example of criteria settings



Results window

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

Criteria/Properties panel

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



Figure 100: Filter/Properties panel

Control buttons panel

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

- > View – to see shadow data. See *Viewing Shadowed files* on page 171
- > Save as – to save the *Results Window* data as a CSV file
- > Add devices – to directly manage and add those devices not recognized and shown in the *Results Window*

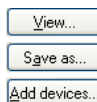


Figure 101: Control button bar

Sorting and applying criteria to specific fields

You can use the *Settings* dialog (see *The Settings dialog* on page 159) to:

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



On the Result Window you can, among other things:

- > Get a list of unsuccessful access attempts to write/read to/from a device
- > See all client error reports
- > See the names and contents of files copied/read to/from devices (only if the Shadow rule applies)

You may or may not see some of these entries. This depends on the role assigned to you by the Enterprise Administrator. See *Defining the Sanctuary Device Control administrators* on page 57 for more details.

For instructions on how to define a query, see *Table 30* on page 163.

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



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

If there are any records that match your query criteria, they appear in the results window list. Query will only return results if you have the corresponding access rights. See *Defining the Sanctuary Device Control administrators* on page 57 for more details.

Available columns

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

Some fields are specific to either central logging or shadowing options while others are common to both of them.

The following table summarizes the column meaning:

<i>Column</i>	<i>Description</i>	<i>Unsuccessful access attempt</i>	<i>Client Error report</i>	<i>Shadowing</i>
Attachment	If true, then a shadowed content can be visualized.	No	No	Yes
Computer	Machine name where the event was recorded.	Yes	Yes	Yes
Device	When available, device class. The	Yes	No	Yes



<i>Column</i>	<i>Description</i>	<i>Unsuccessful access attempt</i>	<i>Client Error report</i>	<i>Shadowing</i>
	device class can be Removable Storage Devices, Floppy, DVD/CD, etc.			
Device Name	Manufacturer's device name.	If available (only for device-attached event)	No	No
Device type	When available, device type. The device class can be Removable Storage Devices, Floppy, DVD/CD, etc.	Yes	No	Yes
File ext.	Contains the extension of the file involved in the access to the device, if any.	Yes	No	Yes
File Name	Contains the name of the file involved in the access to the device, if any.	Yes	No	Yes
File Name (full)	Contains the full name (including path) of the file involved in the access to the device, if any.	Yes	No	Yes
File Path	When relevant, path to the file on the device.	If available	No	Yes
Medium Hash	Unique identifier of the medium (DVD/CD or removable) inserted.	If available (only for DVD/CDs and encrypted media)	No	No
Other	Access mask or DVD/CD serial number. For technical support purposes.	Yes	No	No
Process Name	Process involved in the access to the device.	Yes	No	No
Size	Size of the shadowed file.	N/A	N/A	Yes
Traced On (console)	Date the event occurred on the console computer.	Yes	Yes	Yes
Traced On (endpoint)	Date the event occurred on the client computer.	Yes	Yes	Yes
Traced On (UTC)	Date (Coordinated Universal Time) the event occurred on the client computer.	Yes	Yes	Yes
Transferred On	Date the event record was transferred from the client computer to the SecureWave Application Server.	Yes	Yes	Yes
Transferred On (UTC)	Date (Coordinated Universal Time) the event record was transferred from the client computer to the SecureWave Application Server.	Yes	Yes	Yes



<i>Column</i>	<i>Description</i>	<i>Unsuccessful access attempt</i>	<i>Client Error report</i>	<i>Shadowing</i>
Type	The nature of the event that triggered the log.	No	No	Yes
User	Name of the user who triggered the event (see note after table).	If available	No	Yes
Volume Label	Tag of the volume for which an event was recorded.	If available	No	No

Table 31: Log Explorer module column meaning



If the 'User Name' column is empty for some Shadow records, you will need to use the 'Synchronize Domain Names' command of the 'Tools' menu (or from the Control Panel). If after doing this you still do not see the names, you could try to synchronize (using the same command) directly to the machine's domain where the shadow files were created. It could be a local user who created the shadow files. If in a Novell environment, you should try running the synchronization script.

Viewing access attempts to devices

The *Computer*, *Traced On*, and *Transferred On* fields are always present for every event. You can list the following access event types while activating the filter dialog of the *Type* column:

- > MEDIA-INSERTED: This event occurs when a user inserts a DVD/CD in his drive. Monitoring this event for a given computer informs you what kind of DVD/CD has been inserted in the drive. The following information is normally available:
 - Device type: For example: 'CD'
 - Volume label: Contains the medium tag. Empty for encrypted media insertions.
 - Medium hash: Contains the hash # of the inserted medium (used by SecureWave technical support).
 - Other: Contains the medium serial number (used by SecureWave technical support).



The Sanctuary Client software cannot provide a user name for this event as it is independent from a logged user. It can happen without any logged user or with several of them logged at the same time (remote desktop).

- > **DEVICE-ATTACHED:** This event occurs when a device is connect to a computer. The device name is logged



The Sanctuary Client software cannot provide a user name for this event as it is independent from a logged user. It can happen without any logged user or with several of them logged at the same time (remote desktop).

- > **QUOTA-EXCEEDED:** This event occurs when a user exceeds the daily transfer limit. The following information is normally available:
 - **User Name:** Name of the user who exceeded his quota.
- > **READ-DENIED:** This event occurs when a user tries to access an unauthorized device. The following information is normally available:
 - **Device type:** The device can be a DVD/CD, floppy disk, removable storage devices, COM, LPT, etc.
 - **Volume label:** Contains the floppy disk, DVD/CD or removable device label.
 - **File Name:** Name of the file the user was attempting to read. A backslash indicates that the read attempt was done on the root folder of the medium.
 - **User Name:** Name of the user who tried to access the protected device.
 - **Process Name:** Application used by the user to attempt the access to the protected device.
 - **Other:** Exact access mask in hexadecimal format used by the application to attempt the access to the protected device (used by SecureWave technical support).



Several identical occurrences of this message may appear in the log as some applications, for example Windows File Explorer, may retry automatically when there are unsuccessful access attempts to protected devices. An appropriate setting of the Device log throttling option can reduce significantly the volume of redundant information logged. See the option description on page 238.



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 request 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:** The device can be either a DVD/CD, floppy disk, removable storage devices, COM, LPT, etc.
 - **Volume label:** Contains the floppy disk, DVD/CD or removable device tag.
 - **File Name:** Name of the file the user was attempting to write to the media.
 - **User Name:** Name of the user who tried to access the protected device.
 - **Process Name:** Application used by the user to attempt the access to the protected device.
 - **Other:** Exact access mask in hexadecimal format used by the application to attempt the access to the protected device (used by SecureWave technical support).



Several identical occurrences of this message may appear in the log as some applications, for example Windows File Explorer, may retry automatically when there are unsuccessful access attempts to protected devices. An appropriate setting of the Device log throttling option can reduce significantly the volume of redundant information logged. See the option description on page 238.



System or svchost can execute impersonated mount requests for an encrypted media when the media encryption keys are not present on the client machine. As these request are not identified, the User Name field cannot be retrieved and the corresponding field in the log is empty.

- > **WLAN-BLOCKED:** This event occurs when a WLAN interface is connected to the computer and the WLAN set of rules have been defined for this device. The device name is logged

Viewing client error reports

The *Computer*, *Traced On*, and *Transferred On* fields are always present for every error, other columns are filled in when additional information is available. The following error types can be listed:

- > **SHADOW-BAD-DIRECTORY:** This error occurs when the 'Shadow directory' cannot be created by the Sanctuary Client or the shadow directory is not accessible. See *Shadow directory* on page 241 for information on how to set the directory location
- > **SHADOW-FILE-MALFUNCTION:** This type of error occurs when the Sanctuary Client cannot proceed with the shadowing. You should 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 prevented the writing of a DVD/CD because the format used was unsupported. Please refer to *DVD/CD Supported formats* on page 268 for more details
- > **SHADOW-CD-R-MALFUNCTION:** Sanctuary Client generates this error when it could not carry out the shadowing of a DVD/CD. You should 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 *Chapter 9: Using the Key Pair Generator* in the Setup Guide for explanations 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 not recommended to change the public and private keys in a production environment. If you change the keys in an environment where encrypted media are used, they will have to be formatted and encrypted again using the Media Authorizer.

Viewing Shadowed files

It is recommended that you first filter your data so that only shadowed registers are showing. To do this:

1. Click on the **SETTINGS** button (or on the right part of any heading of any filed).
2. Select the *Attachment* field.
3. Click the **CRITERIA** or ellipsis (...) button.
4. Select *With* and close the dialog by clicking the **OK** button.
5. Click the **EXECUTE** button to close the Settings dialog and create the query.

The files present in the list are an exact copy of those copied/read by the users from/to protected devices when the 'Shadow' rule was in effect. Depending on the selected fields, the registers will show the date the file was copied/read to/from the media (Traced On) and the date the file was transferred to Sanctuary's Database (Transferred On). Sanctuary Device Control also tracks the name of the user that copied the file, the file name (and content), the computer where the copy took place, as well as the device.



Sanctuary Device Control will not open big files (ex. 350 MB) if there are not enough resources available.

Once you list the files, you can right-click on any of them that has the "Attachment" field set to "True" indicating that the full content has been shadowed), and carry out one of these operations from the commands of the contextual menu:

- > *Save as* – Allows you to save the file to a local/network drive.
- > *View* – Permits you to view the contents of the file in a text or binary file internal viewer:

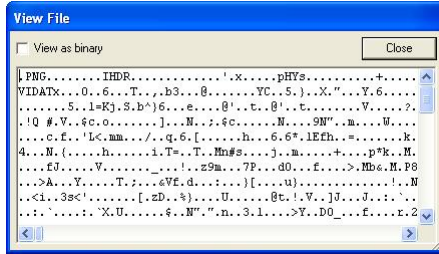


Figure 102: Viewing the content of a shadow file in text form

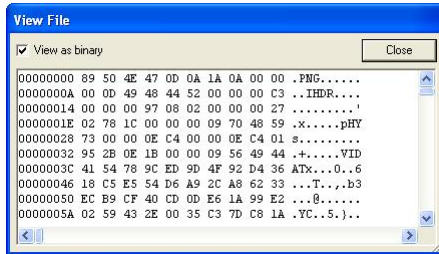


Figure 103: Viewing the content of a shadow file in binary form



Sanctuary Device Control will log the file and administrator name each time a shadowed file is opened. The information is available in the Audit Logs Viewer.

- > **Add device(s)** – Using this option you can include the device(s) to the list of those administrated by Sanctuary Device Control and then grant it all kind of permissions.

You can also do these actions using the Control Button panel located on the lower right part of the main screen.



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. You will only see the name of the file and the "Attachment" field is set to "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/read, the CD image files are interpreted locally and then sent to the server when doing the synchronization. *Appendix A: DVD/CD Shadowing* provides details of how these shadowed files appear in the 'Log Explorer' module.

Forcing an upload of the latest log files

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

To force the immediate retrieval of the latest logs from any client

1. Activate the *Log Explorer* module, if it is not already open. Click on the Log Explorer icon  located in the Modules section of the *Control Panel* of the main window or use the *View→Modules* command.
2. Select *Fetch Log* from the *Explorer* menu or use the *FETCH LOG* button of the dialog. The system prompts you to specify the machine from which



you want to fetch all logs present on the client. You can only fetch logs from those computers that have the Sanctuary client installed.

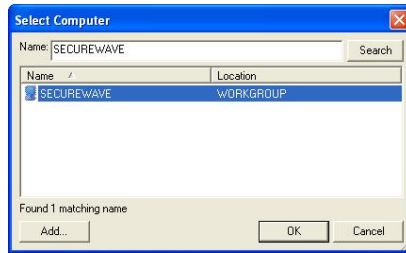


Figure 104. Fetching New Logs

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


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

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



Chapter 6: Using the Audit Logs Viewer

The purpose of the *Audit Logs Viewer* is to display the records of 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. Sanctuary Device Control keeps a full audit trail of all activities carried out by its administrators.

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

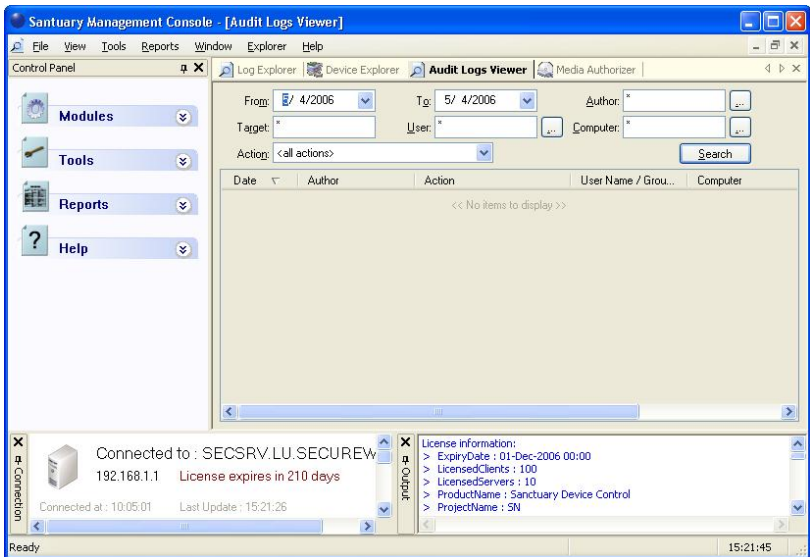



Figure 105: The Audit Logs Viewer main window



If the 'Audit (Device Control)' access of the Sanctuary Management Console Administrator User Access is set to 'No', the currently logged-in administrator is not able to see or use the Audit Logs Viewer module. Please refer to the Defining the Sanctuary Device Control administrators section on page 57 for more details.



To view system administrator activity

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



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

Search options

There are several options you can use to search information in the Audit Log module. They are found on the *Audit Logs Viewer* main window's upper panel.

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

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

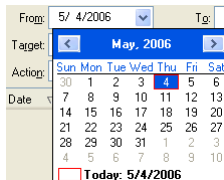


Figure 106: Using the calendar pull-down to select a search date



Sanctuary Device Control Enterprise Administrators have access to all audits. When running under a Windows Active Directory based domain, the Sanctuary Administrator will be only shown audits of computers and users he is allowed to manage. You can use Ctrl+acx.vbs, explained on page 293, to create, view, or modify control rights in the active directory.

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



Figure 107: Using the Author field to do a search

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

The *Target* search field lets you search by the different types of devices available in the system, for example, floppy disk, USB memory stick, DVD, etc. You can type wildcards (* and ?) to limit the search. Using this field not only can you search by devices, but also by User access, Option names, Authorized media names, and Shadow file access.

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

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



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

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

Using the *Computer* field, you can do searches to monitor changes done in certain computers. The names defined here are the same ones used in the *Computer Name* tag of the Windows' *System Properties* dialog.

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

- <all actions>
- ACCESSED SHADOW FILE
- ACCESSED DEVICE LOG
- ADD MANAGED DEVICE
- ADDED MEDIA
- ADDED PERMISSION
- ADDED SCHEDULED PERMISSION
- ADDED TEMPORARY PERMISSION
- AUTHORIZED MEDIA
- AUTOMATIC USER ACCESS UPGRADE
- DELETED DEFAULT OPTION
- DELETED OPTION
- MODIFIED SCHEDULED PERMISSION
- MODIFY USER ACCESS
- PURGED DB AND FILE STORAGE
- REMOVE MANAGED DEVICE
- REMOVED MEDIA
- REVOKED PERMISSION
- REVOKED SCHEDULED PERMISSION
- REVOKED TEMPORARY PERMISSION
- SET DEFAULT OPTION
- SET OPTION
- UNAUTHORIZED MEDIA
- UPDATED MEDIA
- UPDATED PERMISSION
- UPLOADED SHADOWS


Figure 108: Using the Action field to do a search



All fields act interactively: When you change one of them, it does a logical AND with all the others. If, for example, you select a range of dates and then an action, the resulting data will be the Boolean combination of the dates plus the action.

Actions

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

- > Change the size of the displaying field to suit your needs. You must place the cursor in the dividing trace and wait until the mouse cursor changes into a double head arrow: 



- > Sort the list in any order by clicking on any of the column headers. Click once to sort ascending, twice to get a descending order

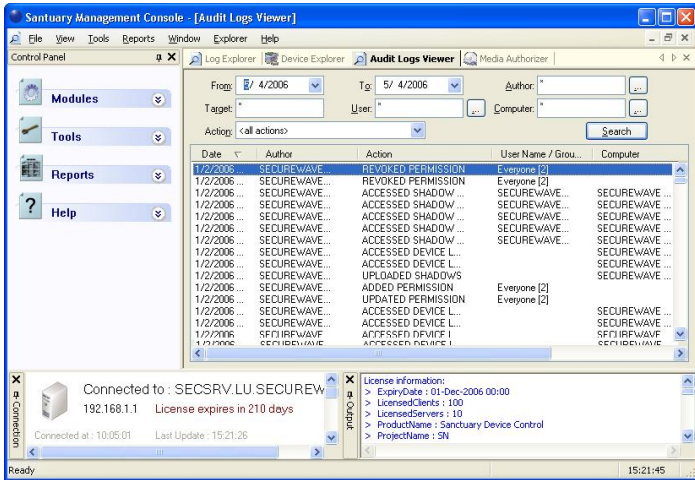


Figure 109: Using the sorting facilities of the Audit Logs Viewer module

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

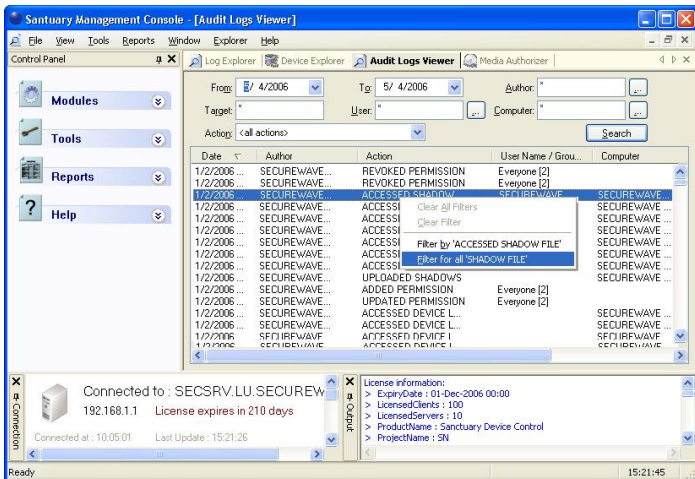


Figure 110: Filtering actions in the Audit Logs Viewer module



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



Figure 111: A filtering pop-up dialog example

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

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

The Audit log viewer contains the following columns:

<i>Column</i>	<i>Description</i>	
Date	Informs you of the date when the administrator did the action. This field is always present.	
Author	Contains who created the action. This field is always present.	
User name/group name	Name of the user or group to which the action was applied.	
Computer	Computer name of the machine that was the target of the action, if any. It is empty if a modification was made to the 'default setting'. Contains the name of the computer in case a computer-specific action was done.	
Target	This field is filled with the device for which the permission modification applied (DVD/CD-Rom, floppy, removable storage devices...). When using the Target field you get a different set of information than that normally received for a device. See the Target field description on page 177 for a detailed review of what you can see when using this option.	
Information	Additional information related to the corresponding register (if applicable). This field shows more details in some cases. For example, if a Sanctuary Administrator erases a scheduled permission, its parameters are included here.	
Action	A code describing the action performed by the administrator. This field is always present. Actions may be:	
	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 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.



Column	Description	
	ADDED PERMISSION	This action corresponds to the adding of a permission in the Device Explorer, the information available is: user, machine, device, read/write, priority.
	ADDED SCHEDULED PERMISSION	The fields available are: user, machine, device, read/write, begin time, end time, weekdays.
	ADDED TEMPORARY PERMISSION	The fields available are: user, machine, device, read/write, begin time, 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 Sanctuary Management Console 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 will lose his implicit Enterprise Administrator privilege, which means he may block himself out. To prevent that from happening, the SecureWave Application Server will make this user an Enterprise Administrator explicitly, a message will be displayed on screen and the user name and role will be traced. See also <i>Defining the Sanctuary Device Control administrators</i> on page 57.
	DELETE DEFAULT OPTION	Whenever a default option that applies to all the machines is deleted (in the <i>Tools</i> → <i>Default Options</i> menu), the option and the user/machine are traced.
	DELETED OPTION	Whenever an option specific to a machine is deleted, the option and the user/machine are traced.
	MODIFIED SCHEDULED PERMISSION	The fields available are: user, machine, device, read/write, begin time, end time, weekdays.
	MODIFY USER ACCESS	When changes are made to the Sanctuary Device Control 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 MANAGED DEVICE	This event corresponds to the removal of a device from the list of managed devices, the device name is logged.
	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 fields available are: user, machine, device, read/write, begin time, end time, weekdays.
	REVOKED TEMPORARY	The fields available are: user, machine, device, read/write, begin time, end time.



<i>Column</i>	<i>Description</i>	
	PERMISSION	
	SET DEFAULT OPTION	A default option is one that applies to all the machines. Whenever a change is done by the administrator to one of these options (by using the <i>Tools → Default Options</i> menu), the option being changed and the user/machine are traced.
	SET 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 32. Audit Logs Viewer Result Information



Chapter 7: 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, which includes flash memory devices, zip drives, etc.

Introduction

You can use the Media Authorizer for three main purposes:

- > Adding individual CDs, DVDs, and removable storage devices onto the system database and then granting permission to use them to users who would otherwise be barred by the defined policies. Each removable device is encrypted to suit your security preferences
- > Centrally data encryption of flash memory sticks that are used outside the organization. An effective way to protect your data in case the device is lost or stolen. This method is used when the user is going to access the device in a computer where there is no Sanctuary Client installed
- > Data encryption for removable devices used in-house on those computers where the Sanctuary client is installed



The Sanctuary Client must be installed on the machines where the Sanctuary Device Administration tools are used to perform encryption and authorization of multi-session DVDs/CDs.

The general process we recommend to 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 cannot grant access permissions to Novell accounts – assigned by clicking on the Add User button.


Although it is advisable to have a Microsoft Certificate Authority installed in your network for security reasons, a user that has the physical encrypted medium, its associated key, password, and permission to access the removable device class, can access the encrypted data without the need of one.



You may have problems decrypting those keys already encrypted using older version of Sanctuary Device Control. Older versions of the Sanctuary Application Server (SXS) did not store the media keys encrypted using user certificates. Instead, clients would request those of currently plugged media, which is not suitable for the new differential update schema available in this version: storing the media keys encrypted with user certificates and sending the encrypted media keys to all the clients differentially. SXS 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 the Setup Guide), defaulting to 180 minutes (three hours). This certificate "refresh" mechanism ensures that when a Sanctuary installation is upgraded, media keys will be created and communicated to clients. It also ensures that if some user certificate expires, SXS will detect them and use a new one when it becomes available.

You can also use our *Easy Exchange* schema to encrypt a device and being able to access it on computers that do not have the Sanctuary Client installed. The user would not need to install any program or have administrative right. See *Easy Exchange* on page 226 for more information. This schema is also used when doing decentralized encryption on removable storage devices. Please see *Decentralized encryption* on page 189 for more information.



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

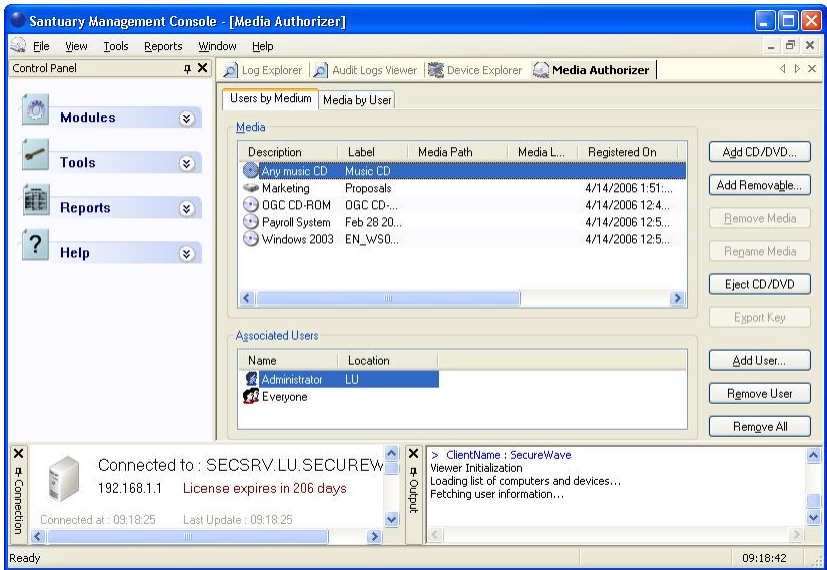


Figure 112: The Media Authorizer main window



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 will see 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 will need to grant the administrator permission to access the DVD/CD in Read or Read/Write mode. If you do not grant this access, 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 is generic Music CDs.



Since Movie DVDs behave as DVD-ROMs, their treatment differs from the procedure used for Music CDs. You need to authorize every 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 is installed' and the ADD REMOVABLE button is disabled. It is not possible to calculate the signature of multisession DVDs/CDs when the SecureWave Client Driver is not installed on the Sanctuary Management Console machine. The Media Authorizer module is significantly slower when the Sanctuary Client 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 Media Authorizer module. Be sure to grant the required permissions to at least read the DVD/CD.
2. Click the ADD CD/DVD button. You are prompted to insert a DVD/CD.
3. Insert the DVD/CD.

The Media Authorizer calculates a unique cryptographic signature of the DVD/CD and displays its label:

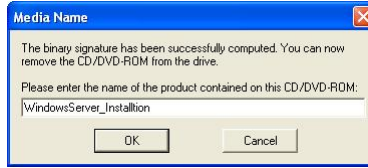


Figure 113: Adding an encrypted DVD or CD

This name is used to register this DVD/CD on the system. You can change it if you need to make it more meaningful.

4. 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

Introduction

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. The encryption is used to achieve two goals:



- > To ensure tamper-proof device identification by associating the identifier of a device with its encryption key
- > To prevent access to the data stored on the device when the device is attached to a computer not protected by Sanctuary Device Control

AES (Advanced Encryption Technology) 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 provides a transparent access to the media. Data copied to the media is encrypted/decrypted transparently upon media access.



Users who have not received access to the encrypted media are not able to read its content (not even the Sanctuary Device Control Administrators).

There are two steps to follow 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 8: Accessing encrypted media outside of your organization* on page 211 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 *Appendix B: Installing a Certificate Authority* on page 279 for more details
- > The Sanctuary Client must be installed on the machines where the Sanctuary Device Administration tools are used to perform encryption

 *You should make sure 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 93 for more details on how to set device permissions.*

Decentralized encryption

The Media Authorizer module is not used to do distributed encryption; it is only valid for a centralized schema. However, decentralized encryption is done using the *Easy Exchange* method (see *Removable device encryption methods comparison* on page 193 and *Easy Exchange* on page 226), one of the proposed solutions to centrally cipher a removable storage device. Please see *Decentralized encryption* on page 231 for a full description on 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 could be denied when trying to read or write to an encrypted removable storage device. This happens 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 address this problem:

1. The user logs off and logs on again, forcing the system to mount the device.
2. The user can unplug and re-plug the device.



3. The user can remove the media from the reader, try to access the media with Windows Explorer and re-insert 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. The USB DiskOnKey devices, for example, are not subject to this limitation.

- > The Sanctuary Client must be installed on the machine where the Sanctuary Management Console is installed
- > It is not possible to define read-only permissions on encrypted media
- > Memory card readers integrated to cameras, printers, or scanners may not work properly if encrypted
- > In case of using memory sticks, they should only have one unique partition



The users do not need to be assigned permissions to the Removable Storage Devices class in the Device Explorer 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 might also map this same volume letter to a Novell's server folder. If you are trying to access a removable device in a Novell system, you may need to assign another letter to it via 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 226 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 the device. 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 114: Adding a specific removable storage device

4. In the *Add Removable Media* dialog, choose the letter corresponding to the *Drive* that 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 (upper and lower case letters and digits).

 *We strongly recommend that you apply a physical label (sticker, note, mark) to every encrypted device in order to distinguish them easily. This sticker should ideally have the label or part of the description written 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, it will ease the administrator's work in identifying the device and why the user cannot access it.*

 *Users will not be able to 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:

<i>Method</i>	<i>Description</i>	<i>Notes</i>
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, will be 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. Consequently, a malicious user might use a data recovery tool to read the sectors and thus gain access to potentially sensitive data. This also applies when sensitive data has previously been deleted – it may still be recoverable. We therefore recommend – generally speaking – this encryption mode to be only used when the device has never had any sensitive data, or the device 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 installed.	

Table 33: 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 34*, *Table 38*, *Table 39*, 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:

<i>Method</i>	<i>Advantages</i>	<i>Disadvantages</i>	<i>Comments</i>	<i>Limitations</i>
Quick Format	<ul style="list-style-type: none"> > It is very fast 	<ul style="list-style-type: none"> > Existing data is lost > The device's sectors are not encrypted > The user needs to use the device in a computer where the Sanctuary client is installed or where our SADEC tool can be installed > Should be used only in fully, wiped, formatted devices 	<ul style="list-style-type: none"> > A malicious user can still recover the previously erased files > If the user is using the removable media in a machine where Sanctuary client is installed, the encryption key is not needed – only the password 	<ul style="list-style-type: none"> > Is based on partitions > 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.
Full & Slow	<ul style="list-style-type: none"> > Data already stored in the device is not lost > All sectors are encrypted 	<ul style="list-style-type: none"> > May take a long time to finish in large capacity devices > The user needs to use the device in a computer where the Sanctuary client is installed or where our SADEC tool can be installed 	<ul style="list-style-type: none"> Use on any kind of device that needs solid encryption; if the user is using the removable media in a machine where Sanctuary client is installed, the encryption key is not needed – only the password 	<ul style="list-style-type: none"> None; the format is not lost, only data is encrypted
Easy Exchange	<ul style="list-style-type: none"> > It is very fast > The user has access to the device's 	<ul style="list-style-type: none"> > Existing data is lost > Device's sectors are not encrypted 	<ul style="list-style-type: none"> The user does not needs administrator's rights to use the device, only the password and the 	<ul style="list-style-type: none"> > Limited to devices ≤ 4GB since FAT16 is used. > Typically used



<i>Method</i>	<i>Advantages</i>	<i>Disadvantages</i>	<i>Comments</i>	<i>Limitations</i>
	data even in computers where Sanctuary client is not installed > No need to install software to use the device		encryption key. If the device is used in a system that has the Sanctuary client installed, the administrator should also grant access to this device.	for USB memory keys but can be used for any device recognized as a removable > Since the encryption is volume based, you can divide the whole available space in 4 GB partitions

Table 34: Encryption methods comparison

See also *Table 38* and *Table 39* for more details.

Possible error messages when 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 having a Certificate Authority installed* on page 209). 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:

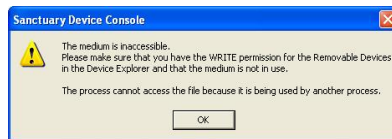


Figure 115: 'Inaccessible medium' error message

- > 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 93 for more details on how to set device permissions

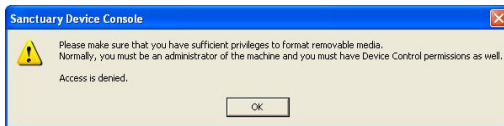


Figure 116: 'Not enough privileges' error message

- > If the device has already been encrypted, you will get the following message.

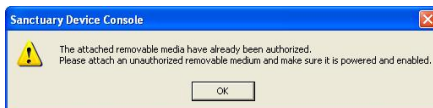


Figure 117: 'Already authorized' error message

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 118: '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 Device clients 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 218

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 217.

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:

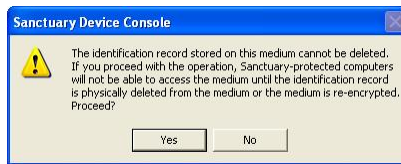


Figure 119: 'Identification record cannot be deleted' error message

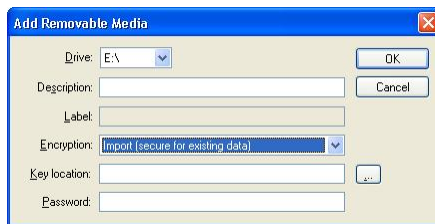


Figure 120: Importing back an already encrypted device



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.

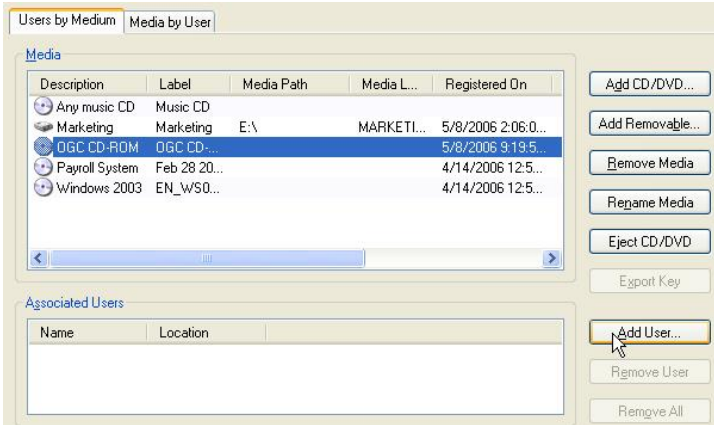


Figure 121: A specific medium with its related users and groups

3. Click the Add User button. The *Select Group, User, Local Group, Local User* dialog is displayed.

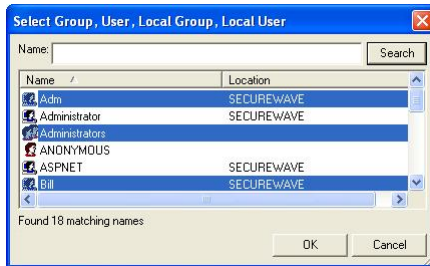


Figure 122: Adding a group or user to a selected medium

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. 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.

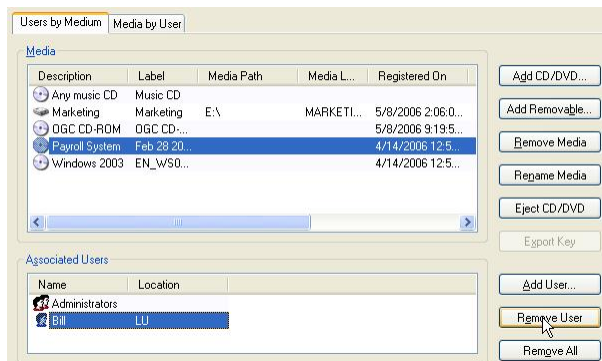


Figure 123: Denying access to DVDs/CDs/encrypted removable media

4. Click REMOVE USER.



If you want to remove all users, simply select the device and click REMOVE ALL.

Users are removed from the list of *Associated Users*, preventing them from accessing the selected media.



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 NOT downloaded at user logon. If a computer is disconnected from the network, the user will only have access to those DVDs/CDs/removable media for which permissions were granted AND were used at least once when the machine was connected to the company network. The



administrator can also export the settings and import them on the client side.

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.

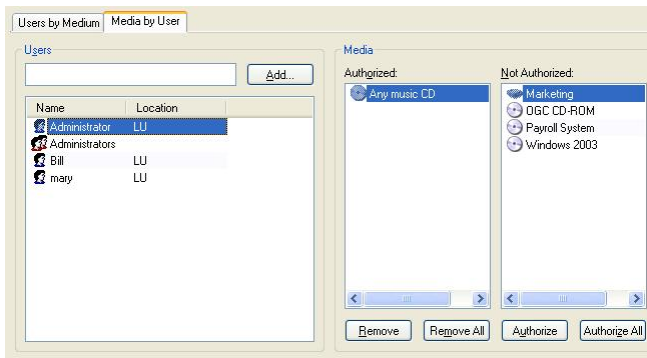


Figure 124: Media by user authorization

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**. 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 from 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 NOT downloaded at user logon. If a computer is disconnected from the network, the user will only have access to the DVDs/CDs/removable media for which permissions were granted AND were used at least once when the machine was connected to the company network. The administrator can also export the settings and import them on the client side.



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:

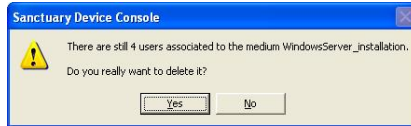


Figure 125: 'Users still associated with medium' warning message

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.

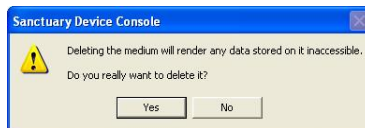


Figure 126: 'Deleting medium' warning message



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:

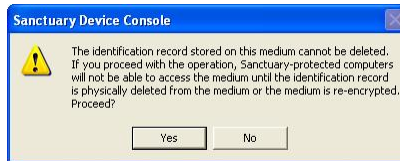


Figure 127: 'Cannot delete identification record' error message

The physical media remains encrypted. As there are no permissions anymore for these devices in the system, the Sanctuary Device clients will consider them as encrypted media coming from other organizations and will prevent 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 218.

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 217
- > Reuse the device and re-encrypt it. This operation will erase 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 Sanctuary Client 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.

More 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/removable storage device
- > Export an encryption key
- > Eject a DVD/CD drive

To rename a DVD/CD/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 128: Renaming a DVD/CD/Removable storage device

4. Confirm or type a new description for the media. Use the **GET DEVICE LABEL** button to recuperate 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 217. 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 134).

1. On the *Users by Medium* tab, select an encrypted removable storage device.
2. Click EXPORT KEY. A dialog is displayed.

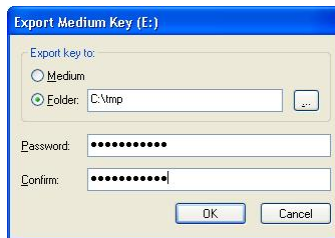


Figure 129: Exporting a medium key

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.

Permissions Priority

Permissions to access DVD/CD and Removable Storage Devices can be defined in the Device Explorer and the Media Authorizer. This section explains how the Sanctuary Client will control access when permissions are defined in both modules.

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 levels. Note that in this example, permissions can be assigned directly to user Bill or to the user groups he belongs.

<i>Device Explorer DVD/CD access defined for user Bill</i>	<i>Permission defined in Media Authorizer for user Bill to 'OfficeXP'</i>	<i>Resulting access when Bill inserts 'OfficeXP' in his drive</i>	<i>Resulting access when Bill inserts any other CD in his drive</i>	<i>Comments</i>
No access is defined (default)	Access granted to 'OfficeXP'	Yes	Denied	When nothing is defined in 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 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 precedence on Media Authorizer permissions, the access to the DVD/CD drive has been specifically denied.
	No access to 'OfficeXP'	Denied	Denied	

Table 35: Resulting access when permissions are defined at the Device Explorer and at the Media Authorizer levels (example 1)



If a user already has permission to use the DVD/CD-ROM drive assigned in Device Explorer, assigning permission to use specific DVDs/CDs in the Media Authorizer has no further effect.

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 levels:

<i>Device Explorer Removable Storage Devices access defined for user Bill</i>	<i>Permission defined in Media Authorizer for user Bill to 'DiskOnKey8'</i>	<i>Resulting access when Bill connects 'DiskOnKey8' to his computer</i>	<i>Resulting access when Bill connects any unencrypted removable storage device</i>	<i>Comments</i>
No access is defined (default)	Access granted to 'DiskOnKey8'	Read/Write	Denied	Even though nothing is defined in 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 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 has 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 has the encryption key nor the password	Denied	Read/Write	



<i>Device Explorer Removable Storage Devices access defined for user Bill</i>	<i>Permission defined in Media Authorizer for user Bill to 'DiskOnKey8'</i>	<i>Resulting access when Bill connects 'DiskOnKey8' to his computer</i>	<i>Resulting access when Bill connects any unencrypted removable storage device</i>	<i>Comments</i>
	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 has the encryption key nor the password	Denied	Denied	
	No access to 'DiskOnKey8'. The user has the encryption key and password	Denied	Denied	

Table 36: Resulting access when permissions are defined at the Device Explorer and at the 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 *Default Permission priority* on page 110 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 having a Certificate Authority installed

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 Device Control 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 93 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 187.
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. Who can use the key? You need to set permissions Read or Read/Write in the *Unauthorized Encrypted Media* class using the *Device Explorer* module so that your users can access this key. Only users with permissions defined in this class will be able to access the encrypted device, providing they also have 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 9: Setting and changing options on page 233 for more information on how to do this.



Chapter 8: 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.

The Sanctuary Device Control 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 will be directly linked to the media password complexity

Exporting encryption keys centrally (by the administrator)

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 213 and *To export the encryption key to the device itself* on page 215 for details.

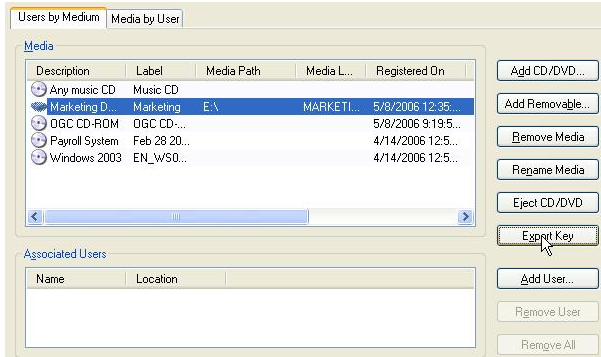


Figure 130: Exporting encryption keys

Exporting encryption keys locally (by the user)

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 received the privilege to do so by means of the permissions dialog (see *Using the permissions dialog* on page 93 for more details).

There are three conditions that need to be met in order for a user to export a medium encryption key locally:

- > The user must have received proper access to the media. Please refer to *Chapter 7: Using the Media Authorizer* on page 183 for more details on granting user access to encrypted media
- > The media must be attached to the user's computer
- > The user must be logged on a computer with the permissions set to *Export To file* or *Export to media*. Please refer to page *Special case: working with the Removable Storage Devices class* on page 96 for more details

If those three criteria are met, then the *Export medium key...* entry is available in the context menu of the encrypted drive in Windows Explorer. Therefore, the user can export its 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 213 and *To export the encryption key to the device itself* on page 215 for details.

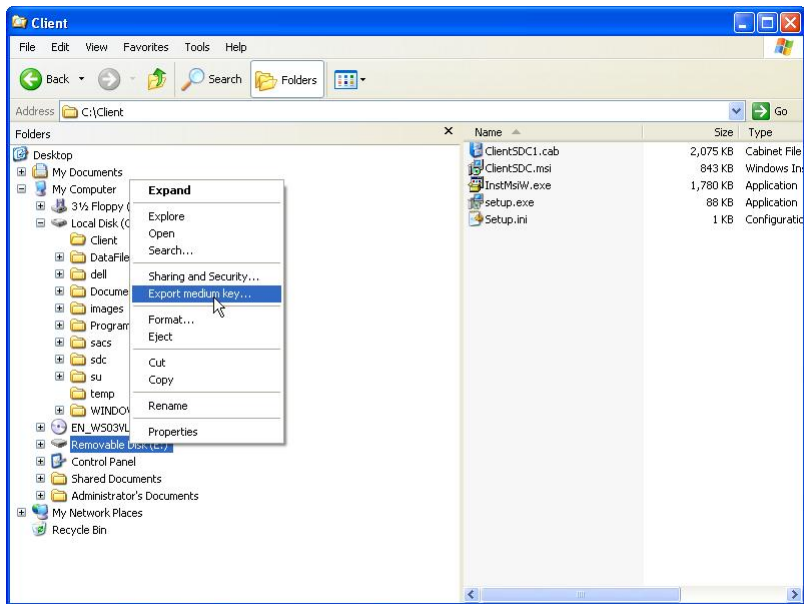


Figure 131: Exporting encryption keys (by the user)

To export the encryption key to a file

This 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 Device Control administrator who does this; see *Exporting encryption keys centrally (by the administrator)* on page 211 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 (by the user)* on page 212 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 132: The 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 239. This option does not apply for administrators performing central export.



If the Sanctuary Device Control Administrator has set the option Encrypted media password (see page 239) to 'Require Password complexity', the password chosen by the user when doing a local export must 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 (!@#%...)*

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. 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 to access the data will be directly linked to the device password complexity.

In the case of a central encryption key export, it is the Sanctuary Device Control administrator who does this; see *Exporting encryption keys centrally (by the administrator)* on page 211 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 (by the user)* on page 212 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 133: The 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 239. This option



applies for local (done by the user), not for central (done by the administrator) export of key to media.



If the Sanctuary Device Control Administrator has set the option to Require Password complexity, the password must 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 (!@#%...)*

4. Click OK.
5. The user will need to 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.

Scenarios for accessing encrypted media from outside your organization

The various scenarios and options for accessing media outside of your organization are discussed in this section.



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 that has Sanctuary Client installed

This is typically the case when two separated organizations protected by Sanctuary Device Control want to exchange data on a Sanctuary Device Control encrypted media.

Unauthorized Encrypted Media is defined as media encrypted using Sanctuary in another organization with a separate implementation of Sanctuary Device Control.



You can let your Sanctuary Device Control Administrators centrally control and authorize the 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 Device Control 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, will not be able to 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 he grants user access to it.

To add a device in the Media Authorizer

1. Attach the device to your administrator computer. This computer should 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 187 for more details.
2. Using the Media Authorizer, click ADD REMOVABLE. The following dialog appears:

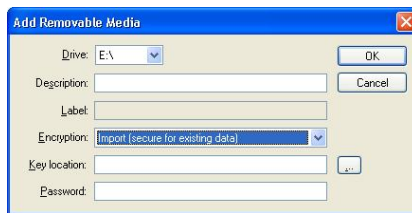


Figure 134: Adding a device in the Media Authorizer (the key is external)

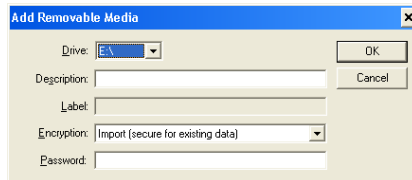


Figure 135: Adding a device in the Media Authorizer (the key resides on the medium)



3. Type the media *Description*. We strongly recommend that a physical label be applied on the device to assist its identification.
4. In the *Encryption* field, choose to import the encrypted device (this is 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 197 for details.

Locally managed access to ‘unauthorized encrypted media’

You may want to delegate trusted users the right to access Sanctuary Device Control encrypted media coming from other organizations. This permission is controlled by the means of the *Removable Storage Devices* class of the Device Explorer. Please refer to *Chapter 4: Managing permissions/rules* on page 93 and *To assign computer-specific permissions to users and groups* on page 112 for more details on how to set permissions.

You can set the following permissions:

- > Scheduled and Temporary permissions to restrict access to the *Removable Storage Devices* for a given time frame
- > Offline and online permissions: 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 can be defined as a Global permission (Default Settings section) or at the computer-specific level (Microsoft Windows Network section) allowing you to restrict the access to these devices on specific computers



- > The permission can be Read-only or Read/Write. If a permission is read-only, your users will only be able to read the content of the unauthorized encrypted media
- > Negative permissions ('None'), can be defined allowing you to specifically deny the 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 *Default Permission priority* on page 110.

To access unauthorized encrypted media from other organizations, your user needs the following:

- > The right permissions in the *Removable Storage Devices* class
- > The encrypted device 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 by following this procedure:

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.

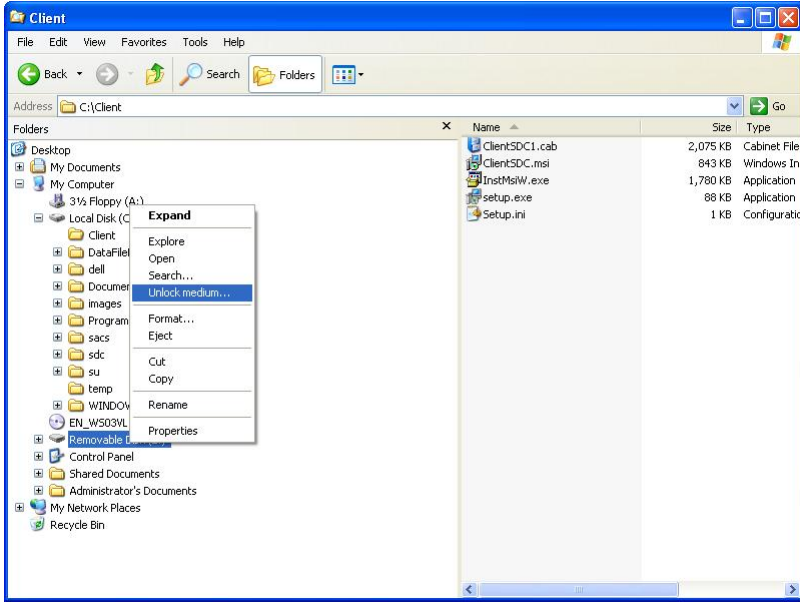


Figure 136: Accessing unauthorized encrypted media

The *Import Medium Key* dialog is displayed.

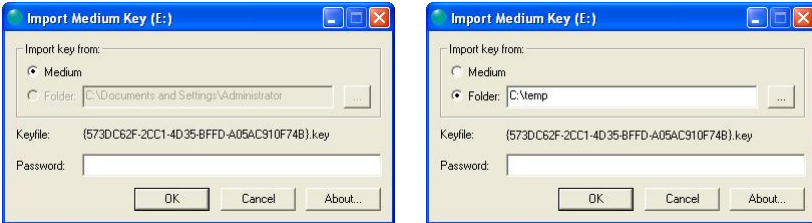


Figure 137: The *Import Medium Key* dialog (import from medium or folder)

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 will be 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.

Differences between locally and centrally managed access to Unauthorized Encrypted Media

The centrally managed access to unauthorized devices has the following characteristics:

- > The media, its encryption key, and password have to be provided to the Sanctuary Device Control 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; temporary / scheduled / permanent access to the Unauthorized Encrypted Media class. He can control when and how unauthorized encrypted media will be accessed but he has no control over which device will be accessed. This control is delegated to the user
- > The administrator can grant users or user groups access to the Unauthorized Encrypted Media class, 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 (Microsoft Windows Network 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 add an externally encrypted device (Import) 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:

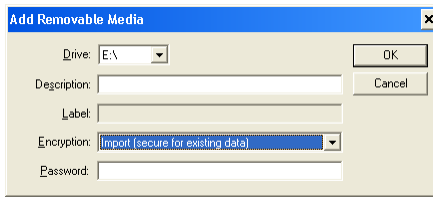


Figure 138: Importing an external device

4. Select the *Import (secure for existing data)* option from the list. Type the password.

The medium is added to the database and appears now 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 139: 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** 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:

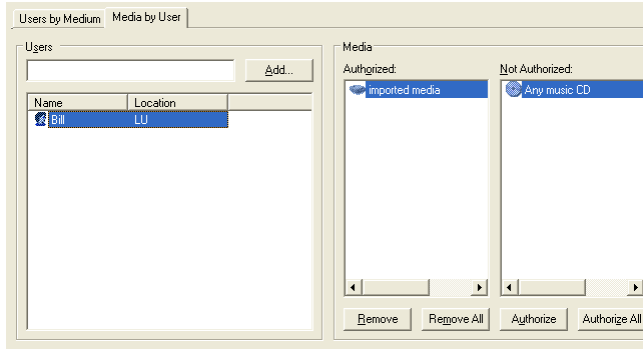


Figure 140: Importing an external device

Accessing media in a machine that does not has the Sanctuary Client installed

This is typically the case when encrypted devices are exchanged between a company protected by Sanctuary Device Control and a machine outside the organization that do not has the client installed.

To access an encrypted device on machines where the Sanctuary Client is not installed, a user has two alternatives:

- > Use the Sanctuary Device Control *Stand-Alone Decryption Tool*
- > Encrypt using the *Easy Exchange* encryption option

Both options are explained in the following subsections.



Sanctuary Device Control Stand-Alone Decryption Tool

Requirements

To use the Sanctuary Device Control Stand-Alone Decryption Tool, the user needs the following:

- > The Sanctuary Device Control Stand-Alone Decryption Tool installed on his computer. This tool can be found on the Sanctuary Device Control CD under the SADEC folder, or it can alternatively be downloaded from the SecureWave web site at:

<http://www.securewave.com/sadec.jsp>



The Sanctuary Device Control Stand-Alone Decryption Tool cannot be installed on computers protected by the Sanctuary Client.

Please refer to the SADEC.pdf guide on the Sanctuary Device Control media for details on how to install the Sanctuary Device Control Stand-Alone Decryption Tool.



The Sanctuary Device Control Stand-Alone Decryption Tool can only be installed on Windows 2000, Windows XP Professional, Windows XP Home Edition, and Windows 2003.

- > The encrypted device attached to his computer
- > If the disk encryption key is not stored on the device, the user needs the encryption key file
- > The password to access the device

To use the 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. Install the Sanctuary Device Control Stand-Alone Decryption Tool.
2. Attach the device to the computer.
3. In Windows Explorer, select the *Unlock medium* option from the right-click (contextual) menu of the encrypted drive.

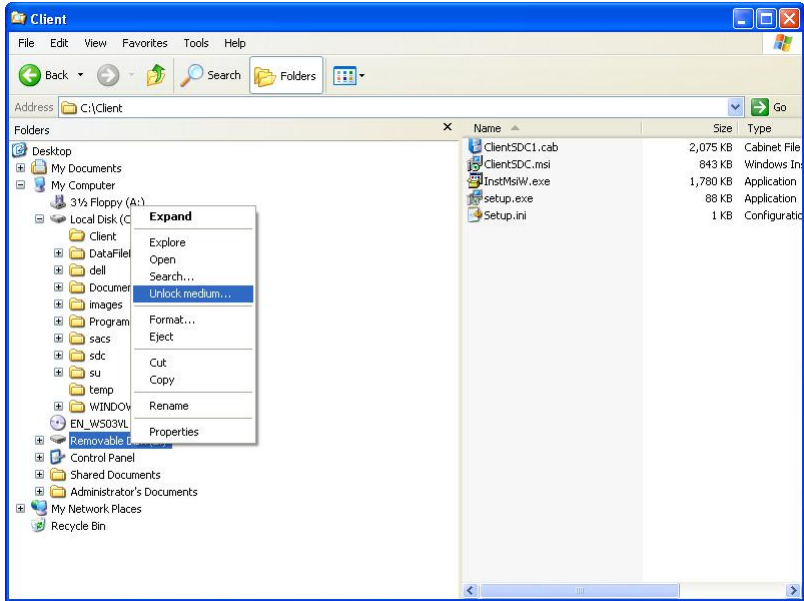


Figure 141: Using the Stand-Alone Decryption tool

The *Import Medium Key* dialog is displayed:

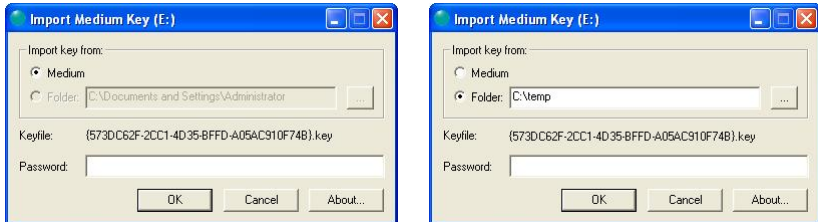



Figure 142: The Import Medium Key dialog when using the Stand-alone decryption tool

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 ellipsis 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 will be 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 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 190 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. Export the key to the medium itself or to a folder providing a password in the process. You need to change the *Encrypted media key export* option in the *Default Options* dialog to *To media or file*.

Once you encrypt the medium this way, the user can transport it safely to another machine. When inserting the medium and running the included 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:

<i>Key's action</i>	<i>Key's location</i>	<i>To access the medium the user must</i>	<i>Notes</i>
Key Exported	To 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.
	To 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 37: Easy Exchange encryption options

In both cases, and only if the user has the correct elements (password plus key), an explorer is shown from where all file extract, add, or remove operations are done:

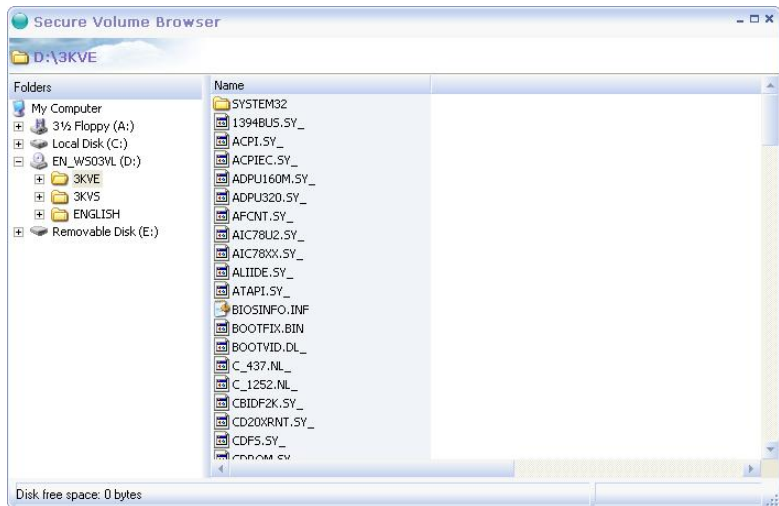


Figure 143: Sanctuary's Secure Volume Browser



The behavior and functionality of this browser is equivalent to Windows Explorer:

- > Copy & paste
- > Multiple selection
- > Contextual 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 the need to install any kind of software whatsoever, and without having administrative privileges. This program 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 will look on the path specified by the -t parameter

If SVolBro.exe is called using another program, all required parameters (password, path of the encrypted folder, and encryption key location) will be transparently interchanged if provided.



You should instruct your 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 since Windows do not has the chance to write them from temporary memory to the volume. You should also insist that they ought to close the 'Secure Volume Browser' window before unplugging the device.



Strong password policy is always enforced for the "Easy Exchange" schema. The password shall be 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 SVolBro.exe interface. Any of the other methods proposed by SvolBro.exe are valid (copy and paste, drag and drop, etc.).



Using encryption within and outside your organization

The following two tables summarize several scenarios while using the Full Encryption or Easy Exchange methods inside and outside your company and depending if Microsoft Certification Authority is installed or not.

	<i>Full Encryption</i>			
	<i>(MS Enterprise CA is installed)</i>		<i>(MS Enterprise CA is not installed)</i>	
	<i>Access to the medium</i>			
	<i>Granted</i>	<i>Not granted</i>	<i>Granted</i>	<i>Not granted</i>
Used within the organization's network (Sanctuary Client 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.	There is a message informing the user that the device is not accessible.	There is a message informing that the device is not accessible. The medium can be unlocked using the right click contextual menu if the user knows the password and has the public encryption key.	There is a message informing the user that the device is not accessible.
Used outside the organization's network (Sanctuary Client is not installed)	The user cannot read data; only garble information is seen.			
Measures for accessing data outside of the network	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 38: Full Encryption method inside and outside your company



	Easy Exchange			
	(MS Enterprise CA is installed)		(MS Enterprise CA is not installed)	
	Access to the medium			
	Granted	Not granted	Granted	Not granted
Used within the organization's network (Sanctuary Client 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.	There is a message informing the user that the device is not accessible.	There is a message informing the user that the device is not accessible. The medium can be unlocked using the right click contextual menu if the user knows the password and has the public encryption key.	There is a message informing the user that the device is not accessible.
Used outside the organization's network (Sanctuary Client is not installed)	The device includes a copy of SVOLBRO.EXE (Sanctuary Volume Browser), no data is available.			
Measures for accessing data outside of the network	The user must start SVOLBRO 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 39: 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 wants to control device encryption centrally using the Authorization Media 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; this can be let to the users themselves or to a designated agent.

Once administrators have set the rules, users are now on their own. These rules can be defined at different levels:

- > At the class level: all data that a user copies to a removable device must be encrypted
- > At the model level: the data a user copies to certain types of devices must be encrypted



- > At a specific, uniquely identified device: anything a user writes to a particular serialized removable media must be encrypted

This feature is backed-up by the Sanctuary Volume Browser tool (SVolBro) allowing access to the device on unprotected machines. There are several important points regarding SVolBro:

- > It is stored on the removable media itself
- > It does not requires any driver at all
- > It does not requires administrative rights
- > It does not makes the USB key be 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 is a mere 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. Please refer to the *Easy Exchange* section on page 226 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 134 for more information, examples, and a step by step guide on how to set decentralized encryption.



Chapter 9: Setting and changing options

There are various options that you would not want to change very often but enable you to tailor *Sanctuary Device Control* to suit you and your organization.

You can change these options either for a specific computer or for the general Sanctuary Client behavior:

- > USB Key Logger
- > Device Control Status Window
- > User Notification
- > Shadow File Upload Delay or Time
- > Shadow Directory
- > SecureWave Application Server Address
- > Encrypted Media Key Export
- > Encrypted Media Export Password
- > Certificate Generation
- > Centralized Device Control Logging
- > Suppress Recurring Log Events
- > Send endpoint maintenance "tickets" to selected computers/users
- > Change log settings

You can find a detailed description of each option and instructions on how to change them in the following sections.



Changing options will not generate a popup window on the client icon informing the user of these modifications.



Changes from previous 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:

<i>New name</i>	<i>Old name (version 3.x or previous)</i>
Certificate Generation	Certificate Generation
Client Hardening	Client Hardening
Device Log	Centralized Device Control Log
Device Log Throttling	Suppress Recurring Log Events
Encrypted Media Password	Encrypted Media Export Password
Log Upload Delay	**
Log Upload Interval	**
Log Upload Threshold	**
Log Upload Time	**
Sanctuary Status	Device Control Status Window
Server Address	SecureWave Application Server Address
Shadow Directory	Shadow Directory
Update Notification	User Notification
USB Keylogger	USB Keylogger
*	Shadow File Upload Delay
*	Encrypted Media Key Export
* discontinued	
** new	

Table 40: Option name comparison

Default options

Sanctuary Device Control allows you to set default options for various aspects of the Sanctuary Client 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*).

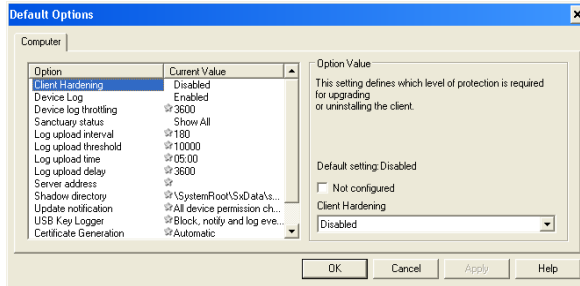



Figure 144: The Default Options dialog

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 Device Explorer 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 Device Explorer, and selecting *Options*.

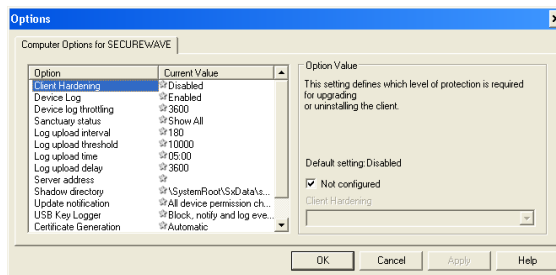




Figure 145: Setting computer-specific options



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 Device Explorer, 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 Device Explorer 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 encrypted media. See *Appendix B: Installing a Certificate Authority for Encryption* on page 279 for more details. If a user has no certificate, the Sanctuary Client driver will automatically create one – using `ntofity.exe`. This option allows you to disable this automatic behavior.

The possible settings are:

- > *Automatic* – (default value) The Sanctuary Client driver will automatically create a certificate for those users that do not have one
- > *Disabled* – The Sanctuary Client driver will 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, he will not be able to access Device Control encrypted media – even if the permission has been granted.

Client hardening

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

You can choose from these settings:

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





Use the *Endpoint Maintenance* command to send maintenance "tickets" to selected computers/users (see *Endpoint Maintenance* on page 49 for more information).

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 151 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.*

 *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 'Centralized Device Control Logging' 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 frame 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.



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.

Encrypted media password

This 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



This option only applies when the 'Export to File' and/or 'Export to Media' option of the removable class permissions is also used.

Log upload threshold

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

Log upload delay

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



Log upload interval

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

Log upload time

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

Sanctuary status

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

- > *Do not Show* – The Sanctuary Client icon is not displayed
- > *Show All* – (default value) The Sanctuary Client icon is displayed. All information is shown to the client user
- > *Show All without Shadow* – The Sanctuary Client icon is displayed. All information except shadowing details can be viewed
- > *Show Allowed* – The Sanctuary Client icon is displayed. Only the information about those devices allowed for the client can be viewed
- > *Show Allowed without Shadow* – The Sanctuary Client 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 he/she, or the group he/she belongs, has permissions.



Server address

This option defines the IP address of the SecureWave Application Server(s) to which the Sanctuary Client driver should connect. You will normally use this option when:

- > A new server is placed in the working environment
- > When you change the IP address or name of the SecureWave Application Server
- > You want to specify more than 3 servers for your clients (done during the client installation – see the Setup Guide for more information)

The default setting is the address(es) provided when installing the client. 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 FQDN (Fully-qualified domain name).

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 will revert 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.

Update notification

This 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 warning will be displayed to the user
- > *Temporary permission changes* – Display a message when temporary permissions are changed. It will also send 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:

<i>Option</i>	<i>Description</i>	<i>Notify user</i>	<i>Block keyboard</i>	<i>Log event</i>
<i>Disabled</i>	Default value. Do not react in any way to the detection of a Keylogger.	✗	✗	✗
<i>Notify user</i>	Only inform the user of the presence of a Keylogger.	✓	✗	✗
<i>Log event to Sanctuary's Console</i>	Only log the event if a Keylogger is detected. The keyboard is not disabled.	✗	✗	✓
<i>Notify user and log event to Sanctuary's Console</i>	If a Keylogger is detected, log the event and inform the user. The keyboard is not disabled.	✓	✗	✓
<i>Block keyboard and notify user</i>	Hinder the keyboard and notify the user if a Keylogger is detected.	✓	✓	✗
<i>Block keyboard and log event to Sanctuary's Console</i>	Hinder the keyboard and log the event if a Keylogger is detected.	✗	✓	✓
<i>Block keyboard, notify, and log event to Sanctuary's Console</i>	Hinder the keyboard, log the event, and notify the user if a Keylogger is detected.	✓	✓	✓

Table 41: USB Keylogger options



Changing from one setting to another requires a client reboot.



Checking settings on a client machine

As long as the *Device Control Status Window* 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.

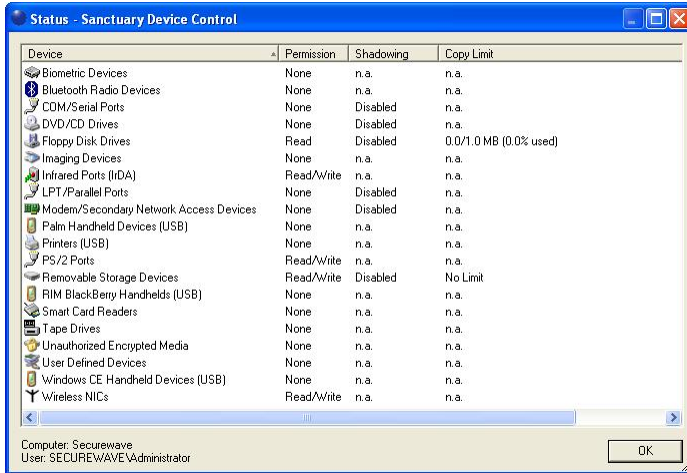



Figure 146: Checking the settings on a client machine


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 10: 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, they 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%.

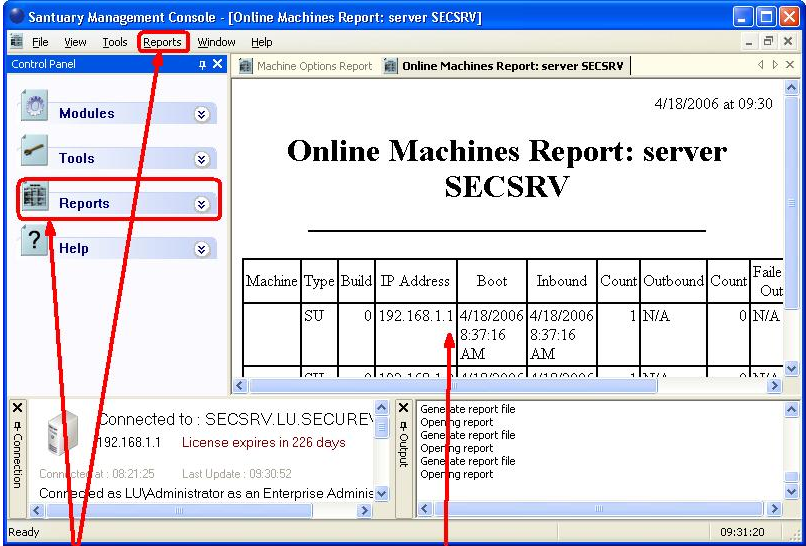
 *Once the output is shown in the window, you can use the 'File → Save as' or 'Print' commands to keep a backup record of your reports. You also have access to the same right click menu as shown for a Web page in Microsoft Internet Explorer.*

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

The following table summarizes the types of reports that can be obtained by a user (controlled in the 'User Access Manager' dialog):

<i>Type of user access</i>	<i>Available Reports</i>
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.

Table 42: Types of reports that can be obtained by an Administrator



Select the desired report from the menu or Control Panel

You get the selected report in the main window panel

Figure 147. 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

Use this report to view all permissions rules defined for a specific user(s). To generate this report, proceed as follows:

1. Select *User Permissions* from the *Reports* menu (or from 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.



The User Permissions report does not show indirect permissions 'inherited' from nested group memberships.

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

2-28-2006 at 07:31

User Permissions

SECURE\Bill (Domain User)

Devices	Computer	Permissions/Priority/Details	User Name / Group Name
CD/DVD-ROM	SECURE\CLIENT	Permissions: Read/Write Event Notification: Enabled Priority: High Details: Shadow option	Via Everyone
Modem	SECURE\CLIENT	Permissions: None Priority: High Details:	SECURE\Bill
SanDisk Cruzer Mini USB Device	<i>Default settings</i>	Permissions: Read/Write Priority: High Details:	SECURE\Bill
Scanner	<i>Default settings</i>	Permissions: Read/Write Priority: High Details:	Via SECURE\Domain Users
Windows CE Devices (USB)	SECURE\CLIENT	Permissions: Read/Write Priority: High Details:	SECURE\Bill

Figure 148: User Permissions report



Device Permissions report

Use this report to view all permissions rules for the devices defined in the Device Explorer module. To generate this report, select *Device Permissions* from the *Reports* menu (or from the *Control Panel*).

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

2-25-2006 at 07:45

Device Permissions

Devices	Default Settings / Computers	User Name / Group Name	Permissions/ Priority Details
BlackBerry (USB)	Default Settings	SECURE\user13	Permissions: Read/Write/Encrypt Priority: High Details: Microsoft Office (import/export)
CD/DVD-ROM	Default Settings	SECURE\Bill	Permissions: Read/Write Priority: High Details:
		SECURE\Cert Publishers	Permissions: Read Priority: High Details: OnLine
		SECURE\Cert Publishers	Permissions: Read/Write Priority: High Details: Offline
	SECURE\CLIENT	SECURE\Bill	Permissions: Read/Write Priority: High Details:
COM/Serial Ports	>>> No users and/or computers you may manage have permissions for this device <<<		
Floppy Disk Drives	Default Settings	Administrators	Permissions: Read/Write Priority: Low Details:
		SECURE\Todd	Permissions: W:Filename R:Enabled Priority: High Details: Shadow option
			Permissions: 1 MB Priority: High Details: Copy Limit
LPT/Parallel Ports	>>> No users and/or computers you may manage have permissions for this device <<<		



Modem	Default Settings	SECURE\GG_MANAGEMENT	Permissions: Read/Write Priority: High Details:
	SECURE\CLIENT	SECURE\Bill	Permissions: None Priority: High Details:
Palm OS Handheld Devices (USB)	>>> No users and/or computers you may manage have permissions for this device <<<		
Removable storage	Default Settings	SECURE\Fred	Permissions: Read/Write Priority: High Details:
SanDisk Cruzer Mini USB Device	>>> No users and/or computers you may manage have permissions for this device <<<		
Scanner	Default Settings	SECURE\Domain Users	Permissions: Read/Write Priority: High Details:
Smart Card Reader	>>> No users and/or computers you may manage have permissions for this device <<<		
Tape Drives	Default Settings	SECURE\Domain Admins	Permissions: Read/Write Priority: High Details:
TwinMOS Mobile Disk USB Device	>>> No users and/or computers you may manage have permissions for this device <<<		
Unauthorized Encrypted Media	>>> No users and/or computers you may manage have permissions for this device <<<		
USB Printer	Default Settings	SECURE\GG_MARKETING	Permissions: Read/Write Priority: High Details:
User Defined Devices	>>> No users and/or computers you may manage have permissions for this device <<<		
Windows CE Devices (USB)	SECURE\CLIENT	SECURE\Bill	Permissions: Read/Write Priority: High Details:

Figure 149: Device Permissions report



Computer Permissions report

Use this report to view 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 from 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.

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

3-01-2006 at 07:45

Computer Permissions

Computer	User Name / Group Name	Devices	Permissions/Priority Details
SECURE\CLIENT	SECURE\Bill	CD/DVD-ROM	Permissions: Read/Write Priority: High Details:
		Modem	Permissions: None Priority: High Details:
		Windows CE Devices (USB)	Permissions: Read/Write Priority: High Details:
	SECURE\John	Modem	Permissions: Read/Write Priority: High Details:06:00 - 20:00 every Mon, Tue, Wed, Thu, Fri
Lu\Sales	Everyone	Removable Storage Devices	Permissions: Read/Write Priority: High Details: (+File filters)

Figure 150: Computer Permissions report



Media by User report

Use this report to view 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.

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

3-30-2006 at 18:20

Media by User Report

1. SECURE\Bill (*Domain User*)

CD/DVD Label	Description	Registered On	Registered By
Music CD	Any music CD		
09PRMCD01	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 Cruiser 128 Mb DK12	12-30-2005	SECURE\Administrator

Figure 151: Media by User report



Users by Medium report

Use this report to view all permissions rules defined to the devices found at the Device Explorer module classified by user(s). To generate this report, select *Users by Medium* from the *Reports* menu (or from the *Control Panel*).

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

1-03-2006 at 18:31

Users by Medium Report

CD/DVD

GE08EU (*Map Point*): Registered the 3-22-2006 by SECURE\Administrator

SECURE\Account (*Domain Group*)

SECURE\adm (*Domain User*)

SECURE\Administrator (*Domain User*)

Music CD (*Any music CD*):

SECURE\Account (*Domain Group*)

09PRMCD01 (*Office XP*): Registered the 1-27-2006 by SECURE\Administrator

SECURE\Account (*Domain Group*)

SECURE\Administrator (*Domain User*)

V2KEE_IE (*Visio*): Registered the 12-30-2005 by SECURE\Administrator

SECURE\Bill (*Domain User*)



vsentd2 (*Visual Studio .Net*): Registered the 1-12-2006 by SECURE\Administrator

SECURE\Administrator (*Domain User*)

SECURE\Bill (*Domain User*)

X05-69971 (*Microsoft Project*): Registered the 1-10-2006 by SECURE\Administrator

SECURE\adm (*Domain User*)

SECURE\Administrator (*Domain User*)

SECURE\Bill (*Domain User*)

Encrypted Media

DK09 (*Mobile Disk DK09*): Registered the 11-30-2005 by SECURE\Administrator

SECURE\adm (*Domain User*)

SECURE\Bill (*Domain User*)

SECURE\Fred (*Domain User*)

SECURE\sandra (*Domain User*)

DK12 (*Mini Cruzer 128 Mb DK12*): Registered the 1-10-2006 by SECURE\Administrator

SECURE\Bill (*Domain User*)

SECURE\Fred (*Domain User*)

Figure 152: Users by Medium report



Shadowing by Device report

Use this report to view a summary of all data being copied/read by user. It is classified in ascending order in the device section. To generate this report, select *Shadowing by Device* from the *Reports* menu (or from the *Control Panel*).

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

1/28/2006 at 09:40

Shadowing by Device between 12-12-2005 and 1-30-2006

Device	User Name	Computer Name	Total Size (Mb)
CD/DVD	SECURE\Administrator	CLIENT	980.730118
	SECURE\Bill	CLIENT	123.359511
		SECSRV	532.046730
	SECURE\Farida	CLIENT	14.199219
		SECSRV	85.147934
	Floppy	SECURE\Bill	CLIENT
SECSRV			0.441463
Removable storage devices	SECURE\Bill	CLIENT	3.113281
		SECSRV	1.117001
	SECURE\Ann	CLIENT	0.906691
	SECURE\Jennifer	SECSRV	10.101629
	SECURE\Marilyn	SECSRV	0.175781

Figure 153: Shadowing by Device report



Shadowing by User report

Use this report to view the total size of data copied/read by user. It is classified in ascending order by quantity. To generate this report, select *Shadowing by User* from the *Reports* menu (or from the *Control Panel*).

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

2/6/2006 at 20:40

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	0.906691
	SECSRV	Floppy	0.000154
SECURE\Marilyne(0.175781 Mb)	SECSRV	Removable	0.175781
SECURE\Jennifer(0.11960 Mb)	SECSRV	CD/DVD	0.010331
		Removable	0.101629
SECURE\Sandy(0.060682 Mb)	SECSRV	CD/DVD	0.027414
		Floppy	0.033268

Figure 154: Shadowing by User report



Online Machines report

Use this report to view 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 will 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 from the *Control Panel*).

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

2/28/2006 at 17:46

Online Machines Report: server SecureWave

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
SecureWave	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
	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 155: 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 will not receive updates when using the <i>Send updates to all</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>SW</i> for Sanctuary Device Control client drivers version 3.1 or older; <i>SX</i> for Sanctuary client drivers version 2.1; <i>SU</i> for Sanctuary client drivers 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



<i>Column</i>	<i>Description</i>
	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 will be 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 will increase in the case of poor connections between the client and the server or in the case of high load on the server side.
Consecutive	Contains the number of consecutive connections failed between the SecureWave Application Server and the client computer. After four unsuccessful connection tries, the client machine is considered as being offline and automatically removed from the online table.

Table 43: Columns of the 'Online Machines' Report



Machine Options report

Use this report to see how the default program's option changed. To generate this report, select *Options* from the *Reports* menu (or from the *Control Panel*). Please refer to *Chapter 9: Setting and changing options* on page 233 for more details on the meaning of each option.

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

2-28-2006 at 16:30

Machine Options Report

Option	Machine	Setting
USB Key Logger	default	(*) Block, notify and Log Event to Sanctuary's console
Device Control Status Window	default	Show All without Shadow
	SECURECLIENT	Show allowed
User notification	default	(*) All permissions changes
Shadow file upload delay or time	default	(*) 60
Shadow directory	default	(*) \SystemRoot\%systemdata%\shadow
Encrypted Media key export	default	To media or file
Encrypted Media export password	default	Allow weak password
Certificate Generation	default	Allow weak
Centralized Device Control Logging	default	Enable
Suppress recurring log events	default	(*) 3600
Client Hardening	Default	(*) Disabled

Figure 156: 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.



Chapter 11: Using Sanctuary Device Control on a Novell network

Novell has always been an active part of the network community. Its roots go back to the early 1980s when it offered a product to share files and printers in a small LAN structure based on PCs. Still going strong today, Novell networks have the same security and data control problems as all other LAN and WAN products in the market. Many modern WANs & LANs share different network operating systems in a heterogeneous environment that often include Novell as a solution.

In this chapter, we analyze the extra component offered by Sanctuary to synchronize those eDirectory objects (OU, group, user, and workstations) so that an administrator can manage them and deny/allow access to I/O devices in a Novell setting.

What components are required?

There are four distinct components necessary for the implementation of Sanctuary Device Control on Novell systems:

- > A Novell server (version 6.5 or later; version 5.x requires confirmation)
- > A SQL server that holds the Sanctuary database – it does not need to have a Novell client, but it may if you are trying to run the synchronization script directly from the server so you do not need to specify the SQL address, user name and password
- > A Sanctuary's script file (written in VBScript) provided on the installation CD under the \scripts directory
- > A Windows machine with a Novell client on which the synchronization script will be executed. This machine must already have Novell's LDAP and ActiveX NDAP installed. You can find these components in Novell's Web site or on your Sanctuary CD

How does the Novell interface works?

Once Sanctuary Device Control installed and configured completely – including the Application Server, Database Server, and Sanctuary's client –, Novell's eDirectory trees are synchronized using an external script and will appear on the Device Explorer module structure (they are also visible in the other modules) so that permissions and rules can be assigned to explicit objects. This VBScript translates



and synchronizes the Globally Unique Identifiers (GUIDs) of eDirectory objects into the Security Identifiers (SID) used internally by Sanctuary.

The administrator can still use the *Synchronize Domain* command of the *Tools* menu (or from the *Control Panel*) to synchronize individual machines or Windows domains.

The administrator must run the synchronization script on a regular basis to synchronize all eDirectory objects. This can either be done by manual or scheduled execution:

- > In the manual execution, the administrator starts the VBScript by running it directly from the Windows' Run menu or command window
- > For a scheduled execution, the administrator uses the Windows Task Scheduler Service (AT or WINAT). Please consult *Chapter 11* of the Setup Guide for an example

Synchronization Script parameters

The script asks for four parameters, only one of them being mandatory:

<i>Parameter</i>	<i>Used for</i>	<i>Notes</i>
Novell server tree name	Novell server's tree name to be synchronized.	Compulsory
SQL server address or name	The address or name of the SQL server hosting the Sanctuary database.	Optional. If none specified, '(local)' is used. This only works when Novell's client, the synchronization script, LDAP, NDAP, and the database are on the same physical machine.
User's name	The user's name used to log into the SQL database.	Optional. If none specified, a 'blank' user is used.
User's password	The user's password used to log the user into the SQL database.	Optional. If none specified, a 'blank' password is used.

Table 44: Novell script's parameters

The user's name and password used to connect to the Novell server are those of the logged one. Take into account that if you do not logon as administrator, you will not have access to some objects of the eDirectory tree. If the SQL credentials are not specified, the current ones are used instead.



If you are using Microsoft SQL 2005 you should specify the SQL server (optionally the user name and password), even if it is local to the machine, as (local)SQLEXPRESS:

```
c:>cscript.exe \path_to_folder\NDSSync.vbs  
Novell_Server_Tree (local)\SQLEXPRESS.
```

How to use the Synchronization Script for Novell

Once all the Sanctuary Device Control installed –the SecureWave Sanctuary Database, SecureWave Application Server, and Console – make sure that the console can communicate with the Application Server and that the administrators can define or modify Sanctuary policies. Once this done, follow these simple steps:

1. Configure initial policies using the well-known accounts (everyone, local system, etc).
2. Deploy Sanctuary Clients. The Sanctuary Clients must be able to communicate with the Application Server and they must adhere to the policies that apply to the well-known accounts.
3. Run the synchronization script, either manually or automatically.
4. Once the script finishes, the account selection dialogs in the console should display the user accounts, groups, and OUs.
5. Specify any of them in some Sanctuary policies.
6. Update the clients and check whether they follow the new policies.



Although any user can start the synchronization process, just like in the Active Directory case, some eDirectory objects may require additional permissions. This depends on the organization's structure and policy. The user must be the database owner or have insert+delete+update permissions to do the synchronization.



Only user, group, OU, and Organization objects are synchronized. If Z.E.N.works is installed, Workstation objects are also synchronized.



Script examples

In this section, we give some typical usage examples. Remember that you can always run the script through Windows' Scheduler Task.

1. `cscript.exe NDSSync.vbs Novell_server_tree`
In this example, we are trying to synchronize objects from the Novell tree called 'Novell_server_tree' and place them on the local database SQL server. You will need to run it directly from the SQL server machine so you need Novell's client + synchronization script + LDAP + NDAP + database on the same physical machine. You can find these components on Novell's Web site or on your Sanctuary CD.
2. In the next example, the script is not run locally from the SQL server machine. You need to specify, besides the Novell server, the emplacement of the database server:
`cscript.exe NDSSync.vbs Novell_Server_tree DB_server`
3. The next example explicitly sets the user and password to access the table in the database since they are not the same as the logged user who runs the script:
`cscript.exe NDSSync.vbs Novell_Server_tree DB_server
Authorized_user User's_Password`
4. If you wish to save the results in a log file, you can use redirection characters:
`cscript.exe NDSSync.vbs Novell_Server_tree > log.txt`



Remember that you need Novell's client, the synchronization script, LDAP, and NDAP – depending on the used parameters and the components physical location – all in a Windows machine.

What can go wrong and how do I fix it?

In this section, you can find a general guidelines to some common error found when running the script. We do not include the obvious ones such as not finding the script or using it directly instead of running it through `cscript.exe`.

The script is not working or it is missing some objects in the eDirectory structure.

Do you have the correct permissions for the Novell server you are specifying? If you do not have administration rights, the script will fail to synchronize all/part of the eDirectory structure.



I get the message 'DB connect failed'

Are you specifying the correct SQL server address, user's name and password? Is the SQL server up and running? Is there a valid connection between your machine and the SQL server (try troubleshooting using the PING command)? Has the database table (sx) been correctly installed?

I get the message 'DBStart failed'

Do you have the correct database rights? You must be a user, or specify the correct one as a parameter, that has insert+delete+update permissions for the database in order to do the synchronization.

I get the message 'DBFeedDomain failed'

Several SQL statements failed to execute. Do you have the proper rights to insert+delete+update in the database table?

I get the message 'DBComplete failed'

Several SQL statements failed to execute. Do you have the proper rights to insert+delete+update in the database table?

There is no synchronization when running NDSSync.vbs script

If you installed SQL Server 2005 Express Edition with our installation wizard, or manually using the Windows Authentication mode, you cannot connect to the SecureWave Sanctuary Database Server machine using credentials different from those of the system administrator provided as script's parameters. Login as administrator of the Database Server machine or enable SQL Authentication for your SQL Server 2005 Express Edition installation.

I get the message "ActiveX component can't create object:
'NWDirLink.NWDDirCtrl.1'"

Is NDAP or/and LDAP installed on the machine from where you are running the script?

3rd Part: Useful 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

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.

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 SecureWave 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+El Torito bootable CDs	◐	◐
ISO+Rock Ridge extensions	◐	◐
High Sierra Group format	○	×
Apple HFS	◐	◐
Legend: × Not supported, writing blocked by the Sanctuary Client ● 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 45: Supported formats for the full shadow or file name only shadow modes



Handling of unsupported shadowing formats

Sometimes the SecureWave Application Server will store 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 will 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 SecureWave client 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 SecureWave client 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 will show you that information. For more details, see *Handling of unsupported shadowing formats* on page 269.



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 SecureWave client 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 will always point to the ISO file system. Joliet file systems are always referenced through a Secondary Volume Descriptor. There are other arrangements, however; a bootable CD or DVD will show 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 will be 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\000000003.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\000000004.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 SK (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 and Windows Server 2003 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 will show up among the unused blocks dumped to the analysis log. Associated files (akin to NTFS streams or Macintosh data and resource forks) will 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 will perform 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 will report 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



will show the false name and the data will be absent. The countermeasure is to finalize such media with the installation of Sanctuary Device Control. This will ensure 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 will be submitted to SXS. 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). SXS will then add the image file in its entirety to the shadow files and make 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, will not be permitted by SK (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 SK (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 will cause SXS 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 will therefore be considered as consisting of 'unused blocks' by Sanctuary Device Control; these blocks will be 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 will 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, SCC 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:

<i>Company</i>	<i>Name of the Software</i>
NERO AG	Nero burning ROM
Sonic Roxio	Easy Media Creator
Alcohol Soft	Alcohol 120%
Microsoft Corp.	Windows XP built-in CD burning software

Table 46: 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.



Appendix B: Installing a Certificate Authority for Encryption

This appendix explains how to install and set up a Windows Certificate Authority.

Requirements

You must install, publish, and properly set a Microsoft Windows Certificate Authority in order to configure a specifically managed removable media. The use of encryption to control and manage this feature fully protects against the intentional or unintentional loss of sensitive data. This section lists all mandatory requirements to install the Certificate Authority needed to implement this specific product feature.



If you are planning to install a Certificate Authority on a stand-alone server that is going to be integrated to your network later, you need to be connected to at least one computer so that Windows can recognize your network interface connector (NIC).

Active Directory

The Windows Certificate authority is tightly integrated to the Windows Active Directory. In order to use encryption of removable storage devices, your domain must be configured to use Active Directory.

Integrate DNS with Active Directory

Although it is not a requirement to have the DNS integrated with Active Directory, it is important that the DNS server be properly configured. Please refer to the Microsoft's Web site to get more information on how to check the configuration of your DNS servers.

To check if your Microsoft DNS is properly configured and integrated with Active Directory, open the DNS Management Console and check that the DNS zone contains the "_msdcs" records.



The following screenshot shows how to check the DNS zone:

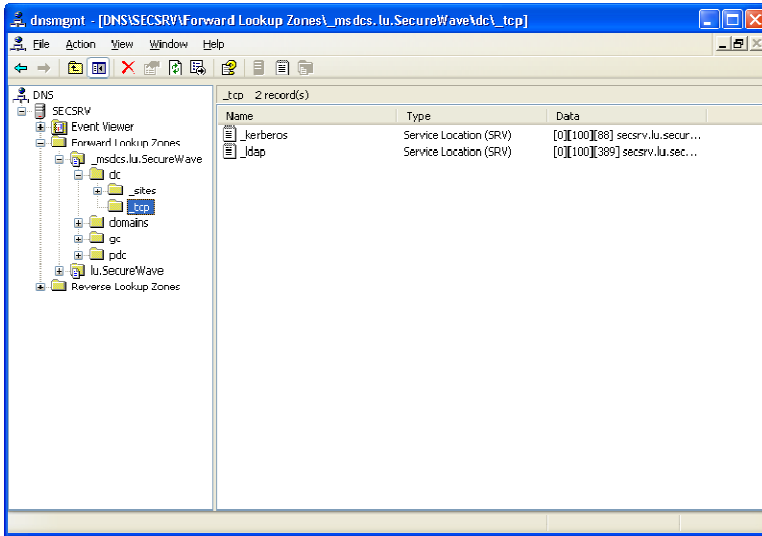


Figure 157: Verifying the DNS zone

Installing the Certificate Services

If there are no certificate services installed on your network, you should follow this step-by-step procedure for the installation of the Microsoft Certificate Services.

1. Log on to one of the Active Directory Domain controllers as a domain administrator.
2. Go to the *Start|Settings|Control Panel* menu.
3. Click on the **ADD OR REMOVE PROGRAMS** icon.
4. Select **ADD/REMOVE WINDOWS COMPONENTS** located on the left part of the screen.
5. Select the *Certificate Services* entry in the list of components and click on **NEXT**.

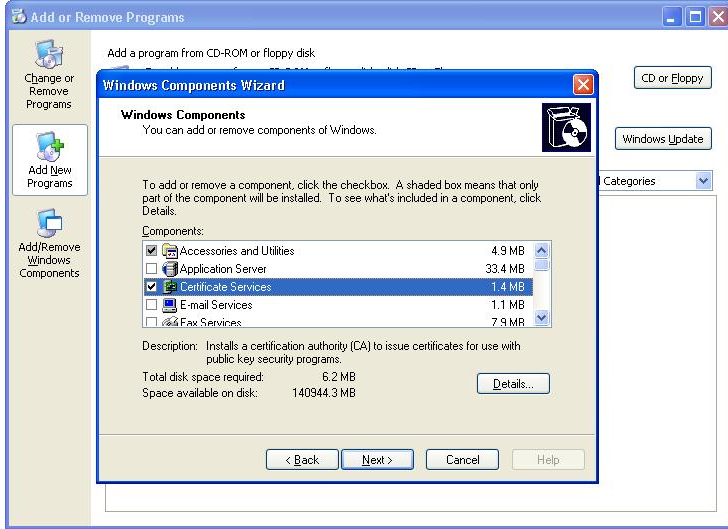


Figure 158: Adding certificate services

6. Select the *Enterprise root CA* and click on NEXT.

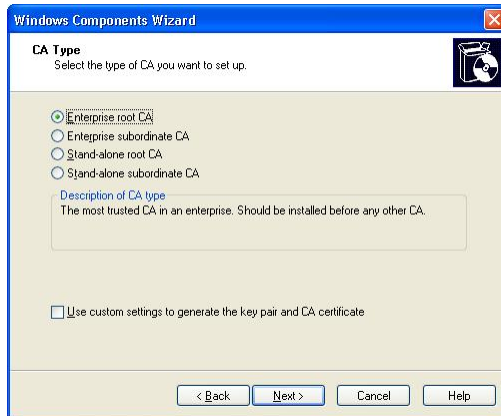


Figure 159: The Windows components wizard (1st page)



7. Choose a *Common name* and *Distinguished name* suffix that will identify this CA and click on NEXT.

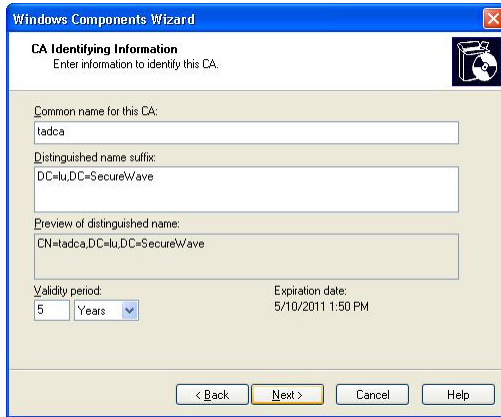


Figure 160: The Windows components wizard (2nd page)

8. Choose an appropriate location for the Certificate Database Settings and click on NEXT.

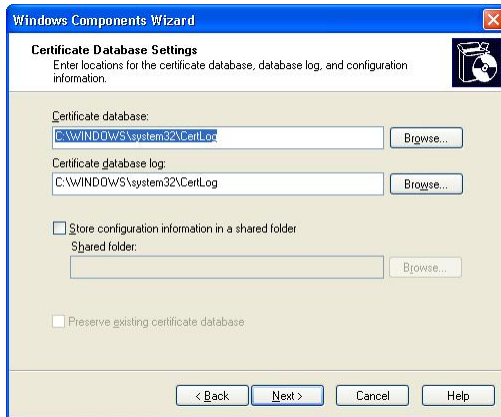


Figure 161: The Windows components wizard (3rd page)



Windows proceeds with the installation of the certificate services.

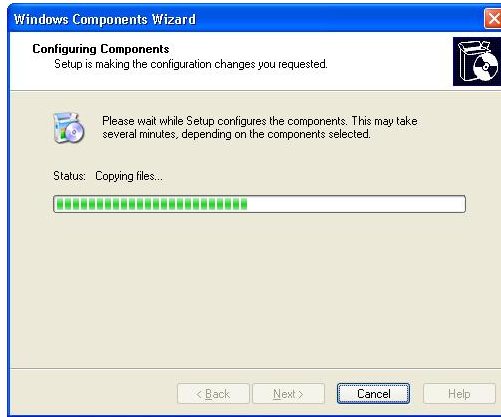


Figure 162: The Windows components wizard (final page)



After the installation of the Sanctuary Client on the user's machine, the user has to log on at least once in order to be able to access any encrypted media for which he was granted access rights. During this first logon, the user certificate is issued by the Certificate Authority. This certificate is used by the SecureWave Application Server to deliver per-media rights for users. The Certificate is stored locally on the user's machine and additionally published to the Active Directory.



Depending on your Active Directory configuration and replication between domain controllers setting, it may take some time to issue a certificate during the first user logon and publish it to the Active Directory. During that period, the user is not authorized to access the media.



You will need to install a root enterprise level CA. There are two types of enterprise level Certificate Authority: root and subordinate. In this case, 'root and subordinate' are just Microsoft terms that identify hierarchy, thus, subordinate cannot exist without root. Since we use Active Directory (AD) integration, the CA must be able to publish and issue certificates using (AD). Only enterprise level CA is integrated with AD. The CA software of other vendors that support AD integration can also be used.



Checking that certificates are correctly issued to the users

If a user is prevented access to an encrypted medium which he has received proper rights, verify that the Certificate Authority has correctly issue the certificates for this user. The following is a step-by-step procedure to check that a user certificate has been correctly issued:

1. Log on to the user's machine.
2. Go to the `START\RUN` menu.
3. Enter `mmc.exe` in the *Open* field and click on OK.
4. In the Microsoft Management console, open the *File* menu and select *Add/Remove Snap-in* (or press *Ctrl+M*).
5. Click on *ADD*.
6. In the *Add Standalone Snap-in* dialog, choose *Certificates* and click on *Add*.

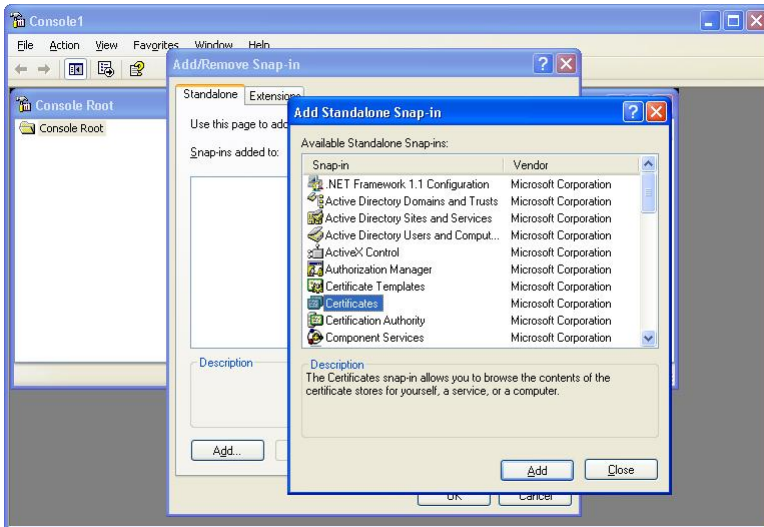


Figure 163: The certificate snap-in



7. In the *Certificates Snap-in* dialog, choose *My user account* and click on FINISH, CLOSE and OK.

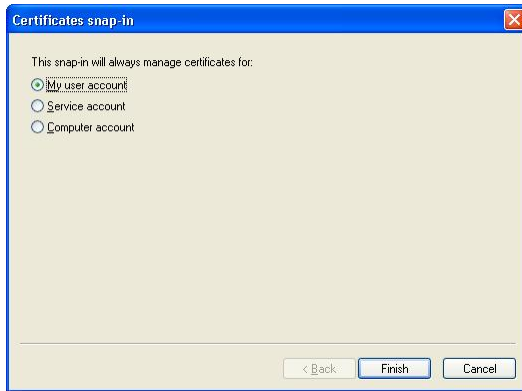


Figure 164: The certificate snap-in: user account

8. Open the *Certificates – Current User* of the *Personal* node . You should see at least one entry with the *Encrypting File System, Secure Email, Client Authentication* setting in the *Intended purposes* column.

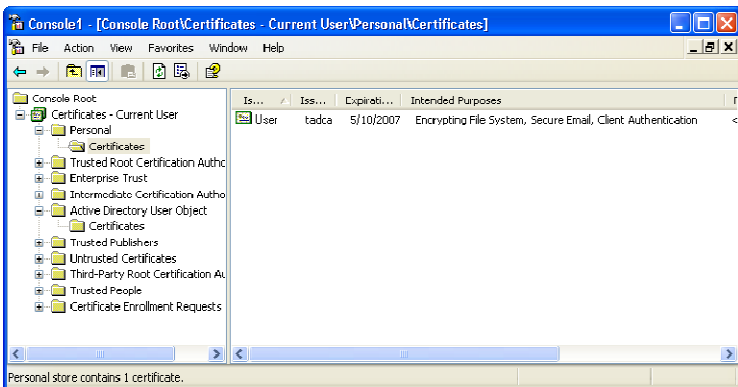


Figure 165: The console: certificate intended purposes



9. Check that the same certificate entry is present under the *Certificates – Current User* node of the *Active Directory User Object*.

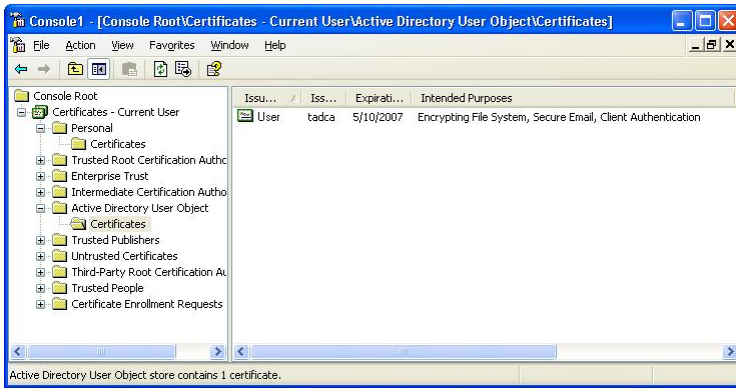


Figure 166: Verifying the user's certificate

If the certificates are correctly issued and present on the user's machine as described above, this user will be able to access any authorized media for which he has received appropriate permissions.



The access permissions to encrypted removable media are retrieved from the SecureWave Application Server by the client following any of these events:

- > *The user inserts and accesses an encrypted media.*
- > *The user inserts the encrypted media and then logs on.*

It is mandatory that the SecureWave Application Server be online and accessible upon these events. The received rights and disk encryption keys are cached locally in a protected area of the hard drive, so that the user will be able to access the encrypted media when his computer is disconnected from the network.



Appendix C: Important Notes

In this appendix, you will find the most common installation difficulties that you will encounter when using Sanctuary Device Control.

- > The next table summarizes the Wireless NICs you can block using the Sanctuary Device Control permissions rules:

<i>Wireless NICs that can be block using Sanctuary Device Control permissions rules</i>	
If you are using Windows 2000	Nortel BayStack 660 in 802.11 Mode; BreezeCOM Wireless LAN PC Card
	Symbol Spectrum24 WLAN Adapter
	Raytheon RayLink WireLess LAN Adapter
	Lucent-Based IEEE 802.11 PC Cards: WaveLAN/IEEE PC Card (5 volt); WaveLAN/IEEE PC Card (3.3 and 5 volt); WaveLAN/IEEE PC Card (3.3 volt); WaveLAN/IEEE PC Card (NCR, 5 volt); WaveLAN/IEEE PC Card (NCR, 3.3 and 5 volt); Cabletron RoamAbout 802.11 PC Card
	PCX500 Cards. All of Aironet's A500 based cards: Aironet PC2500 DS Wireless PCMCIA LAN Adapter; Aironet PC2500 DS Wireless ISA LAN Adapter (Legacy Mode); Aironet PC2500 DS Wireless ISAPNP LAN Adapter; Aironet PC3100 FH Wireless PCMCIA LAN Adapter; Aironet PC3100 FH Wireless ISA LAN Adapter (Legacy Mode); Aironet PC3100 FH Wireless ISAPNP LAN Adapter Aironet PC3500 FH Wireless PCMCIA LAN Adapter; Aironet PC3500 FH Wireless ISA LAN Adapter (Legacy Mode); Aironet PC3500 FH Wireless ISAPNP LAN Adapter; Aironet PC4500 DS Wireless PCMCIA LAN Adapter; Aironet PC4500 DS Wireless ISA LAN Adapter (Legacy Mode); Aironet PC4500 DS Wireless ISAPNP LAN Adapter; Aironet PC4800 DS Wireless PCMCIA LAN Adapter; Aironet PC4800 DS Wireless ISA LAN Adapter (Legacy Mode); Aironet PC4800 DS Wireless ISAPNP LAN Adapter
If you are using Windows XP	3Com: 3CRWE62092A Wireless LAN PC Card; 3Com 3CRWE62092A Wireless LAN PC Card
	Sierra Wireless AirCard 300; CDPD Adapter Nortel; BayStack 660 Wireless PCMCIA Adapter; BreezeNET Wireless LAN PC Card; Symbol Spectrum24 WLAN PC Card
	Symbol LA-41x1 Spectrum24 Wireless LAN; PC Card Symbol LA-41x3; Spectrum24 Wireless LAN PCI Card
	Intel(R) PRO/Wireless 2011 LAN PC Card; Intel(R) PRO/Wireless 2011 LAN PCI Card; Intel(R) PRO/Wireless 2915ABG chipset
	Ericsson DSSS Wireless LAN PC Card; Ericsson DSSS Wireless LAN PCI Card
	Nortel Networks e-mobility 802.11b Wireless LAN; PC Card Nortel Networks e-mobility 802.11b Wireless LAN PCI Card 3Com 3CRWE737A AirConnect Wireless LAN PC Card 3Com 3CRWE777A AirConnect Wireless LAN PCI Card
	Raytheon RayLink WireLess PCMCIA LAN Adapter
	Compaq WL110 Wireless LAN PC Card
	Dell TrueMobile 1150 Series Wireless LAN Card; Dell TrueMobile 1150 Series; Wireless LAN Mini PCI Card IBM High Rate; Wireless LAN PC Card IBM High Rate; Wireless LAN Mini PCI Card IBM Internal High Rate; Wireless LAN PC Card ELSA Airlancer MC11 High Rate; Wireless LAN PC Card ORINOCO; Wireless LAN PC Card (5

<i>Wireless NICs that can be block using Sanctuary Device Control permissions rules</i>	
	volt) ORiNOCO; Wireless LAN PC Card (3.3 and 5 volt) ORiNOCO; Wireless LAN PC Card (3.3 volt) Sony PCWA-C100; Wireless PC Card Toshiba; Wireless LAN Card Toshiba; Wireless LAN Mini PCI Card NCR-WaveLAN; Wireless LAN PC Card Buffalo WLI-PCM-L11; Wireless LAN Adapter RoamAbout 802.11 DS (Cabletron) & RoamAbout 802.11 DS (Enterasys)
	Cisco Wireless ISAPNP LAN Adapter (Generic PC2500 DS) Cisco Wireless ISAPNP LAN Adapter (Generic PC3100 FH) Cisco Wireless ISAPNP LAN Adapter (Generic PC3500 FH); Cisco Wireless ISAPNP LAN Adapter (Generic PC4500 DS); Cisco Wireless ISAPNP LAN Adapter (Generic PC4800 DS); Cisco PC2500 DS Wireless PCMCIA LAN Adapter; Cisco PC3100 FH Wireless PCMCIA LAN Adapter; Cisco PC3500 FH Wireless PCMCIA LAN Adapter; Cisco PC4500 DS Wireless PCMCIA LAN Adapter; Cisco PC4800 DS Wireless PCMCIA LAN Adapter; Cisco Systems 340 Series Wireless LAN Adapter; Cisco Systems 350 Series Wireless LAN Adapter; Cisco Systems 340 Series PCI Wireless LAN Adapter; Cisco Systems 350 Series PCI Wireless LAN Adapter; Cisco PC4800 DS Wireless PCI LAN Adapter

Table 47: Wireless NICs that can be blocked using the Sanctuary Device Control permissions rules

- > 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*, *Audit Logs Viewer*, 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 SecureWave 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) can not 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
- > 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 running the Sanctuary Command & Control (SCC) service in the system account: since this account has no default permissions to access removable media (including floppy disks), the SCC cannot dismount the removable media preventing the server's upload of 'fresh' shadow files. When running interactively, it has access to the removable media and can dismount them. In this case, files are transmitted as soon as the media is removed. Give Read/Write permissions to the system account if you want an immediate upload of shadow files
- > When the Media Authorizer exports a key to a file, it does not use the *Sanctuary Kernel* (SK) to do so – it obtains the key directly from the server. This is done for administrative purposes. However, it still has to use SK to export the key to the medium – but SK does not know about the administration status of the user and refuses to export if the *Encrypted Media key Export* default option is not configured properly (*To file* or *To media* or



file). Please see *Chapter 9: Setting and changing options* on page 233 for more details

- > If a *Copy Limit* rule (see page 130) 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'. Sanctuary's client 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 'RW' 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 141 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 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 141 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.



Appendix D: Controlling administrative rights for Sanctuary's administrators

VBScript Tools

When installing your SecureWave solution, you get a Visual Basic Script file tool. This tool is provided to narrow down administrative rights to control Organizational Units/Users/Computers/Groups for special users designated as Sanctuary's administrators.

You can find this tool in the installation folder, usually under the SCRIPTS directory. You can also locate it on your installation CD.

Ctrlacx.vbs, explained in this appendix, is a tool to create, view, or modify control rights in the active directory.

Ctrlacx.vbs

Introduction

This Visual Basic Script file can be use to set, view, or modify the *Manage Sanctuary Settings* control rights in the Active Directory. This will allow Active Directory administrators to delegate Sanctuary Management for computers, users, groups, and organizational units without entrusting any other tasks (which is required by default). This script may also be use to show the other control/rights defined in the Active Directory forest.

The file is located in the Script folder of your installation directory or directly in your Sanctuary's CD.

Once the script run, it creates a special entry in the permissions list of the organization unit called *Manage Sanctuary Settings*. This entry only affects Sanctuary Device Control software administrator users and the devices they control. If you assign this setting to a specific user, who is also a Sanctuary Administrator (as defined on the *User Access Manager* dialog of the console), he would only be able to manage the designated users/groups/computers for which he has rights directly from the Sanctuary Management Console.



After finishing the outlined procedure, you need to synchronize with the domain before these rights are activated. To do this, use the *Synchronize Domain Members* item of the *Tools* menu (or from the *Control Panel*).

Requirements

You must have the *Windows Script Host* (WSH, WSCRIPT.EXE, CSCRIPT.EXE) interpreter installed on your system before you can run any VBScript. Some antivirus programs will reject the execution of these types of scripts.

Usage

To use `ctrlacx.vbs`:

1. Open a command screen (*Start -> Run -> Command*) to run the script or execute it directly from the *Run* dialog using the following syntax:

```
cscript Ctrlacx.vbs [-parameter list]>file.txt
```

The previous syntax sends the output directly to a text file specified, in this case, by *file.txt*. If you want to use it interactively, utilize the following syntax:

```
Ctrlacx.vbs [-parameter list]
```

- or -

```
Wscript Ctrlacx.vbs [-parameter list]
```

<i>Parameter</i>	<i>Description</i>
-?	Displays a brief description of each possible parameter. You must run this script in interactive mode or from the command line in order to see the text.
-e	Enumerate all control access rights. Condensed output
-v	Enumerate all control access rights. Detailed output (verbose)
-q cn	Displays a control right by its canonical name (cn)
-s	Display SecureWave's <i>Manage Sanctuary Settings</i> rights
-create	Creates or updates SecureWave's <i>Manage Sanctuary Settings</i> rights
-delete	Deletes SecureWave's <i>Manage Sanctuary Settings</i> rights

Table 48: Ctrlacx script options



Examples

```
cscript CtrlIacx.vbs -e > MyFile.txt
```

List all control access rights in condensed mode redirecting the output to MyFile.txt file.

```
ctrlIacx.vbs -s
```

Show the *Manage Sanctuary Settings* rights interactively.

What to do after running the script

Once you run the script on a domain machine, you have to assign the delegation rights you just created for Sanctuary. To do this, follow these steps:

1. Run the script with the *-Create* parameter to generate or update SecureWave's rights on the active directory.
2. Open the MMC (Microsoft Management Console) window.
3. Activate the *Advanced Features* option from the *View* menu as shown in *Figure 167*.

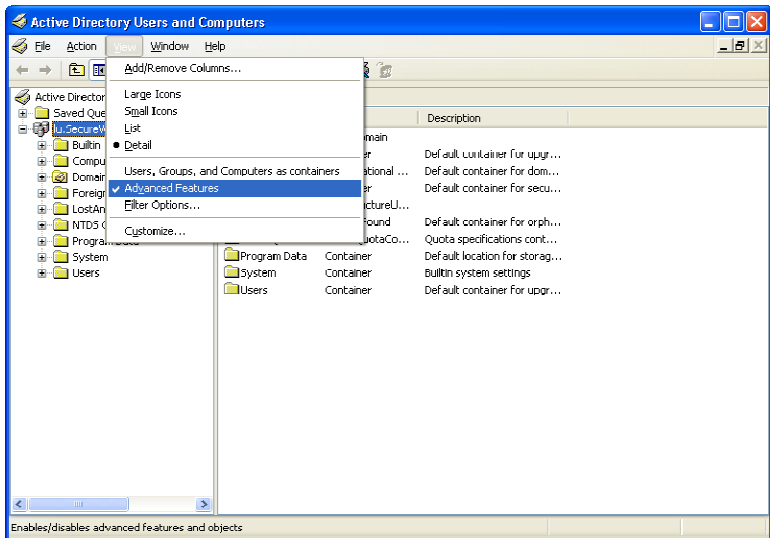


Figure 167: Advanced feature option of the MMC



4. Right click on the desired Organizational Unit (OU) and select *Properties* from the pop-up menu.
5. Go to the *Security* tab and click on the **ADVANCED** button to open the *Advanced Security Settings* dialog. Go to the *Permissions* tab and click on **ADD** or **EDIT**.
6. Select the user or group to which you want to delegate rights, as shown in *Figure 168*, click on **OBJECT TYPES** and select also *Computers*. Click on the **OK** button to close the dialog.

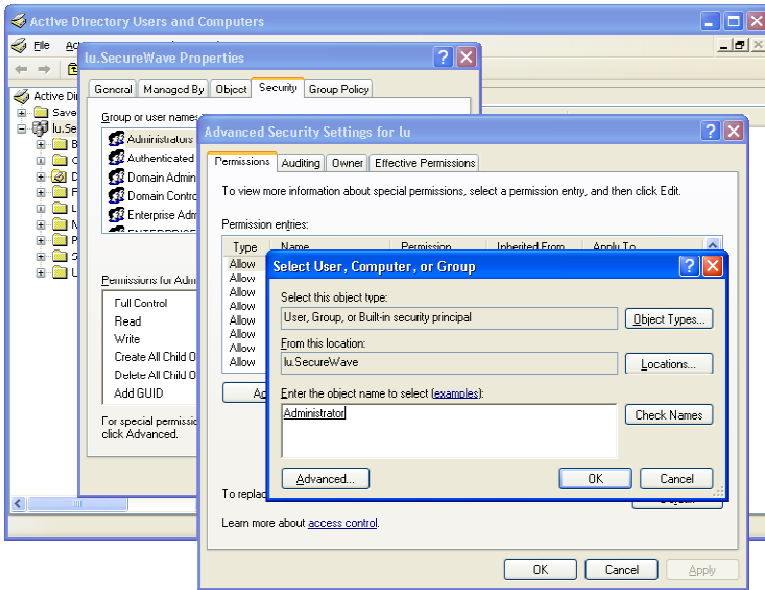


Figure 168: Select user, computer, or group to which delegate.

7. Click on the **OK** button to open the *Permissions entry* dialog as shown in *Figure 169*.

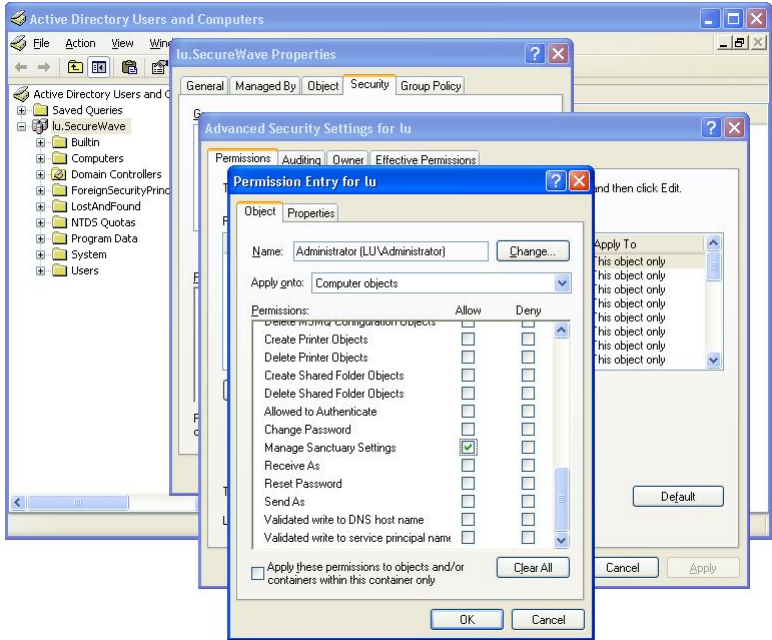


Figure 169: Manage Sanctuary Settings object

- Three important objects exist in the *Apply onto* field of this dialog that are relevant to the Sanctuary settings: *Computer objects*, *Group objects*, and *User objects*. Figure 3 shows only one of them: *Computer objects*. The script narrows the Active Directory rights by creating a special entry in each of the above-mentioned objects: *Manage Sanctuary Settings*. If you assign this permission to a user, he/she can only manage the designated users/groups/computers in the Sanctuary Management Console.

Note the special check box option in the permissions entry: *Apply these permissions to objects and/or containers within this container only*. If activated, you will see only the real objects – users or computers from this OU – in the console and nothing from the child OUs beneath.

The 'new' delegated administrator can now manage those objects (users/computers/groups) explicitly assigned to him.



Glossary

ADSI

Acronym for *Active Directory Service Interface*. Previously known as OLE Directory Services, ADSI makes it easy to create directory management applications using high-level tools such as Basic, Java, or C/C++ without having to worry about the underlying differences between the dissimilar namespaces.

AES

Advanced Encryption Standard. A symmetric key encryption technique that is replacing the commonly used DES standard. It is the result of a worldwide call for submissions of encryption algorithms issued by NIST in 1997 and completed in 2000.

CAB

File extension for *cabinet* files. 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

The CSV, Comma Separated Value, file format allows easy data table retrieval into a variety of applications. It is often used to exchange data between disparate applications. The file format has become a pseudo standard throughout the industry, even among non-Microsoft platforms. Common examples of applications that use this format are spreadsheets and databases. You can also see and edit these files using an ASCII text editor (Notepad, Word, WordPad, Excel, etc.).

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.



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 (*Remote Access Service*) 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 *Global Unique Identifier* number generated when the NDS object is created. It is simply an object's NDS attribute. In order to ensure data consistency, Novell eDirectory implements a globally unique ID (GUID) for all objects within the directory. The total number of unique keys (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.

IOCP

I/O (Input/Output) Completion Port.

LDAP

Lightweight Directory Access Protocol. An LDAP directory entry consists of a collection of attributes and is referenced unambiguously with a name, called a distinguished name (DN). For example, "cn=Bill Dove: ou=marketing: o=securewave" — "cn" for common name, "ou" for organizational units, "o" for



organization. LDAP directory entries feature a hierarchical structure that reflects political, geographic, and/or organizational boundaries.

MAPI

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

MDAC

Microsoft Data Access Components. 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

A *Remote Procedure Call* is a protocol that allows a computer program running on one host to run a subroutine on another host. RPC is used to implement the client-server model of distributed computing.

RSA Encryption

In 1977, Ron Rivest, Adi Shamir, and Len Adleman developed the public key encryption scheme that is now known as RSA, after their initials. The method uses modular exponentiation, which can be performed efficiently by a computer, even when the module and exponent are hundreds of digits long.

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.

SXS

SecureWave Application Server. The main component of all Sanctuary's products. Beside calculating hashes, authorizing applications and devices, it serves as a bridge between the database and the client.

TAO

Track-At-Once.

TCP/IP

Acronym for *Transmission Control Protocol/Internet Protocol*. The protocol used by the client computers to communicate with the SecureWave Application Servers.

VBScript

A scripting language created by Microsoft embedded in many applications used in Windows. Although it allows for powerful interoperability and functionality, it also creates a great deal of security risks unless it is tightly controlled.

Well-Known Security Identifiers

A security identifier (SID) is a unique value used to identify a security principal or security group. The values of certain SIDs remain constant across all installations of Windows systems and for this reason are termed well-known SIDs. Everybody, Local, Guest, Domain Guest, etc. are some examples of SIDs.

WMI

Acronym for *Windows Management Instrumentation*. WMI is a standard technology to access management information in an enterprise environment. WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components. You can use WMI to automate administrative tasks in an enterprise environment. WMI improves administrative control by allowing administrators to correlate data and events from multiple sources and vendors on a local or enterprise basis. It is used as a complement to ADSI.



WSH

Acronym for *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 (aka Zenworks). With it, you can 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: SecureWave Device Control components.....	20
Figure 2: Client driver – internal works.....	24
Figure 3: Obtaining a List of Accessible Devices.....	26
Figure 4: Connecting to the server.....	37
Figure 5: Connection / Output window.....	38
Figure 6: The Sanctuary Device Control screen.....	39
Figure 7: License status warning.....	40
Figure 8: Docked Control Panel.....	40
Figure 9: Docked window.....	40
Figure 10: Floating Control Panel.....	41
Figure 11: Floating windows.....	41
Figure 12: Minimized windows.....	42
Figure 13: Endpoint maintenance.....	50
Figure 14: The Default Options dialog.....	53
Figure 15: The Synchronizing Domains dialog.....	54
Figure 16: Adding workgroup computers.....	55
Figure 17: The Connect As dialog.....	55
Figure 18: Performing database maintenance.....	56
Figure 19: Defining the administrators' roles.....	58
Figure 20: The four level removable device class structure.....	65
Figure 21: The four level removable device class structure with permission examples.....	65
Figure 22: Computers and computer groups.....	67
Figure 23: Device Explorer main window.....	75
Figure 24: The Device Explorer two main sections.....	77
Figure 25: Context menu.....	81
Figure 26: Show all members.....	83
Figure 27: Event notification: selecting the users/groups.....	85
Figure 28: Event notification: options.....	85



Figure 29: Event notification: finish the rule definition 85

Figure 30: Event notification: new permission rule as shown for the device class 86

Figure 31: Using Drag & Drop to move devices to a newly created group 88

Figure 32: Main permissions dialog 94

Figure 33: Bus dialog used for Scheduled Permissions and Shadow 94

Figure 34: General Permissions dialog exceptions 95

Figure 35: Removable permissions settings example 1 97

Figure 36: Removable permissions settings example 2 97

Figure 37: Removable permissions settings example 3 97

Figure 38: Removable permissions settings example 4 98

Figure 39: Defining a file filter 100

Figure 40: Assigning default permissions to users and groups 108

Figure 41: The Permissions dialog 108

Figure 42: The Select Group, User, Local Group or Local User dialog when adding default permissions 109

Figure 43: The Select Computer dialog showing multiple selection in action 113

Figure 44: Assigning permissions in the Device Explorer module 113

Figure 45: Defining Read, Read/Write, or None permissions when adding permissions 114

Figure 46: The Select Group, User, Local Group or Local User dialog 114

Figure 47: Modifying permissions 115

Figure 48: Removing permissions 116

Figure 49: Add a Scheduled permission 116

Figure 50: The Choose User dialog when adding a scheduled permission 117

Figure 51: Selecting the bus when adding scheduled permissions 117

Figure 52: Defining Read, Read/Write, or None permissions when adding scheduled permissions 118

Figure 53: The Choose Timeframe dialog when adding a scheduled permission 118

Figure 54: Modifying a scheduled permission 119

Figure 55: Adding a Temporary permission 120

Figure 56: The Choose User dialog when adding a temporary permission 121

Figure 57: Selecting the bus when adding temporary permissions 121

Figure 58: Defining Read, Read/Write, or None permissions when adding a temporary permission 122



Figure 59: The Choose Period dialog when adding a temporary permission122

Figure 60: Defining Read, Read/Write, or None permissions when adding online/offline permission 124

Figure 61: Importing permission settings 126

Figure 62: The Choose User dialog when adding a shadow rule.....127

Figure 63: Selecting the bus when adding temporary permissions 128

Figure 64: Defining the type of shadow for a device..... 129

Figure 65: Finishing the shadow rule definition 129

Figure 66: The Choose User dialog when adding a copy limit rule..... 130

Figure 67: Defining a copy limit..... 131

Figure 68: The status screen on the client's side: copied/remaining bytes 131

Figure 69: Decentralized encryption: the user receives an Access Denied message and an invitation to encrypt it.....137

Figure 70: Password complexity is required to encrypt the device.....137

Figure 71: Decentralized encryption: the user proceeds to encrypt the device using the *Encryption* option of the contextual menu.....137

Figure 72: Decentralized encryption: the encryption process begins137

Figure 73: Decentralized encryption for a group defined at a device group level (1/2)..... 138

Figure 74: Decentralized encryption for a group defined at a device group level (2/2) 138

Figure 75: Decentralized encryption at the unique device level (1/2) 139

Figure 76: Decentralized encryption at the unique device level (2/2)..... 139

Figure 77: Decentralized encryption at the class level (1/2) 140

Figure 78: Decentralized encryption at the class level (2/2) 140

Figure 79: Decentralized encryption using a "delegated" user (1/2)141

Figure 80: Decentralized encryption using a "delegated" user (2/2)141

Figure 81: Managing devices 143

Figure 82: Managing devices – selecting the computer 143

Figure 83: Managing devices – choosing the devices from the selected computer..... 144

Figure 84: Removing devices 145

Figure 85: Confirming the removal of a device 145

Figure 86: Priority setting 147

Figure 87: Sending updates to client computers 149

Figure 88: The send update item from the contextual menu 149



Figure 89: The Log Explorer main window..... 153

Figure 90: Saving your new template..... 156

Figure 91: Managing your templates 156

Figure 92: Components of the Log Explorer window 157

Figure 93: Navigation/Control bar..... 157

Figure 94: Column Headers..... 158

Figure 95: Show/hide columns 159

Figure 96: How to open the Settings dialog..... 159

Figure 97: Settings dialog..... 160

Figure 98. Stacking the query 160

Figure 99: Example of criteria settings 163

Figure 100: Filter/Properties panel..... 164

Figure 101: Control button bar 164

Figure 102: Viewing the content of a shadow file in text form..... 172

Figure 103: Viewing the content of a shadow file in binary form 172

Figure 104. Fetching New Logs..... 174

Figure 105: The Audit Logs Viewer main window..... 175

Figure 106: Using the calendar pull-down to select a search date..... 176

Figure 107: Using the Author field to do a search 177

Figure 108: Using the Action field to do a search 178

Figure 109: Using the sorting facilities of the Audit Logs Viewer module 179

Figure 110: Filtering actions in the Audit Logs Viewer module..... 179

Figure 111: A filtering pop-up dialog example..... 180

Figure 112: The Media Authorizer main window 185

Figure 113: Adding an encrypted DVD or CD 187

Figure 114: Adding a specific removable storage device 191

Figure 115: 'Inaccessible medium' error message 194

Figure 116: 'Not enough privileges' error message 195

Figure 117: 'Already authorized' error message 195

Figure 118: 'Already encrypted' error message 195

Figure 119: 'Identification record cannot be deleted' error message 196

Figure 120: Importing back an already encrypted device..... 196



Figure 121: A specific medium with its related users and groups	198
Figure 122: Adding a group or user to a selected medium	198
Figure 123: Denying access to DVDs/CDs/encrypted removable media	199
Figure 124: Media by user authorization	200
Figure 125: 'Users still associated with medium' warning message	202
Figure 126: 'Deleting medium' warning message	202
Figure 127: 'Cannot delete identification record' error message	203
Figure 128: Renaming a DVD/CD/Removable storage device	204
Figure 129: Exporting a medium key	205
Figure 130: Exporting encryption keys	212
Figure 131: Exporting encryption keys (by the user)	213
Figure 132: The Export Medium Key dialog to export the encryption key to a file	214
Figure 133: The Export Medium Key dialog to export the encryption key on the device itself	215
Figure 134: Adding a device in the Media Authorizer (the key is external)	217
Figure 135: Adding a device in the Media Authorizer (the key resides on the medium)	217
Figure 136: Accessing unauthorized encrypted media	220
Figure 137: The Import Medium Key dialog (import from medium or folder)	220
Figure 138: Importing an external device	222
Figure 139: Importing an external device	222
Figure 140: Importing an external device	223
Figure 141: Using the Stand-Alone Decryption tool	225
Figure 142: The Import Medium Key dialog when using the Stand-alone decryption tool....	225
Figure 143: Sanctuary's Secure Volume Browser	227
Figure 144: The Default Options dialog	235
Figure 145: Setting computer-specific options	235
Figure 146: Checking the settings on a client machine	243
Figure 147: Obtaining a report	246
Figure 148: User Permissions report	247
Figure 149: Device Permissions report	249
Figure 150: Computer Permissions report	250
Figure 151: Media by User report	251
Figure 152: Users by Medium report	253



Figure 153: Shadowing by Device report.....254

Figure 154: Shadowing by User report255

Figure 155: Online Machines report.....256

Figure 156: Machine options report 258

Figure 157: Verifying the DNS zone 280

Figure 158: Adding certificate services 281

Figure 159: The Windows components wizard (1st page) 281

Figure 160: The Windows components wizard (2nd page).....282

Figure 161: The Windows components wizard (3rd page)282

Figure 162: The Windows components wizard (final page).....283

Figure 163: The certificate snap-in 284

Figure 164: The certificate snap-in: user account..... 285

Figure 165: The console: certificate intended purposes..... 285

Figure 166: Verifying the user's certificate 286

Figure 167: Advanced feature option of the MMC.....295

Figure 168: Select user, computer, or group to which delegate..... 296

Figure 169: Manage Sanctuary Settings object 297



Index of Tables

Table 1: Permissions list updates depending on network connection status	25
Table 2: Novelties in this version	36
Table 3: The four available modules in the Sanctuary Device Control	43
Table 4: The File menu items	47
Table 5: The View menu items.....	47
Table 6: The Window menu items	47
Table 7: The Tools menu items.....	48
Table 8: The Report menu items	51
Table 9. The Explorer Menu	52
Table 10: The Help menu items.....	53
Table 11: Administrator's prerogatives	59
Table 12: Administrator's roles.....	60
Table 13: Standard Windows' device classes as seen on the Device Explorer module in the Default Settings section	63
Table 14: Managing unique individual removable devices.....	65
Table 15: Simultaneous permissions definitions for all Windows' standard device classes in the Device Explorer module.....	69
Table 16: Default settings when first installing the program (these apply to "Everyone")	78
Table 17: Possible assignments by device	80
Table 18: Keyboard Shortcuts used on the Device Explorer module.....	81
Table 19: Device classes that can have Device Groups.....	87
Table 20: Allowed settings when working with the Removable Storage Devices class.....	96
Table 21: File type filtering possibilities	99
Table 22: Filter type filtering extensions	101
Table 23: File filter settings and permission relation.....	101
Table 24: File filter settings examples	106
Table 25: Applied permissions.....	111
Table 26: Permissions example.....	134



Table 27: Resulting access.....	148
Table 28: Permission settings priority.....	148
Table 29: Limitations while using the Log Explorer module under other user/domain account	154
Table 30: How to use the available criteria dialogs.....	163
Table 31: Log Explorer module column meaning	167
Table 32: Audit Logs Viewer Result Information.....	182
Table 33: Available encryption methods.....	192
Table 34: Encryption methods comparison	194
Table 35: Resulting access when permissions are defined at the Device Explorer and at the Media Authorizer levels (example 1).....	206
Table 36: Resulting access when permissions are defined at the Device Explorer and at the Media Authorizer levels (example 2)	208
Table 37: Easy Exchange encryption options.....	227
Table 38: Full Encryption method inside and outside your company.....	230
Table 39: Easy Exchange encryption method inside and outside your company.....	231
Table 40: Option name comparison	234
Table 41: USB Keylogger options	242
Table 42: Types of reports that can be obtained by an Administrator	245
Table 43: Columns of the 'Online Machines' Report	257
Table 44: Novell script's parameters	260
Table 45: Supported formats for the full shadow or file name only shadow modes	268
Table 46: Supported DVD/CD burning software.....	278
Table 47: Wireless NICs that can be blocked using the Sanctuary Device Control permissions rules	288
Table 48: Ctrlacx script options.....	294



Index

A

Accessing encrypted media outside of your organization; 211, 216
Active directory; 58, 112, 177, 188, 279, 280, 283, 286
 Delegation; 58
 Service Interface; 299
Add
 A specific removable device; 190
 Managed device; 180
 Removable; 190
Adding DVD/CD; 186
 Pre-requisites; 186
Administration tools; 20, 21
Administrator; 57, 58, 177
 Roles; 30
ADSI; 299
Advanced Encryption Standard; 188, 299
AES; 188, 299
AFD; 20, 21, 36
Allow weak password; 239
Analysis of a CD image; 270
Assigning permissions to use DVD/CDs/Encrypted Media; 197, 200
ATA; 34
Audit File Directory; 20, 21, 36
Audit logs maintenance; 56
Audit Logs Viewer; 43, 175
 Accessed device log; 180
 Accessed shadow file; 180
 Action column; 180
 Actions; 178
 Add managed device; 180
 Added media; 180
 Added permission; 181
 Added scheduled permission; 181
 Added temporary permission; 181
 Author column; 180
 Authorized media; 181

 Automatic user access upgrade; 181
 Computer column; 180
 Data column; 180
 Deleted default option; 181
 Deleted option; 181
 Information column; 180
 Modified scheduled permission; 181
 Modify user access role; 181
 Purged DB and file storage; 181
 Remove managed device; 181
 Removed media; 181
 Revoked permission; 181
 Revoked scheduled permission; 181
 Revoked temporary permission; 181
 Search options; 176
 Set default option; 182
 Set option; 182
 Target column; 180
 Unauthorized media; 182
 Updated Media; 182
 Updated permission; 182
 Uploaded shadows; 182
 User/group name column; 180

B

Biometric devices; 31, 88
BlackBerry; 91
Bluetooth; 30, 34
 Radio devices; 31, 89

C

CAB; 299
Central log files; 56
Centralized device control logging; 142, 151, 152
Centralized encryption; 29
Certificate generation



- Disabled; 237
- Certificates; 188, 284, 285, 286
 - Installing; 280
 - Requirements; 279
 - Services; 280
 - Verifying; 284
- CIM; 303
- Client computer; 22, 25, 54, 110, 115, 119, 125, 129, 144, 148, 153, 199, 201, 235, 240, 267, 299
- Client Hardening; 49
- Client ticket; 49
 - Create; 50
 - Rules; 49
- COM; 89
 - Printers; 288
 - Serial ports; 31, 89
- COM+; 289
- Comments; 82
- Common Information Model; 303
- Compatible mode; 60
- Computer groups; 82
- Computer-specific
 - Options; 235
 - Permissions; 112, 218
- Connect
 - As; 55
 - To the SXS Server; 37
- Contact information; 14
- Context-sensitive permissions; 28
- Copy limit; 28, 130, 288
- Cscript.exe; 299, 304
- CSV; 174, 299
- ctrlacx.vbs; 177, 293
 - Configuration steps; 295
 - Examples; 295
 - Introduction; 293
 - Parameters; 294
 - Requirements; 294
 - Usage; 294
- D**
- DAO; 299
- Data file directory; 56
- Data File Directory; 21
- Database; 20, 21, 25
 - Maintenance; 48
- Database maintenance; 56
- DataFileDirectory; 20
- DCC; 300
- Decentralized encryption; 29, 70, 183
- Default
 - Options; 48, 234
 - Permissions; 107
 - Settings; 107, 112
- Default Permissions; 106
- Delegation; 300
- Device
 - Import; 222
- Device Attached; 168
- Device Explorer; 43, 44, 54, 75, 93, 148, 149, 206, 207, 235, 236
 - Introduction; 76
- Device groups; 87
 - Add; 87
- Device log
 - Disabled; 238
 - Enabled; 238
- Devices in logical groups; 66
- DFD; 20
- DN; 300
- DNS; 189, 279
- DVD/CD
 - Drives; 22, 31, 89
 - Shadowing; 29, 173, 267
 - Supported formats; 268, 273
 - Unsupported formats; 269, 273
- E**
- Easy Exchange; 226
- Encrypted Media; 22, 197
 - Import; 222
- Encrypting media; 70
- Encryption; 183
 - Adding removable drives; 187
 - Centralized; 29
 - Decentralized; 29, 70
 - Examples; 71
 - Easy exchange (insecure for existing data); 192
 - Encrypt Removable; 190



- Error messages; 194
- Export key on medium; 215
- Export key to file; 213
- Full & Slow (secure for existing data); 192
- Import (secure for existing data); 196, 203
- Import a device; 222
- Key Length; 188
- Limitations; 189
- Lost or broken media; 203
- Method; 192
- Password; 218, 220, 225
- Password strength; 214, 216
- Pre-requisites; 188
- Quick Format (insecure for existing data); 192
- Users by medium; 197, 199, 200
- Endpoint Maintenance; 49, 238
- Enterprise Administrators; 58, 177
- Event Log; 238
- Executable program; 300
- Explicitly deny; 76, 132
- Explorer menu; 52
- Export
 - Encryption key; 205, 211
 - Key
 - To file; 212
 - To media or file; 212
 - Medium key; 212

F

- Fetch Latest Log Files; 153
- File filters; 98
 - Examples; 102
- File Menu; 46
- File shadowing; 28
- File type filtering; 98
 - Examples; 102
- FireWire; 34
- Floppy disk drives; 32, 89, 90

G

- GUID; 300

H

- Help menu; 53

I

- IDE; 34
- Identifying devices; 62
- Identifying users and user groups; 61
- iFolder; 300
- Imaging devices; 32
- Imaging Devices; 89
- Import; 222
- Important notes; 287
- Incorrect logoff; 289
- Individual option settings; 237
- Informing client computers; 148
- Infrared (IrDA) ports; 30, 32
- Insert Computer; 112
- Installing a Certificate Authority; 279
- IOCP; 300
- IrDA; 30, 34
 - Ports; 89

K

- Key logger; *See* Keylogger
- Key Pair
 - Generation; 21
 - Generator; 22
- Keyboard shortcuts; 81
- Keylogger; 30, 242

L

- Label; 191
- LDAP; 300
- Log Explorer; 43, 45, 151
 - Force latest log; 173
 - Save to CSV; 174
- Log in as a different user; 38
- Log system; 238
- LPT/Parallel ports; 31, 90

M

- Managing specific computers; 67
- MAPI; 301



- MDAC; 301
- Media
 - By user; 200
 - Label; 191
 - Label column; 185
 - Media Authorizer; 43, 45, 183, 186, 187, 188, 197, 206, 212
 - Media Description; 191
 - Media-inserted; 167
- Microsoft Certificate Authority; 183, 189
- Microsoft Windows Network; 112
- Modem; 32, 90
- MSDE; 301
- Multiple permissions; 132
- N**
- NDAP; 301
- NDS; 301
- Negative permission; 76, 80, 110, 132, 206, 208, 219, 301
- Network interface controllers; 33
- NIC1; 302
- None; 76, 80, 110, 132, 206, 208, 219
- Novell; 259
 - Components; 259
 - FAQ; 262
 - Interface; 259
 - Synchronization script; 259
 - Parameters; 260
 - Usage examples; 262
 - Using; 261
- Novell support; 27
- O**
- Offline updates; 28
- Omnibook; 289
- Online/Offline permissions; 132
- Options; 22, 53, 233, 234
 - Centralized device control log; 234
 - Certificate generation; 234, 237
 - Changes; 234
 - Client hardening; 234, 237
 - Device control status window; 234
 - Device log; 234, 238
 - Device log throttling; 234, 238
 - Encrypted media export password; 234
 - Encrypted media key export; 234
 - Encrypted media password; 234, 239
 - Log upload delay; 234, 239
 - Log upload interval; 234, 240
 - Log upload threshold; 234, 239
 - Log upload time; 234, 240
 - Sanctuary status; 234, 240
 - SecureWave Application Server address; 234
 - Server address; 234, 241
 - Shadow directory; 234, 241
 - Shadow file upload delay; 234
 - Suppress recurring log events; 234
 - Update notification; 234, 241
 - USB Keylogger; 234, 242
- Organizational Units; 58
- OU; 302
- P**
- Palm handheld devices; 90
- Palm Handheld Devices; 32
- PCMCIA; 27, 28, 32, 34
- Per-device
 - Encryption; 29
 - Permissions; 29, 146
- Permissions; 107, 114
 - Dialog; 93
 - None; 301
 - Online/Offline; 123
 - Priority; 110, 206
 - Send to client; 61
 - Types; 67
- Plug & Play; 27, 34, 88, 187
- Poor performance; 288
- Pre-defined device classes; 63
- Printer
 - USB; 90



- Printers
 - USB; 32
- Private Key; 302
- Protection process; 26
- PS/2
 - Keylogger; 30
 - Ports; 30, 32, 90, 288
- Public Key; 302
- Purge Online Table; 48
- Q**
- Quick Format (insecure for existing data); 184, 196, 203
- Quota exceeded; 168
- R**
- Read denied; 168
- Read-only; 27, 190
- Removable; 32, 90, 187
 - Storage devices; 32, 90
- Remove
 - Copy limit; 132
 - DVD/CD/Encrypted Media; 201, 202
 - DVD/CDs; 202
 - Encrypted media; 202
 - Offline and online permissions; 125
 - Permissions to DVD/CD/Encrypted Media; 199, 201
 - Scheduled permissions; 119
 - Shadow; 129
 - Temporary permissions; 122
- Reports; 245, 288
 - Computer permissions; 51, 250
 - Device permissions; 51, 248
 - Machine options; 51, 258
 - Media by user; 51
 - Media by user; 251
 - Menu; 51, 245, 247, 248, 250, 251, 252, 254, 255, 256, 258
 - Online machines; 51, 256
 - Shadowing by device; 51, 254
 - Shadowing by user; 51, 255
 - User options; 51
 - User permissions; 51, 247
 - Users by medium; 51, 252
 - RIM BlackBerry handhelds; 33
 - Root-level permissions; 106
 - RPC; 302
 - RSA; 170
 - Definition; 302
- S**
- SADEC; 211, 224
- Salt; 23, 49
- Sanctuary Client; 20, 22, 23
- Sanctuary Device Control
 - Advantages; 19
 - Controlling your environment; 18
 - Description; 17
 - Features; 27
 - Internal workings; 23
 - Introduction; 17
 - Offline control; 26
 - System architecture; 20
- Sanctuary Management Console; 22, 37, 39
 - Connection window; 40
 - Control panel; 39
 - Main window*; 39
 - Menu; 39
 - modules; 43
 - Output window; 40
 - Status bar; 40
- SAO; 302
- Scanners; 33, 89, 289
- Scheduled permissions; 28, 63, 116, 119
- SCSI; 34
- Search
 - by Action; 176
 - by Author; 176
 - by Computer; 176
 - by Date; 176
 - by Target; 176
 - by User Name; 176
- Secondary hard disks; 91
- Secondary hard drives; 187
- Secondary network access devices; 32, 90



SecureWave Application Server; 20,
21, 22, 25, 37, 46, 47, 57, 59, 275, 276,
303

Send updates; 148

To a specific computer; 48

To all computers; 48, 54, 110, 115,
119, 125, 129, 144, 148, 235, 236

SHA-1; 302

Shadow

Bad directory; 170

Bad public key; 170

CD R malfunction; 170

CD R mode unsupported; 170

File malfunction; 170

Files; 56

Shadowing; 45, 151

a device; 127

Devices; 126

File Name; 173

Show all members; 83

SK; 20

Smart Card readers; 33, 91

SMC; 20

Specifically deny access; 80, 206,

208, 219, 301

SQL Server; 301, 303

Supported devices; 31

Types; 88

Supported DVD/CD burning software;
278

SVolBro.exe; 226

SX; 20

SXDomain; 22, 23

SXS; 20, 37, 57, 59, 275, 276, 303

Synchronize Domain; 48, 54, 55, 62,
76

T

TA0; 303

Tape drives; 33, 91

TCP/IP; 303

Temporary

Access; 28

Permissions; 63, 120, 241

Ticket; 50

Time zones; 288

Tools menu; 48, 150

Traced on; 171

Transferred on; 171

U

Unable to communicate with WLD
driver; 186

Unauthorized Encrypted Media; 33,
216, 217, 218, 219, 221

Unique devices; 29, 64

Unlock medium; 219, 224

Unsuccessful access attempts; 165

USB; 34, 89

Printer support; 30

Printers; 32

User

Access; 48, 57

defined classes; 64

Defined devices; 28, 33, 91, 141

V

VBScript; 303

Tools; 293

View menu; 47

Viewing

Access attempts to devices; 167

Client error reports; 170

Shadow files; 171

W

Well-Known Security Identifiers; 303

Window menu; 47

Windows CE handheld devices; 33, 91

Windows Management

Instrumentation; 303

Windows NT4; 301

Windows Script Host; 304

Wireless NICs; 30, 33, 91, 287

Wlan blocked; 170

WMI; 303

Workgroup; 188

Computers; 54

Write denied; 169

WScript.exe; 304

WSH; 304



Z

Z.E.N.works; 304
ZENworks; 304