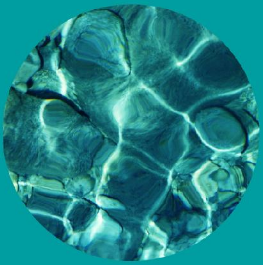
SecureWave

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.

Trademarks

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

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

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

You can contact our technical support team at:

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

or by sending an email to support@securewave.com

Published: April 2006

Sanctuary Device Control — Version v3.2.0

Contents

About this guide

Introduction

The real world can be harsh: Trojans, worms, viruses, hackers, and even careless or disgruntled employees threat 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 10). 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: Using the Log Explorer* provides information on how to view a copy of traced files, errors, and access attempts on client computers.

> *Chapter 5: Using the Audit Logs Viewer* explains how to view administrative logs and copies of files ('shadow files') users have copied into certain devices.

> *Chapter 6: Using the Media Authorizer* illustrates how to create a database of known DVD/CDs and encrypted media and how to assign their rights to individual users and groups.

> *Chapter 7: Accessing encrypted media outside of your organization* explains how to use encrypted media outside the company.

> *Chapter 8: Setting and changing options* describes how to tailor the Default and Computer-specific options to suit you and your organization.

> *Chapter 9: Reports* explains how to obtain the various HTML reports generated by Sanctuary Device Control.

> *Chapter 10: 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 the files written to 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:

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

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

Alternatively, you can write to customer support at:

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

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 to 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 copied to external devices or specific ports (file names only or full copy of files transferred)

- Encrypt media with the powerful AES algorithm
- Block some media (DVDs/CDs) while permitting other specific ones to be used

You can find a full list of characteristics in the *Major features* section on page *23*.

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 to 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*
- One or more *SecureWave Application Server* (also known as *SXS*)
- The *Sanctuary Client Driver* (SK)
- Administrative tools – especially the *Sanctuary Device Console* or (SMC)

The following image shows this relation:

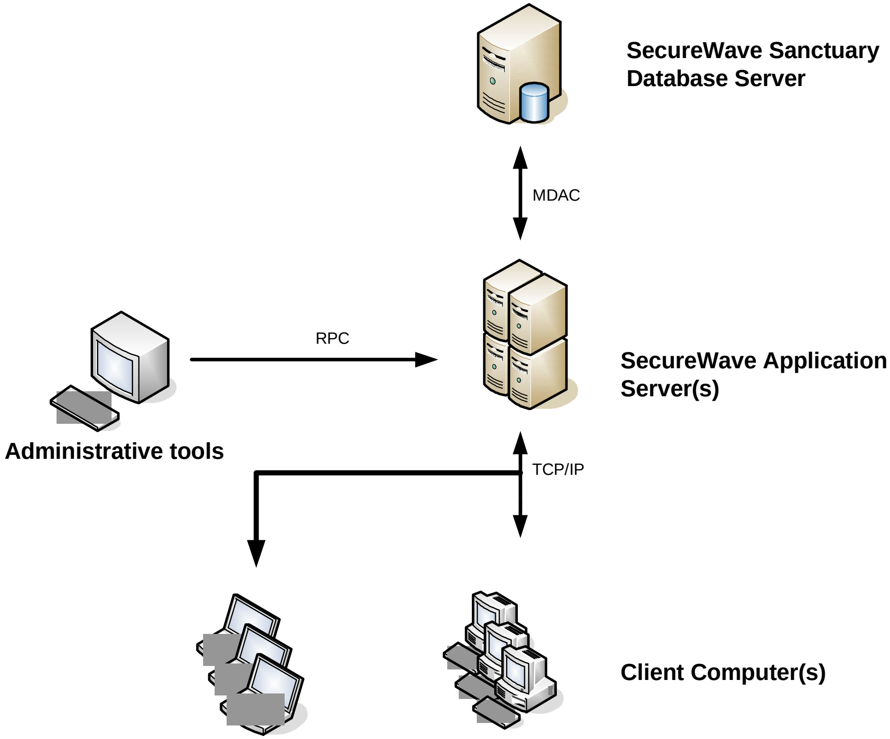

SecureWave Sanctuary Database Server
MDAC
RPC
SecureWave Application Server(s)
Administrative tools
TCP/IP
Client Computer(s)

Figure 1: SecureWave Device Control components

SecureWave Application Server

Each Sanctuary Device Control installation requires at least one Application Server. This server is used to communicate with the Sanctuary Clients and to obtain the list of devices and permissions for each client from the central database.

The SecureWave Application Server has the following features:

- It is a Windows Service.
- It runs under an account capable of reading Domain users/groups/computers accounts from the Domain Controller.

The administration tool described in this guide is the Sanctuary Device Console, while the *Key Pair Generator* and the *SXDomain* command-line tool are described in the setup guide. You can also refer to the 'Setup Guide' (PDF file) located on the Sanctuary CD or in the 'Program File' directory.

Database

As it is the case with the Application Server, each Sanctuary Device Control site must have one database. This is the master storage point for the user policies and permissions. The database uses Microsoft SQL Server 2000/2005, or MSDE2000.

Administration Tools

Administrators use the Sanctuary Device Console (label as Management Console 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.

You can administrate the system using:

- The Sanctuary Device Control
- The Key Pair Generation
- The SXDomain command-line tool

Sanctuary Device Console

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

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.

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

SXDomain command-line tool

The SXDomain command-line tool is used to inform the Database of the changes done to the domains, users, groups, and workstations within your network.

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.

The end-user cannot interact with the Sanctuary Client, except to receive notifications when his/her permissions changes. The user cannot change in any way its settings or permissions.

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

The user can also update his settings using the *Refresh Settings* command of the system tray icon.

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. These 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.

The Administrator can also manage specific devices by type or brand if needed. He/She just needs to assign the 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 the existing device class permission to the device. If a device is unknown and does not belong to a predefined device class, our software will apply the most restrictive permission rule and deny access 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 program can log this action, optionally, for the Administrators to analyze.

The following schema summarizes these steps:

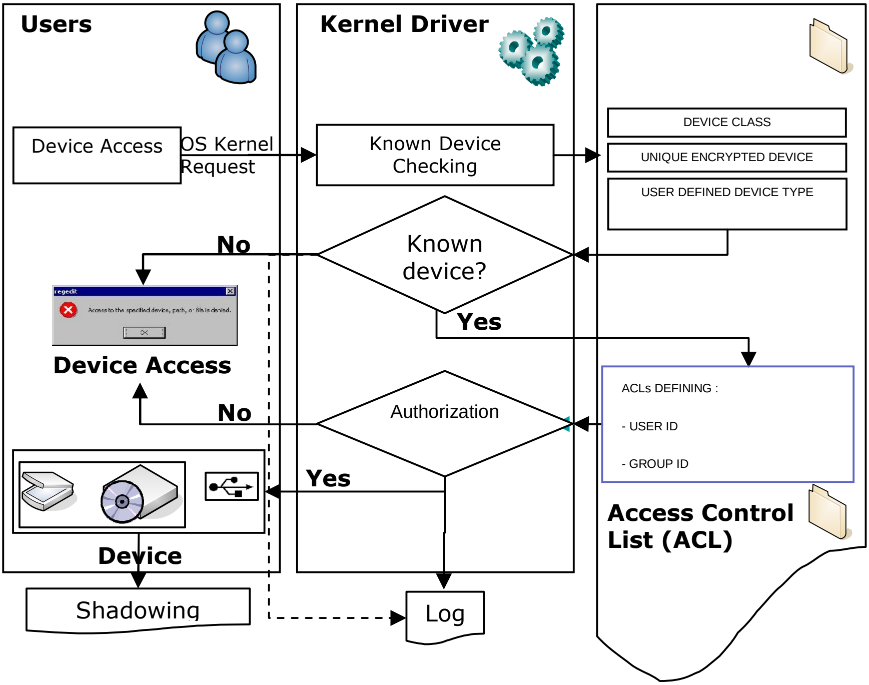


Figure 2: Internal Working

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

The Sanctuary Device Console connects to the Application Server to carry out administrative changes. Therefore, at no time does the Sanctuary Device 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 *Sanctuary 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:

Network connection	*Permission updates are done:*
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 *Refresh settings* 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 *Shadowing devices* on page *106* 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. The SecureWave Application Server then cryptographically signs the list, compresses it, and forwards it to the *client computer*.

The process is summarized in the following diagram.

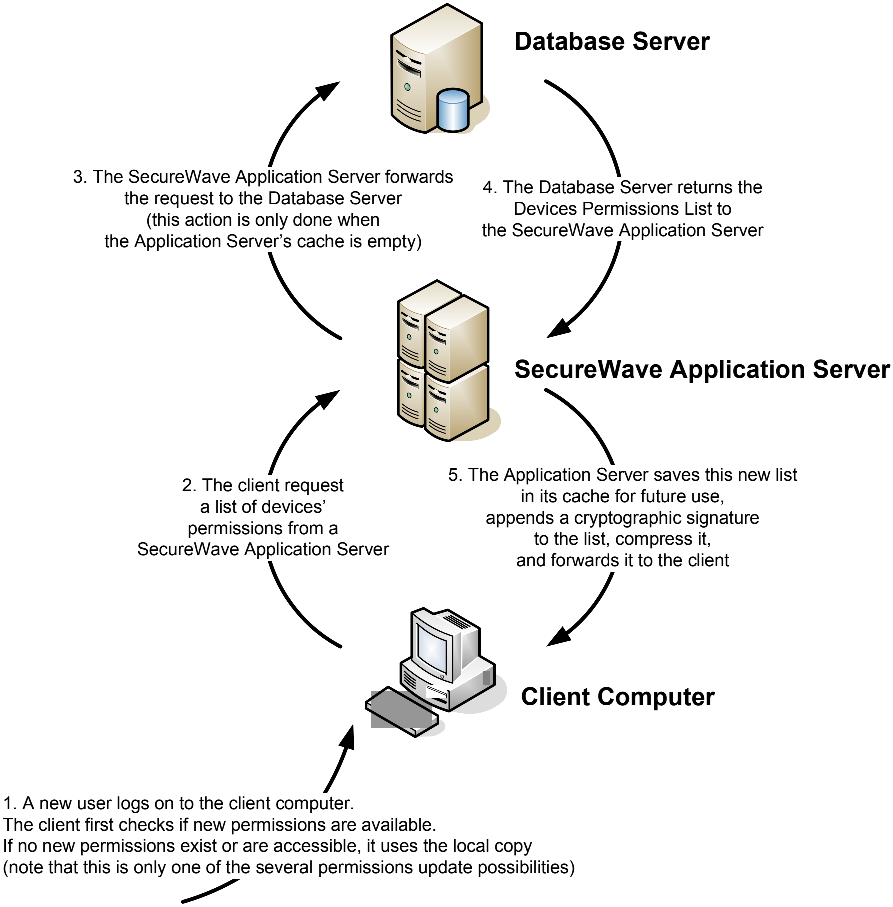

Database Server
3. The SecureWave Application Server forwards the request to the Database Server (this action is only done when the Application Server's cache is empty)
4. The Database Server returns the Devices Permissions List to the SecureWave Application Server
SecureWave Application Server
2. The client request a list of devices' permissions from a SecureWave Application Server
5. The Application Server saves this new list in its cache for future use, appends a cryptographic signature to the list, compress it, and forwards it to the client
Client Computer
1. A new user logs on to the client computer. The client first checks if new permissions are available. If no new permissions exist or are accessible, it uses the local copy (note that this is only one of the several permissions update possibilities)

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 the local copy it has 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 a user tries to delete or tamper the list: he 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.

Intuitive user interface

Device access is controlled by means of a native Access Control List, the same way as for files and folders. Permissions can apply at different levels: all machines, machine groups, specific machines, or even groups of 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 to file-system based devices such as Recordable DVD/CD, floppy, Zip and PCMCIA drives, as well as to serial and parallel ports. This feature is available on a per user basis.

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. So, 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.

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.

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 to 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 *USB Key Logger* on page *195* 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 Device 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 *251* to learn how to set rights to control Organizational Units/Users/Computers/Groups.

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 to 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 *69* 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 those 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 (USB)

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

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 RIM handhelds (USB)

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 a permission for this class of devices will be able to access devices that were encrypted by Sanctuary Device Control in another organization.

USB printers

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

User-defined devices

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

Windows CE handheld devices (USB)

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 *245* 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

Since USB, FireWire, and PCMCIA 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 to 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 Device 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 file (only if Shadow is active).
- Define the types of media a user can use in his computer.
- 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 HTML reports: User permissions, Device permissions, Computer permissions, Media by user, Users by medium, Shadowing by device, Shadowing by user, Online machines, and Options.
- etc...

Novelties & changes from previous versions

If you are upgrading from a previous version of our software, use this table to see at-a-glance the recent changes to the *Device Explorer* module:

Name in previous versions	*New class name for this version*
CD/DVD-ROM	DVD/CD Drives
Floppy	Floppy Disk Drives
Removable	Removable Storage Devices
COM	COM/Serial Ports
LPT	LPT/Parallel Ports
TAPE	Tape Drives
Modem	Modem/Secondary Network Access Devices
Smart Card Reader	Smart Card Readers
Windows CE Devices (USB)	Windows CE Handheld Devices (USB)
Palm OS Handheld Devices (USB)	Palm Handheld Devices (USB)
Scanner	Imaging Devices
User Defined Devices	User Defined Devices
USB Printer	Printers (USB)
BlackBerry (USB)	RIM BlackBerry Handhelds (USB)
Unauthorized Encrypted Media	Unauthorized Encrypted Media
Previously an option	Bluetooth Radio Devices
Previously set during setup	Wireless NICs
Previously an option	Infrared Ports (IrDA)
Previously an option	PS/2 Ports
Previously handled in other classes	Biometric Devices

Table 2: Device class name changes from previous versions

New to this version we have:

Category	Feature
Unified client	Each one of the programs that form our Sanctuary suite previously required an independent client component. We have designed a unified client component that now works with our entire software suite, depending on those modules that you have purchased and installed in your server.
UNC for Novell	The client now resolves UNC (Universal Naming Convention) Novell names showing them in reports and user selection when authorizing devices.
Novell	Support for Novell's eDirectory (Novell v6.5 or above)
Root-level permissions	You can now define permissions that apply to all devices using the Device Explorer module. You can have, for example, a "non-blocking mode" for all devices. Of course, applying an "all-blocking mode" is equally possible.
Update permissions	Now you can send permissions updates to computers not connected to the network by file transfer.

Category	Feature
	Offline updates: Now you can send permissions updates to computers not connected to the network by file transfer.
Shadowing	A new column has been added to allow you quickly find the shadow (copied data) entries with attached data (using a clip 📎 symbol). The size of file copied is now available even if you only choose to shadow the ‘File Name’.
Rules	The ‘Copy Limit’ now applies additionally to Administrators. If you do not want to limit data copied to a device by the administrators, then modify the default ‘Copy Limit’ rule defined in the ‘Device Explorer’ module.
	It is now possible to define online/offline permissions. This makes it possible for users to access certain devices when they are online and apply a different device policy when they are offline. Online: The client can communicate directly with the server. Offline: The client cannot communicate directly with the server.
	Temporary and Scheduled permissions now apply in the pre-defined LOCAL client time. If you define permissions from 08h00 to 17h00, they will always apply between 08h00 and 17h00 local client computer time, whatever the time zone.
	Future temporary permissions can now be defined: For example, an Administrator can assign access to a user’s floppy disk drive from the first to the 15th of the next month because he will be attending a trade show.
	You can now have simultaneous Per-Device/Class/Computer Group/Device Group permissions. You do not need to switch anymore from one mode to another. You can now define permissions for a class and device model at the same time. Using this feature you can set, for example, access to all types of removable devices for Administrators but limit certain user to his MP3 reader (classified also as a removable device).
Modules	Enhanced search and filter capabilities added to the previously called ‘Administrator Audit’ (now ‘Log Explorer’).
And many, many more. Please see the Readme.txt file located on your CD installation disk for a full list of features and changes	

Table 3: Novelties in this version

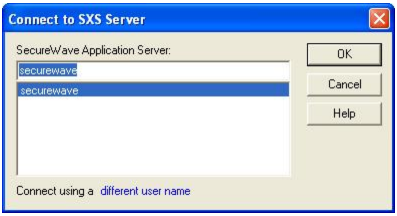
Starting up the Sanctuary Device Control

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

Connecting to the Server

When you initially launch the Sanctuary Device 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.



SecureWave Application Server: securewave

securewave

Connect using a different user name

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. 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:

secrsrv.secure.com[1234]

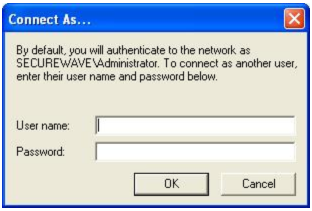
✍ *Please refer to the description of the registry key settings of the Application Server in the 'Setup Guide' for more details on how to configure the server to use a fixed port.*

💣 *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. Click on the OK button. The *Sanctuary Device Console* screen appears, as shown on the next section.

If the Sanctuary Device Console screen does not appear, an error message is displayed. This indicates that there were problems when all the internal tests were carried out. Check that you have the required permissions to connect to that server, on domain rights and Sanctuary Device Console rights level. See *Defining the Sanctuary Device Control administrators* on page *50*.

If you choose to click on the *Connect using a different user name* link, instead of using your credentials — default way to establish a connection —, the *Connect As* dialog box opens:



Connect As...

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

User name:

Password:

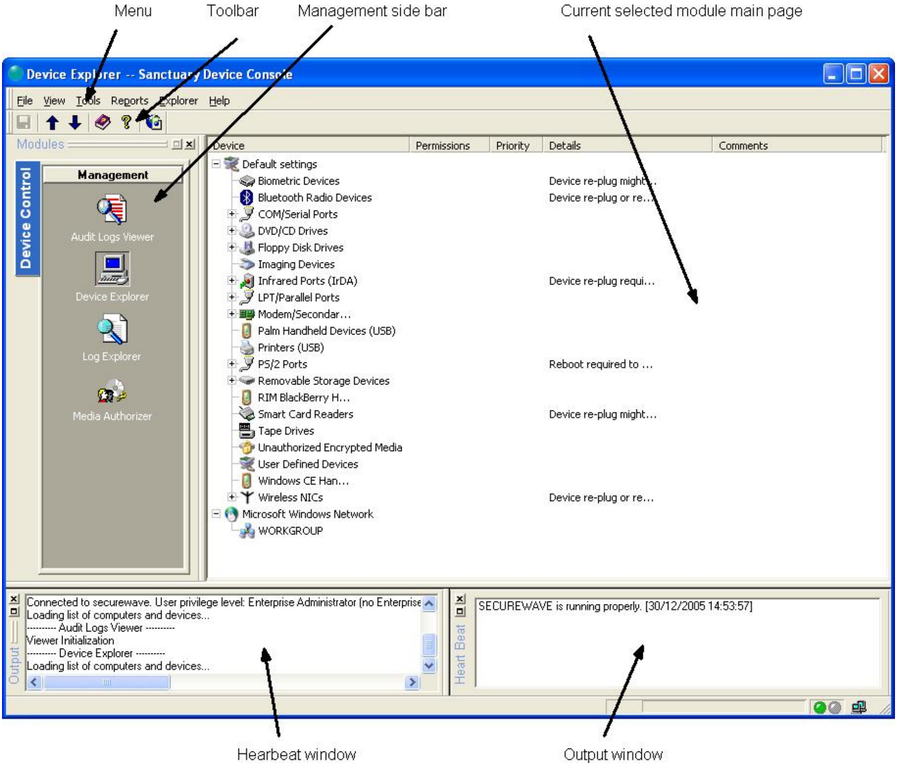
Figure 5: The Connect As dialog

Enter the user name and password that you may want to use to connect to the SecureWave Application Server in this dialog. Prefix the user name by a workstation name for local accounts and by a domain name for domain accounts (e.g. DOMAIN1\ADMIN1).

The Sanctuary Device Control screen

When you begin a Sanctuary Device Console session, the *Sanctuary Device Console Screen* is displayed. The Sanctuary Device 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.



Device	Permissions	Priority	Details	Comments
Default settings				
Biometric Devices			Device re-plug might...	
Bluetooth Radio Devices			Device re-plug or re...	
COM/Serial Ports				
DVD/CD Drives				
Floppy Disk Drives				
Imaging Devices				
Infrared Ports (IrDA)			Device re-plug requi...	
LPT/Parallel Ports				
Modem/Secondar...				
Palm Handheld Devices (USB)				
Printers (USB)				
PS/2 Ports			Reboot required to ...	
Removable Storage Devices				
RIM BlackBerry H...				
Smart Card Readers			Device re-plug might...	
Tape Drives				
Unauthorized Encrypted Media				
User Defined Devices				
Windows CE Han...				
Wireless NICs			Device re-plug or re...	
Microsoft Windows Network				
WORKGROUP				

```
Connected to securewave. User privilege level: Enterprise Administrator (no Enterprise
Loading list of computers and devices...
--------- Audit Logs Viewer ---------
Viewer Initialization
--------- Device Explorer ---------
Loading list of computers and devices...
```

```
SECUREWAVE is running properly. [30/12/2005 14:53:57]
```

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 these depend on the module you are working with. As with nearly all Windows' programs, you can use the ALT key to have immediate access to the different commands. You can use, for example, ALT+P+A to get an HTML Online Machine report.

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

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

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

The *Output* window shows you important information messages. Here you can find those messages generated by updates sent to the clients, file fetching, I/O failures, and error messages. Use the sidebars to navigate through the text.

The *Heartbeat* window shows all the system messages as reported by all the application servers to the Sanctuary Device Control. Use the sidebars to navigate through the text.

Sanctuary modules, menus and tools

The four control modules

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

Module	Icon	Used to ...	In-depth description
Device Explorer		Grant access to I/O devices for specific users or groups. Establish copy limits and activate shadowing.	*Chapter 3: Using the Device Explorer*
Log Explorer		> View records of files copied from any PC to authorized I/O devices, and view the contents of the files themselves. > View the attempts to access or connect unauthorized devices.	*Chapter 4: Using the Log Explorer*
Audit Logs Viewer		View records of all operations made by the administrators on the system.	*Chapter 5: Using the Audit Logs Viewer*
Media Authorizer		> 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.	*Chapter 6: Using the Media Authorizer*

Table 4: 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 5: Using the Audit Logs Viewer* on page *139*.

The Device Explorer

The Device Explorer module is the main nucleus of the Sanctuary Device Console program. 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.

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

- Read data
- Read/Write data
- No access to data
- Online permission

- Offline permission
- Scheduled permission
- Temporary permission
- Shadow permission (a copy of all data written to certain I/O devices)
- Data Copy limit permission

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 devices — is accessible from the Log Explorer module.

This module forms a core part of the control routine that should be done by administrators. Although the driver enforces 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 three 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): 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.

You can find in this log several fields that will help you identify possible policies violations. You can find more information on *Chapter 4: Using the Log Explorer* on page *123*.

The Media Authorizer

Administrators can use the Sanctuary Device 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.

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 on *Chapter 6: Using the Media Authorizer* on page *149*.

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:

Menu	Description
Connect…	Allows you to attach to a SecureWave Application Server in another server or/and with another user name in order to carry out administrative tasks.
Disconnect	Allows you to detach the SecureWave Application Server from the current server. You need to do this in order to reconnect using a different user or server.
Save As…	Save the contents of the main page in CSV format (only available for specific modules).
Exit	Exit the Sanctuary Device Console program.

Table 5: The File menu items

The View menu

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

Menu	Description
Previous	View the previous Module on the list.
Next	View the next Module on the list.
Modules List	Show a submenu that allows you to select any Module.
Modules	Show/hide the Module icons on the left of the screen.
Toolbar	Show/hide the toolbar below the menus.
Output	Show/hide the Output window (data fetch info).
Heartbeat	Show/hide the Heartbeat window (system messages).
Choose Columns	Choose size, position, and visibility of the different columns shown on screen (only available for specific modules).
Refresh (or F5)	Refresh the contents of the screen.

Table 6: The View menu items

The Tools menu

In 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:

Menu	Description
Synchronize Domain members	Allows you to add or update the database with the current list of users and groups of a domain or a local workstation.
Database Maintenance	Here you can delete the shadow files and central event logging entries created before a given date from the database and data file directory.
User Access	Use this command to 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 *Appendix D: Controlling administrative rights for Sanctuary's administrators* on page *251* to learn how to set rights to control Organizational Units/Users/Computers/Groups
Default Options	Here you can change the default computer options settings. You can find more information on *Chapter 8: Setting and changing options* on page *191*.

Menu	Description
Send Updates to all computers	Allows you to send the latest changes to all computers on the network.
Send Updates to	Allows you to send the latest changes to a specific computer on the network.
Purge Online Table	SecureWave Application Servers keep a record of the connected clients. Sometimes, clients are disconnected without notifying their server that they are not available anymore. In this case orphan entries are left in the online table and it impacts 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.

Table 7: The Tools menu items

Sanctuary Device Control keeps a copy of the users' information in its database. When a new user logs on, Sanctuary Device Control stores its Security Identifier (SID) but not its name. The same applies when you add a new computer to the domain: Sanctuary Device Control 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.

The Reports menu

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

Menu	Description
User Permissions…	Allows you to select one or more users and generate a report of their device permissions.
Device Permissions	Here you can generate a report of users' permissions for each device.
Computer Permissions…	Use this command to select a computer and generate a report of the permissions assigned to the user for the use of the different devices of that machine.

Menu	Description
Media by User...	This item lets you select a User or Group and generate a report of the DVDs/CDs they are allowed to use. ✍ *DVDs/CDs authorized as a result of a User being a member of a Group are not listed.* Specific (encrypted) media that users are allowed to use will also be listed in this report.
Users by Medium	Generates 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.
Shadowing by Device...	This item allows you to generate a device grouped report of users copying data to devices.
Shadowing by User...	Generates a report for all users with the total amount of data copied to the different devices.
Online Machines	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.
Options	Presents you with a report including all computer's options as currently defined in the system. These can be changed using the command *Tools → Define Options...*

Table 8: The Report menu items

Please refer to *Chapter 9: Reports* on page *203* for more detailed information.

The Explorer menu

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

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:

Menu	Description
Help	This command allows you to view the help file.
Contents	Use this command to go directly to the contents tab of the help file.
Search...	Use this item to lookup information in the help file.
About...	This item displays information about the current version of Sanctuary Device Control. This is useful when contacting SecureWave technical support staff.
SecureWave on the Web	You can go to the SecureWave home page from here. There you can find updated information about all Sanctuary products.

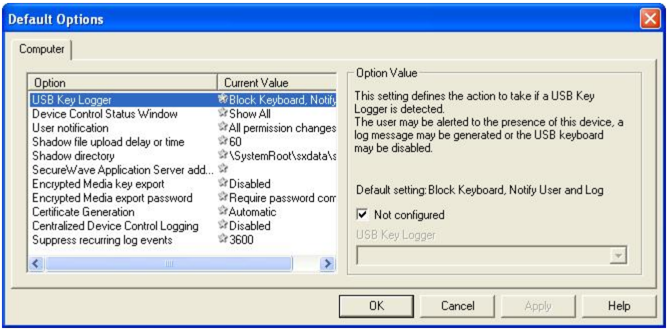
Table 9: The Help menu items

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:



Default Options

Computer

Option	Current Value
USB Key Logger	Block Keyboard, Notify
Device Control Status Window	Show All
User notification	All permission changes
Shadow file upload delay or time	60
Shadow directory	\SystemRoot\sxdata\s
SecureWave Application Server add...	
Encrypted Media key export	Disabled
Encrypted Media export password	Require password com
Certificate Generation	Automatic
Centralized Device Control Logging	Disabled
Suppress recurring log events	3600

Option Value

This setting defines the action to take if a USB Key Logger is detected.
The user may be alerted to the presence of this device, a log message may be generated or the USB keyboard may be disabled.

Default setting: Block Keyboard, Notify User and Log

☑ Not configured

USB Key Logger

Figure 7: 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 checked, 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.

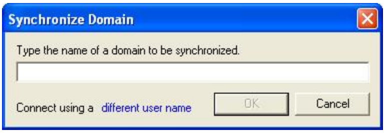
If you change an option, the client computers need to be informed. You can do this by selecting *Send Updates to All Computers* or *Send Updates to* on the *Tools* menu, or you can right-click on the computer in Device Explorer and select *Send Updates to <computername>* from the popup menu.

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

Please refer to *Chapter 8: Setting and changing options* on page *191* 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. The following dialog appears.



Synchronize Domain

Type the name of a domain to be synchronized.

Connect using a different user name

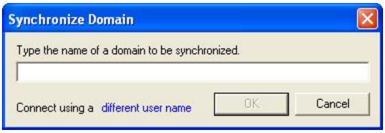
Figure 8: The Synchronizing Domains dialog

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. The following dialog appears:



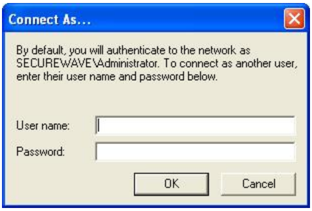
Synchronize Domain

Type the name of a domain to be synchronized.

Connect using a different user name

Figure 9: 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:



Connect As...

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

User name:

Password:

Figure 10: The Connect As dialog

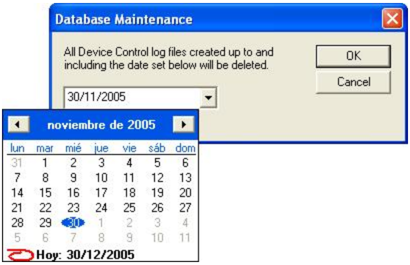
Type in the user name and password for the local administrator for the computer you want to add. Make sure you include the computer's name in the user name. When you have done so, click the OK button twice (to close the corresponding dialog). This adds the computer to the database and you can then proceed 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 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:



Database Maintenance

All Device Control log files created up to and including the date set below will be deleted.

30/11/2005

noviembre de 2005

lun	mar	mié	jue	vie	sáb	dom
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

Hoy: 30/12/2005

Figure 11: Performing database maintenance

You can click on the field's arrow to select the date visually from a calendar. Clicking the OK button will delete the *Central log files* and *Shadow files* before the selected 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).*

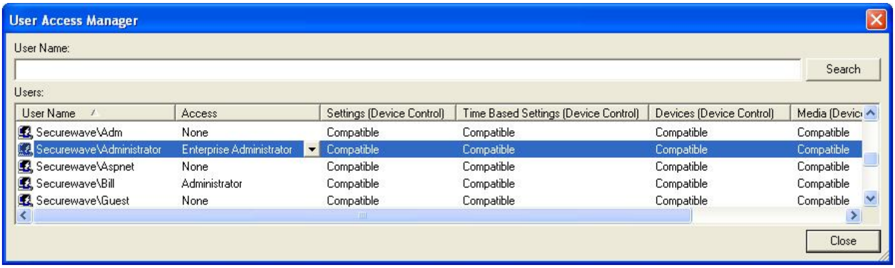
Defining the Sanctuary Device Control administrators

Before proceeding to use the program, we recommend to 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 Device 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 in the Sanctuary Console also changes his role for Sanctuary Device Control.*

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 as shown below.



User Access Manager

User Name:

Users:

User Name	Access	Settings (Device Control)	Time Based Settings (Device Control)	Devices (Device Control)	Media (Devic
Securewave\Adm	None	Compatible	Compatible	Compatible	Compatible
Securewave\Administrator	Enterprise Administrator	Compatible	Compatible	Compatible	Compatible
Securewave\Aspnet	None	Compatible	Compatible	Compatible	Compatible
Securewave\Bill	Administrator	Compatible	Compatible	Compatible	Compatible
Securewave\Guest	None	Compatible	Compatible	Compatible	Compatible

Figure 12: 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 Device Console without being able to assign other users as administrators.

If you are delegating administrative rights using Active Directory Organizational Units, the Sanctuary Device Console Administrators will have the following prerogatives:

Action	*Type of Administrator*	*Comments*
View all permissions.	All Administrators	
Modify global-level permissions.	Enterprise Administrators	
	Members of the 'Manage Device Console Settings' role.	ONLY for the users they are 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,	ONLY for the machines they are allowed to manage.

	including the WELL-KNOWN accounts).	
Modify machine-group 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).	IF AND ONLY IF they are allowed to manage ALL the machines in the machine group for ALL accounts in BOTH CASES, including the WELL-KNOWN accounts.

Table 10: 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 Device Console. Be careful when adding/removing ‘Administrators’ from the list and ensure that there is always at least one Enterprise Administrator.*

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

Option	*This Administrator can do these actions when selecting the ‘Yes’ option*	*Comments*
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.	

Option	*This Administrator can do these actions when selecting the 'Yes' option*	*Comments*
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').
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)'.

Table 11: Administrator's roles

✍ *There are no restrictions on 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 his default rights.*

The *Compatible* mode is to be used when Sanctuary Device Control and Sanctuary suite use a common SecureWave Database and 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* 251 *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 Device 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 16*.

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

You can send permissions updates to computers not connected to the network by file transfer. See *To export and import permission settings* on page *105* 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 what server they reside on. 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, and use the *Synchronize Domain Members* item on the *Tools* menu 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.

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 15: Default settings when first installing the program (these apply to Everyone)* on page *72* and *Table 16: Possible assignments by device* on page *74* 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 *113* 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:

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

Table 12: Standard Windows' device classes as seen on the Device Explorer module of the Default Settings section

These classes are given access rights according to *Table 15: Default settings when first installing the program (these apply to Everyone)* on page *72*. 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 *To assign default permissions* on page *86* for more information

> Online/Offline permissions; see *To assign online and offline permissions* on page *102* for more information

> Scheduled permissions; see *To assign scheduled permissions to users and groups* on page *97* for more information

> Temporary permissions; see *To assign temporary permissions to users* on page *100* for more information

> Shadow; see *Shadowing devices* on page *106* for more information

> Copy limit; see *Copy limits* on page *109* 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 here. Imagine that a user connects a webcam to his computer, a webcam that needs no special drivers to be identified and ready to work. In an unprotected environment, the user can immediately begin recording and sending potentially illegal images over email or other medium. Since his 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 his device since no rule has been defined for him here 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 on the Default Settings section of the Device Explorer module. Please refer to *Managing devices* on page *113* 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.

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 *81* 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:

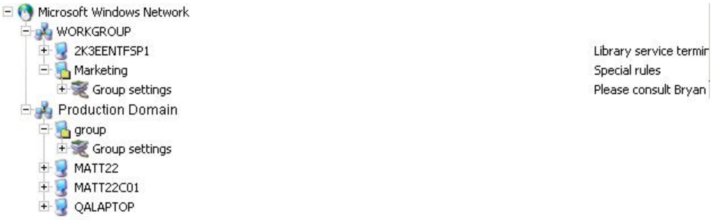


Figure 13: Computers and computer groups

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 *118* for further details.

Defining different types or permissions

You are normally confronted with what kind of permissions you can define for a device class. Take for example the Floppy Disk Drives, Sanctuary Device Control offers the best of both worlds: total control and flexibility when the time comes to assign multiple permissions to access devices. For this specific example you can add independent Read, Read/Write, Online, Offline, Schedule, Temporary, Copy Limit, and Shadow rules and permissions: define only one or a combination of them at the same time (depends on the device class as specified on *Table 13: Simultaneous permissions definitions for all Windows' standard device classes in the Device Explorer module* found on page *60*).

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

> 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

> Copy Limit rule: define 5 MB

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

	*Section in the Device Explorer module**													
	Default Settings							*Microsoft Windows Network*						
Name of the class	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 Adapters	✓	✓	✓	✓	×	✓	×	✓	✓	✓	✓	✓	✓	×
Palm handheld devices (USB)	✓	✓	✓	✓	×	×	×	✓	✓	✓	✓	✓	×	×
Printers (USB)	✓	✓	✓	✓	×	×	×	✓	✓	✓	✓	✓	×	×
PS/2 Ports	✓	✓	✓	×	×	×	×	✓	✓	✓	×	×	×	×
Removable storage devices	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓
RIM BlackBerry handhelds (USB)	✓	✓	✓	✓	×	×	×	✓	✓	✓	✓	✓	×	×
Smart Card Readers	✓	✓	✓	×	×	×	×	✓	✓	✓	×	×	×	×
Tape drives	✓	✓	✓	✓	×	×	×	✓	✓	✓	✓	✓	×	×
Unauthorized Encrypted media	✓	✓	✓	✓	×	×	×	✓	✓	✓	✓	✓	×	×
User defined devices	✓	✓	✓	✓	×	×	×	✓	✓	✓	✓	✓	×	×
Windows CE handheld devices (USB)	✓	✓	✓	✓	×	×	×	✓	✓	✓	✓	✓	×	×
Wireless NICs	✓	✓	✓	×	×	×	×	✓	✓	✓	×	×	×	×

* Code used:
P=Permissions; ON=Online permissions; OF=Offline Permissions;
SC=Schedule; TE=Temporary Permissions; SH=Shadow; CL=Copy limit

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

Encrypting removable media & authorizing specific DVDs/CDs

If you deal with media containing sensible data that is moved around between computers or leaves the company premises, you should consider encrypting it. If the medium is lost or stolen, the intruder must defeat several layers of protection before having access to the actual data. The encryption process alters the data in such a way that it 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.

Once the procedure if finished and the associated users defined – no groups allowed here – the access to the device will be completely transparent for the user(s).

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.

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.

Ghost image deployment

One common problem administrators face is deploying a ‘standard’ computer to a new user or when changing new equipment. Administrators normally do this by installing all necessary software on a ‘fresh’ computer and then using ‘Ghost’ software to create an image. The administrator then imprints this image to all new computers. Sanctuary Client can be part of this image. To include our software as part of this process, follow these steps:

1. Install Sanctuary Client on the machine to be 'ghosted', as you would do for a normal client computer. Check the Setup Guide if in doubt.
2. Change all drivers to start on demand mode:

   Use Regedit to modify the values found in
   `HKLM\System\CurrentControlSet\Services\`

```
scomc: Start, REG_DWORD = 4
sk: Start, REG_DWORD = 4
```

3. Reboot the computer. The driver is installed but does not run.

   delete ALL entries which start with '`\SystemRoot\SxData\...`' in `HKLM\System\CurrentControlSet\Services\sdevpm\Parameters`

   delete the key 'DeviceIndex' found in `HKLM\System\CurrentControlSet\Services\sdevpm\Parameters`

   delete the key 'LastSeenComputerName' found in `HKLM\System\CurrentControlSet\Services\scomc\Parameters`

   if there is another value than (default) with (value not set), delete this one as well

4. Proceed to create the Ghost image from this 'standard' computer.

When deploying the Ghost image:

1. Change the SID and the name of the computer (using Ghostwalker or the freeware SIDchanger tool from SYSinternals: http://www.sysinternals.com).

2. Change the starting mode of each driver back to its original state.

   Use Regedit to modify the following values in `HKLM\System\CurrentControlSet\Services\`

```
scomc: Start, REG_DWORD = 2
sk: Start, REG_DWORD = 0
```

3. Reboot the ‘new’ computer.

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) and no modification to the Sanctuary permission rules is required.

> If a computer group exists (a one-click operation to create using our software) 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 off-line (or on-line).

> 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 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 512MB, 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.*

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 accustom 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* assignations.

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 groups possible. 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 (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 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.*

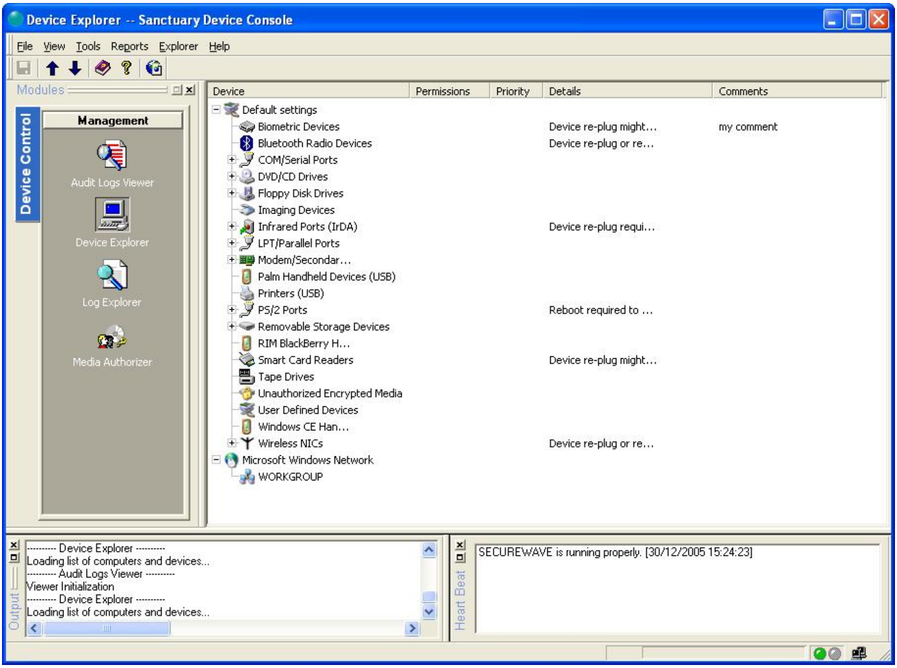
2nd Part: The modules and functions in detail

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 *Device Control* navigation panel of the main window.



Device	Permissions	Priority	Details	Comments
Default settings				
Biometric Devices			Device re-plug might...	my comment
Bluetooth Radio Devices			Device re-plug or re...	
COM/Serial Ports				
DVD/CD Drives				
Floppy Disk Drives				
Imaging Devices				
Infrared Ports (IrDA)			Device re-plug requi...	
LPT/Parallel Ports				
Modem/Secondar...				
Palm Handheld Devices (USB)				
Printers (USB)				
PS/2 Ports			Reboot required to ...	
Removable Storage Devices				
RIM BlackBerry H...				
Smart Card Readers			Device re-plug might...	
Tape Drives				
Unauthorized Encrypted Media				
User Defined Devices				
Windows CE Han...				
Wireless NICs			Device re-plug or re...	
Microsoft Windows Network				
WORKGROUP				

```
--------- Device Explorer ---------
Loading list of computers and devices...
--------- Audit Logs Viewer ---------
Viewer Initialization
--------- Device Explorer ---------
Loading list of computers and devices...
```

```
SECUREWAVE is running properly. [30/12/2005 15:24:23]
```

Figure 14: 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 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 *10: Using Sanctuary Device Control on a Novell network on page* 217*.*

✍ *If the 'Settings (Device Control)' access of the Sanctuary Device Console Administrator User Access is set to No, this administrator will have limited access. See* Table 10 *and Table 11 on pages 52 & 53*

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

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 he is offline (or vice versa).

> Get a copy (shadow) of all data written to 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 he/she tries to gain access to an otherwise unauthorized device.

Changes from previous version

If you are upgrading from a previous versions of our software, use this table to see at-a-glance the recent changes to the *Device Explorer* module:

Device classes as seen on the Device Explorer Module	
Name in previous versions	*New class name for this version*
CD/DVD-ROM	DVD/CD Drives
Floppy	Floppy Disk Drives
Removable	Removable Storage Devices
COM	COM/Serial Ports
LPT	LPT/Parallel Ports
TAPE	Tape Drives
Modem	Modem/Secondary Network Access Devices
Smart Card Reader	Smart Card Readers
Windows CE Devices (USB)	Windows CE Handheld Devices (USB)
Palm OS Handheld Devices (USB)	Palm Handheld Devices (USB)
Scanner	Imaging Devices
User Defined Devices	User Defined Devices
USB Printer	Printers (USB)
BlackBerry (USB)	RIM BlackBerry Handhelds (USB)
Unauthorized Encrypted Media	Unauthorized Encrypted Media
Previously an option	Bluetooth Radio Devices
Previously set during setup	Wireless NICs
Previously an option	Infrared Ports (IrDA)
Previously an option	PS/2 Ports
Previously handled in other classes	Biometric Devices

Table 14: Changes from previous versions

How does the Device Explorer works?

When first installing the software, all permissions are set to their default settings (see the following table). 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:

> In the Default Settings section you can find those permissions that apply to every machine. Here you can modify all authorizations that are 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 *73* 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 *113*.

> 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).

Device	*Permissions*	*Shadow*	*Copy limit*
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 15: 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.

<table>
<tr><th>Device Class</th><th colspan="2">Allowed Permissions</th><th>Applies to</th><th>Notes</th></tr>
<tr><td>Biometric devices</td><td colspan="2">Read-Write /None</td><td>Only to Local System or Everyone</td><td>Device re-plug might be required to grant access for an already blocked device</td></tr>
<tr><td>Bluetooth radio devices</td><td colspan="2">Read-Write /None</td><td>Only the Local System or Everyone group</td><td>Device re-plug or reboot required to enforce updated permissions</td></tr>
<tr><td>COM/Serial ports</td><td colspan="2">Read-Write/None</td><td>Any user or group</td><td>-</td></tr>
<tr><td>DVD/CD drives</td><td colspan="2">Read only/ Read-Write/None</td><td>Any user or group</td><td>-</td></tr>
<tr><td>Floppy disk drives</td><td colspan="2">Read only/ Read-Write/None</td><td>Any user or group</td><td>-</td></tr>
<tr><td>Imaging devices (for example a Scanner)</td><td colspan="2">Read-Write /None</td><td>Any user or group</td><td>-</td></tr>
<tr><td>Infrared Ports (IrDA)</td><td colspan="2">Read-Write /None</td><td>Only to Local System or Everyone</td><td>Device re-plug required to grant access for an already blocked port</td></tr>
<tr><td>LPT/Parallel ports</td><td colspan="2">Read-Write/None</td><td>Any user or group</td><td>-</td></tr>
<tr><td rowspan="2">Modem/Secondary Network Adapters</td><td>Regular modems</td><td>Read-Write/None</td><td>Any user or group</td><td>-</td></tr>
<tr><td>ISDN modems or network adapters</td><td>Read-Write/None</td><td>Only the Everyone group</td><td>Device re-plug or reboot required to enforce updated permissions</td></tr>
<tr><td>Palm handheld devices (USB)</td><td colspan="2">Read-Write /None</td><td>Any user or group</td><td>-</td></tr>
</table>

Device Class	Allowed Permissions	Applies to	Notes
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	-
RIM BlackBerry handhelds (USB)	Read-Write /None	Any user or group	-
Smart Card Readers	Read-Write/None	Only Local System or Everyone	Device re-plug might be required to grant access for an already blocked device
Tape drives	Read-Write/None	Any user or group	Some backup units do not use the Microsoft supplied drivers and cannot be controlled by Sanctuary Device Control
Windows CE handeld devices (USB)	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 16: 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.

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, multiple select, and using drag & drop

You can use multiple selection (with the SHIFT and CTRL key) to assign permissions as a whole saving you considerable time and effort. You can, for example, select the Floppy Disk and LPT Port in the Default Settings and then right-click to get a contextual menu to set permissions:

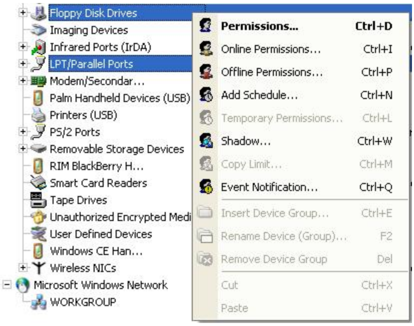


Figure 15: Context menu

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 Device 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:

Shortcut	*Description*
CRTL+D	Add/Modify permission for the selected item(s)
CRTL+P	Add/ Modify Offline permission for the selected item(s)
CRTL+I	Add/ Modify Online permission for the selected item(s)
CRTL+N	Add/ Modify a schedule for the selected item(s)
CRTL+L	Add/ Modify a temporary permission for the selected item(s)
CRTL+W	Add/ Modify Shadow settings

Shortcut	*Description*
CRTL+M	Define the Copy limit for the selected item(s)
CRTL+E	Insert Device Group
F2	Rename Computer Group/Device
DELETE	Delete entry (see note below)
CRTL+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 17: 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* 77 *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 administrators of the Sanctuary Device Control. 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, double-click on the *Comments* column of the item you want to edit. 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’ and this can cause errors when trying to only change lower to uppercase.

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. The ‘hidden’ computer(s) is displayed.

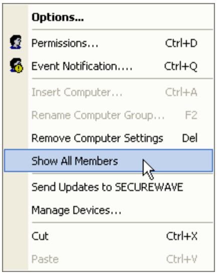

Options...
Permissions... Ctrl+D
Event Notification.... Ctrl+Q
Insert Computer... Ctrl+A
Rename Computer Group... F2
Remove Computer Settings Del
Show All Members
Send Updates to SECUREWAVE
Manage Devices...
Cut Ctrl+X
Paste Ctrl+V

Figure 16: 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).

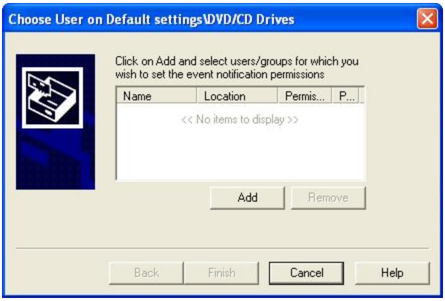
To create an event notification for a specific user, follow these steps:

1. Activate the Device Explorer module by clicking on its icon: .

2. Click on the device class where you want to create the rule and then use the CRTL+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.

4. Click on NEXT. The following dialog appears:



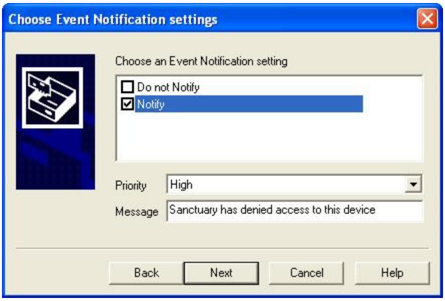
Choose User on Default settings\DVD/CD Drives

Click on Add and select users/groups for which you wish to set the event notification permissions

Name	Location	Permis...	P...
<< No items to display >>			

Figure 17: Event notification: selecting the users/groups

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



Choose Event Notification settings

Choose an Event Notification setting

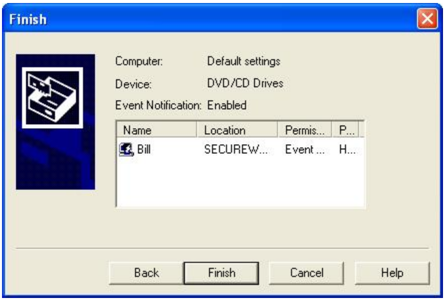
☐ Do not Notify
☑ Notify

Priority: High

Message: Sanctuary has denied access to this device

Figure 18: Event notification: options

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

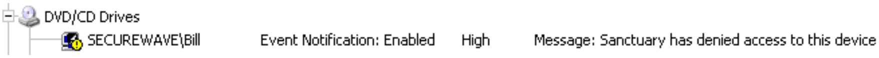


Computer: Default settings
Device: DVD/CD Drives
Event Notification: Enabled

Name	Location	Permis...	P...
Bill	SECUREW...	Event ...	H...

Figure 19: Event notification: finish the rule definition

You now see a new permission rule defined for the device class. In the following figure you see an example for the DVD/CD Drives class for user Bill.



DVD/CD Drives
SECUREWAVE\Bill Event Notification: Enabled High Message: Sanctuary has denied access to this device

Figure 20: 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 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 in 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.

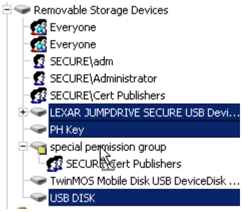
> Select any device, at its upper level or class, and use *Insert Device Group* from the *Explorer* menu.

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

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

Table 18: Device classes that can have Device Groups

Once a device group is created, you can add any device of the same class to this newly created group. To do this select all the devices using the SHIFT or CTRL keys and then use Drag & Drop to move these devices to the new group:



Removable Storage Devices
Everyone
Everyone
SECURE\adm
SECURE\Administrator
SECURE\Cert Publishers
LEXAR JUMPDRIVE SECURE USB Devi...
PH Key
special permission group
SECURE\Cert Publishers
TwinMOS Mobile Disk USB DeviceDisk ...
USB DISK

Figure 21: Using Drag & Drop to move devices to a newly created group

Once a group created, you can use the Drag&Drop functionality to move devices between different groups. You can also use the shortcut key commands: Cut (CTRL+C), Copy (CRTL+C), and Paste (CTRL+V) for the same purpose. These commands are also available from the right click context menu.

Supported device types

The Device Explorer can be used to control access to a variety of I/O devices. Setting access to the *Default settings*, Device Explorer's root node, allows the user to access that device 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, 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 will, 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

Conventional parallel printer ports, including 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 (USB)

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 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.*

PS/2 Ports

A standard port to connect a keyboard and mouse. 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 our other Sanctuary products.

Removable Storage Devices

Removable disk drives of any kind not included within the Floppy 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 (USB)

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.*

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 to use this class of devices will be able to access those encrypted by Sanctuary Device Control in another organization. See *Chapter 7: Accessing encrypted media outside of your organization* on page *175*.

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 (USB)

Handheld Windows CE computers (using PocketPC OS) connected to the PC through a USB port. Examples: HP iPAQ, XDA.

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.*

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 at:

- 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, the previously defined device group '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 4: Using the Log Explorer* on page *123* for more details) without denying them access. You can combine this feature with a "Shadow" (see *Shadowing devices* on page *106* for more details) at device class level for a full log control.

How do you assign default permissions to a node?

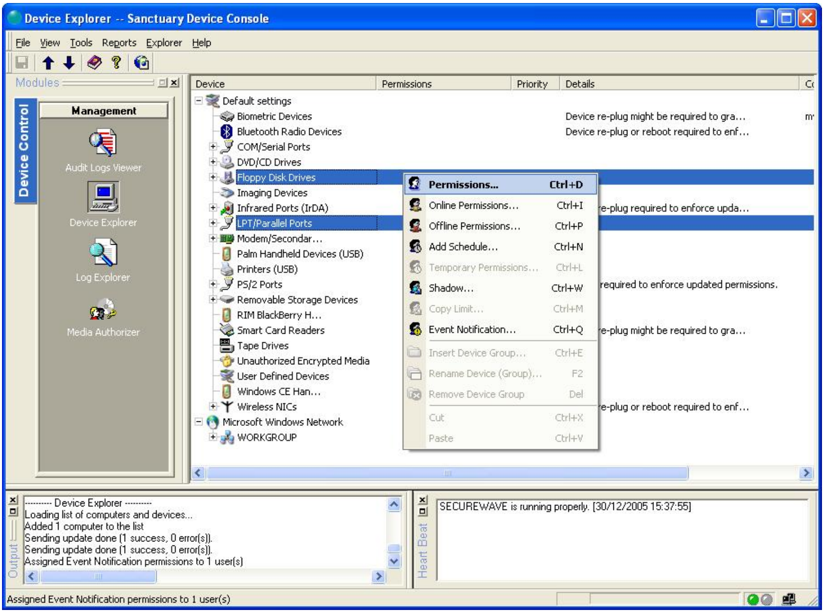
To assign permissions, follow the steps outlined in the next section. The only difference is that you should select the nodes described on the previous list (root of the Device Explorer tree, a specific device class, device group, computer or group settings of a computer group in the Microsoft Windows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

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 one or several devices (use the SHIFT or CTRL key) within the 'Default settings' list. Right-click on the device selection and choose *Permissions* from the popup menu. Alternatively, select the devices and then select *Add / Modify Permissions...* from the Explorer menu or use the CTRL+D shortcut key.


Device Explorer -- Sanctuary Device Console
File View Tools Reports Explorer Help
Modules
Device Control
Management
Audit Logs Viewer
Device Explorer
Log Explorer
Media Authorizer
Device
Permissions
Priority
Details
Default settings
Biometric Devices
Bluetooth Radio Devices
COM/Serial Ports
DVD/CD Drives
Floppy Disk Drives
Imaging Devices
Infrared Ports (IrDA)
LPT/Parallel Ports
Modem/Secondar...
Palm Handheld Devices (USB)
Printers (USB)
PS/2 Ports
Removable Storage Devices
RIM BlackBerry H...
Smart Card Readers
Tape Drives
Unauthorized Encrypted Media
User Defined Devices
Windows CE Han...
Wireless NICs
Microsoft Windows Network
WORKGROUP
Device re-plug might be required to gra...
Device re-plug or reboot required to enf...
re-plug required to enforce upda...
required to enforce updated permissions.
re-plug might be required to gra...
re-plug or reboot required to enf...
Permissions... Ctrl+D
Online Permissions... Ctrl+I
Offline Permissions... Ctrl+P
Add Schedule... Ctrl+N
Temporary Permissions... Ctrl+L
Shadow... Ctrl+W
Copy Limit... Ctrl+M
Event Notification... Ctrl+Q
Insert Device Group... Ctrl+E
Rename Device (Group)... F2
Remove Device Group Del
Cut Ctrl+X
Paste Ctrl+V
Output
Heart Beat

```
--------- Device Explorer ---------
Loading list of computers and devices...
Added 1 computer to the list
Sending update done (1 success, 0 error(s)).
Sending update done (1 success, 0 error(s)).
Assigned Event Notification permissions to 1 user(s)
```

```
SECUREWAVE is running properly. [30/12/2005 15:37:55]
```

Assigned Event Notification permissions to 1 user(s)

Figure 22: Assigning default permissions to users and groups

The *Permissions* dialog is displayed.

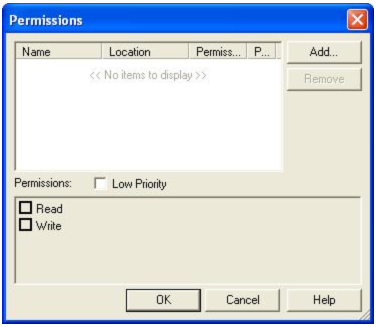


Figure 23: The Permissions dialog

2. Click on the Add button.

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

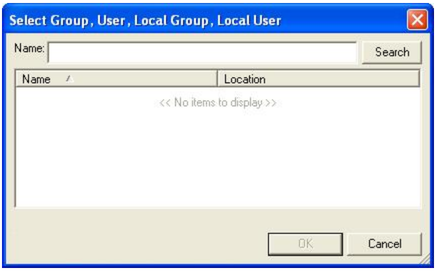
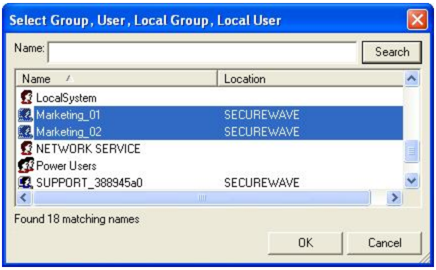

Select Group, User, Local Group, Local User
Name:
Search
Name
Location
<< No items to display >>
OK
Cancel

Figure 24: 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.

4. Back in the *Permissions* dialog, select the user(s)/group(s) you want to assign permissions to, and then activate the appropriate options. Select between Read Only, Read/Write, or None (not selecting any option). Use the Ctrl or Shift key to make multiple selections. The value (multiple) means that the user or group has different permissions on the device

selection. A user having a read-only access to floppy and a read/write access to the modem is an example of multiple permissions.



Select Group, User, Local Group, Local User

Name:

Name	Location
LocalSystem	
Marketing_01	SECUREWAVE
Marketing_02	SECUREWAVE
NETWORK SERVICE	
Power Users	
SUPPORT_388945a0	SECUREWAVE

Found 18 matching names

Figure 25: Defining Read, Read/Write, or None attributes when adding default permissions

5. Click OK to finish.

The *Permissions* column in the main window now shows those options (Read, Read/Write, or None – not selecting Read nor Write) 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. 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 73 *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, 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 he is a member, at the Default level and computer-specific level:

Default Setting	Default Permission Priority	Computer-specific permission	Computer Specific permission priority	Resulting permission	Explanation
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-only	
			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:

None	Highest ↓ Lowest
Read/Write	
Read only	

Table 19: Applied permissions

✍ *Please refer to* Permissions Priority *on page* 169 *for an explanation of the priority rules interacting between those permissions defined at the Device Explorer level and those defined at the Media Authorizer level.*

Read/Write permissions

Only those devices that support a file system can be set to read-only mode. For all others, the only possible permission is either None or Read/Write. Read-only applies to floppy drives, DVD/CD drives, and Removable media. See *Table 16: Possible assignments by device* on page *74* 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 it and select *Insert Computer*. Alternatively, select *Insert Computer* from the *Explorer* menu or use the CRTL+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:

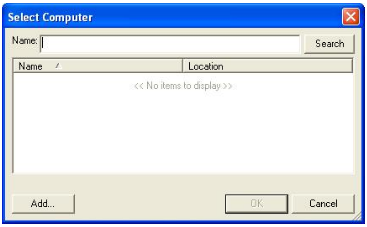
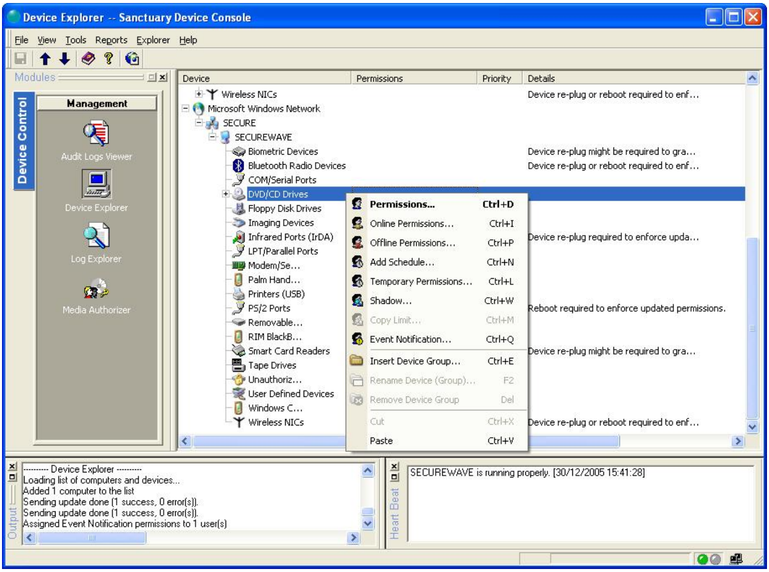


Figure 26: The Select Computer dialog showing multiple selection in action

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 return to the Device Explorer.



```
--------- Device Explorer ---------
Loading list of computers and devices...
Added 1 computer to the list
Sending update done (1 success, 0 error(s)).
Sending update done (1 success, 0 error(s)).
Assigned Event Notification permissions to 1 user(s)
```

```
SECUREWAVE is running properly. [30/12/2005 15:41:28]
```

Figure 27: 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 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.

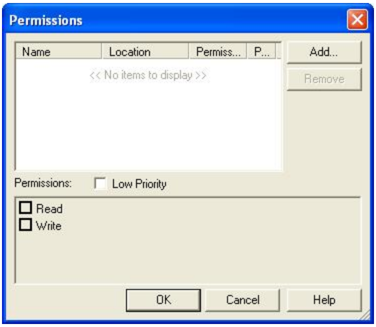


Figure 28: Defining Read, Read/Write, or None permissions when adding permissions

5. Click on ADD.

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

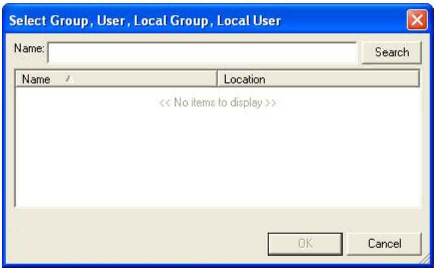

Select Group, User, Local Group, Local User
Name:
Search
Name
Location
<< No items to display >>
OK
Cancel

Figure 29: 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.

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.*

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.

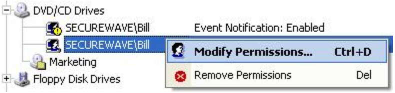


Figure 30: Modifying permissions

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.*

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.

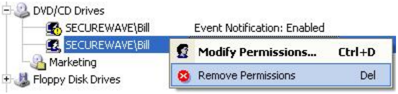


Figure 31: Removing permissions

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.

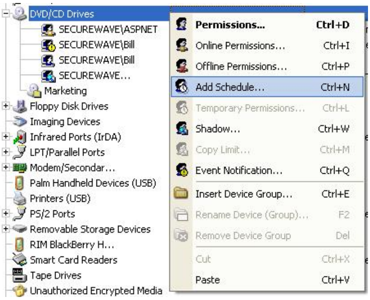
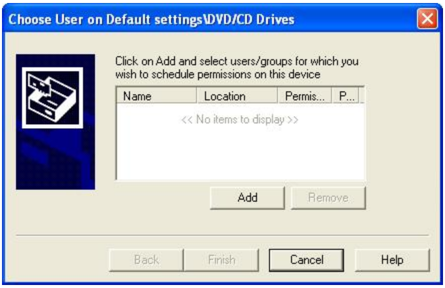


Figure 32: Add a Scheduled permission

The *Choose User* dialog is displayed.

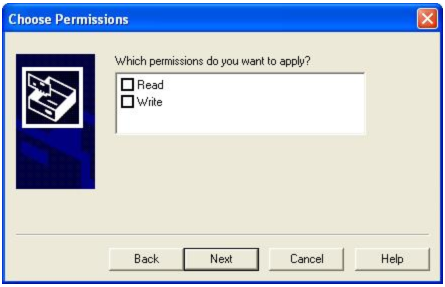

Choose User on Default settings\DVD/CD Drives

Click on Add and select users/groups for which you wish to schedule permissions on this device

Name	Location	Permis...	P...
<< No items to display >>			

Figure 33: 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. Then click NEXT. The *Choose Permissions* dialog is displayed. 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.



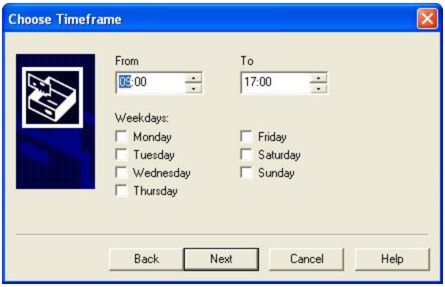
Choose Permissions

Which permissions do you want to apply?

□ Read
□ Write

Figure 34: Defining Read, Read/Write, or None permissions when adding scheduled permissions

3. Choose the permissions that you want to apply to the schedule. Then click NEXT. The *Choose Timeframe* dialog is displayed.



Choose Timeframe

From: 09:00

To: 17:00

Weekdays:

□ Monday
□ Tuesday
□ Wednesday
□ Thursday
□ Friday
□ Saturday
□ Sunday

Figure 35: The Choose Timeframe dialog when adding a scheduled permission

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

5. Click NEXT and then click 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. You can, alternatively, send the list immediately by selecting the 'Send Updates to All Computers' or 'Send Updates To' item on the 'Tools' menu.*

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.

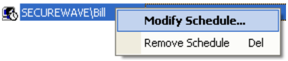


Figure 36: Modifying a scheduled permission

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.

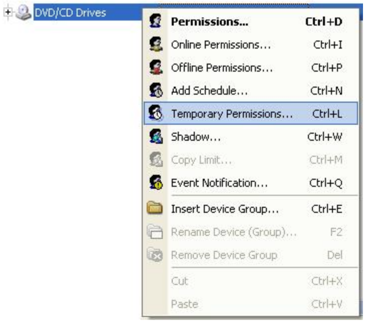
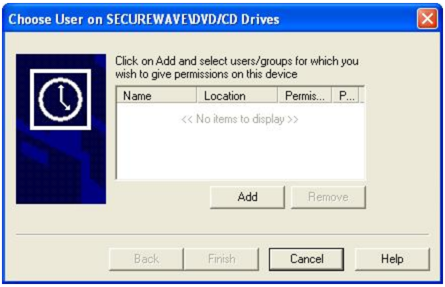

DVD/CD Drives
Permissions... Ctrl+D
Online Permissions... Ctrl+I
Offline Permissions... Ctrl+P
Add Schedule... Ctrl+N
Temporary Permissions... Ctrl+L
Shadow... Ctrl+W
Copy Limit... Ctrl+M
Event Notification... Ctrl+Q
Insert Device Group... Ctrl+E
Rename Device (Group)... F2
Remove Device Group Del
Cut Ctrl+X
Paste Ctrl+V

Figure 37: Adding a Temporary permission

The *Choose User* dialog is displayed.

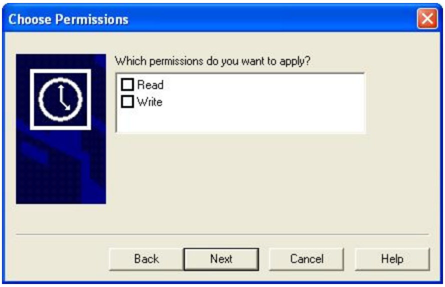

Choose User on SECUREWAVE\DVD/CD Drives
Name
Location
Permis...
P...
<< No items to display >>
Add
Remove
Back
Finish
Cancel
Help

Click on Add and select users/groups for which you wish to give permissions on this device

Figure 38: 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 Permissions* dialog is displayed.



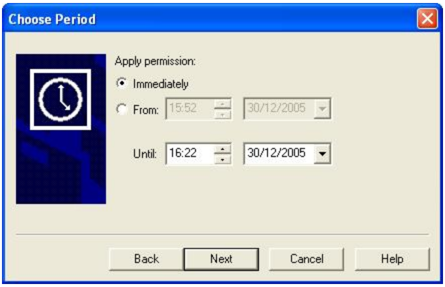
Which permissions do you want to apply?

□ Read
□ Write

Figure 39: Defining Read, Read/Write, or None permissions when adding a temporary permission

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

The *Choose Period* dialog is displayed.



Choose Period

Apply permission:

● Immediately

○ From: 15:52 30/12/2005

Until: 16:22 30/12/2005

Figure 40: The Choose Period dialog when adding a temporary permission

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

5. Click NEXT and then click FINISH.

To remove temporary permissions

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

To assign 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 completely his DVD/CD writer 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.

To assign Online or Offline permissions, use the following procedure (it is the same one 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).

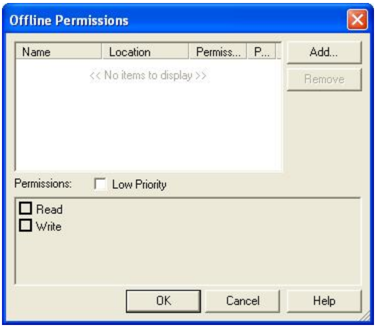


Figure 41: Defining Read, Read/Write, or None permissions when adding online/offline permission

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 Read or Read/Write options and accept by clicking on OK.

✍ *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. 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.
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.

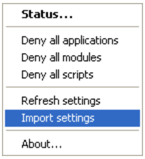


Figure 42: Importing permission settings

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 to a device, use the shadowing rule. This rule is available for:

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

You can define shadowing for:

- A user or group of users on a specific device for a computer
- A user or group of users on a class of devices (only those shown in the upper list)
- A user or group of users on a group of devices

✍ *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 his computer is disconnected from the network, the shadow information is transferred to the server as soon as the machine is reconnected to the network.*

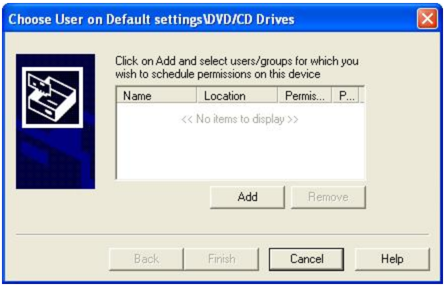
The removable devices also have an 'Encryption' mode that does 'shadowing' even when the device has been encrypted. Please see *Chapter 6: Using the Media Authorizer* on page *149* for more information.

✍ *If you choose the* Enabled *option, shadow is not active for encrypted devices. You need to select* Encryption *instead.*

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.



Choose User on Default settings\DVD/CD Drives

Click on Add and select users/groups for which you wish to schedule permissions on this device

Name	Location	Permis...	P...
<< No items to display >>			

Figure 43: The Choose User dialog when adding a shadow rule

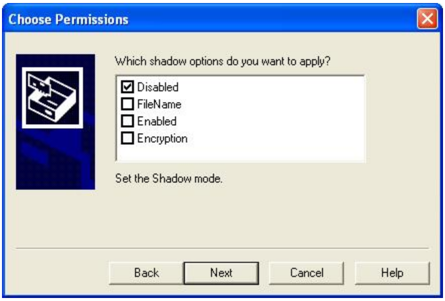
2. Click on the ADD button and select the user(s)/groups(s) from the *Select Group, User, Local Group or Local User* dialog.

3. Select either *Enabled*, *Disabled*, *Filename*, or *Encrypted* (some devices only support Enable and Disable: Encrypted is only allowed for the Removable Devices) to switch shadowing on or off.

   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, you will not see a clip icon 📎 by the file name in the Log Explorer module. 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 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 or resources and hard disk space. When full shadowing is enabled, you see a clip icon 📎 by the name in the Log Explorer module.

   You will only find the *Encryption* option in the Removable Devices class. This mode will shadow full content of all data copied to the device even if the device is encrypted. See *Chapter 6: Using the Media Authorizer* on page *149* for more details.



Choose Permissions

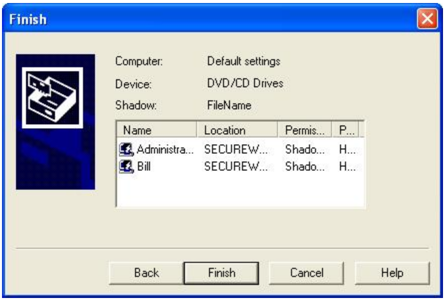
Which shadow options do you want to apply?

☑ Disabled
☐ FileName
☐ Enabled
☐ Encryption

Set the Shadow mode.

Figure 44: Defining the type of shadow for a device

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



Finish

Computer: Default settings
Device: DVD/CD Drives
Shadow: FileName

Name	Location	Permis...	P...
Administra...	SECUREW...	Shado...	H...
Bill	SECUREW...	Shado...	H...

Figure 45: Finishing the shadow rule definition

5. 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. 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 limits

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

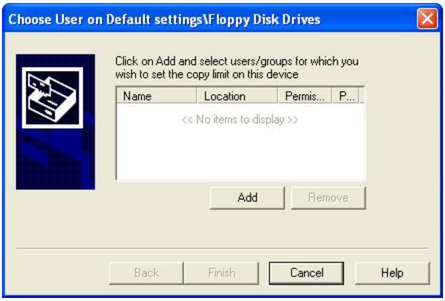
> *Copy limit can also be applied to Administrators. If you do not want this restriction to apply to them, you should modify the default copy limit rule as defined in the 'Device Explorer' module.*

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 1MB to floppies and 5MB to 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.



Choose User on Default settings\Floppy Disk Drives

Click on Add and select users/groups for which you wish to set the copy limit on this device

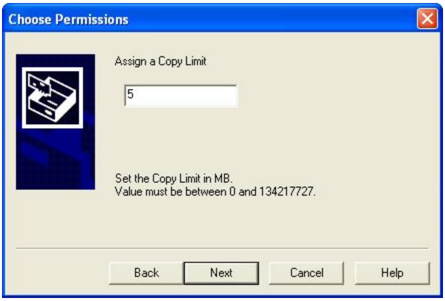
Name	Location	Permis...	P...

<< No items to display >>

Figure 46: 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):



Assign a Copy Limit

5

Set the Copy Limit in MB.
Value must be between 0 and 134217727.

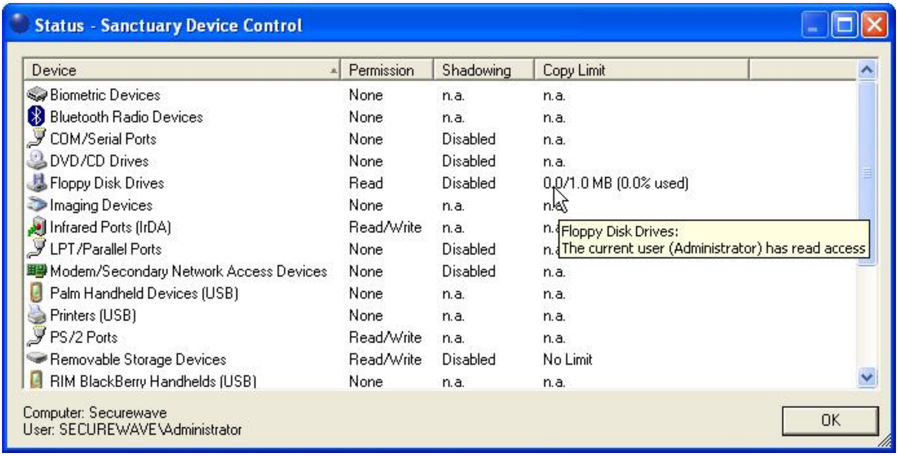
Figure 47: Defining a copy limit

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 a user selects the *Status* item of the icon tray pop-up menu, he/she can see how many bytes have been copied and how many are there remaining for his working day. This only applies to those devices that have the copy limit rule set as shown on *Figure 48*.



Device	Permission	Shadowing	Copy Limit
Biometric Devices	None	n.a.	n.a.
Bluetooth Radio Devices	None	n.a.	n.a.
COM/Serial Ports	None	Disabled	n.a.
DVD/CD Drives	None	Disabled	n.a.
Floppy Disk Drives	Read	Disabled	0.0/1.0 MB (0.0% used)
Imaging Devices	None	n.a.	n.a.
Infrared Ports (IrDA)	Read/Write	n.a.	n.
LPT/Parallel Ports	None	Disabled	n.
Modem/Secondary Network Access Devices	None	Disabled	n.a.
Palm Handheld Devices (USB)	None	n.a.	n.a.
Printers (USB)	None	n.a.	n.a.
PS/2 Ports	Read/Write	n.a.	n.a.
Removable Storage Devices	Read/Write	Disabled	No Limit
RIM BlackBerry Handhelds (USB)	None	n.a.	n.a.

Floppy Disk Drives:
The current user (Administrator) has read access

Computer: Securewave
User: SECUREWAVE\Administrator

Figure 48: 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* 47 *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.

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 only on his laptop.

When Bill logs onto his laptop, he will have the following permissions:

> Read/Write access to DVD/CD. The priority of 'None' is low and can be overwritten by computer-specific permissions (only if its priority is '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.

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 he plugs it in the computer.

Nevertheless, if you want to define permissions more precisely, you can set rules for certain models of devices (device types). In this case, and only in this case, it is your responsibility to set up and manage the devices for which you want to define device model-specific 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. 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

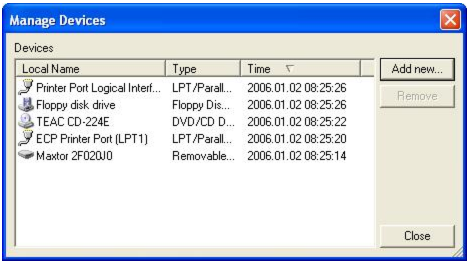
> Infrared Ports (IrDA)

> 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 Device 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:



Local Name	Type	Time
Printer Port Logical Interf...	LPT/Parall...	2006.01.02 08:25:26
Floppy disk drive	Floppy Dis...	2006.01.02 08:25:26
TEAC CD-224E	DVD/CD D...	2006.01.02 08:25:22
ECP Printer Port (LPT1)	LPT/Parall...	2006.01.02 08:25:20
Maxtor 2F020J0	Removable...	2006.01.02 08:25:14

Figure 49: 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:

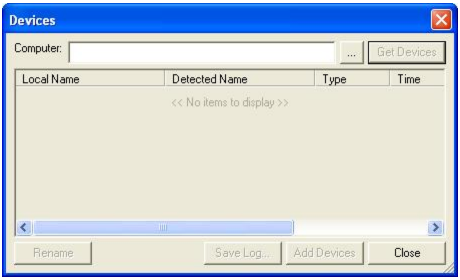
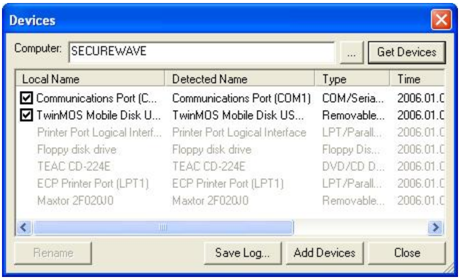


Figure 50: Managing devices – selecting the computer

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.



Computer: SECUREWAVE

Local Name	Detected Name	Type	Time
☑ Communications Port (C...	Communications Port (COM1)	COM/Seria...	2006.01.0
☑ TwinMOS Mobile Disk U...	TwinMOS Mobile Disk US...	Removable...	2006.01.0
Printer Port Logical Interf...	Printer Port Logical Interface	LPT/Parall...	2006.01.0
Floppy disk drive	Floppy disk drive	Floppy Dis...	2006.01.0
TEAC CD-224E	TEAC CD-224E	DVD/CD D...	2006.01.0
ECP Printer Port (LPT1)	ECP Printer Port (LPT1)	LPT/Parall...	2006.01.0
Maxtor 2F020J0	Maxtor 2F020J0	Removable...	2006.01.0

Figure 51: 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.

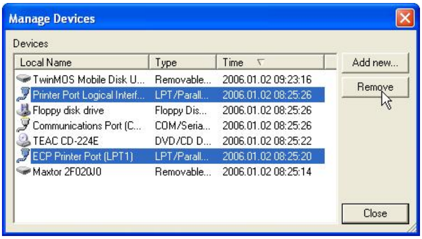
✍ *The list of new devices is not sent to the client computer immediately. This list is downloaded the next time a user logs onto that computer. You can, alternatively, send the list immediately by selecting the 'Send Updates to All Computers' or 'Send Updates To' item on the 'Tools' menu.*

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.

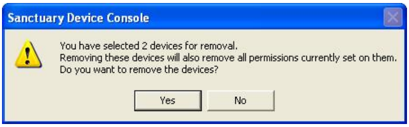
2. Select the device(s) you want to remove. Use the Shift/Ctrl key to make multiple selections.



Local Name	Type	Time
TwinMOS Mobile Disk U...	Removable...	2006.01.02 09:23:16
Printer Port Logical Interf...	LPT/Parall...	2006.01.02 08:25:26
Floppy disk drive	Floppy Dis...	2006.01.02 08:25:26
Communications Port (C...	COM/Seria...	2006.01.02 08:25:26
TEAC CD-224E	DVD/CD D...	2006.01.02 08:25:22
ECP Printer Port (LPT1)	LPT/Parall...	2006.01.02 08:25:20
Maxtor 2F020J0	Removable...	2006.01.02 08:25:14

Figure 52: Removing devices

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



You have selected 2 devices for removal.
Removing these devices will also remove all permissions currently set on them.
Do you want to remove the devices?

Figure 53: Confirming the removal of a device

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

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 *109* for more information). You would ideally place all different models of Zip drive readers in a device group (see *Device Groups* on page *81* for details) and set a permission to this group of devices for the domain group ‘Marketing’.

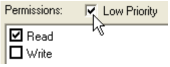
> To set permissions to the whole class, select the device on the *Default settings* section and right-click on it selecting the type of *Permissions* you need from the popup menu. You can assign general, online, offline, schedule, shadow, and copy limit permissions to the device as a whole.

> 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):



Permissions: ☑ Low Priority

☑ Read

□ Write

Figure 54: 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 prepared especially for them to do this on, which you carry out a Shadowing of the 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. 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.

Device level where the permission is defined	*Permission applied*	*Priority*	*Result to apply to the specific device*
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	

Device level where the permission is defined	*Permission applied*	*Priority*	*Result to apply to the specific device*
Class	Read/Write	High	Read/Write
Type	Read	High	
Class	Read	Low	Read/Write
Type	Read/Write	Low	

Table 20: Resulting access

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

Permission setting	*Order*
None	↓
Read/Write	
Read	

Table 21: Permission settings priority

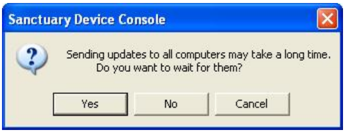
✍ *We can distinguish between two removable devices of the same make by using the Media Authorizer module.*

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.

The following dialog will show when you choose the *Send Updates to All Computers* command:

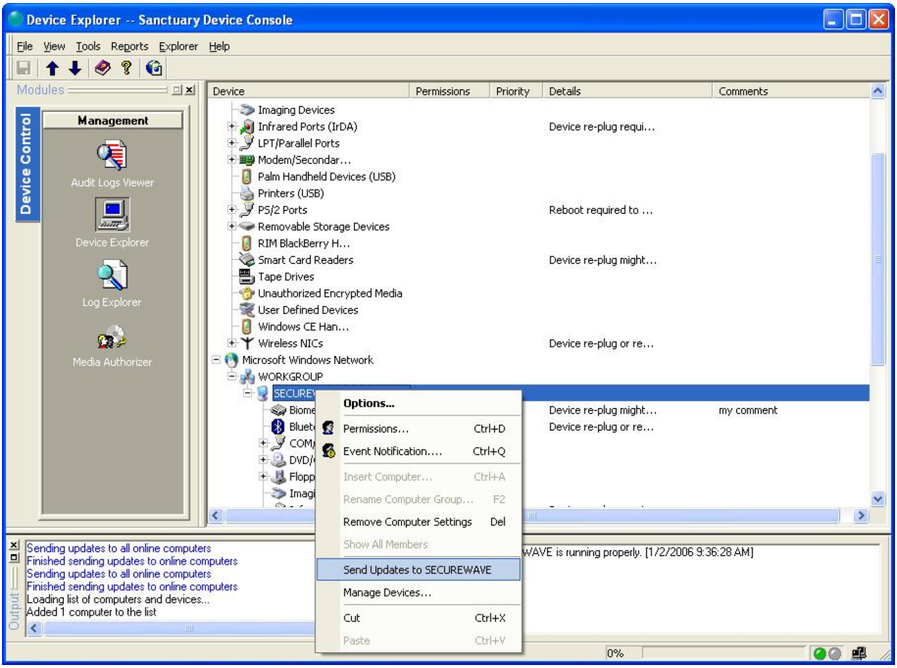

Sanctuary Device Console

Sending updates to all computers may take a long time.
Do you want to wait for them?

Figure 55: Sending updates to client computers

If you click on the YES button, the program can take a lot of time sending the updates since this process is done in a synchronously way; 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 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 and select *Send Updates to: <computername>* from the popup menu (or select the same option from the *Tools* menu).


Device Explorer -- Sanctuary Device Console
File View Tools Reports Explorer Help
Modules
Device Control
Management
Audit Logs Viewer
Device Explorer
Log Explorer
Media Authorizer
Options...
Permissions... Ctrl+D
Event Notification.... Ctrl+Q
Insert Computer... Ctrl+A
Rename Computer Group... F2
Remove Computer Settings Del
Show All Members
Send Updates to SECUREWAVE
Manage Devices...
Cut Ctrl+X
Paste Ctrl+V
Output
0%

Device	Permissions	Priority	Details	Comments
Imaging Devices				
Infrared Ports (IrDA)			Device re-plug requi...	
LPT/Parallel Ports				
Modem/Secondar...				
Palm Handheld Devices (USB)				
Printers (USB)				
PS/2 Ports			Reboot required to ...	
Removable Storage Devices				
RIM BlackBerry H...				
Smart Card Readers			Device re-plug might...	
Tape Drives				
Unauthorized Encrypted Media				
User Defined Devices				
Windows CE Han...				
Wireless NICs			Device re-plug or re...	
Microsoft Windows Network				
WORKGROUP				
SECURE				
Biome			Device re-plug might...	my comment
Bluet			Device re-plug or re...	
COM/				
DVD/				
Flopp				
Imagi				

```
Sending updates to all online computers
Finished sending updates to online computers
Sending updates to all online computers
Finished sending updates to online computers
Loading list of computers and devices...
Added 1 computer to the list
```

```
WAVE is running properly. [1/2/2006 9:36:28 AM]
```

Figure 56: The send update item from the contextual menu

You do not need to use the *Tools* menu when you set Temporary Permissions. They are sent out automatically as soon as they are 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 *on page* 214*. 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 BIN\Tools directory of your Sanctuary Device Control Media.*

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

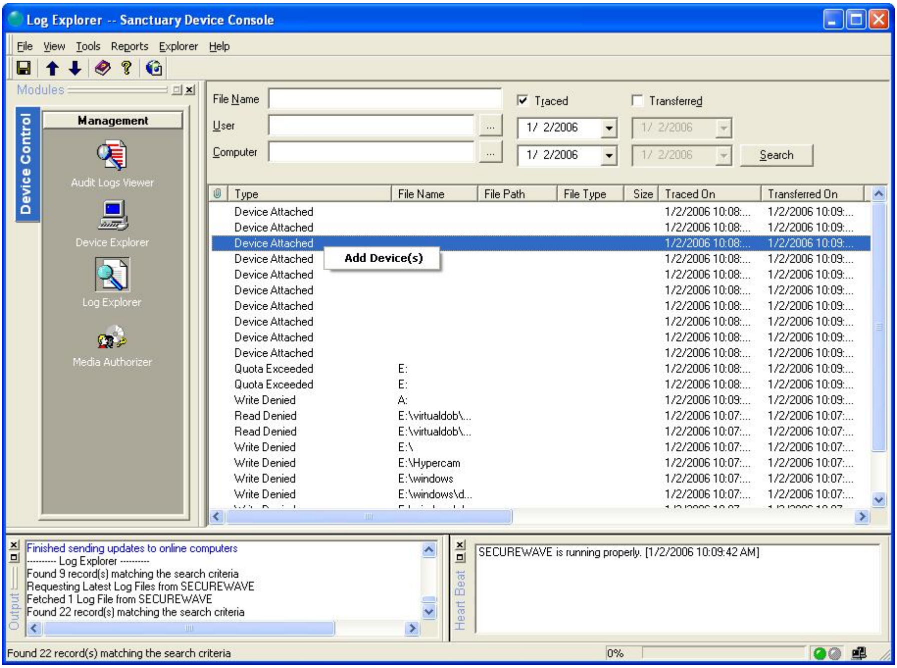
Chapter 4: Using the Log Explorer

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 he did not have permission, 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 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 by right clicking on the register and selecting *Add device(s)* directly from the menu. If the log file was generated using a previous version of the client driver, this right click menu is not available. Please see *Managing devices* on page *113* for a full description on how to add specific devices.



File Name
User
Computer
☑ Traced 1/ 2/2006 1/ 2/2006
☐ Transferred 1/ 2/2006 1/ 2/2006

Type	File Name	File Path	File Type	Size	Traced On	Transferred On
Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
Quota Exceeded	E:				1/2/2006 10:08:...	1/2/2006 10:09:...
Quota Exceeded	E:				1/2/2006 10:08:...	1/2/2006 10:09:...
Write Denied	A:				1/2/2006 10:09:...	1/2/2006 10:09:...
Read Denied	E:\virtualdob\...				1/2/2006 10:07:...	1/2/2006 10:07:...
Read Denied	E:\virtualdob\...				1/2/2006 10:07:...	1/2/2006 10:07:...
Write Denied	E:\				1/2/2006 10:07:...	1/2/2006 10:07:...
Write Denied	E:\Hypercam				1/2/2006 10:07:...	1/2/2006 10:07:...
Write Denied	E:\windows				1/2/2006 10:07:...	1/2/2006 10:07:...
Write Denied	E:\windows\d...				1/2/2006 10:07:...	1/2/2006 10:07:...

```
Finished sending updates to online computers
---------- Log Explorer ----------
Found 9 record(s) matching the search criteria
Requesting Latest Log Files from SECUREWAVE
Fetched 1 Log File from SECUREWAVE
Found 22 record(s) matching the search criteria
```

```
SECUREWAVE is running properly. [1/2/2006 10:09:42 AM]
```

Found 22 record(s) matching the search criteria 0%

Figure 57: Adding a device directly from the log Explorer menu

> 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* 223 *for details on what can and cannot be shadowed when writing to a recordable CD or DVD.*

> You can see which files have been copied from a PC to an authorized device (shadowing): By default, Shadowing is turned off. It can be enabled either for all users or a specific one (go to the Device Explorer, 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 to a floppy, recordable DVD/CD, or removable drives but you may also want to extend such control over LPT and COM ports.

> You can add a frequently used or attached device

✍ *Shadowing is available for files copied to 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.*

✍ *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 Device 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', he 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* 50 *for more details.*

✍ *If you can see a clip* 📎 *icon, 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.*

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 — 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 Latest Log Files* in the *Explorer* menu.

If you choose to 'Fetch Latest Log Files' 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. Please refer to Shadowed file upload delay or time *on page* 198 *for more information.*

You can access the *Log Explorer* by clicking on the icon located on the *Device Control* navigation panel of the main window

Specifying search criteria

Use the search criteria fields located in the upper panel of the Log Explorer window to:

> Get a list of unsuccessful access attempts to write/read to a device.

> See all the client error reports.

> See the names and contents of files copied to 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 *50* for more details.

To set the rules for a search, do one or more of the following actions:

> In the *Filename* field enter the appropriate wildcards to narrow the search. (e.g. to search for all Word documents, type '*.doc'). This field only applies to shadow files; it has no effect for the central logging of errors and access attempts.

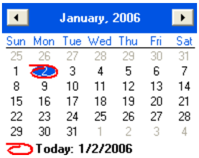
> If you want to search for actions by a specific user, type the name of the user or click the ... button to browse for it. You can use wildcards in the user's name (*, ?). If you click on the button or press ENTER, the *Select User, Local User* dialog is displayed — simply select a user from the list and then click the OK and SEARCH buttons.

✍ *If you get an empty username list, make sure you synchronize the domain users and, in case this does not resolve the names in future logs, also synchronize the local users of the offending machine. However, this will not resolve names in existing logs.*

> If you want to search for actions on a specific computer, type the name in the *Computer* field or click the ... button to browse for it. You can use wildcards in

the computer's name (*, ?). If you click on the button or press ENTER, the *Select Computer* dialog is displayed — simply select a computer from the list and then click the OK and SEARCH buttons.

> If you want to select only traced events between two specific dates, activate the TRACED checkbox, and enter suitable dates in the date fields. If you click on the arrow button at the right of the date fields, you display a calendar that allows you to pick a date visually:



January, 2006

Sun	Mon	Tue	Wed	Thu	Fri	Sat
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

Today: 1/2/2006

Figure 58: The calendar pull down menu

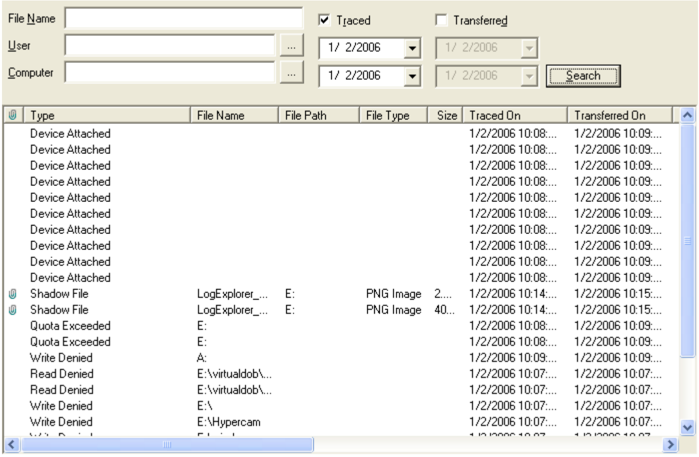
> If you want to select only the information transmitted to the server between specific dates, activate the TRANSFERRED checkbox, and enter suitable dates in the two date fields. If you click on the arrow button at the right of the date fields, you display a calendar that allows you to pick a date visually.

✍ *You can enter search criteria into as many of these fields as you want.*

When you have selected all the fields, click the SEARCH button. The list of shadow files and events is displayed.

✍ *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 the Boolean combination of the dates plus the user log.*

✍ *Note the clip* 📎 *icon. It indicates that the full content of the file is available for review.*



File Name [ ] ☑ Traced □ Transferred

User [ ] ... 1/ 2/2006 1/ 2/2006

Computer [ ] ... 1/ 2/2006 1/ 2/2006 Search

📎	Type	File Name	File Path	File Type	Size	Traced On	Transferred On
	Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
	Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
	Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
	Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
	Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
	Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
	Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
	Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
	Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
	Device Attached					1/2/2006 10:08:...	1/2/2006 10:09:...
📎	Shadow File	LogExplorer_...	E:	PNG Image	2....	1/2/2006 10:14:...	1/2/2006 10:15:...
📎	Shadow File	LogExplorer_...	E:	PNG Image	40...	1/2/2006 10:14:...	1/2/2006 10:15:...
	Quota Exceeded	E:				1/2/2006 10:08:...	1/2/2006 10:09:...
	Quota Exceeded	E:				1/2/2006 10:08:...	1/2/2006 10:09:...
	Write Denied	A:				1/2/2006 10:09:...	1/2/2006 10:09:...
	Read Denied	E:\virtualdob\...				1/2/2006 10:07:...	1/2/2006 10:07:...
	Read Denied	E:\virtualdob\...				1/2/2006 10:07:...	1/2/2006 10:07:...
	Write Denied	E:\				1/2/2006 10:07:...	1/2/2006 10:07:...
	Write Denied	E:\Hypercam				1/2/2006 10:07:...	1/2/2006 10:07:...

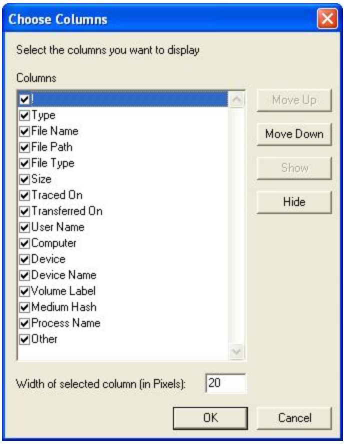
Figure 59: The Log Explorer main window

If there are any records that match your query criteria, they appear in the window's list. Enterprise Administrators can search for items on any Computer and by any User. On the other hand, Sanctuary Device Control Administrators are limited to the users or[1] computers they are allowed to manage when running under Active Directory.

[1] The Sanctuary Device control Administrator will only see files that have been generated on one of the computers or by one of their users — on any machine, he/she manages.

Available columns

You can control the visibility, size, and position of a column from the *View* menu. Select the *View→Choose columns…* to show the following dialog:



Choose Columns

Select the columns you want to display

Columns

☑ !
☑ Type
☑ File Name
☑ File Path
☑ File Type
☑ Size
☑ Traced On
☑ Transferred On
☑ User Name
☑ Computer
☑ Device
☑ Device Name
☑ Volume Label
☑ Medium Hash
☑ Process Name
☑ Other

Width of selected column (in Pixels): 20

Figure 60: Available columns for the Log Explorer window

This dialog controls the presence, size, and appearance of the columns in the Log Explorer module. Some fields are specific to either central logging or shadowing options while others common to both of them.

The following table summarizes the column meaning:

Column	Description	Unsuccessful access attempt	Client Error report	Shadowing
📎 (Represented in the previous image as a !)	The row in which the clip is located has a shadowed content that can be visualized.	No	No	Yes
Type	An item can be a shadow file, a given error or an unsuccessful access.	Different access types	Error type	Shadow file
File Name	Contains the name of the file involved in the access to the device, if any.	Yes	No	Yes
File Path	When relevant, path to	If available	No	Yes

Column	Description	Unsuccessful access attempt	Client Error report	Shadowing
	the file on the device.			
Size	Size of the shadowed file.	N/A	N/A	Yes
File Type	Type of the file determined by the file extension.	No	No	Yes
Traced On	Date 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
User Name	Name of the user who triggered the event (see note after table).	If available	No	Yes
Computer	Machine name where the event was recorded.	Yes	Yes	Yes
Device	When available, device class. The device class can be Removable Storage Devices, Floppy, DVD/CD,...	Yes	No	Yes
Device Name	Manufacturer's device name.	If available (only for device-attached event)	No	No
Volume Label	Tag of the volume for which an event was recorded.	If available	No	No
Medium Hash	Unique identifier of the medium (DVD/CD or removable) inserted.	If available (only for DVD/CDs and encrypted media)	No	No
Process Name	Process involved in the access to the device.	Yes	No	No
Other	Access mask or DVD/CD serial number. For technical support purposes.	Yes	No	No

Table 22: 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. 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.*

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:

> 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 a device for which he has no permissions. 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* Suppress recurring log events *option can reduce significantly the volume of redundant information logged. See the option description on page* 202*.*

✍ *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* Suppress recurring log events *option can reduce significantly the volume of redundant information logged. See the option description on page* 202*.*

✍ *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* option on page *199* 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 *226* 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 you 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

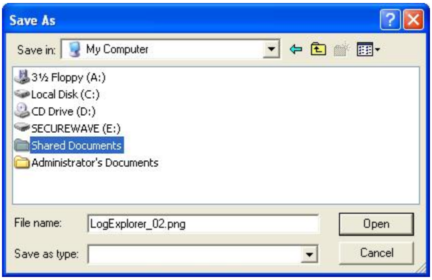
Complete the fields in the top panel of the Log Explorer window to get a list of all the files copied.

The files present in the list are an exact copy of those copied by the users onto the protected devices. The registers will show the date the file was copied onto the media (Traced On) and the date the file was transferred to our Database (Transferred On). Sanctuary Device Control also tracks the name of the user that copied the file, the file name, 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 clip symbol 📎 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. This is also the default option and is carried out if you double-click on the file.



Save As

Save in: My Computer

3½ Floppy (A:)
Local Disk (C:)
CD Drive (D:)
SECUREWAVE (E:)
Shared Documents
Administrator's Documents

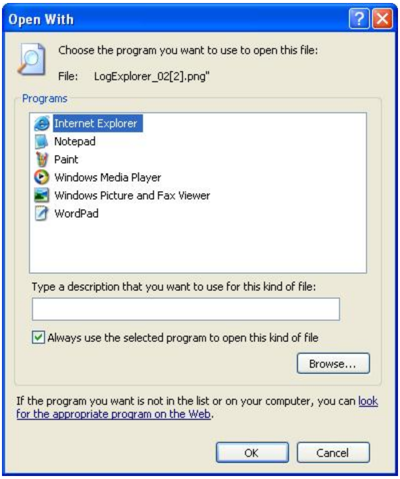
File name: LogExplorer_02.png

Save as type:

Figure 61: Saving a shadowed file

> *Open:* Opens the file using its default application.

> *Open with:* Allows you to choose the application with which you open a file



Open With

Choose the program you want to use to open this file:

File: LogExplorer_02[2].png"

Programs

Internet Explorer
Notepad
Paint
Windows Media Player
Windows Picture and Fax Viewer
WordPad

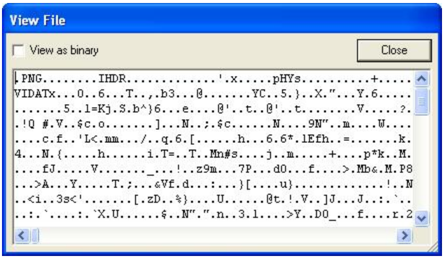
Type a description that you want to use for this kind of file:

☑ Always use the selected program to open this kind of file

If the program you want is not in the list or on your computer, you can look for the appropriate program on the Web.

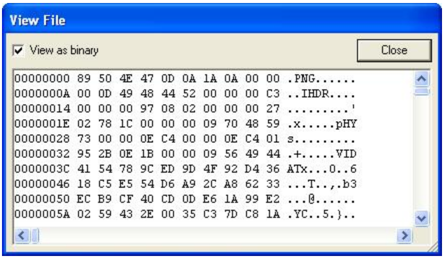
Figure 62: Selecting the program to use when opening a shadow file

> *View contents:* Allows you to view the contents of the file in a text or binary file viewer.



```
.PNG........IHDR.............'.x.....pHYs..........+.....
VIDATx...0..6...T..,.b3...@.......YC..5.}..X."...Y.6.....
.......5..l=Kj.S.b^}6...e....@'..t..@'..t........V.....?.
.!Q #.V..$c.o.......]...N..;.$c......N....9N"..m....W....
....c.f..'L<.mm.../..q.6.[......h...6.6*.lEfh..=.......k.
4...N.{.....h......i.T=..T..Mn#s....j..m.....+....p*k..M.
....fJ.....V......._...!..z9m...7P...d0...f....>.Mb&.M.P8
...>A...Y.....T.;...&Vf.d...:...}[....u}.............!..N
..<i..3s<'.......[.zD..%}....U......@t.!.V..]J...J..:.`..
..:.`....:.`X.U......$..N".".n..3.l....>Y..D0_...f....r.2
```

Figure 63: Viewing the content of a shadow file in text form



```
00000000 89 50 4E 47 0D 0A 1A 0A 00 00 .PNG......
0000000A 00 0D 49 48 44 52 00 00 00 C3 ..IHDR....
00000014 00 00 00 97 08 02 00 00 00 27 .........'
0000001E 02 78 1C 00 00 00 09 70 48 59 .x.....pHY
00000028 73 00 00 0E C4 00 00 0E C4 01 s.........
00000032 95 2B 0E 1B 00 00 09 56 49 44 .+.....VID
0000003C 41 54 78 9C ED 9D 4F 92 D4 36 ATx...0..6
00000046 18 C5 E5 54 D6 A9 2C A8 62 33 ...T..,.b3
00000050 EC B9 CF 40 CD 0D E6 1A 99 E2 ...@......
0000005A 02 59 43 2E 00 35 C3 7D C8 1A .YC..5.}..
```

Figure 64: Viewing the content of a shadow file in binary form

✍ *Sanctuary Device Control will log the file name and the administrator name each time he/she opens one of the shadowed files. The information is available in the Audit Logs Viewer.*

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 there is no clip 📎 symbol indicating that there is no available content for the file.

✍ *The full content of the file is always shadowed 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.*

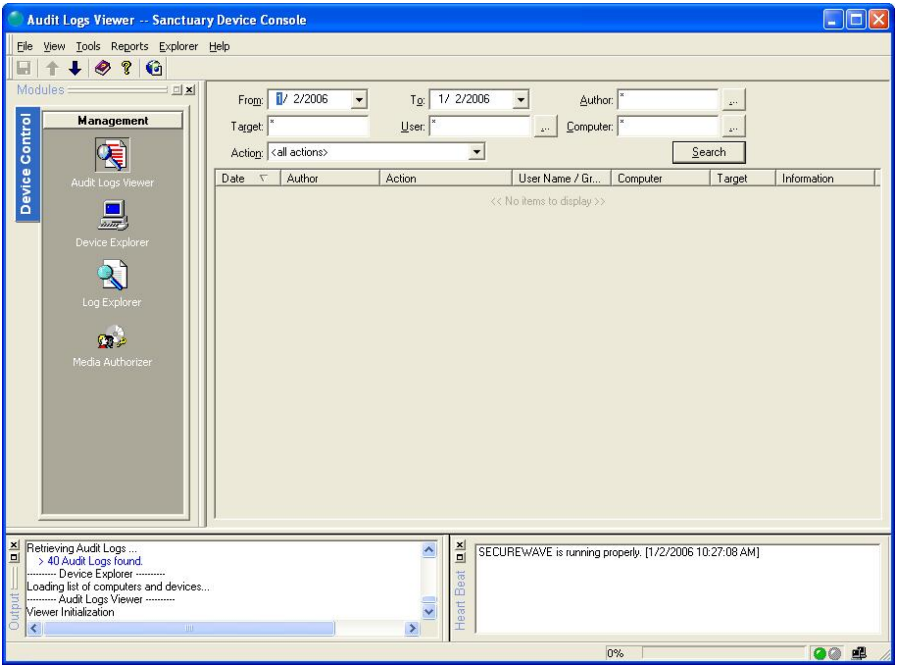
DVD/CD Shadowing

When CDs or DVDs are written, 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 the shadowed files and how they appear in the Log Explorer.

Chapter 5: 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 *Device Control* navigation panel of the main window.



From: 1/ 2/2006 To: 1/ 2/2006 Author: *

Target: * User: * Computer: *

Action: <all actions>

```
Retrieving Audit Logs ...
  > 40 Audit Logs found.
---------- Device Explorer ----------
Loading list of computers and devices...
---------- Audit Logs Viewer ----------
Viewer Initialization
```

```
SECUREWAVE is running properly. [1/2/2006 10:27:08 AM]
```

Figure 65: The Audit Logs Viewer main window

✍ *If the 'Audit (Device Control)' access of the Sanctuary Device 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 s*ection on page* 50 *for more details.*

Search options

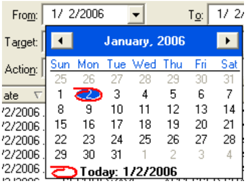
There are several options you can use to search information in the Audit Log. They are found on the upper panel in the right side of the *Audit Logs Viewer* window.

You can do a search by:

- Date
- Author
- Target
- User name
- Computer
- Action

You can enter search criteria into as many of these fields as you want.

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:



From: 1/ 2/2006

To: 1/ 2/

January, 2006

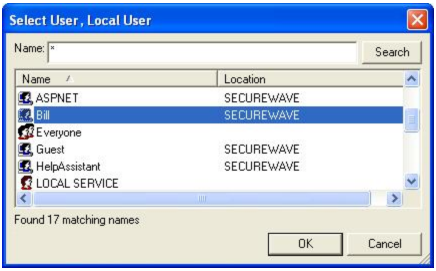
Sun	Mon	Tue	Wed	Thu	Fri	Sat
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

Today: 1/2/2006

Figure 66: 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 Device Control Administrator will be only shown audits of computers and users he is allowed to manage. You can use ctrlacx.vbs, explained on page* 251, *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 *,?) in the *Author* field or click on the ellipsis (...) button at one side of the field to get a search dialog:



Name: *

Name	Location
ASPNET	SECUREWAVE
Bill	SECUREWAVE
Everyone	
Guest	SECUREWAVE
HelpAssistant	SECUREWAVE
LOCAL SERVICE	

Found 17 matching names

Figure 67: Using the author to do a search

You can choose the user directly from this dialog or use the SEARCH button.

The *Target* search field lets you search by the different types of devices available in the computer, for example, floppy disk, USB memory stick, DVD, etc. You can type wildcards (*,?) 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 are accessed.

> When options are changed.

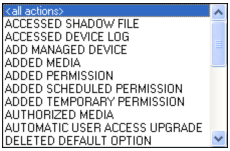
> Name of the authorized media.

If you want to know who changed an option and when, type the option or part of it (using wildcards, for example, flop to get all changes to the Floppy disk drive) 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 (*, ?) in the user name specification. You can use the ellipsis ... button to do a quick user name search.

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

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



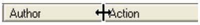
<all actions>
ACCESSED SHADOW FILE
ACCESSED DEVICE LOG
ADD MANAGED DEVICE
ADDED MEDIA
ADDED PERMISSION
ADDED SCHEDULED PERMISSION
ADDED TEMPORARY PERMISSION
AUTHORIZED MEDIA
AUTOMATIC USER ACCESS UPGRADE
DELETED DEFAULT OPTION

Figure 68: Using an action to do a search

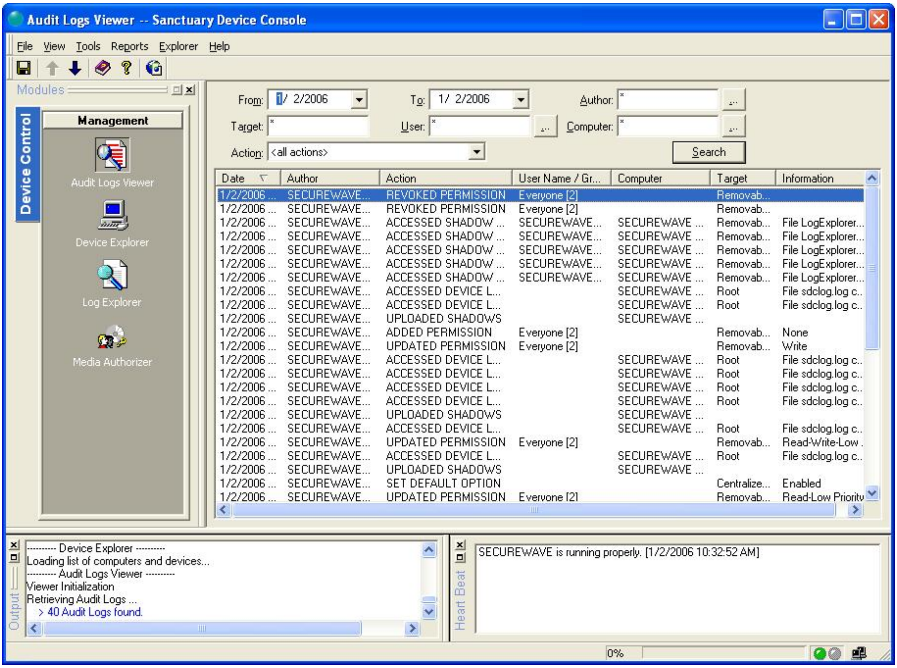
All fields act interactively: When you change one of them, it does a logical AND with all the others. If, for example, you select a range of dates and then an action, the resulting data will be the Boolean combination of the dates plus the action.

Actions

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

> You can always 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.



From: 1/ 2/2006 To: 1/ 2/2006 Author: *

Target: * User: * Computer: *

Action: <all actions>

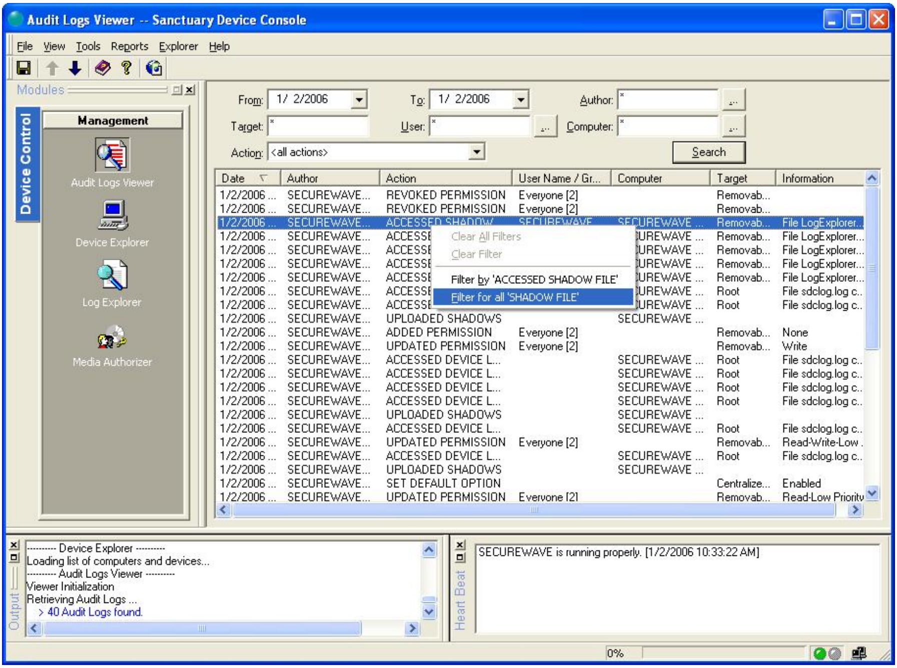
Date	Author	Action	User Name / Gr...	Computer	Target	Information
1/2/2006 ...	SECUREWAVE...	REVOKED PERMISSION	Everyone [2]		Removab...	
1/2/2006 ...	SECUREWAVE...	REVOKED PERMISSION	Everyone [2]		Removab...	
1/2/2006 ...	SECUREWAVE...	ACCESSED SHADOW ...	SECUREWAVE...	SECUREWAVE ...	Removab...	File LogExplorer...
1/2/2006 ...	SECUREWAVE...	ACCESSED SHADOW ...	SECUREWAVE...	SECUREWAVE ...	Removab...	File LogExplorer...
1/2/2006 ...	SECUREWAVE...	ACCESSED SHADOW ...	SECUREWAVE...	SECUREWAVE ...	Removab...	File LogExplorer...
1/2/2006 ...	SECUREWAVE...	ACCESSED SHADOW ...	SECUREWAVE...	SECUREWAVE ...	Removab...	File LogExplorer...
1/2/2006 ...	SECUREWAVE...	ACCESSED SHADOW ...	SECUREWAVE...	SECUREWAVE ...	Removab...	File LogExplorer...
1/2/2006 ...	SECUREWAVE...	ACCESSED DEVICE L...		SECUREWAVE ...	Root	File sdclog.log c...
1/2/2006 ...	SECUREWAVE...	ACCESSED DEVICE L...		SECUREWAVE ...	Root	File sdclog.log c...
1/2/2006 ...	SECUREWAVE...	UPLOADED SHADOWS		SECUREWAVE ...		
1/2/2006 ...	SECUREWAVE...	ADDED PERMISSION	Everyone [2]		Removab...	None
1/2/2006 ...	SECUREWAVE...	UPDATED PERMISSION	Everyone [2]		Removab...	Write
1/2/2006 ...	SECUREWAVE...	ACCESSED DEVICE L...		SECUREWAVE ...	Root	File sdclog.log c...
1/2/2006 ...	SECUREWAVE...	ACCESSED DEVICE L...		SECUREWAVE ...	Root	File sdclog.log c...
1/2/2006 ...	SECUREWAVE...	ACCESSED DEVICE L...		SECUREWAVE ...	Root	File sdclog.log c...
1/2/2006 ...	SECUREWAVE...	ACCESSED DEVICE L...		SECUREWAVE ...	Root	File sdclog.log c...
1/2/2006 ...	SECUREWAVE...	UPLOADED SHADOWS		SECUREWAVE ...		
1/2/2006 ...	SECUREWAVE...	ACCESSED DEVICE L...		SECUREWAVE ...	Root	File sdclog.log c...
1/2/2006 ...	SECUREWAVE...	UPDATED PERMISSION	Everyone [2]		Removab...	Read-Write-Low ...
1/2/2006 ...	SECUREWAVE...	ACCESSED DEVICE L...		SECUREWAVE ...	Root	File sdclog.log c...
1/2/2006 ...	SECUREWAVE...	UPLOADED SHADOWS		SECUREWAVE ...		
1/2/2006 ...	SECUREWAVE...	SET DEFAULT OPTION			Centralize...	Enabled
1/2/2006 ...	SECUREWAVE...	UPDATED PERMISSION	Everyone [2]		Removab...	Read-Low Priority

```
---------- Device Explorer ----------
Loading list of computers and devices...
---------- Audit Logs Viewer ----------
Viewer Initialization
Retrieving Audit Logs ...
   > 40 Audit Logs found.
```

```
SECUREWAVE is running properly. [1/2/2006 10:32:52 AM]
```

Figure 69: 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.



From: 1/ 2/2006 To: 1/ 2/2006 Author: *

Target: * User: * Computer: *

Action: <all actions>

Date	Author	Action	User Name / Gr...	Computer	Target	Information
1/2/2006 ...	SECUREWAVE...	REVOKED PERMISSION	Everyone [2]		Removab...	
1/2/2006 ...	SECUREWAVE...	REVOKED PERMISSION	Everyone [2]		Removab...	
1/2/2006 ...	SECUREWAVE...	ACCESSED SHADOW	SECUREWAVE	SECUREWAVE ...	Removab...	File LogExplorer...
1/2/2006 ...	SECUREWAVE...	ACCESSE		UREWAVE ...	Removab...	File LogExplorer...
1/2/2006 ...	SECUREWAVE...	ACCESSE		UREWAVE ...	Removab...	File LogExplorer...
1/2/2006 ...	SECUREWAVE...	ACCESSE		UREWAVE ...	Removab...	File LogExplorer...
1/2/2006 ...	SECUREWAVE...	ACCESSE		UREWAVE ...	Removab...	File LogExplorer...
1/2/2006 ...	SECUREWAVE...	ACCESSE		UREWAVE ...	Root	File sdclog.log c...
1/2/2006 ...	SECUREWAVE...	ACCESSE		UREWAVE ...	Root	File sdclog.log c...
1/2/2006 ...	SECUREWAVE...	UPLOADED SHADOWS		SECUREWAVE ...		
1/2/2006 ...	SECUREWAVE...	ADDED PERMISSION	Everyone [2]		Removab...	None
1/2/2006 ...	SECUREWAVE...	UPDATED PERMISSION	Everyone [2]		Removab...	Write
1/2/2006 ...	SECUREWAVE...	ACCESSED DEVICE L...		SECUREWAVE ...	Root	File sdclog.log c...
1/2/2006 ...	SECUREWAVE...	ACCESSED DEVICE L...		SECUREWAVE ...	Root	File sdclog.log c...
1/2/2006 ...	SECUREWAVE...	ACCESSED DEVICE L...		SECUREWAVE ...	Root	File sdclog.log c...
1/2/2006 ...	SECUREWAVE...	ACCESSED DEVICE L...		SECUREWAVE ...	Root	File sdclog.log c...
1/2/2006 ...	SECUREWAVE...	UPLOADED SHADOWS		SECUREWAVE ...		
1/2/2006 ...	SECUREWAVE...	ACCESSED DEVICE L...		SECUREWAVE ...	Root	File sdclog.log c...
1/2/2006 ...	SECUREWAVE...	UPDATED PERMISSION	Everyone [2]		Removab...	Read-Write-Low ...
1/2/2006 ...	SECUREWAVE...	ACCESSED DEVICE L...		SECUREWAVE ...	Root	File sdclog.log c...
1/2/2006 ...	SECUREWAVE...	UPLOADED SHADOWS		SECUREWAVE ...		
1/2/2006 ...	SECUREWAVE...	SET DEFAULT OPTION			Centralize...	Enabled
1/2/2006 ...	SECUREWAVE...	UPDATED PERMISSION	Everyone [2]		Removab...	Read-Low Priority

```
--------- Device Explorer ---------
Loading list of computers and devices...
--------- Audit Logs Viewer ---------
Viewer Initialization
Retrieving Audit Logs ...
   > 40 Audit Logs found.
```

```
SECUREWAVE is running properly. [1/2/2006 10:33:22 AM]
```

Figure 70: Filtering actions of 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:

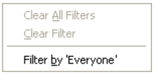


Figure 71: A filtering pop-up dialog example

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*.

The Audit log viewer contains the following columns:

> Date: When the action was performed by the administrator.

> Author: Who did the action.

> Action: Code describing the action performed by the administrator:

- 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.
- ADD MANAGED DEVICE: This event corresponds to the adding of a new device by an administrator with the Manage Devices functionality. The device name is logged.
- ADDED MEDIA: Corresponds to the adding of a new device with the Media Authorizer; the label and description are logged.
- ADDED 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 Device 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 *Defining the Sanctuary Device Control administrators* on page *50*.
- DELETE DEFAULT OPTION: Whenever a default option that applies to all the machines is deleted (in the *Tools→ Default Options* 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 ROLE: 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 PERMISSION: The fields available are: user, machine, device, read/write, begin time, end time.

- SET DEFAULT OPTION: A default option is one that applies to all the machines. Whenever a change is done by the administrator to one of these options (by using the *Tools*, *Default Options* 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.

- UNAUTHORIZED MEDIA FOR ALL USERS: 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 machine name is logged.

> User Name / Group Name: Group name of user name that is the target of the action performed by the administrator.

> 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 made.

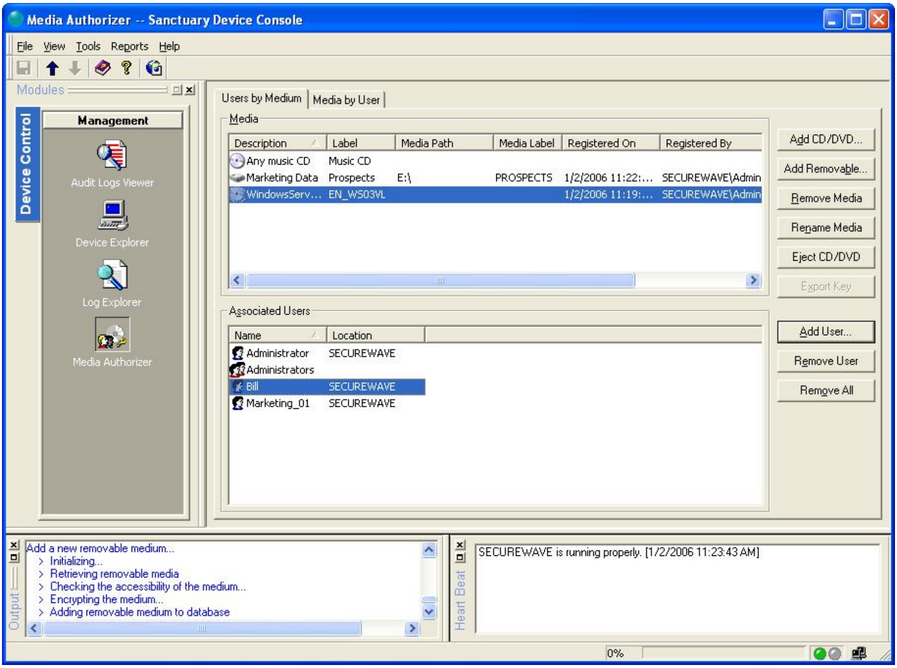
> Target is filled with the device for which the permission modification applied. (DVD/CD-Rom, floppy, removable storage devices…). When using the Target field you get a different set of information than that normally received for a device. See the Target field description on page *141* for a detailed review of what you can see when using this option.

> The Information field shows more details in some cases. For example, if a Sanctuary Administrator erases a scheduled permission, its parameters are included here.

Chapter 6: Using the Media Authorizer

This chapter explains how you can use Media Authorizer to permit access for specific users to individual CDs, DVDs, and removable media (where 'removable media' means any device recognized as 'Removable Storage Devices' by Windows, which includes flash memory devices, zip drives, etc.).

You can access the *Media Authorizer* by clicking on the icon located on the *Device Control* navigation panel of the main window.



Description	Label	Media Path	Media Label	Registered On	Registered By
Any music CD	Music CD				
Marketing Data	Prospects	E:\	PROSPECTS	1/2/2006 11:22:...	SECUREWAVE\Admin
WindowsServ...	EN_WS03VL			1/2/2006 11:19:...	SECUREWAVE\Admin

Name	Location
Administrator	SECUREWAVE
Administrators	
Bill	SECUREWAVE
Marketing_01	SECUREWAVE

```
Add a new removable medium...
  > Initializing...
  > Retrieving removable media
  > Checking the accessibility of the medium...
  > Encrypting the medium...
  > Adding removable medium to database
```

```
SECUREWAVE is running properly. [1/2/2006 11:23:43 AM]
```

Figure 72: 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 media has just been added. They may differ when a user with access to the encrypted device has changed its label. In this case, an administrator connecting the media to his computer will see that the Label column has kept the original media label while the Media Label column holds the modified value.*

Introduction

You can use the Media Authorizer for three main purposes:

- Adding individual CDs, DVDs and removable storage devices onto the system database. Each removable device is encrypted to suit your security preferences.
- Granting permission to use individual DVDs/CDs/removable storage devices to users who would otherwise be barred from using them.

  > *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.*

- 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.

The general process we recommend you follow when authorizing media is:

1. Set up as many CDs, DVDs or removable storage devices as you want.
2. For each device, grant access to all appropriate users.

Although 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 it.

> ✍ *You can always use the ‘Event Notification’ rule to inform the user when a removable encrypted medium is plugged to the computer. You can add it at the ‘Unauthorized Encrypted Media’ class as a specific event notification with high priority.*

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. See *Easy Exchange* on page *188* for more information.

Adding CDs and DVDs

The default-installed configuration denies access to CDs and DVDs drives. You will need to grant the user or group permission to access in Read or Read/Write mode a DVD/CD. Before doing so, each one must be added to the database.

✍ *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, there is a pre-requisite that you must do:

- Install the Sanctuary Client on any machine where you are going to authorize multisession DVDs/CDs.

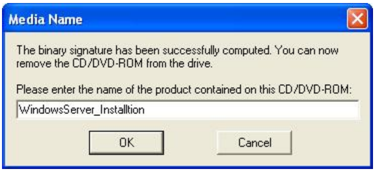
  If this is not done, the output window displays: 'Error opening driver: please make sure that Sanctuary Client is installed' and the ADD REMOVABLE button is disabled. It is not possible to calculate the signature of multisession DVDs/CDs when the SecureWave Client Driver is not installed on the Sanctuary Device Console machine. Media Authorizer is significantly slower when the Sanctuary Client is not installed.

To add a specific CD or DVD

To add a specific DVD/CD to the system database, proceed as follows:

1. In the Sanctuary Device Console, switch to the Media Authorizer module.
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:



Media Name

The binary signature has been successfully computed. You can now remove the CD/DVD-ROM from the drive.

Please enter the name of the product contained on this CD/DVD-ROM: WindowsServer_Installtion

Figure 73: Adding an encrypted DVD or CD

This is the name that will be 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 and groups. Its details are shown on the *Media Authorizer* screen.

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.*

Adding removable storage devices

Introduction

Even though the general computing term ‘removable media’ may include any device that you can remove 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 IDE hardisk, it will be recognized as a Removable Storage Device and you should define permission rules for them.

✍ *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. First, to ensure tamper-proof device identification by associating the identifier of a device with its encryption key. Second, 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 encrypt 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 7: Accessing encrypted media outside of your organization* on page *175* 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 Device Control 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 *237* 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 Device Control administrator has Read and Write access to the removable storage devices. Please refer to* To assign default permissions *on page* 86 *for more details on how to set device permissions.*

Limitations

There are some limitations you should be aware of 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:

  The user logs off and logs on again, forcing the system to mount the device.

  The user can unplug and re-plug the device reader.

  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 Device 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 function properly with encrypted devices.

> 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, the Novell client 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* 188 *for more information.*

✍ *You cannot use our encryption methods on those keys that already offer their own "embedded encryption" option.*

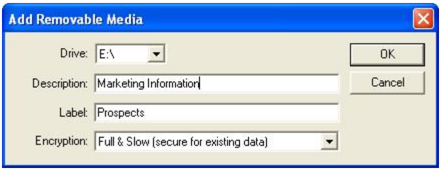
To add a specific removable storage device

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 in the database. During this process, a unique identifier is written to the device and the device 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 Device Console, switch to the Media Authorizer module.

3. Click ADD REMOVABLE. The *Add Removable Media* dialog is displayed.



Drive: E:\
Description: Marketing Information
Label: Prospects
Encryption: Full & Slow (secure for existing data)

Figure 74: 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 will be used to label the device after its formatting. This information will appear 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 (letters from A to Z, a to z and numbers from 0 to 9).

✍ *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.*

7. Choose the appropriate *Encryption* method. Select either:

Full & Slow (secure for existing data) to encrypt the media while preserving any file written to the media. 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) to quickly encrypt the device.

💣 *When using the quick format encryption mode, 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. In general, we therefore recommend this encryption mode is only used when the device has never had any sensitive data, or the device has been securely wiped.*

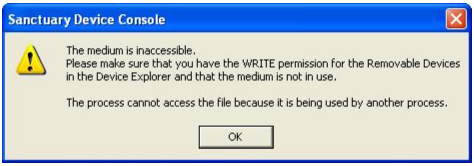
-or-

Easy Exchange (insecure for existing data): to quickly encrypt the device with the added advantage of being able to access the device in computers that do not have the Sanctuary Client installed. Although you can use our stand-alone decryption tool (SADEC) to install it on a computer, the user needs administrative rights, not always a good choice. Using this schema, the user can still use the encrypted device if he knows the password and has the original encryption key used to encode the peripheral.

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 *173*). 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. for a Flash drive if 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.

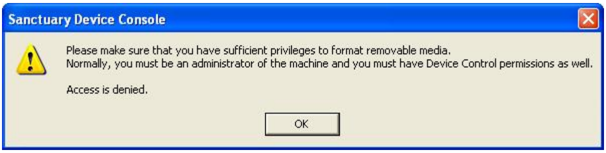


The medium is inaccessible.
Please make sure that you have the WRITE permission for the Removable Devices in the Device Explorer and that the medium is not in use.

The process cannot access the file because it is being used by another process.

Figure 75: '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 access to the Removable Storage Devices class or to the sub-class corresponding to the device model in the Device Explorer. Please refer to *To assign default permissions* on page *86* for more details on how to set device permissions.

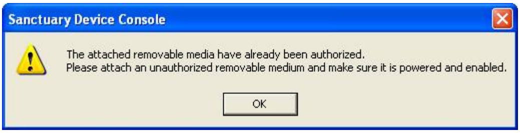

Sanctuary Device Console

Please make sure that you have sufficient privileges to format removable media.
Normally, you must be an administrator of the machine and you must have Device Control permissions as well.

Access is denied.

Figure 76: 'Not enough privileges' error message

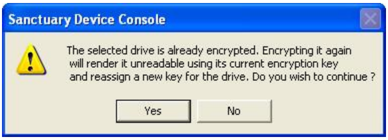
> If the device has already been encrypted, you will get the following message. Only non-encrypted media can be encrypted. If you are trying to re-encrypt a device you should first remove it from the system using the REMOVE MEDIA button.


Sanctuary Device Console

The attached removable media have already been authorized.
Please attach an unauthorized removable medium and make sure it is powered and enabled.

Figure 77: 'Already authorized' error message

> 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.


Sanctuary Device Console

The selected drive is already encrypted. Encrypting it again
will render it unreadable using its current encryption key
and reassign a new key for the drive. Do you wish to continue ?

Figure 78: '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.

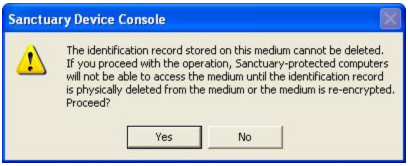
> Although the correct procedure to remove a device is to attach it to the administrator's computer before removing it, there are situations where an encrypted device must be removed from the database while it was not attached on the administrator's computer. The physical device remains encrypted. As 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 access to the 'Unauthorized Encrypted Media' device class in Device Explorer. See *Locally managed access to 'unauthorized encrypted media'* on page *182*.

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 *181*.

Reuse the device and re-encrypt it. This operation will erase the device content. In this case, you can user the *Quick Format (insecure for existing data)* command.

If you remove the media when it is not connected to the computer, you get the following message:


Sanctuary Device Console

The identification record stored on this medium cannot be deleted. If you proceed with the operation, Sanctuary-protected computers will not be able to access the medium until the identification record is physically deleted from the medium or the medium is re-encrypted. Proceed?

Figure 79: 'Identification record cannot be deleted' error message

Authorizing access

Once you have added CDs/DVDs/encrypted removable storage devices to the system database, you can grant access to them to specific users for two reasons:

> To allow users who are not allowed to use the DVD/CD drive to be permitted to use specific DVDs/CDs.

> To allow specific users to access encrypted media.

✍ *It is not possible to grant read-only access to encrypted media.*

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’ which you can select to allow users access to all audio CDs.

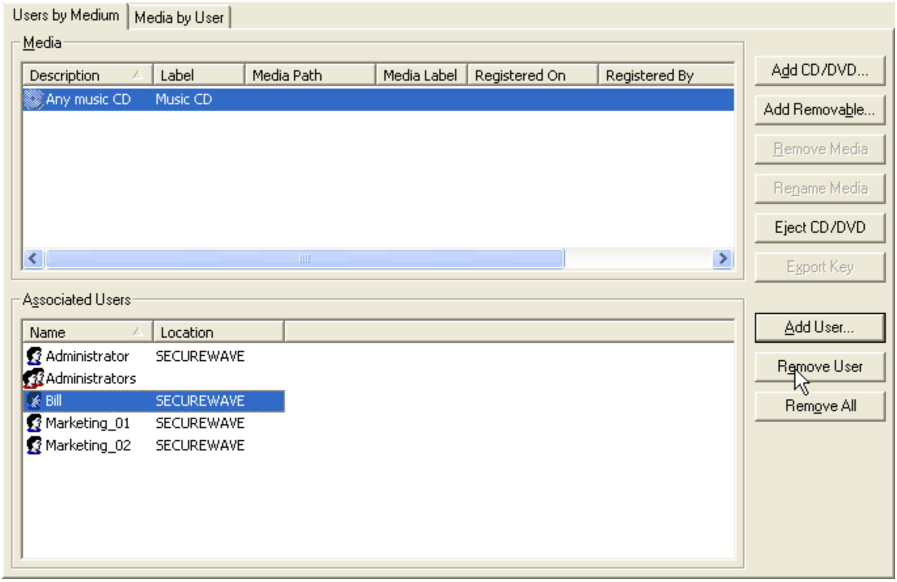
Selecting users for a device

You can select each of the CDs, DVDs and removable storage devices that you’ve added to the system database and assign permissions to them.

To grant access to use DVDs/CDs/encrypted removable media

To assign permission to a user to enable him to use a DVD/CD or removable media, proceed as follows:

1. Select the Users by Medium in the Media Authorizer.
2. Select the DVD/CD/removable device you want to grant access to.

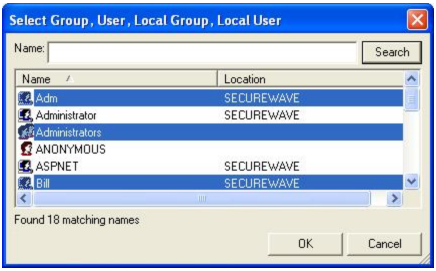


Description	Label	Media Path	Media Label	Registered On	Registered By
Any music CD	Music CD				

Name	Location
Administrator	SECUREWAVE
Administrators	
Bill	SECUREWAVE
Marketing_01	SECUREWAVE
Marketing_02	SECUREWAVE

Figure 80: 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.



Name	Location
Adm	SECUREWAVE
Administrator	SECUREWAVE
Administrators	
ANONYMOUS	
ASPNET	SECUREWAVE
Bill	SECUREWAVE

Found 18 matching names

Figure 81: 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.

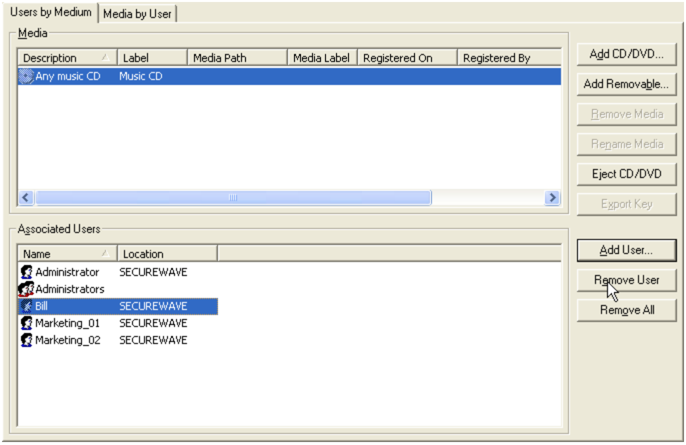
To deny access to DVDs/CDs/encrypted removable media

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.

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.



Description	Label	Media Path	Media Label	Registered On	Registered By
Any music CD	Music CD				

Name	Location
Administrator	SECUREWAVE
Administrators	
Bill	SECUREWAVE
Marketing_01	SECUREWAVE
Marketing_02	SECUREWAVE

Figure 82: 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.

The user is removed from the list of *Associated Users*, preventing them from accessing the selected media.

✍ *Changes in permissions to access DVDs/CDs/removable media are picked up 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 that he has been granted the right to use AND that he has used at least once when he was connected to the company network.*

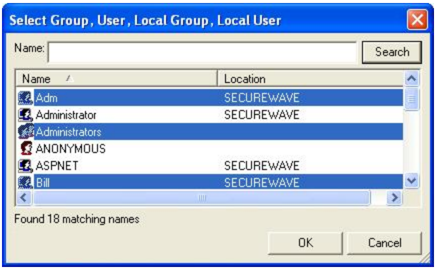
Selecting devices for a user

You can select each individual user on your system, and grant them access to the CDs, DVDs, and removable storage devices that you've 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.

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



Name	Location
Adm	SECUREWAVE
Administrator	SECUREWAVE
Administrators	
ANONYMOUS	
ASPNET	SECUREWAVE
Bill	SECUREWAVE

Found 18 matching names

Figure 83: Selecting users/groups to grant access to use a DVD/CD/encrypted removable media

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 media you selected are 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.

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 picked up 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 that he has been granted the right to use AND that he has used at least once when he was connected to the company network.*

Removing media from the database

This section describes how to remove the three categories of media from the system database:

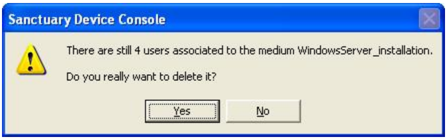
- CDs and DVDs.
- Encrypted removable storage devices.

> Lost or damaged media.

To remove a DVD/CD

1. Select the Users by Medium tab.
2. Select the DVD/CD in the *Authorized* list on the *Media* panel.
3. Click REMOVE MEDIA.

The media is removed from the database unless there are users associated with the DVD/CD, in which case a warning message is displayed.


Sanctuary Device Console

There are still 4 users associated to the medium WindowsServer_installation.

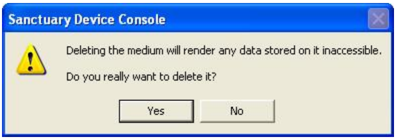
Do you really want to delete it?

Figure 84: 'Users still associated with medium' warning message

You can click YES to remove the media from the database.

To remove an encrypted removable storage device

1. Attach the device to your (the administrator's) computer.
2. Select it from the *Authorized* list on the *Media* panel.
3. Click REMOVE MEDIA.


Sanctuary Device Console

Deleting the medium will render any data stored on it inaccessible.

Do you really want to delete it?

Figure 85: 'Deleting medium' warning message

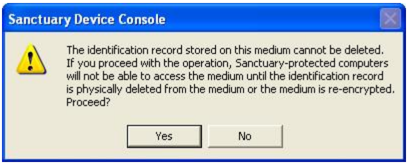
All encrypted data present on the device will be lost. After the device has been removed, it will be formatted.

To remove lost or damaged media from the database

If some of your media is lost or damaged you may want to remove it from the database. Although you have no physical access to it, you can still delete it by selecting it and clicking REMOVE MEDIA.

✍ *We recommend that you only delete devices that you know are lost or damaged and will not be recovered.*

A warning message is displayed:



The identification record stored on this medium cannot be deleted. If you proceed with the operation, Sanctuary-protected computers will not be able to access the medium until the identification record is physically deleted from the medium or the medium is re-encrypted. Proceed?

Figure 86: '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 media password, the media encryption key, and has received proper access to the 'Unauthorized Encrypted Media' device class in the Device Explorer module. See *Locally managed access to 'unauthorized encrypted media'* on page *182*.

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 will be inserted in the database again and its content preserved. See *Centrally managed access to unauthorized encrypted media* on page *181*.

> 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 for the diskprobe.exe tool found in the Windows resource kit if you are unsure 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, there are a few more tasks you can carry out:

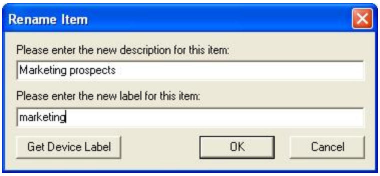
> Rename a DVD/CD/removable storage device.

> 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.
2. Select the DVD/CD/removable storage device you want to rename.
3. Click RENAME MEDIA. A dialog is displayed.



Rename Item

Please enter the new description for this item: Marketing prospects

Please enter the new label for this item: marketing

Figure 87: 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.
6. Click OK. The media is renamed.

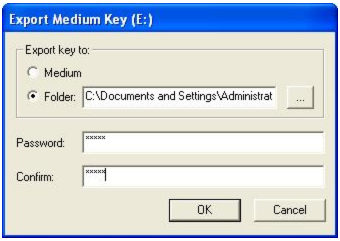
Exporting encryption keys

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 See *Centrally managed access to unauthorized encrypted media* on page *181*.

If you are planning to export the key, you must first enable the 'Encrypted Media Key Export' option.

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



Export Medium Key (E:)

Export key to:

○ Medium

● Folder: C:\Documents and Settings\Administrat

Password: *****

Confirm: *****

Figure 88: 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:

Device Explorer DVD/CD access defined for user Bill[1]	Permission defined in Media Authorizer for user Bill[1] to 'OfficeXP'	Resulting access when Bill inserts 'OfficeXP' in his drive	Resulting access when Bill inserts any other CD in his drive	Comments
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 23: 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.

[1] Permissions can be defined for the user Bill, in this example, or for the groups he belongs to.

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:

Device Explorer Removable Storage Devices access defined for user Bill[1]	Permission defined in Media Authorizer for user Bill to 'DiskOnKey8'	Resulting access when Bill connects 'DiskOnKey8' to his computer	Resulting access when Bill connects any unencrypted removable storage device	Comments
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	
	No access to 'DiskOnKey8'. The user has the encryption key and password	Read/Write	Read-Only	

Device Explorer Removable Storage Devices access defined for user Bill[1]	Permission defined in Media Authorizer for user Bill to 'DiskOnKey8'	Resulting access when Bill connects 'DiskOnKey8' to his computer	Resulting access when Bill connects any unencrypted removable storage device	Comments
'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 24: 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' 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, to the Removable Storage Devices class or one of its 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 *90* for more details on how permission priorities are applied.

Rights defined in Media Authorizer are cumulative. If a user is a member of ten groups, he will have access to all the CDs that were granted to the groups he is a member of. Please note that Encrypted media cannot be granted to groups.

Encrypting devices without having a Certificate Authority installed

There are sometimes that a Certificate Authority is not present and you are not willing to install it 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. Please see *To assign default permissions* on page *86* for more information.

2. Close all programs that might use the media, including Windows Explorer. You are now ready to encrypt the device.

3. Proceed to encrypt the device in the normal way. See the procedure on page *152*.

4. Export the media encryption keys on the media itself and provide a password.

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. 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 SDC.

✍ *If you plan to use this feature, please remember to 'Disable' the 'Certificate Generation' option for the client machine. Otherwise, the client creates a user certificates because it does not exists and you end up with unused client certificates. Please refer to* Chapter 8: Setting and changing options *on page* 191 *for more information on how to do this.*

Chapter 7: Accessing encrypted media outside of your organization

There may be situations when data on a specifically authorized (encrypted) device would need to be accessed from a machine that is not part of your organization. This machine may or may not be protected by Sanctuary Device Control.

Exporting encryption keys

In order to make a device accessible its encryption key must be imported. Before an encryption key may be imported, it must be exported.

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:

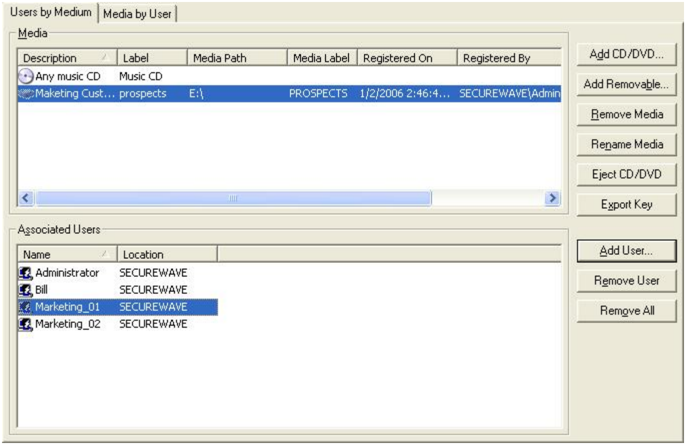
> The most secure way is to export the media encryption key to a file and send it via a different channel (e-mail for example) to the person that needs to access the encrypted media outside the organization.

> 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 *177* and *To export the encryption key on the device itself* on page *179* for details.



Description	Label	Media Path	Media Label	Registered On	Registered By
Any music CD	Music CD				
Maketing Cust…	prospects	E:\	PROSPECTS	1/2/2006 2:46:4…	SECUREWAVE\Admin

Name	Location
Administrator	SECUREWAVE
Bill	SECUREWAVE
Marketing_01	SECUREWAVE
Marketing_02	SECUREWAVE

Figure 89: 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 *Encrypted Media Key Export* option (see page *199* for more details).

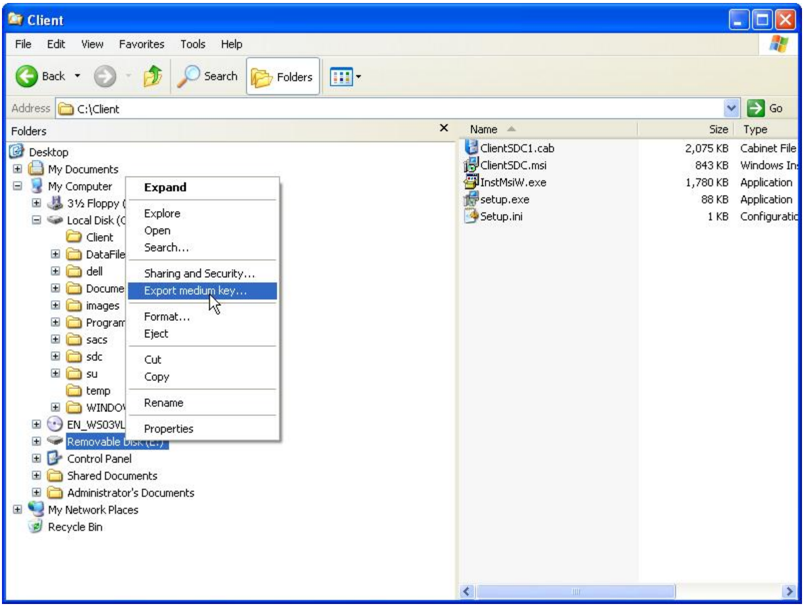
There are three conditions that need to be met in order for a user to export a medium encryption key locally:

- The user must have received proper access to the media. Please refer to *Chapter 6: Using the Media Authorizer* on page *149* 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 that has the *Encrypted Media Key Export* option set to *To file* or *To media or file*. Please refer to page *199* 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 *177* and *To export the encryption key on the device itself* on page *179* for details.



Name	Size	Type
ClientSDC1.cab	2,075 KB	Cabinet File
ClientSDC.msi	843 KB	Windows In
InstMsiW.exe	1,780 KB	Application
setup.exe	88 KB	Application
Setup.ini	1 KB	Configuratic

Figure 90: 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 (e-mail 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 *175* 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 *176* for more details.

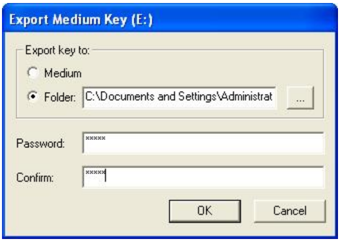
1. Either:

   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.



Export Medium Key (E:)

Export key to:

○ Medium

● Folder: C:\Documents and Settings\Administrat

Password: *****

Confirm: *****

Figure 91: 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 Export Password *option as described on page* 200*. This option does not apply for administrators performing central export.*

✍ *If the Sanctuary Device Control Administrator has set the option* Encrypted Media Export Password *(see page* 200*) to 'Require Password complexity', the password chosen by the user when doing a local export must meet the following requirements:*

Be at least 8 characters long,

Contain upper case and lower case letters,

Contain numbers,

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 e-mail and communicate the password by phone.

To export the encryption key on 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 *175* 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 *176* for more details.

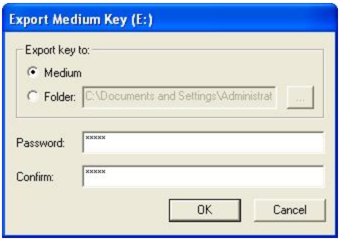
1. Either:

   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.



Export Medium Key (E:)

Export key to:

● Medium

○ Folder: C:\Documents and Settings\Administrat

Password: *****

Confirm: *****

Figure 92: 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 Export Password *option as described on page* 200. *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 8 characters long,*
>
> *Contain upper case and lower case letters,*
>
> *Contain numbers,*
>
> *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 he has not 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 from a machine with the Sanctuary Client

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

Unauthorized Encrypted Media are defined as media that were encrypted using the Sanctuary Device Control product in another organization than yours 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. Alternatively, you can grant trusted users the right to use encrypted devices from other organizations.

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.

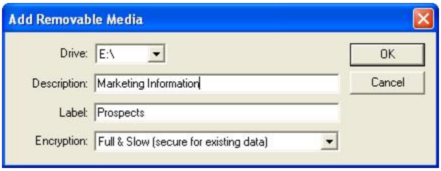
With this method, your users, even if they have the unauthorized encrypted media, its encryption key and password will not be able to use it unless the administrator has authorized the device and granted them the right to use it with the Media Authorizer.

The central authorization is done in two steps. The administrator first adds the device in the Media Authorizer, and then he grants user access to it.

To add a device in the Media Authorizer

1. Attach the device to your, the administrator's, computer. The administrator should have installed the Device Control Client on his computer and have read and write access to the Removable Storage Devices category. See *Adding removable storage devices* on page *152* for more details.

2. Using the Media Authorizer, click Add Removable. The following dialog appears:



Add Removable Media

Drive: E:\

Description: Marketing Information

Label: Prospects

Encryption: Full & Slow (secure for existing data)

Figure 93: Adding a device in the Media Authorizer

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 but because this wipes the device, then only do this when you want to re-use a device from another organization.

5. Only if the key was exported to a file, in the *Key location* field, browse for the file using the ellipsis button (...).

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 unauthorized encrypted medium can now be handled as any other encrypted media.

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 *160* 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 *Unauthorized Encrypted Media* class of the Device Explorer. Please refer to *To assign default permissions* on page *86* and *To assign computer-specific permissions to users and* groups on page *93* for more details on how to set permissions.

You can set the following permissions:

- The Scheduled and Temporary permissions will allow you to restrict the access to the *Unauthorized Encrypted Media* for a given period of time.

- Offline and online permissions: Assign Read or Read/Write permissions depending if the user is directly connect or not to the network.

- Permissions for the *Unauthorized Encrypted Media* class can be defined as a Global permission or at the computer-specific level 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.

The priorities that apply for the Unauthorized Encrypted Media class are the same as the ones described in *Default Permission priority* on page *90*.

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

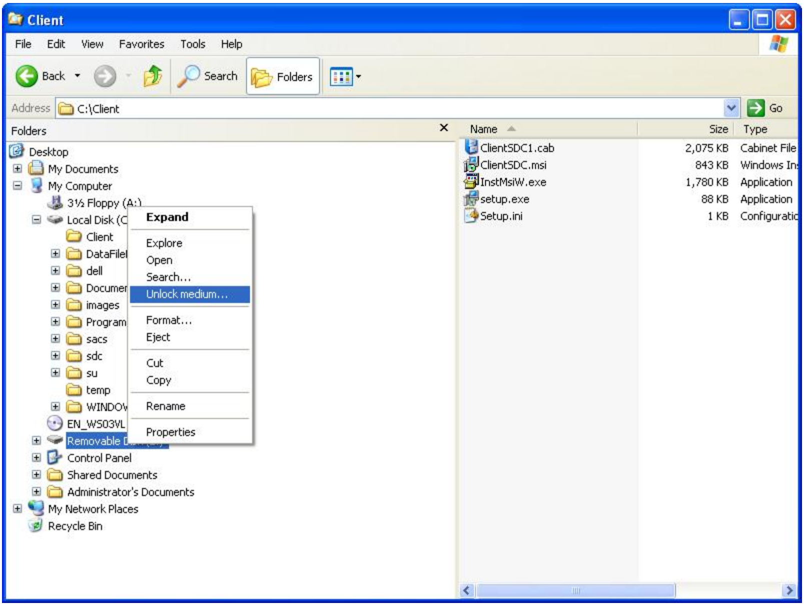
- The right to the *Unauthorized Encrypted Media* class.
- The encrypted device attached to his computer.
- The encryption key file, if the disk encryption key is not stored on the device.
- The password to access the device.

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:

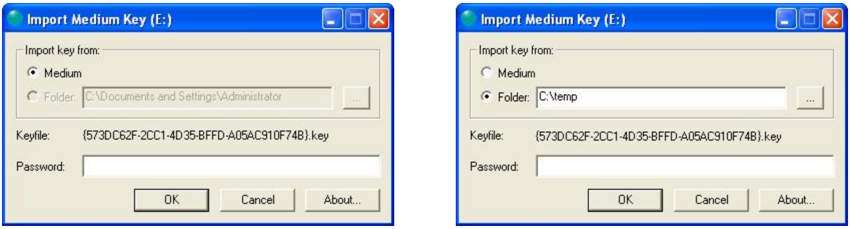
1. Attach the device to the computer.
2. In Windows Explorer, select the *Unlock medium* option from the right-click (contextual) menu of the encrypted drive.



Name	Size	Type
ClientSDC1.cab	2,075 KB	Cabinet File
ClientSDC.msi	843 KB	Windows In
InstMsiW.exe	1,780 KB	Application
setup.exe	88 KB	Application
Setup.ini	1 KB	Configuratio

Figure 94: Accessing unauthorized encrypted media

The *Import Medium Key* dialog is displayed.



Import Medium Key (E:)

Import key from:
● Medium
○ Folder: C:\Documents and Settings\Administrator
Keyfile: {573DC62F-2CC1-4D35-BFFD-A05AC910F74B}.key
Password:

Import Medium Key (E:)

Import key from:
○ Medium
● Folder: C:\temp
Keyfile: {573DC62F-2CC1-4D35-BFFD-A05AC910F74B}.key
Password:

Figure 95: 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 the file 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 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 keys and password have to be provided to the Sanctuary Device Control Administrator.
- The password and encryption key file are required only by the administrator when he adds the media to the list of encrypted media.
- The administrator cannot grant read-only access, because the *Media Authorizer* only allows read / write access.
- The administrator cannot grant groups of users access to a specific device. He has to grant each user access individually.
- The administrator controls the access to each encrypted device individually. It is not possible for his users to use a device that was 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 keys and password have to be provided directly 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 groups of users 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 or at the computer-specific level. 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.

Accessing from a machine without the Sanctuary Client

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 have 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 the address:

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 will need the encryption key file.

> The password to access the device and/or the encrypted key file.

To use the Stand-Alone Decryption Tool

Providing the requirements 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.

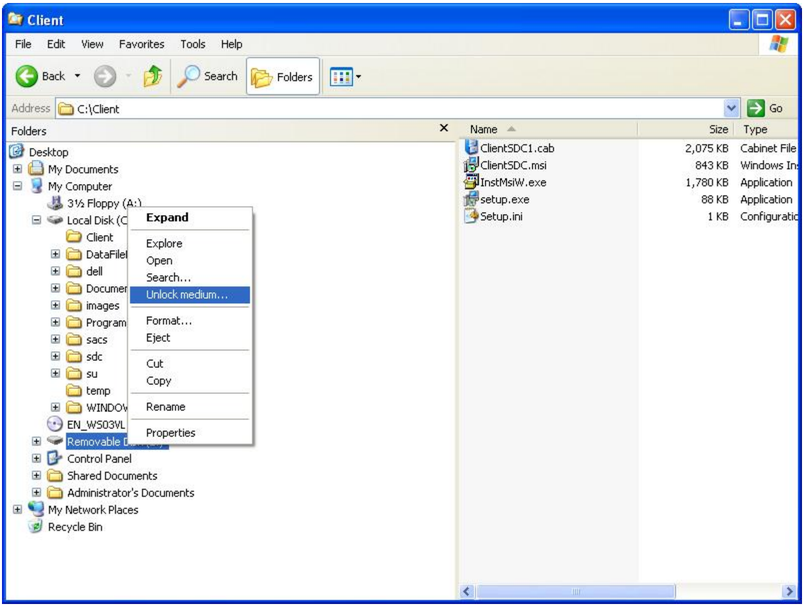
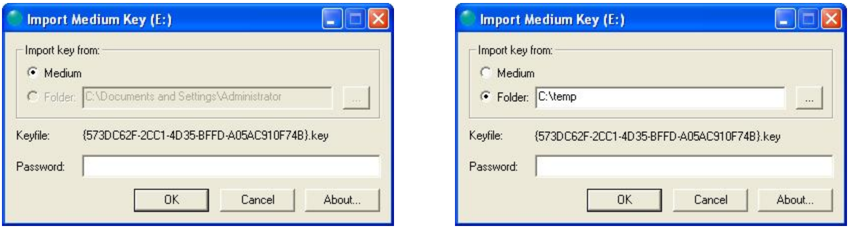


Figure 96: Using the Stand-Alone Decryption tool

The *Import Medium Key* dialog is displayed:


Import Medium Key (E:)

Import key from:
● Medium
○ Folder: C:\Documents and Settings\Administrator

Keyfile: {573DC62F-2CC1-4D35-BFFD-A05AC910F74B}.key

Password:

Import Medium Key (E:)

Import key from:
○ Medium
● Folder: C:\temp

Keyfile: {573DC62F-2CC1-4D35-BFFD-A05AC910F74B}.key

Password:

Figure 97: 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 the file 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 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 add a specific removable storage device* on page *155* 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:

Key's action	*Key's location*	*To access the medium the user must*	*Notes*
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 25: 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:

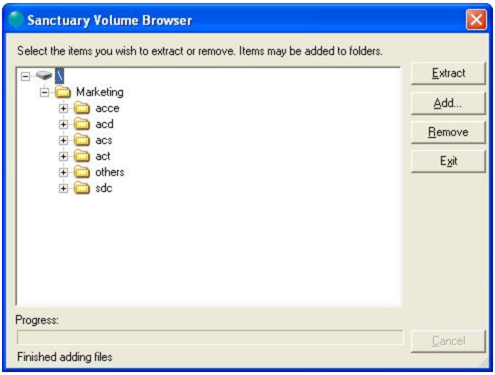


Figure 98: Sanctuary volume browser

The user can use his data without the need to install any kind of software whatsoever, and without administrative privileges.

Chapter 8: 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 Server Application Address
- Encrypted Media Key Export
- Encrypted Media Export Password
- Certificate Generation
- Centralized Device Control Logging
- Suppress Recurring Log Events

You can find the 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 the modifications.*

Changes from previous versions

If you are upgrading from a previous version of Sanctuary Device Control it may be useful for you to know about changes to this list of options. Details are provided in the following table of the options from v2.8.3 indicating which have remained as such and what has become of those that are no longer options in this version:

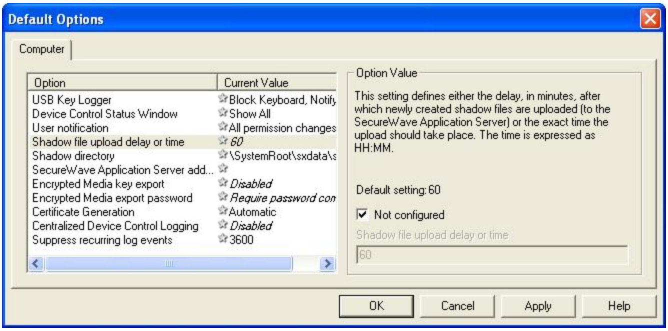
V2.8.3 Option	In this version
Floppy shadow mode	Now a rule in the Device Explorer.
CD/DVD-ROM shadow mode	Now a rule in the Device Explorer.
PS/2 port	Now a rule in the Device Explorer.
Removable Storage Devices shadow mode	Now a rule in the Device Explorer.
COM shadow mode	Now a rule in the Device Explorer.
LPT shadow mode	Now a rule in the Device Explorer.
Modem shadow mode	Now a rule in the Device Explorer.
Infrared (IrDA) port	Now a rule in the Device Explorer.
Bluetooth port	Now a rule in the Device Explorer.
Show tray icon	Renamed to *Device Control Status Window* and allows more definitions. See page *195.*
User notification	Still an option. See page *197*.
Device control log mode	Replaced by *Centralized Device Control Logging*.
Daily copy limit	Now a rule in the Device Explorer.
Shadowed file upload delay or time	Still an option. See page *198*.
Shadow directory	Still an option. See page *199*.
SecureWave application server address	Still an option. See page *199*.
Encrypted media key export	Still an option. See page *199*.
Encrypted media export password	Still an option. See page *200*.
Secondary hard drives	Now treated like a removable storage device.
Certificate generation	Still an option. See page *201*.
Centralized device control logging	Still an option. See page *201*.
Suppress recurring log events	Still an option. See page *202*.
Time resynchronization interval	Not available anymore.
USB keylogger	Did not exist. See page *195*.

Table 26: Changes from previous versions

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.



Option	Current Value
USB Key Logger	☆Block Keyboard, Notify
Device Control Status Window	☆Show All
User notification	☆All permission changes
Shadow file upload delay or time	☆*60*
Shadow directory	☆\SystemRoot\sxdata\s
SecureWave Application Server add...	☆
Encrypted Media key export	☆*Disabled*
Encrypted Media export password	☆*Require password con*
Certificate Generation	☆Automatic
Centralized Device Control Logging	☆*Disabled*
Suppress recurring log events	☆3600

Option Value

This setting defines either the delay, in minutes, after which newly created shadow files are uploaded (to the SecureWave Application Server) or the exact time the upload should take place. The time is expressed as HH:MM.

Default setting: 60

☑ Not configured

Shadow file upload delay or time

60

Figure 99: The Default Options dialog

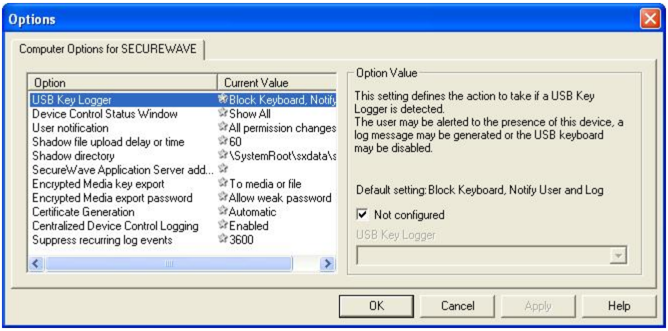
The tab label is simply 'Computer' indicating that the options are not specific to a particular machine, but are the defaults for all machines in Sanctuary Device Control. If you do not override these default options for a specific computer, then these are applied to all computers in Sanctuary Device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

For each option, if the *Not configured* checkbox is checked, 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 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*.



Option	Current Value
USB Key Logger	✩Block Keyboard, Notify
Device Control Status Window	✩Show All
User notification	✩All permission changes
Shadow file upload delay or time	✩60
Shadow directory	✩\SystemRoot\sxdata\s
SecureWave Application Server add...	✩
Encrypted Media key export	✩To media or file
Encrypted Media export password	✩Allow weak password
Certificate Generation	✩Automatic
Centralized Device Control Logging	✩Enabled
Suppress recurring log events	✩3600

Option Value

This setting defines the action to take if a USB Key Logger is detected.
The user may be alerted to the presence of this device, a log message may be generated or the USB keyboard may be disabled.

Default setting: Block Keyboard, Notify User and Log

☑ Not configured

USB Key Logger

Figure 100: Setting computer-specific options

Notice that the tab label is 'Computer Options for <computername>', to show which computer you are changing options for.

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 a default option, select *Tools→ Default Options*.

   -or-

   To change an option for a specific computer, right-click on the computer in Device Explorer, and select *Options*.

   The *Options* dialog is displayed, with the tab name indicating whether you are changing default settings 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, 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.

USB Key Logger

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. The USB version of this device can be blocked, either as a general option or as a computer specific one.

The possible settings are:

Option	*Description*	*Notify user*	*Block keyboard*	*Log event*
Do nothing	Do not react in any way to the detection of a keylogger.	✗	✗	✗
Notify user	Only inform the user of the presence of a Keylogger.	✓	✗	✗
Log event	Only log the event if a Keylogger is detected. The keyboard is not disabled.	✗	✗	✓
Notify + Log	If a keylogger is detected, log the event and inform the user. The keyboard is not disabled.	✓	✗	✓
Block keyboard + Notify	Hinder the keyboard and notify the user if a Keylogger is detected.	✓	✓	✗
Block + Log	Hinder the keyboard and log the event if a Keylogger is detected.	✗	✓	✓
Block, Log and Notify	Hinder the keyboard, log the event, and notify the user if a Keylogger is detected.	✓	✓	✓

Table 27: USB Keylogger options

✍ *Changing from one setting to another requires a client reboot.*

Device Control Status Window

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.

✍ *The icon will still show if you have another product of our Sanctuary suite installed. Only those options related to Sanctuary Device Control will be hidden.*

> *Show All.* Default. The Sanctuary Client icon is displayed and all information is available to the client user.

> *Show All without Shadow.* The Sanctuary Client icon is displayed and all information except shadowing details can be viewed.

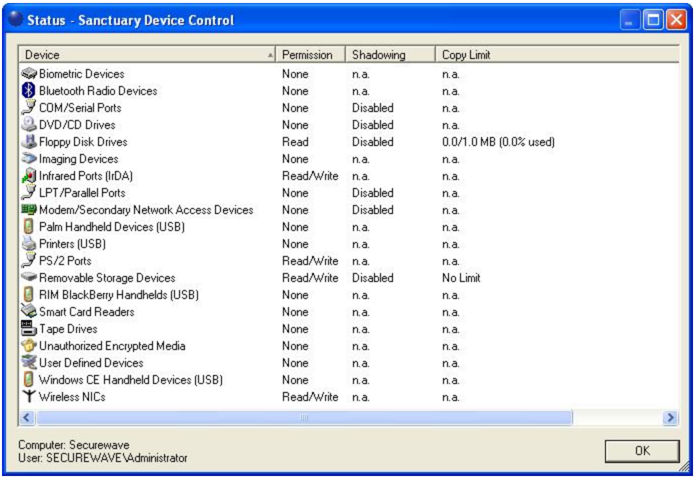
> *Show Allowed.* The Sanctuary Client icon is displayed and rule information about only the allowed devices on the client can be viewed.

> *Show Allowed without Shadow.* The Sanctuary Client icon is displayed and only the information about the allowed devices on the client can be viewed except 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.*

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.



Status - Sanctuary Device Control

Device	Permission	Shadowing	Copy Limit
Biometric Devices	None	n.a.	n.a.
Bluetooth Radio Devices	None	n.a.	n.a.
COM/Serial Ports	None	Disabled	n.a.
DVD/CD Drives	None	Disabled	n.a.
Floppy Disk Drives	Read	Disabled	0.0/1.0 MB (0.0% used)
Imaging Devices	None	n.a.	n.a.
Infrared Ports (IrDA)	Read/Write	n.a.	n.a.
LPT/Parallel Ports	None	Disabled	n.a.
Modem/Secondary Network Access Devices	None	Disabled	n.a.
Palm Handheld Devices (USB)	None	n.a.	n.a.
Printers (USB)	None	n.a.	n.a.
PS/2 Ports	Read/Write	n.a.	n.a.
Removable Storage Devices	Read/Write	Disabled	No Limit
RIM BlackBerry Handhelds (USB)	None	n.a.	n.a.
Smart Card Readers	None	n.a.	n.a.
Tape Drives	None	n.a.	n.a.
Unauthorized Encrypted Media	None	n.a.	n.a.
User Defined Devices	None	n.a.	n.a.
Windows CE Handheld Devices (USB)	None	n.a.	n.a.
Wireless NICs	Read/Write	n.a.	n.a.

Computer: Securewave
User: SECUREWAVE\Administrator

Figure 101: 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 shows if a permission of this type has been assigned to a device and how much has already been consumed.

User 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*. This means that no messages will be displayed to the user.

- *Temporary permission changes*. This will only 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 permission changes*. Default. This will cause a message to be displayed when any change is made to permissions that affects the user, including permanent, scheduled, offline, online, and temporary permissions.

Shadowed file upload delay or time

This allows you to specify when the shadow and log files temporarily stored on the client computer are uploaded to the SecureWave Application Server.

The default setting is every 60 minutes. If you clear the *Not configured* checkbox, you can type in an alternative value:

- If you type in a number, this is the interval in minutes between uploads.
- If you type in a time, in the format HH:MM using the 24-hour clock, then this is the time of day for a once-daily shadow files upload.

If you schedule a shadow file upload for a computer at a time when the computer is not available on the network, the upload occurs the next time the computer is connected to the network.

When you are using devices which transfer data during a long period of time (e.g. server backup to external Firewire hard disk), make sure the upload delay is longer than the duration of the transfer, EVEN when you are not shadowing anything. Failing to do so may result in a failed backup or interrupted copy process/DVD-writing process. So when using DVD/CD writers, it is highly recommended to set the upload delay to at least twice the maximum amount of time needed to burn a CD on the slowest DVD/CD writer in your infrastructure.

Shadow directory

The shadow directory is the temporary directory 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, exist. 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.*

SecureWave Application Server address

This option defines the IP address of the SecureWave Application Server(s) that the Sanctuary Client driver should connect to. 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.

The default setting is the address provided at the time of the client installation. 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).

Encrypted Media Key Export

This option defines whether users may export the keys used to encrypt media. The possible settings are:

- *Disabled.* Default. It is impossible to export media keys. The encrypted media can only be read by users who have been granted access to the media on computers that are protected by Sanctuary Device Control.
- *To file.* Users are allowed to export media keys to a file. The encrypted media will be usable outside of the organization by anybody having the encryption

key file and the password for the media. See *Chapter 7: Accessing encrypted media outside of your organization* on page *175* for more details.

> *To media or file.* Users are allowed to export media keys to a file or directly to the media. If the user exports the key to the media, the media will be usable outside of the organization by anybody having the password for the media. See *Chapter 7: Accessing encrypted media outside of your organization* on page *175* for more details.

Exporting the encryption keys directly to media is significantly less secure as the level of difficulty to access data will be directly linked to the media password complexity.

Encrypted Media Export 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. The password needs to meet the following requirements:

Be at least 8 characters long.

Contain upper case and lower case letters.

Contain numbers.

Contain at least one non alphabetical character (!@#$%*...).

> *Allow weak password.* Any password except the blank password is accepted.

This option only applies when the Encrypted Media Key Export option is set to 'To file' or 'To media or file'.

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 *237* for more details. If a user has no certificate, the Sanctuary Client will automatically create one — using rtnotify.exe. This option allows you to disable this automatic behavior.

The possible settings are:

> *Automatic.* Default. The Sanctuary Client will automatically create a user certificate if the user has none.

> *Disabled.* The Sanctuary Client 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 he has been granted access to it.*

Centralized Device Control Logging

The centralized logging determines what is logged in the central logging system when the user attempts to access a protected device. The possible settings are:

> *Disabled.* Default. Nothing is written to the central logging.

> *Enabled.* Attempts to access a prohibited device and client errors are written to the central logging system and can be viewed in the Log Explorer. See *Chapter 4: Using the Log Explorer* on page *123* for more details.

✍ *Some programs like Windows Explorer or some anti-virus programs may attempt repeatedly devices access. The Sanctuary Client can filter out similar access occurrences; see Suppress recurring log events 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' denied line 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.*

Suppress recurring log events

When the centralized device logging option is enabled, the Sanctuary Client logs all access attempts to protected devices. Some programs like the Windows Explorer or some anti-virus programs may try to access the devices repeatedly, causing massive volume of similar information to be logged in the system. The *Suppress recurring log events* option allows you to define a period of time during which all similar occurrences of an already logged-on event will be 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 the similar event in the Log Explorer.

✍ *This setting applies only to Read/Write denied events. Every time another event occurs, such as a device is plugged in, an error is reported, and so on, the logging of one read/write event is allowed and the logging history period is reset. This allows you to see if a read/write event occurred after a new device has been connected to the computer for example.*

Chapter 9: Reports

The Reports menu 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 that can be viewed using Internet Explorer or any other Web browser defined on your system. The reports can be printed, copied, converted, saved, and modified as required. Reports are provisional files created in the Report folder located in your temporary directory — WINDOWS %TEMP%.

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

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

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

Type of user access	*Available Reports*
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', and '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 28: Types of reports that can be obtained by a user

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

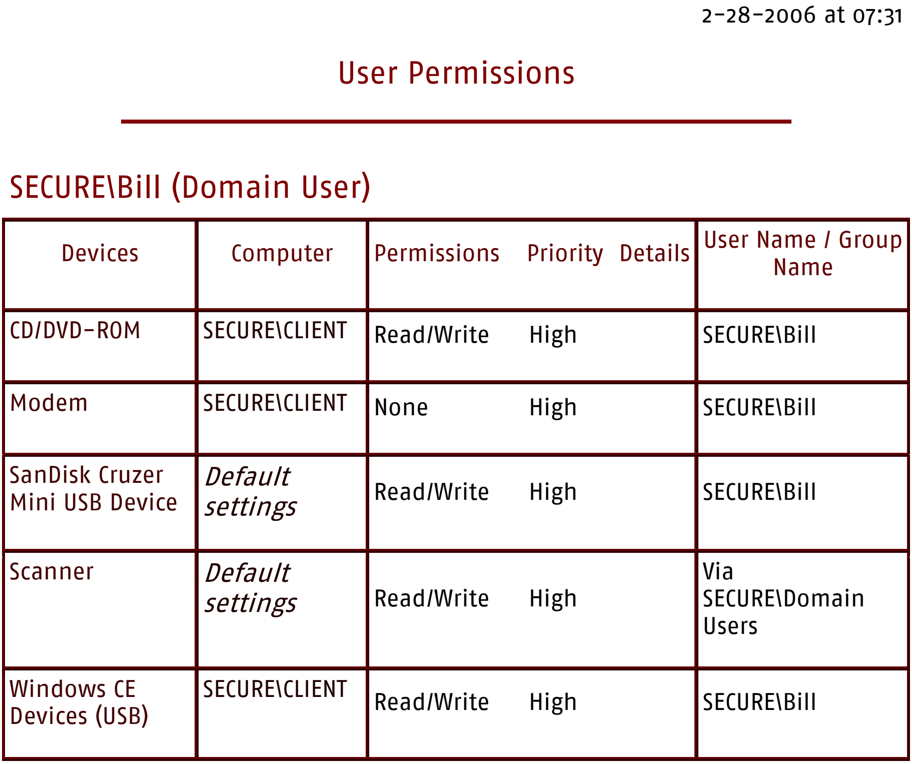
User Permissions report

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.
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	Read/Write	High		SECURE\Bill
Modem	SECURE\CLIENT	None	High		SECURE\Bill
SanDisk Cruzer Mini USB Device	*Default settings*	Read/Write	High		SECURE\Bill
Scanner	*Default settings*	Read/Write	High		Via SECURE\Domain Users
Windows CE Devices (USB)	SECURE\CLIENT	Read/Write	High		SECURE\Bill

Figure 102: User Permissions report

Device Permissions report

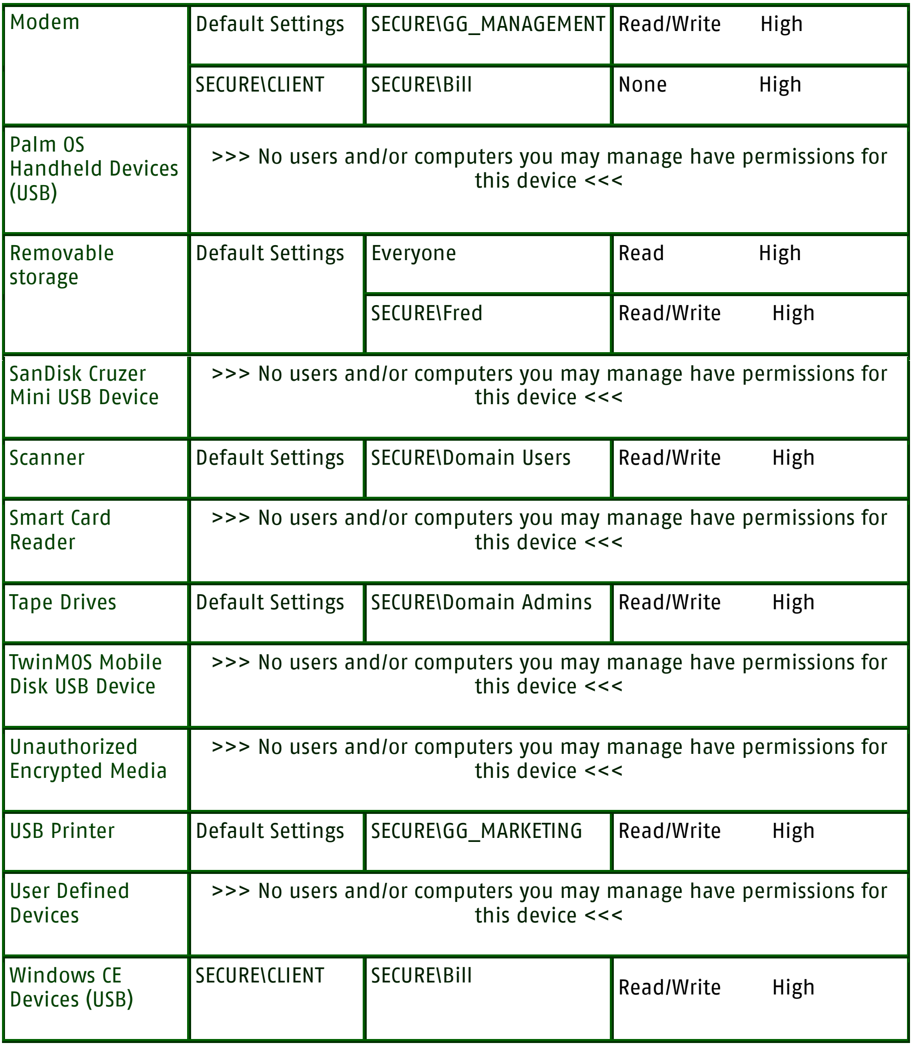
Use this report to view all permissions rules for the devices defined in the Device Explorer module. To generate this report, select *Device Permissions* from the *Reports* menu.

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	Read/Write	High	
CD/DVD-ROM	Default Settings	Administrators	Read/Write	High	
		SECURE\Bill	Read/Write	High	
		SECURE\Cert Publishers	Read	High	Online
		SECURE\Cert Publishers	Read/Write	High	Offline
	SECURE\CLIENT	SECURE\Bill	Read/Write	High	
COM/Serial Ports	>>> No users and/or computers you may manage have permissions for this device <<<				
Floppy Disk Drives	Default Settings	Administrators	Read/Write	Low	
		SECURE\Todd	Shadow Filename	High	Shadow Option
			1 MB	High	Copy Limit
LPT/Parallel Ports	>>> No users and/or computers you may manage have permissions for this device <<<				



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

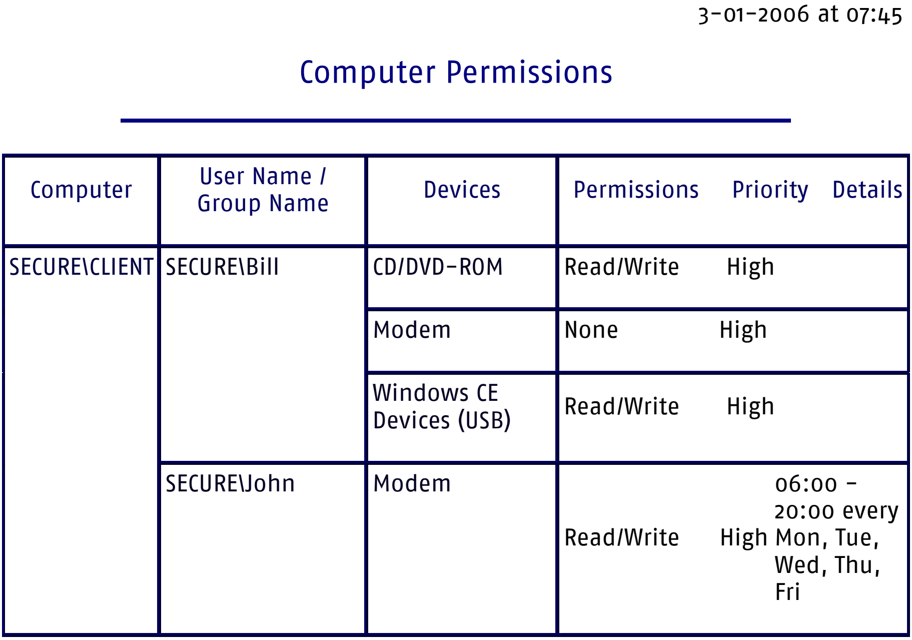
Figure 103: Device Permissions report

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.
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	Read/Write	High	
		Modem	None	High	
		Windows CE Devices (USB)	Read/Write	High	
	SECURE\John	Modem	Read/Write	High	06:00 - 20:00 every Mon, Tue, Wed, Thu, Fri

Figure 104: 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.
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		
O9PRMCD01	*Office XP*	3-02-2006	SECURE\Chuck
V2KEE_IE	*Visio*	1-01-2005	SECURE\Administrator
vsentd2	*Visual Studio .Net*	2-02-2006	SECURE\Administrator
X05-69971	*Microsoft Project*	2-22-2006	SECURE\Emily

Encrypted Media Label	Description	Registered On	Registered By
DK09	*Mobile Disk DK09*	2-15-2006	SECURE\Administrator
DK12	*Mini Cruzer 128 Mb DK12*	12-30-2005	SECURE\Administrator

Figure 105: 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.

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)*

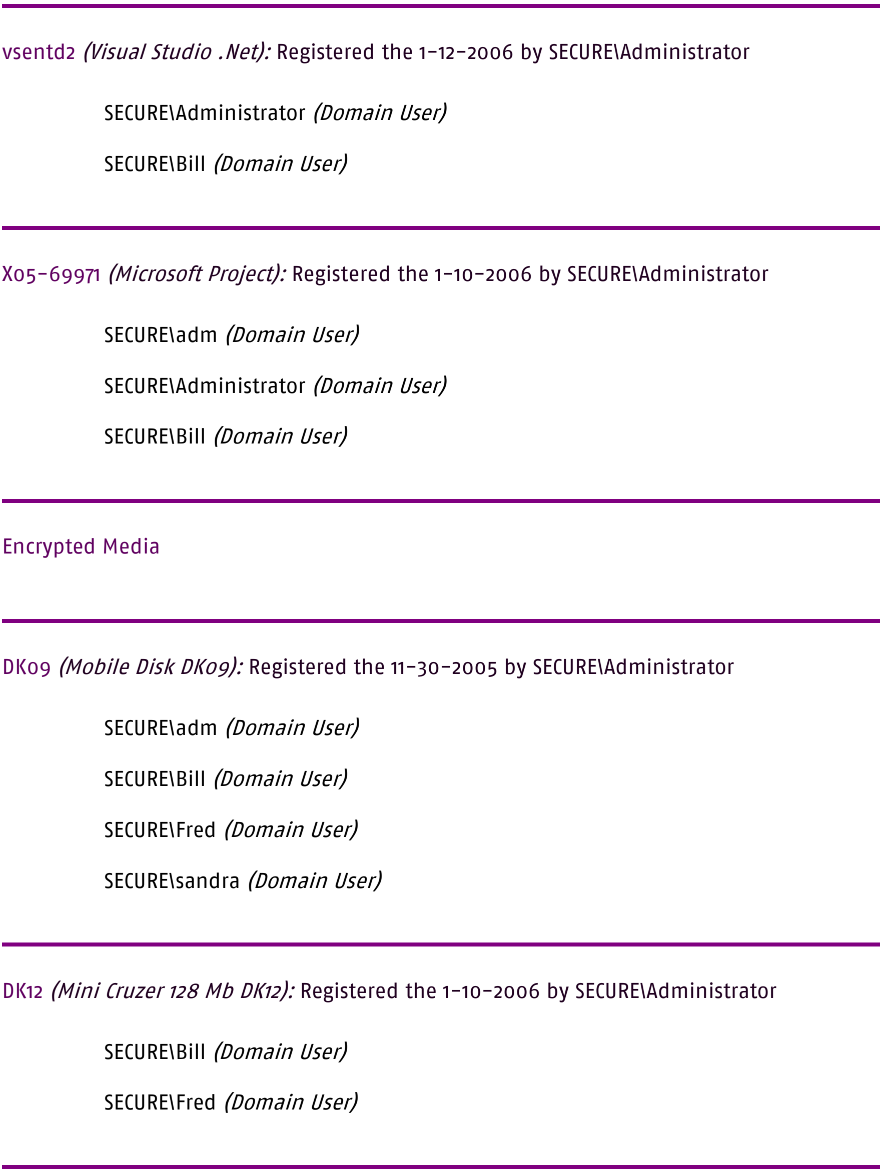
O9PRMCD01 *(Office XP):* Registered the 1-27-2006 by SECURE\Administrator

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)*

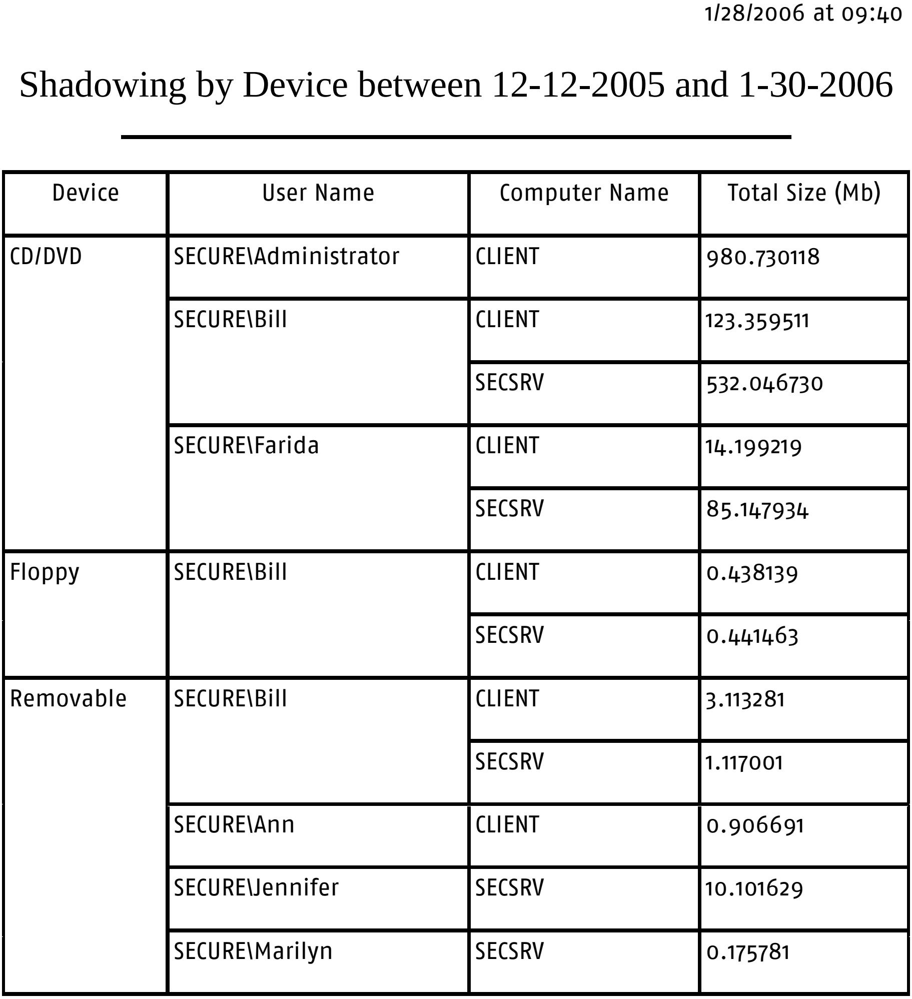
SECURE\Fred *(Domain User)*

Figure 106: Users by Medium report

Shadowing by Device report

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

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

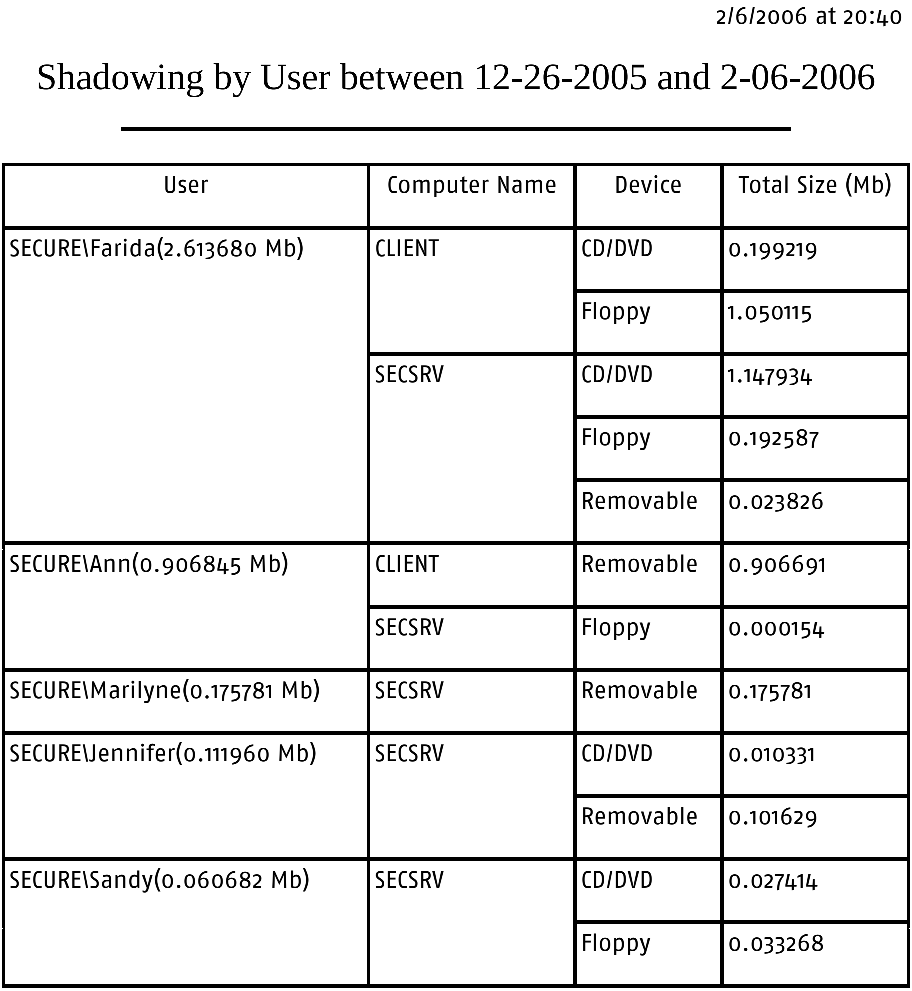
Device	User Name	Computer Name	Total Size (Mb)
CD/DVD	SECURE\Administrator	CLIENT	980.730118
	SECURE\Bill	CLIENT	123.359511
		SECSRV	532.046730
	SECURE\Farida	CLIENT	14.199219
		SECSRV	85.147934
Floppy	SECURE\Bill	CLIENT	0.438139
		SECSRV	0.441463
Removable	SECURE\Bill	CLIENT	3.113281
		SECSRV	1.117001
	SECURE\Ann	CLIENT	0.906691
	SECURE\Jennifer	SECSRV	10.101629
	SECURE\Marilyn	SECSRV	0.175781

Figure 107: Shadowing by Device report

Shadowing by User report

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

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

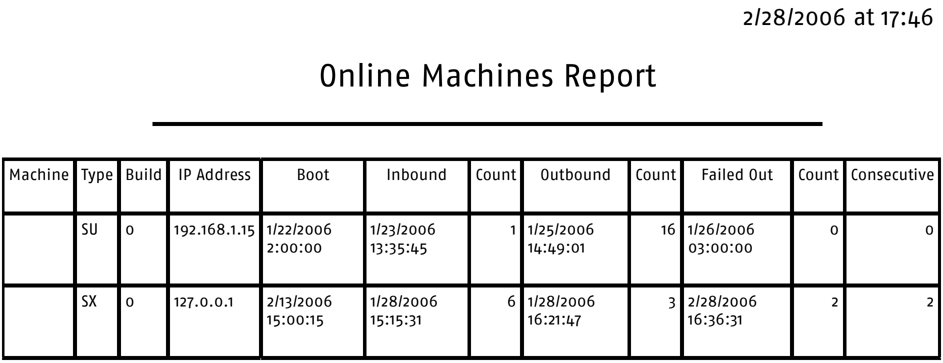
User	Computer Name	Device	Total Size (Mb)
SECURE\Farida(2.613680 Mb)	CLIENT	CD/DVD	0.199219
		Floppy	1.050115
	SECSRV	CD/DVD	1.147934
		Floppy	0.192587
		Removable	0.023826
SECURE\Ann(0.906845 Mb)	CLIENT	Removable	0.906691
	SECSRV	Floppy	0.000154
SECURE\Marilyne(0.175781 Mb)	SECSRV	Removable	0.175781
SECURE\Jennifer(0.111960 Mb)	SECSRV	CD/DVD	0.010331
		Removable	0.101629
SECURE\Sandy(0.060682 Mb)	SECSRV	CD/DVD	0.027414
		Floppy	0.033268

Figure 108: 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.

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



2/28/2006 at 17:46

Online Machines Report

Machine	Type	Build	IP Address	Boot	Inbound	Count	Outbound	Count	Failed Out	Count	Consecutive
	SU	0	192.168.1.15	1/22/2006 2:00:00	1/23/2006 13:35:45	1	1/25/2006 14:49:01	16	1/26/2006 03:00:00	0	0
	SX	0	127.0.0.1	2/13/2006 15:00:15	1/28/2006 15:15:31	6	1/28/2006 16:21:47	3	2/28/2006 16:36:31	2	2

Figure 109: Online Machines report

Below is an explanation of the columns:

- Machine: Always empty.
- Type: This column holds the kind of client driver installed on the client computer: *SU* for Sanctuary Unified driver and *SX* for Sanctuary Custom Edition driver.
- IP Address: This column holds the IP address of the machine as registered in the online table.
- Build: Always zero.
- Boot: This field contains the date and time the SecureWave Application server last received a boot notification from the client machine.

  A value of '1601-01-01 02:00:00' indicates that the Application Server did not receive a boot notification. However, it did receive a logon notification or the user selected the *Refresh settings* option on the contextual menu of the

Sanctuary Client icon (located on the system tray). This notification applies for machines that could not contact a SecureWave application Server at boot.

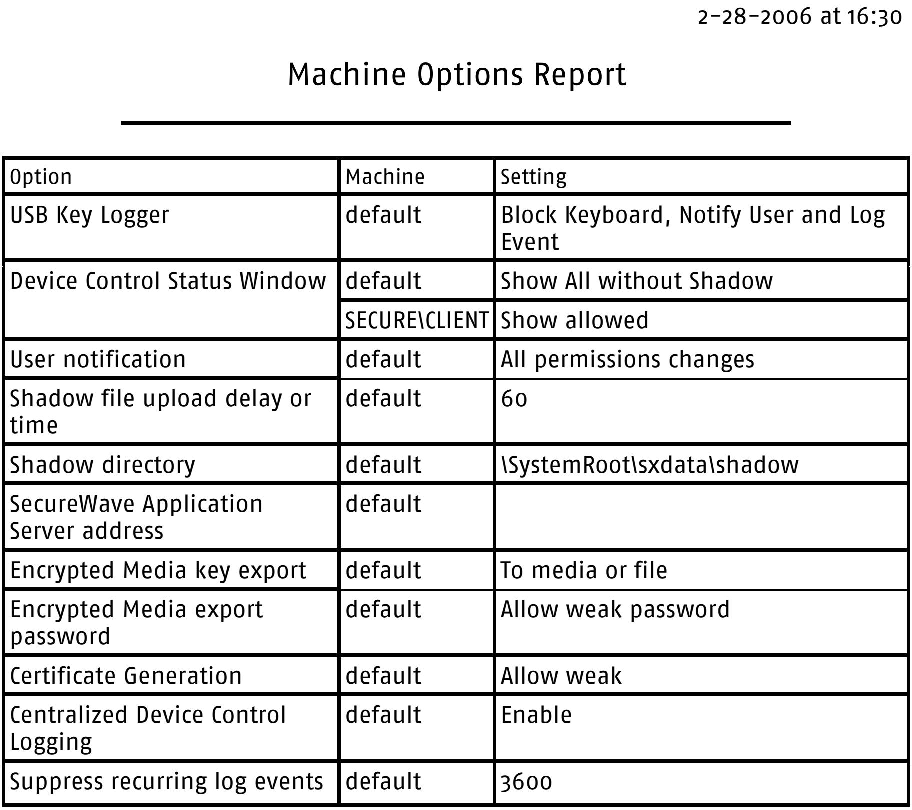
When the user selects the *Refresh settings*, all modifications done by the administrator to his machine/profile will be updated.

- 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 between the client computer and the SecureWave Application server.
- Count: (Referring to the Outbound connection) Contains the number of connections that the SecureWave Application server initiated with the client computer.
- Failed out: This field contains the date and time of the last unsuccessful connection between the SecureWave Application server and the client computer.
- Count: (Referring to the failed out connection) Contains the total number of connections that failed between the SecureWave Application Server and the client computer. This number will increase in the case of poor connections between the client and the server or in the case of high load on the server.
- 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.

Options report

Use this report to see how the default program's option changed. To generate this report, select *Options* from the *Reports* menu. Please refer to *Chapter 8: Setting and changing options* on page *191* 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 Keyboard, Notify User and Log Event
Device Control Status Window	default	Show All without Shadow
	SECURE\CLIENT	Show allowed
User notification	default	All permissions changes
Shadow file upload delay or time	default	60
Shadow directory	default	\SystemRoot\sxdata\shadow
SecureWave Application Server address	default	
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

Figure 110: Machine options report

Chapter 10: 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 suite 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 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:

Parameter	Used for	Notes
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 29: 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, Sanctuary 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 doing nothing or its 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 MSDE 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 MSDE 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 to CD-R, CD-RW, DVD-R, DVD+R, DVD-RW, DVD+RW and DVD-RAM media, its analysis, and the extraction of the original files that were selected to be written to the media. The information is stored by the SecureWave Application Server and can be retrieved in summary form or with full file data through the Log Explorer 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 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 3rd 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 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.

Format	*Full shadow mode*	*File name only shadow mode*
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 30: 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 Device 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.

Analysis of the CD image

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 Datafile 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 *227.*

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\00000003.cdshadow)
```

The above entry (all this data is in only one line in the original log) shows the file 'This is the first file in the root directory' being added to the list of shadow files. Had the file been imported from an earlier recording session on the same disc, the entry would have read '[000000004] This is the first file in the root directory: file data are in an earlier session (LBA NNN) -- skipping this file.', where 12345 would have given the block number of the file's data on the disc itself.

```
[000000005] This is the second file in the root directory:
Added file name and data (path "\", shadowid 10824,
location 1;0;4;cdshadow;000\000\00000004.cdshadow)
<ROOT>: extracting files from subdirs.
This is the first subdirectory: extracting files from directory.
```

Having processed all the files in the root directory, the first of the subdirectories (in this case 'This is the first subdirectory') is examined in the same way. We omit here all other entries of this type to save space, but they do appear fully in the analysis log.

The final stage consists in checking any block that contains data (i.e., not filled with zeros) but is not part of any file or subdirectory, and to check for partially-unused blocks, in whose unused portions data may be hidden. Since this image has not been manually falsified, no such blocks exist:

```
Verifying that unused blocks do not contain any data.
0 hidden blocks with data were dumped to the log.
0 partial blocks with extra data were dumped to the log.
Image analysis completed.
Image parsing ended (result 0).
Log closed.
```

Once this is done, the analysis of the image is now complete. If a fatal error occurs (one for which the client cannot guarantee that the shadow files and the log contain all data recorded to the disc), the image file itself would also have been added as a shadow file. You can easily verify this condition, since the name of these files in the shadow files list is deliberately chosen to be distinctive.

Supported and unsupported CD formats

Summary

Track-at-once (TAO) recordings for data generally work 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!) are 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:

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

Table 31: 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 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

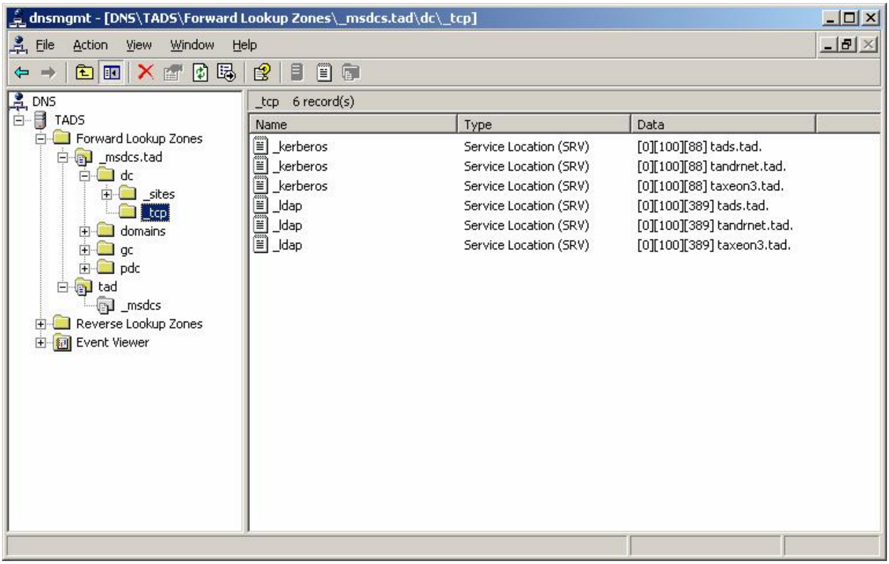
The Windows Certificate authority is tightly integrated to the Windows Active Directory. In order to use encryption of removable storage devices, your domain must be configured to use Active Directory.

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:



_tcp 6 record(s)

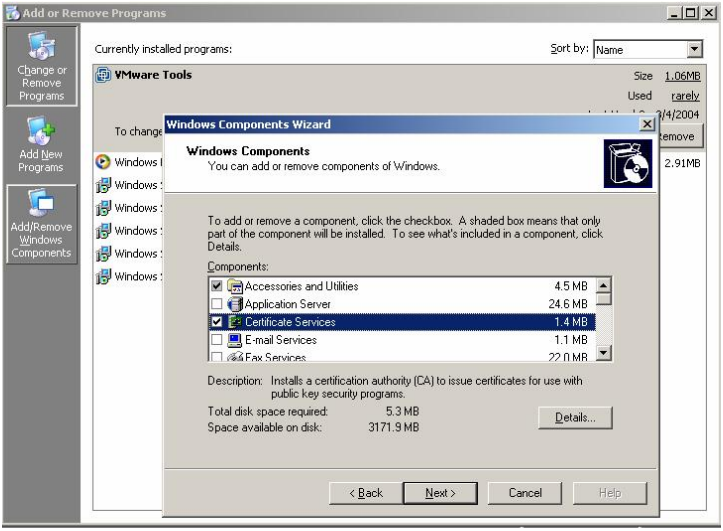
Name	Type	Data
_kerberos	Service Location (SRV)	[0][100][88] tads.tad.
_kerberos	Service Location (SRV)	[0][100][88] tandrnet.tad.
_kerberos	Service Location (SRV)	[0][100][88] taxeon3.tad.
_ldap	Service Location (SRV)	[0][100][389] tads.tad.
_ldap	Service Location (SRV)	[0][100][389] tandrnet.tad.
_ldap	Service Location (SRV)	[0][100][389] taxeon3.tad.

Figure 111: 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.



Windows Components Wizard

Windows Components
You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

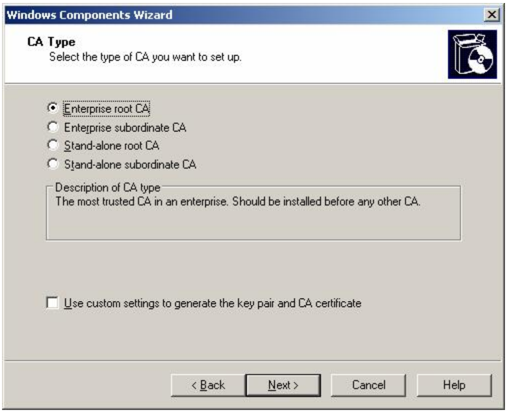
☑	Accessories and Utilities	4.5 MB
□	Application Server	24.6 MB
☑	Certificate Services	1.4 MB
□	E-mail Services	1.1 MB
□	Fax Services	22.0 MB

Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.

Total disk space required: 5.3 MB
Space available on disk: 3171.9 MB

Figure 112: Adding certificate services

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



Windows Components Wizard

CA Type
Select the type of CA you want to set up.

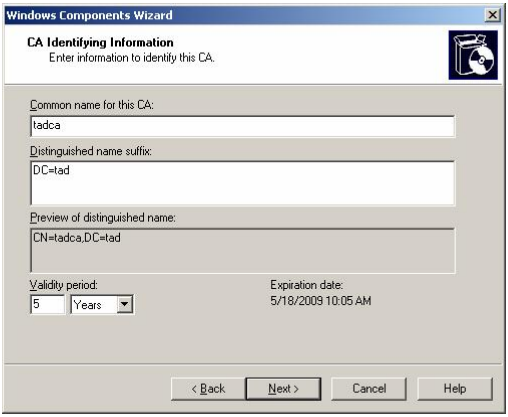
● Enterprise root CA
○ Enterprise subordinate CA
○ Stand-alone root CA
○ Stand-alone subordinate CA

Description of CA type
The most trusted CA in an enterprise. Should be installed before any other CA.

□ Use custom settings to generate the key pair and CA certificate

Figure 113: The Windows components wizard (1st page)

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



Windows Components Wizard

CA Identifying Information
Enter information to identify this CA.

Common name for this CA: tadca

Distinguished name suffix: DC=tad

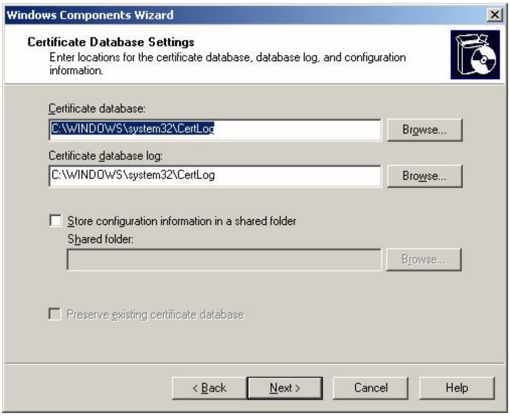
Preview of distinguished name: CN=tadca,DC=tad

Validity period: 5 Years

Expiration date: 5/18/2009 10:05 AM

Figure 114: The Windows components wizard (2nd page)

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



Windows Components Wizard

Certificate Database Settings
Enter locations for the certificate database, database log, and configuration information.

Certificate database: C:\WINDOWS\system32\CertLog

Certificate database log: C:\WINDOWS\system32\CertLog

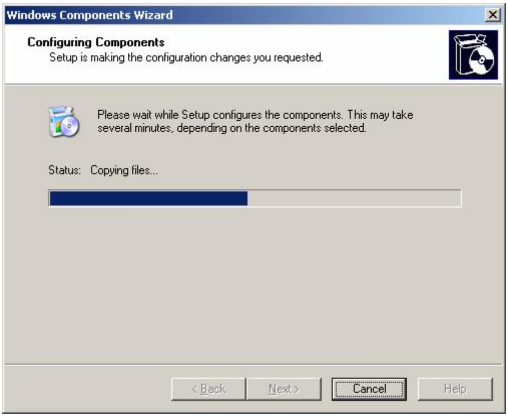
□ Store configuration information in a shared folder

Shared folder:

□ Preserve existing certificate database

Figure 115: The Windows components wizard (3rd page)

Windows proceeds with the installation of the certificate services.



Configuring Components

Setup is making the configuration changes you requested.

Please wait while Setup configures the components. This may take several minutes, depending on the components selected.

Status: Copying files...

Figure 116: 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.*

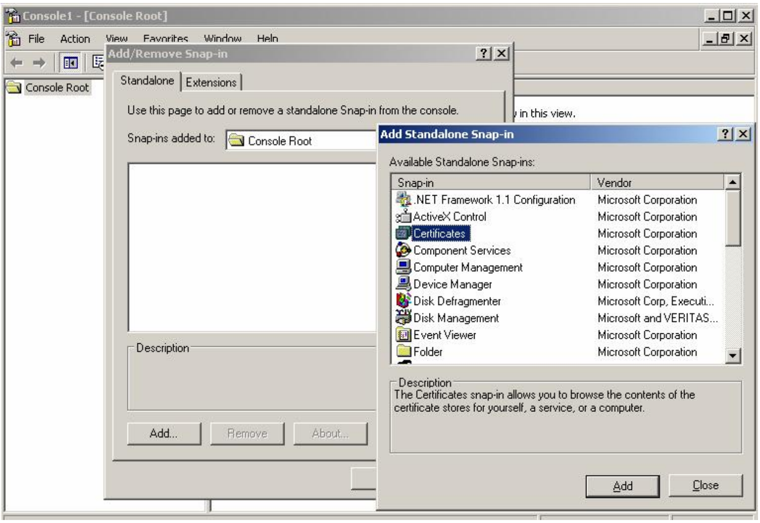
✍ *Depending on your Active Directory configuration and replication between domain controllers setting, it may take some time to issue a certificate during the first user logon and publish it to the Active Directory. During that period, the user is not authorized to access the media.*

✍ *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 the 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*.
5. Select ADD.
6. In the *Add Standalone Snap-in* dialog, choose *Certificates* and select ADD.



Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

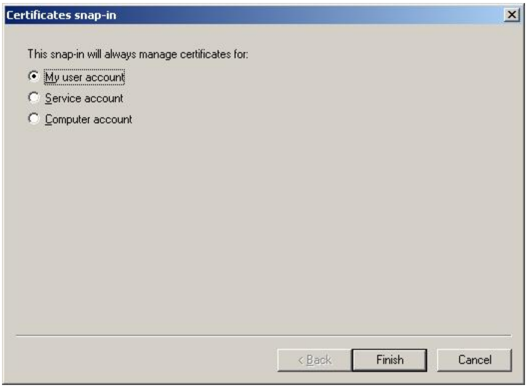
Snap-in	Vendor
.NET Framework 1.1 Configuration	Microsoft Corporation
ActiveX Control	Microsoft Corporation
Certificates	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
Disk Defragmenter	Microsoft Corp, Executi...
Disk Management	Microsoft and VERITAS...
Event Viewer	Microsoft Corporation
Folder	Microsoft Corporation

Description

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Figure 117: The certificate snap-in

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



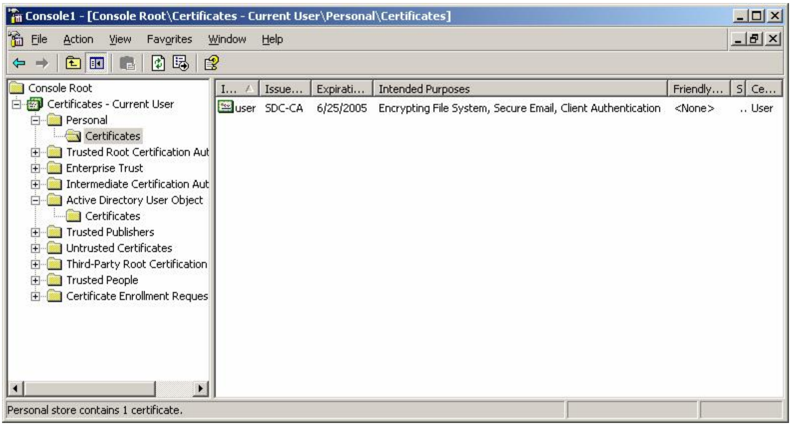
Certificates snap-in

This snap-in will always manage certificates for:

● My user account
○ Service account
○ Computer account

Figure 118: The certificate snap-in: user account

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



Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

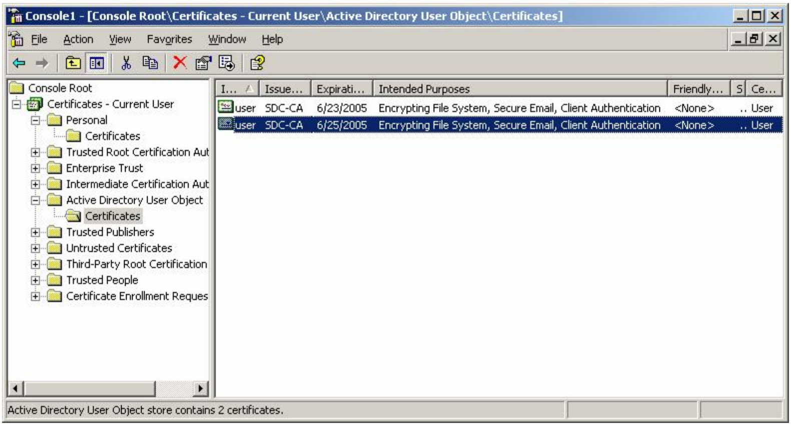
Console Root
- Certificates - Current User
  - Personal
    - Certificates
  - Trusted Root Certification Aut
  - Enterprise Trust
  - Intermediate Certification Aut
  - Active Directory User Object
    - Certificates
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification
  - Trusted People
  - Certificate Enrollment Reques

I...	Issue...	Expirati...	Intended Purposes	Friendly...	S	Ce...
user	SDC-CA	6/25/2005	Encrypting File System, Secure Email, Client Authentication	<None>	..	User

Personal store contains 1 certificate.

Figure 119: The console: certificate intended purposes

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


Console1 - [Console Root\Certificates - Current User\Active Directory User Object\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Aut
Enterprise Trust
Intermediate Certification Aut
Active Directory User Object
Certificates
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification
Trusted People
Certificate Enrollment Reques

I...	Issue...	Expirati...	Intended Purposes	Friendly...	S	Ce...
user	SDC-CA	6/23/2005	Encrypting File System, Secure Email, Client Authentication	<None>	..	User
user	SDC-CA	6/25/2005	Encrypting File System, Secure Email, Client Authentication	<None>	..	User

Active Directory User Object store contains 2 certificates.

Figure 120: 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:

Wireless NICs you can block using the Sanctuary Device Control permissions rules	
If you are using Window 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 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

Wireless NICs you can block using the Sanctuary Device Control permissions rules	
	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 32: 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 of the Date filter settings you use in the *Reports*, *Audit Logs Viewer* module, and *Log Explorer* module. 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.

> The *Shadow File Upload Delay or Time* setting can be tricky if you assign more than 6 hours as value. For example, if you set 720 (every twelve hours) or 1440 (every 24 hours) as the field value, the upload will be done every hour (default value).

> 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 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 knows 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 8: Setting and changing options* on page *191* for more details.

> If a *Copy Limit* rule (see page *109*) 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 'R/W' or 'No Permission' can be assigned to their memory and I/O data transfer cannot be shadowed. Recent models, however, adhere to the "standard" schema of declaring their memory to the *Removable Storage Device* class (ex. Sony Ericsson W800).

Please see *Managing devices* on page *113* 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 *113* 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.

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]
```

Parameter	*Description*
-?	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 *Manage Sanctuary Settings* rights
-create	Creates or updates SecureWave's *Manage Sanctuary Settings* rights
-delete	Deletes SecureWave's *Manage Sanctuary Settings* rights

Table 33: Ctrlacx script options

Examples

```
cscript Ctrlacx.vbs –e > MyFile.txt
```

List all control access rights in condensed mode redirecting the output to MyFile.txt file.

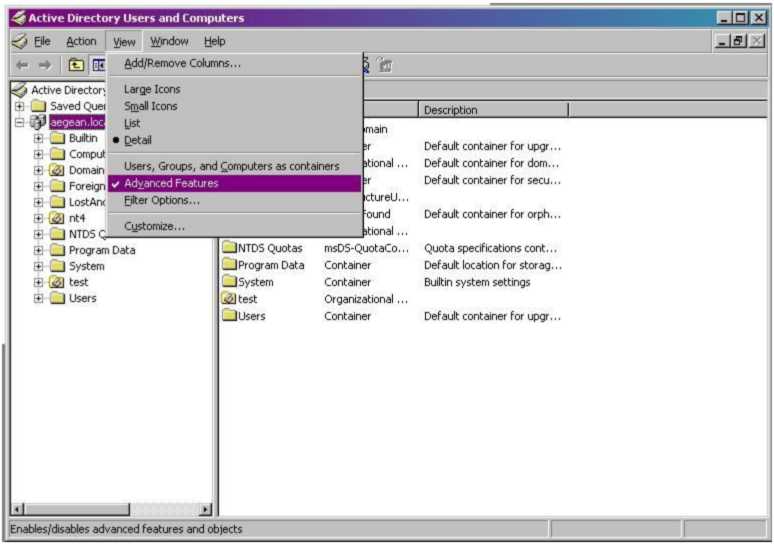
```
ctrlacx.vbs -s
```

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 121*.



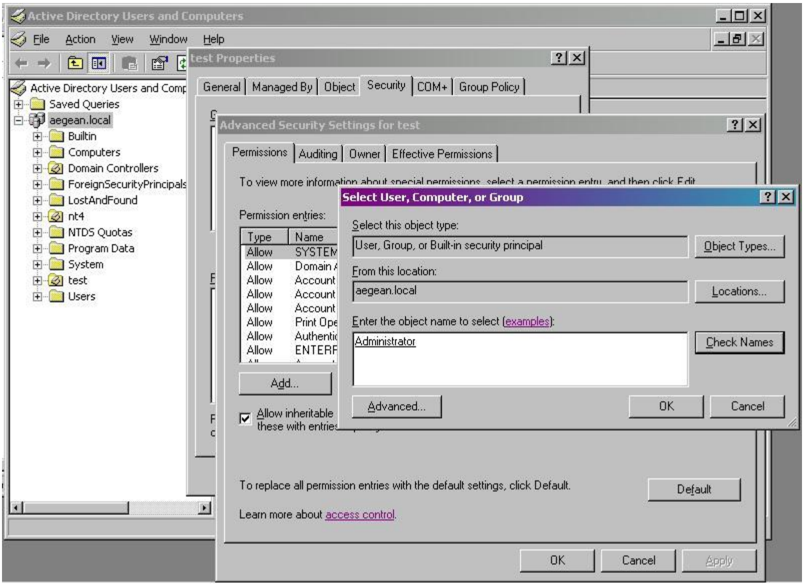
Enables/disables advanced features and objects

Figure 121: 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 122*, and click on OK to close the dialog.



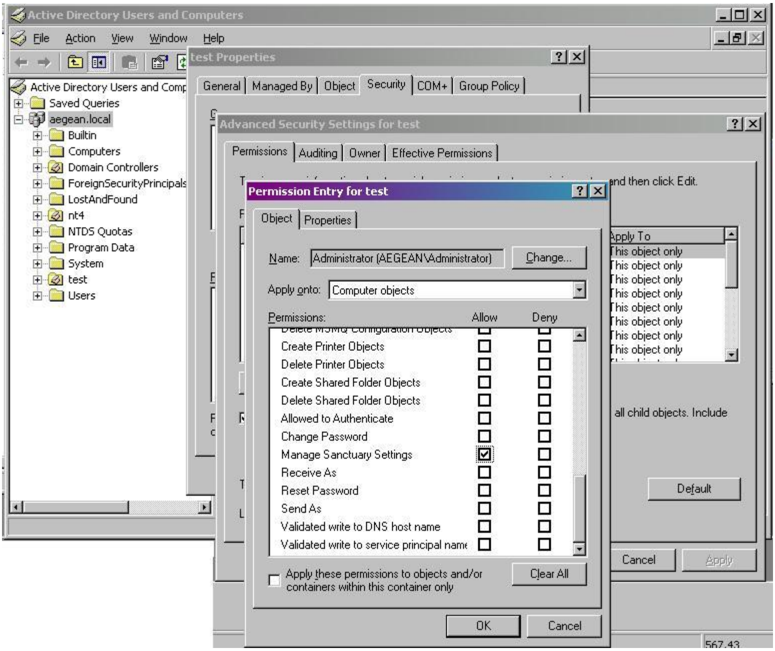
Select this object type:
User, Group, or Built-in security principal

From this location:
aegean.local

Enter the object name to select (examples):
Administrator

Figure 122: Select user, computer or group to which delegate.

7. Click on the OK button to open the *Permissions entry* dialog as shown in *Figure 123*.


Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Comp
Saved Queries
aegean.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
LostAndFound
nt4
NTDS Quotas
Program Data
System
test
Users
test Properties
General | Managed By | Object | Security | COM+ | Group Policy
Advanced Security Settings for test
Permissions | Auditing | Owner | Effective Permissions
and then click Edit.
Apply To
This object only
all child objects. Include
Default
Cancel
Apply

Permission Entry for test

Object | Properties

Name: Administrator (AEGEAN\Administrator) Change...

Apply onto: Computer objects

Permissions:	Allow	Deny
Create Printer Objects	□	□
Delete Printer Objects	□	□
Create Shared Folder Objects	□	□
Delete Shared Folder Objects	□	□
Allowed to Authenticate	□	□
Change Password	□	□
Manage Sanctuary Settings	☑	□
Receive As	□	□
Reset Password	□	□
Send As	□	□
Validated write to DNS host name	□	□
Validated write to service principal name	□	□

□ Apply these permissions to objects and/or containers within this container only

Clear All

OK Cancel

Figure 123: Manage Sanctuary Settings object

8. 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.

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.

MDAC

Microsoft Data Access Components. A component required by computers using Windows to connect to SQL Server or MSDE databases.

MSDE

Microsoft SQL Server Desktop Engine. A free component partially substituting the SQL Server you need to run Sanctuary Device Control. Sanctuary Device Control uses MSDE 2000.

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 batabase: 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.

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.

SQL Server

Microsoft's industry standard database server. You will need it, or the MSDE component, to run Sanctuary Device Control.

SXS

SecureWave Application Server

TAO

Track-At-Once.

TCP/IP

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

Index of Tables

Index