



SecureWave
Sanctuary[®]
Safeguarding Tomorrow



Sanctuary Suite Setup Guide

Liability Notice

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

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

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

SecureWave claims copyright in this program and documentation as an unpublished work, revisions of which were first licensed on the date indicated in the foregoing notice.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

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

Trademarks

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

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

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

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

You can contact our technical support team at:

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

or by sending an email to support@securewave.com

Published on: April 2006



Contents

Introduction	5
Additional information	7
Symbol explanation	8
Typefaces.....	8
Support and contact information	9
Product-Chapter relation.....	10
Chapter 1: Installing Server Side Components.....	13
Introduction.....	13
System requirements.....	14
Small, medium, and big networks.....	15
Trusted domains	16
Basic security rules	17
The boot sequence.....	17
The seal/chassis intrusion protector	17
Password protect the BIOS	17
Administrative rights.....	18
Power Users	18
Access Policy.....	18
NTFS Partition	18
Recovery Console.....	19
Safe mode	19
Service packs and hot fixes	19
Firewalls	19
Password policies	19
Access policy	20
Private and Public Key Generation.....	20
Sanctuary infrastructure	20
Installing all server components onto a single computer.....	22
Before you install	23
Part 1: Installing the SQL database engine	23
Part 2: Installing the SecureWave Sanctuary Database	24
Part 3: Installing the SecureWave Application Server	25
Part 4: Installing the Sanctuary Management Console	30
Part 5: Installing the Sanctuary Client Driver	31
Part 6: Testing your installation	31
Installing Sanctuary in a Workgroup.....	32
Chapter 2: Installing the Database Components.....	33
Choosing a SQL engine	33
Before you install	34
Part 1: Install the SQL database engine.....	34
Part 2: Install the SecureWave Sanctuary Database.....	36



Chapter 3: Installing SecureWave Application Server	41
Before you install	41
The installation procedure	44
Upgrading from a previous SecureWave Application Server version	54
Chapter 4: Installing the Sanctuary Console	57
Before you install	58
The installation procedure	58
Chapter 5: Installing the Sanctuary Client on your guest computers	63
System requirements	63
Requirements for the overall system	63
Requirements for the client computer	64
The installation procedure	64
Unattended installation of the Sanctuary Client	72
Uninstalling the Sanctuary Client	72
Load balancing methods	72
What is load balancing	72
How does round robin DNS works?	73
Advantages of DNS Round Robin	73
Chapter 6: The Authorization Service tool	75
What is the Sanctuary Authorization Service tool?	75
Installation	76
Chapter 7: Testing your Sanctuary Device Control installation	81
Permissions	81
Temporary permissions	82
Scheduled permissions	83
CD authorization	84
Shadowing	85
Auditing	86
Reporting	86
Summary	87
Chapter 8: Testing your Sanctuary installation	89
Performing an initial scan	89
Creating a Scan Template	89
Utilizing your new Template	90
Authorizing your new file hashes	90
Authorizing Files	91
Try to log on a machine with the client installed	92
Auditing	93
Audit Logs Viewer	93
Log Explorer	94
Database Exploration	95
Local Authorization	96
Summary	98



Chapter 9: Using the Key Pair Generator	99
Introduction.....	99
Starting the key pair generator	100
Generating a key pair	100
Deploying the key pair.....	101
Chapter 10: Unattended Client Installation	103
Installing Sanctuary Client: MST file generation.....	104
Using the Sanctuary Client Deployment tool to install the Clients	111
Using the command-line to install the Clients.....	117
Using Windows Group Policy to install the Clients.....	118
Chapter 11: Using the SXDomain Command-line Tool	123
Introduction.....	123
The SXDomain parameters	123
Examples.....	124
Scheduling domain synchronizations	125
Chapter 12: Registering your Sanctuary Product	129
Licensing.....	129
Obtaining a license	129
License file location	130
License file format	130
License-related SXS actions at start-up.....	132
License-related SXS actions while running.....	132
License-related Client actions.....	133
Appendix A: Troubleshooting	135
Contacting SecureWave Support	135
Troubleshooting Tips	135
Database backup	137
Microsoft SQL Server backup	137
MSDE 2000 backup.....	138
SecureWave Application Server backup	140
Appendix B: Detailed System Requirements and Limitations.....	141
System requirements.....	141
Sanctuary Device Control	142
Terminal services limitations	142
The RunAs command limitations	143
Appendix C: Registry Keys	145
SecureWave Application Server registry keys.....	145
Sanctuary Client registry keys	148
Appendix D: Upgrading from previous versions	151
Sanctuary Device Control	152
Sanctuary Server Edition.....	152



Upgrading SecureEXE Clients	152
Upgrading Server-side components	153
Appendix E: Installing Sanctuary on Windows XP SP2/2003 SP1	155
Connection between SecureWave Application Server and the database	155
Connection between the console and the Application Server	156
Step 1: Configuring a fixed port on the Server	157
Step 2: Opening the port on the Server Firewall	157
Connecting using the Endpoint Mapper	157
Summary	159
Connection between the client and the SecureWave Application Server	159
Configuring the firewall	160
Appendix F: Opening firewall ports for client deployment	163
To manually open the ports in a computer-by-computer basis	163
To open the ports in a computer-by-computer basis with a .bat file	164
To open the firewall ports via an Active Directory Group policy	164
To create the Group Policy (GPO):	165
To improve security	167
Appendix G: Using your Sanctuary Synchronization Script for Novell:	
Quick Guide	169
Introduction	169
Step by step guide to install your Sanctuary Synchronization Script	169
Appendix H: Using Novell shares for your DataFileDirectory	173
DataFileDirectory access to a Novell share	173
Transparent SXS authentication for Novell eDirectory	173
Appendix I: Importing file definitions during setup	179
Appendix J: Using Sanctuary Server Edition with Sanctuary Device	
Control	181
Checking your database and application server version	181
Checking your blocking options	183
Glossary	185
Index of figures	189
Index of Tables	193
Index	195



Introduction

This guide explains how to install your Sanctuary suite.

- > *Chapter 1: Installing Server Side Components* guides you through the process of installing the Sanctuary server-side components on a single computer
- > *Chapter 2: Installing the Database Components* explains how to set up the database needed by the Sanctuary suite
- > *Chapter 3: Installing SecureWave Application Server* explains how to set up the SecureWave Application Server
- > *Chapter 4: Installing the Sanctuary Console* explains how to set up the console used for our Sanctuary suite
- > *Chapter 5: Installing the Sanctuary Client on your guest computers* guides you on how to set up the Sanctuary Client Driver on the computers that will be protected by Sanctuary
- > *Chapter 6: The Authorization Service tool* illustrates the setup of this SUS/WSUS (Software Update Services & Windows Server Update Services) update partner tool used for our Sanctuary suite programs (Sanctuary Server Edition, Sanctuary Custom Edition, and Sanctuary Terminal Services Edition)
- > *Chapter 7: Testing your Sanctuary Device Control installation* guides you through the basic tests of Sanctuary Device Control functionality
- > *Chapter 8: Testing your Sanctuary installation* guides you on how to test basic Sanctuary Server Edition & Sanctuary Custom Edition functionality
- > *Chapter 9: Using the Key Pair Generator* explains you how to generate public and private keys before you deploy the Sanctuary Client to other machines
- > *Chapter 10: Unattended Client Installation* shows you how to deploy clients silently
- > *Chapter 11: Using the SXDomain Command-line Tool* explains how to synchronize information between the Sanctuary Database and the domain controller
- > *Chapter 12: Registering your Sanctuary Product* explains the Sanctuary licensing model
- > *Appendix A: Troubleshooting* gives you general guidelines on how to diagnose problems that may occur during Sanctuary installation



- > *Appendix B: Detailed System Requirements and Limitations* details the hardware and software you need for an optimum operation of the software
- > *Appendix C: Registry Keys* shows detailed information on registry key settings for servers and clients
- > *Appendix D: Upgrading from previous versions* explains how to upgrade from a previous version of SecureNT to Sanctuary Device Control and SecureEXE to Sanctuary Server Edition & Sanctuary Custom Edition
- > The *Appendix E: Installing Sanctuary on Windows XP SP2/2003 SP1* explains how to configure this system to work with Sanctuary programs
- > In *Appendix F: Opening firewall ports for client deployment* you will find the procedure to open those required ports needed for the client deployment technique described on *Chapter 10: Unattended Client Installation*
- > The *Appendix G: Using your Sanctuary Synchronization Script for Novell*: Quick Guide shows a quick setup guide for using Sanctuary Device Console on Novell environment
- > *Appendix H: Using Novell shares for your DataFileDirectory* undertakes the task of explaining how to set the data file directory (DataFileDirectory or DFD) in your Novell server when using Sanctuary Device Control
- > In *Appendix I: Importing file definitions during setup* you find the necessary information to use the Sanctuary File Definitions (SFD) for Sanctuary Server Edition & Sanctuary Custom Edition during the setup phase
- > *Appendix J: Using Sanctuary Server Edition with Sanctuary Device Control* explains how to install this product with other of our proposed solutions
- > The *Glossary* provides definitions of standard terms used throughout the guide
- > The *Index of figures*, *Index of Tables*, and *Index* provide quick access to specific figures, tables, information, items, or topics

Some of these chapters are only relevant for some programs of our product suite. For example, *Chapter 7: Testing your Sanctuary Device Control installation* is only applicable, obviously, if you installed Sanctuary Device Control.



Each chapter has an introduction paragraph explaining to which part of our suite they correspond.



Additional information

In addition to the documents and the online help provided with your Sanctuary product, further information is available on our web site at:

<http://www.SecureWave.com>

In this regularly updated Web site, you can find:

- > The latest software upgrades and patches (for registered users)
- > The very latest troubleshooting tips and answers to Frequently Asked Questions (FAQ)
- > Other general support material that you may find useful
- > New information about our Sanctuary suite
- > Our Knowledge Base (KB), with FAQ (Frequent Asked Questions) and practical information of your every day use of Sanctuary solutions



Symbol explanation

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



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



Time. This symbol indicates the description of 'short-cut' or tips 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.

Typefaces

We use the following typefaces to differentiate different types of contents throughout this guide:

- > *Italic* Represent fields, menu options, and cross-references
- > Fixed width Shows messages or commands typed at the command prompt
- > SMALL CAPS Represents buttons you select



Support and contact information

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

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



Product-Chapter relation

This section outlines the relation between product and chapter.

- > *Chapter 1: Installing Server Side Components:* applies to all our products
- > *Chapter 2: Installing the Database Components:* applies to all our products
- > *Chapter 3: Installing SecureWave Application Server :* applies to all our products
- > *Chapter 4: Installing the Sanctuary Console:* applies to all our products
- > *Chapter 5: Installing the Sanctuary Client on your guest computers:* applies to all our products
- > *Chapter 6: The Authorization Service tool:* only applies to our Sanctuary suite programs (Sanctuary Server Edition, Sanctuary Terminal Service Edition, and Sanctuary Custom Edition)
- > *Chapter 7: Testing your Sanctuary Device Control installation:* only applies to Sanctuary Device Control
- > *Chapter 8: Testing your Sanctuary installation:* only applies to our Sanctuary suite programs (Sanctuary Server Edition, Sanctuary Terminal Service Edition, and Sanctuary Custom Edition)
- > *Chapter 9: Using the Key Pair Generator :* applies to all our products
- > *Chapter 10: Unattended Client Installation:* applies to all our products
- > *Chapter 11: Using the SXDomain Command-line Tool:* applies to all our products
- > *Chapter 12: Registering your Sanctuary Product:* applies to all our products
- > *Appendix A: Troubleshooting:* applies to all our products
- > *Appendix B: Detailed System Requirements and Limitations:* applies to all our products
- > *Appendix C: Registry Keys:* applies to all our products
- > *Appendix D: Upgrading from previous versions:* applies to all our products
- > *Appendix E: Installing Sanctuary on Windows XP SP2/2003 SP1:* applies to all our products
- > *Appendix F: Opening firewall ports for client deployment:* applies to all our products



- > *Appendix G: Using your Sanctuary Synchronization Script for Novell:* Quick Guide: applies to all our products
- > *Appendix H: Using Novell shares for your DataFileDirectory:* applies to all our products
- > *Appendix I: Importing file definitions during setup:* only applies to our Sanctuary suite programs (Sanctuary Server Edition, Sanctuary Terminal Service Edition, and Sanctuary Custom Edition)
- > *Appendix J: Using Sanctuary Server Edition with Sanctuary Device Control:* only applies to Sanctuary Server Edition



Chapter 1: Installing Server Side Components

The information in this chapter applies to all Sanctuary software suite products.

This chapter guides you through the procedure for installing the various server side components.

Introduction

Despite the fact that Sanctuary Software is an extremely powerful security solution, its setup is straightforward. The installation routine can be broken down into these stages:

1. Install the *SecureWave Sanctuary Database* on the computer that is to hold devices and/or executables authorization information. You can find a detailed installation procedure explanation on page 33.
2. Install the *SecureWave Application Server* on the computers that will serve as intermediate between the Sanctuary clients and the SecureWave Sanctuary Database distributing the list of device/software permissions for each client computer and/or User/group. See page 36.
3. Install the *Sanctuary Management Console* on the computer(s) you are going to use to configure Sanctuary, and subsequently carry out your day-to-day administrative tasks and procedures. See page 54.
4. Install a *Client*, test the predefined permissions to devices and/or executables. You can install it on the same machine as the one used for the *SecureWave Sanctuary Database*, *SecureWave Application Server*, and *Sanctuary Console* (some limitations apply). See page 63.
5. Define some *test permissions* for devices and/or executables using the console installed on step 3 and test them on the client machine. See page 81 (Sanctuary Device Control) and/or page 89 (Sanctuary Server Edition & Sanctuary Custom Edition).
6. Define company's *Policies* (permissions, rules, and settings). Determining and defining which users get access to which devices and/or executables. This step is done before installing or rolling out any clients. If you install clients without a good policy definition, this will result in a loss of productivity.



7. Plan the client installation strategy and proceed to *deploy your clients* in production machines to begin enjoying immediately the benefits of being protected by Sanctuary. See page 63 & 103.

You can find a detailed explanation of the functions carried out by the various Sanctuary components in the corresponding Administrator's Guides. We recommend that you read them thoroughly before starting the installation.

At any time after installing the *SecureWave Sanctuary Database*, *SecureWave Application Server*, *Sanctuary Console*, or the *Sanctuary Client* you can modify or uninstall the components by running their respective setup.exe files.

If any setup routine stops, (e.g. if a severe error is encountered or if it is canceled by user request) the routine attempts to clean up and roll back any modifications it made to your computer. It also produces log files containing the reason why the setup failed. They are placed in %TMP% directory and named sxdbi.log, setupclt.log, and setupxs.log. If your setup fails, and you make a support call to SecureWave, you will be asked to send these files to help us diagnose the problem.

Once the installation is completed, the next step is the Policy Definition, where you define which users get access to which devices and/or executables. This step is very important before any clients are installed or rolled out. If you install clients without a good policy definition, this will result in a loss of efficiency.



If policies are not defined or incorrectly defined, it could prevent users from accessing their devices. Define policies BEFORE installing any clients!

System requirements

In order to carry out a successful installation of the SecureWave's server side components: SecureWave Sanctuary Database (DB), SecureWave Application Server (SXS), and Sanctuary Console, you should consider the following points.

In a large environment, within a test setting, we recommend installing the database on a different computer than that of the SecureWave Application Server (SXS). However, for a production network, we recommend installing them on the same computer that also includes the Sanctuary Console component.

Therefore, taking this in consideration, your environment must meet the following requirements:

- > One or more computers to run the DB, SXS, and Sanctuary Console components
- > One or more client computers to install the Sanctuary Client drivers



- > TCP/IP networking protocols. SecureWave client drivers and server communicate only over TCP/IP
- > Appropriate firewall settings. See *Appendix C: Registry Keys*, on page 145, for mandatory open ports details
- > If you are installing:
 - Sanctuary Device Control: the client can be running on Windows 2000 (Service Pack 3 or later), XP Professional, or 2003
 - Sanctuary Server Edition & Sanctuary Custom Edition: The server computers can be running on Windows 2000 (Service Pack 3 or later) Server or Windows 2003 Server
- > MDAC 2.8 (or later) required for the SecureWave Application Server in order to communicate with the database
- > If used in large environments, it is strongly recommended to use Microsoft SQL Server 2000 or 2005 instead of MSDE. See our online knowledgebase on <http://www.SecureWave.com> for more details
- > The license file, SecureWave.lic, which you received from SecureWave. If you lost it or did not receive one with your software, you can obtain it by contacting technical support (support@SecureWave.com) or re-applying for an Evaluation License at our main website (<http://www.SecureWave.com>)
- > A Microsoft CA installed and published on you Active Directory structure before you can encrypt a removable device



We do not longer support Windows NT.

Small, medium, and big networks

In the context of this document, we define:

- > Small network –it usually has only one server, it can be an existing one or even a workstation used as a server. The server controls a unique domain. In these cases, we recommend using MSDE as the database repository and install the database server, application server, and console on the same machine. This network has, typically, less than 500 client machines.
- > Medium network – it has two or more servers, one of them a dedicated SQL database server and probably two or more domains with a trusted relation between them. In this case, the application server should be installed on at



least two computers for load balancing and failover purposes. It goes from 500 to approximately 5,000 client machines.

- > Big network – it has several servers and domains with complex trust relations among them. It also has a high-end dedicated SQL server machine clusters. You should install the application server on two or three servers. It has between 5,000 and 20,000 client machines. You can easily cope with even bigger networks adding more SecureWave Application Servers.

Trusted domains

In the case where you use several domains, expanding through different forest, and want to manage devices permissions centrally on all or some of them, you should create trust relationships between them. Sanctuary suite will not work across domains and/or forest if you do not establish first these relations – some of them are created by default depending on your operating system.

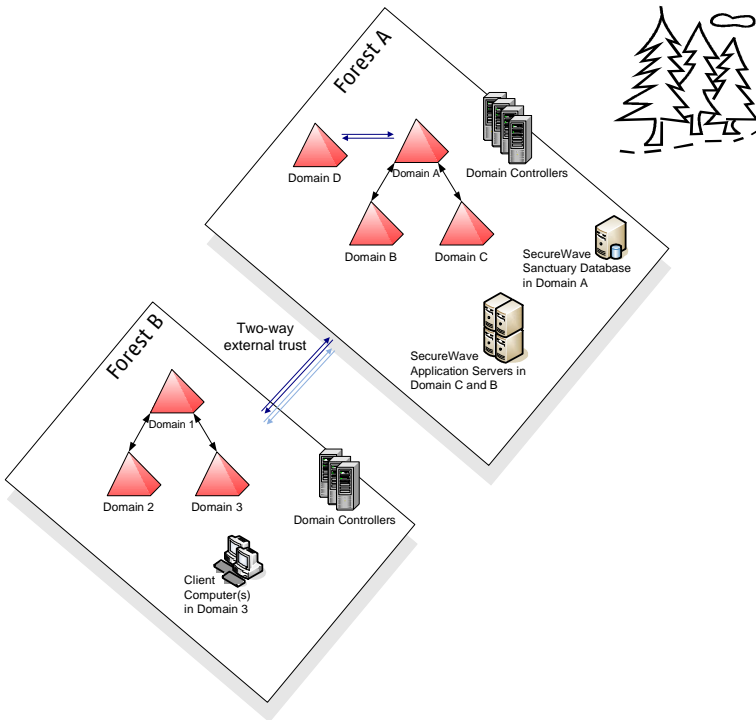


Figure 1: Trust relationships



Basic security rules

This section lists a series of basic security rules that should be met for any computer that you want to install on a production network.

The boot sequence

Change the boot sequence so that the machine does not boot first from the floppy, then the DVD/CD-ROM, and, finally, the hard disk drive. The Hard Disk Drive should always be the first boot device. If the Floppy or the DVD/CD-ROM is the first boot device, someone can use a bootable medium that can directly access the hard disk drive and reset the administrator password in seconds.



This does not apply for SCSI setups, since you can simply change the boot ID or LUN boot and bypass any boot sequence. Adaptec PCI BIOS are not password protected, but recent PC BIOS versions give you the extra choice to boot from a "SCSI DEVICE", overriding SCSI controller settings.

The seal/chassis intrusion protector

Protect the hardware with a seal and/or chassis intrusion protection hardware. Otherwise, it would take only a few minutes to obtain a local administrator access using an external boot device that accesses the local (not-booted) hard disk. In a similar way, you should also protect your hubs/switches and restrict access to the server rooms.

Password protect the BIOS

Although this is important, it may still be useless without chassis intrusion security, since someone just needs to locate the CMOS reset jumper. You can use full hard disk encryption to defy this threat if you cannot ensure reasonable physical security for your systems.



Some workstations have an intrusion trigger which stores in the BIOS (and displays) when the machine cover has been removed.



Administrative rights

Local users should *NEVER* be members of the local group called *Administrators*. Sanctuary uses Windows Security (Classical Windows authentication, of which NTFS forms part). If a user is the administrator of his own computer, then he has complete, unrestricted access to this computer. There are so many ways to uninstall, disable, or change the configuration of programs and services (and time settings) when you are a local administrator that it would not make sense to add more protection using Sanctuary. For example, one could delete files, registry keys, uninstall the product, delete the driver entries, and use the recovery console... In addition to this, viruses will execute if you have an administrator account unless you are using the other component of our suite (Sanctuary Server Edition, Sanctuary Custom Edition, and Sanctuary Terminal Service Edition).

Consequently, it is not a good practice to grant the users administrative rights to their computers. It is impossible to control/manage a desktop when the user has local administrative rights (thus higher TCO). Nevertheless, some special programs require administrative rights to run properly. You can easily find tools that allow users to run programs with administrative rights while they are not administrators of their workstations. 'RunAs Professional' is one of them.

Power Users

Users who are members of the built-in 'Power Users' group are a special case which requires careful consideration. Power Users have varying permissions and privileges on their local machines – depending on the operating system version –: install and run applications, change permissions, customize settings, modify and create accounts, etc. This may give them an unwanted direct or indirect ability to bypass or tamper with the system policies. Non-trusted users should never be members of the Power Users group, unless you secure the execution environment.

Access Policy

In general, you should have an access policy as restrictive as possible (using NTFS permissions). By default, you should deny all access and then, give access only when/if necessary.

NTFS Partition

NTFS (New Technology File System) is an update of the FAT32 (File Allocation Table), FAT12 (initial version of FAT), FAT16, and VFAT systems which, in turn, are also updates from the old MS-DOS FAT system. NTFS offers several enhancements and advantages over the older systems. Among them, we can quote a superior architecture, support for larger files, enhanced reliability, automatic encryption



and decryption, disk quota tracking and limiting, change journals, disk defragmenter, sparse file support, and – most important to us – improved security and permissions when managing files.

Of course, this list is not all-inclusive; there are other important features, but the main point here is to make you aware of the advantages of using this file partition system.

Recovery Console

The Recovery Console, which is part of the Windows DVD/CD-ROM or MSDN, allows the user to disable any driver related to Sanctuary. However, this requires the local administrator password. This is one of the reasons why you should always change the boot sequence as described in 'The boot sequence' paragraph above. If you fail to do this, then you allow a user to boot on other operating system boot disks. He could, for example, boot from the CD with a Linux OS and manipulate the NTFS partitions.

Safe mode

Safe mode boot causes no threat to Sanctuary drivers, which continue to run even when you boot in this mode.

Service packs and hot fixes

In general, you should always install the latest service packs and hot fixes for the operating system and the different applications you use.

Firewalls

Traditional perimeter-based security systems, like firewalls, are complementary to the protection brought to you by Sanctuary Software.

Password policies

You should have a strong security policy, in particular regarding the choice of the passwords. You should refuse blank or too short/simple passwords, enforcing long and complex character sequences.



Access policy

In general, you should have an access policy as restrictive as possible (using NTFS, permissions, etc.). By default, deny all access, and then just give access if and when necessary.

Private and Public Key Generation

You should not deploy Sanctuary software in a production environment without a securely generated key pair. Use the keygen.exe tool included on your installation CD to create your own unique private and public key. The private key (sx-private.key) is literally the 'key' to the security offer by Sanctuary solutions and you should take proper care of it.

Sanctuary infrastructure

Below is a diagram of a typical Sanctuary infrastructure. An implementation can have many SecureWave Application Servers and one SecureWave Sanctuary Database connected over a wide area, therefore making SecureWave software very scalable.

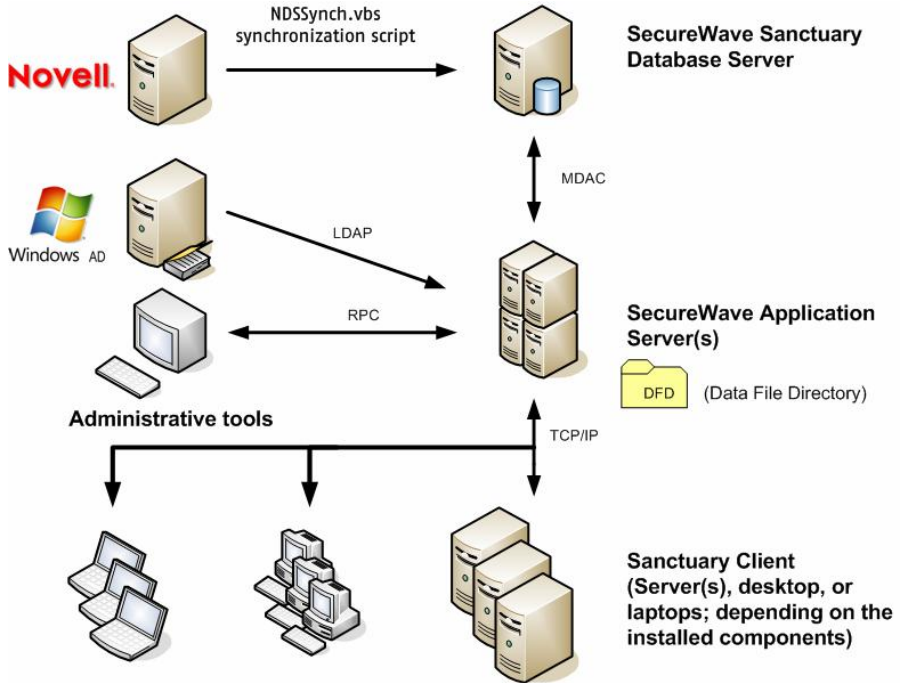


Figure 2: Sanctuary's infrastructure

We do not describe in this guide the installation of Microsoft SQL Server in replication mode.

We assume the following setup during the installation process described in this guide and for the explanation found in *Chapter 7: Testing your Sanctuary Device Control installation* on page 81 and in *Chapter 8: Testing your Sanctuary installation* on page 89:

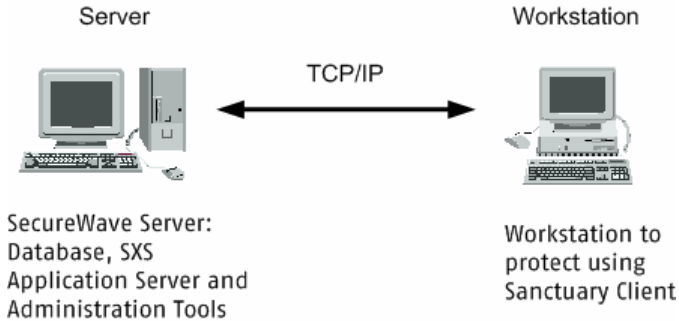


Figure 3: Sanctuary's setup

Installing all server components onto a single computer

This section describes how to install all SecureWave Server components on the same computer. This is the recommended procedure for evaluation purposes. See also *Small, medium, and big networks* on page 15.

The installation of each component is described in detail in *Chapter 2: Installing the Database Components*, *Chapter 3: Installing SecureWave Application Server*, and in *Chapter 4: Installing the Sanctuary Console*.

- ⚡ *Although you can use Windows XP for the database or/and console, you cannot use it for the SecureWave Application Server (or client component in the case of Sanctuary Server Edition). If you are planning to spread Sanctuary components among several machines, one of them in an XP operating system – database and/or management console –, you should read carefully Appendix E: Installing Sanctuary on Windows XP SP2/2003 SP1 on page 155 before proceeding.*
- ⚡ *If you are planning to install several SecureWave Application Servers – each one of them on a different machine, including the Database Server – using Workgroups instead of Domains, there is NO domain administrator account to create a trusted database connection between them. In this case, the connection to your Database Server is done using Windows Authentication instead of SQL Authentication; thus, the communication fails if the Administrator's names and passwords are not the same on each one of these machines. You should always use the same Administrator's name AND password for all SXS and DB servers in this kind of scenario.*



Before you install

You must make sure that the computer meets the minimum requirements before you begin the installation process. See *Appendix B: Detailed System Requirements* on page 141 for more details.

Part 1: Installing the SQL database engine



This part of the setup will install MSDE 2000. You can skip this step if you have already an MSDE 2000 or SQL Server 2000/2005 running on a machine which will be used to host the Sanctuary Database.



You should activate the Server service before trying to install MSDE on your machine. This is especially true for Novell users that do not necessary need this service running on their machines.

If you do not have a SQL server installed in your organization, the first step is evaluating your particular needs. In this phase you should consider if you are going to install the free SQL engine or by the full-blown system. In *Choosing a SQL engine*, on page 33, you will find some basic guidelines to make your decision.

1. Log on to the computer that is going to hold the SQL Database engine. The account you use must have administrative rights.
2. Close all programs running on the computer.
3. Insert the Sanctuary CD in your DVD/CD drive. Execute `RUN.VBS`, found in the `\SERVER\MSDE` folder of the CD. The only dialog of this installation is displayed.



Figure 4: MSDE password setting

4. Enter a password of your choice. This will be used to access the MSDE 2000 engine, and be used by the Microsoft MSDE 2000 SP4 engine setup routine. It will be used for the "sa" account of the MSDE database.



Read the HTML document *Server\MSDE\ReadmeSql2k32desksp4.htm* of the CD for further details about MSDE 2000. The installation will not continue unless you enter a password.

5. After entering a password, click OK to continue.



Make sure that the TCP/IP protocol is enabled for your MSDE database. You can use the 'SvrNetCN.exe' tool that you can find in the 'Microsoft SQL Server' folder under 'Program files' to check/enable/disable protocols.

The 'sx' database installation is described in detail in *Chapter 2: Installing the Database Components* on page 24.

Part 2: Installing the SecureWave Sanctuary Database

The Database component requires a Microsoft SQL Server 7 compatible database server. This can either be SQL Server 2000, SQL Server 2005, or MSDE 2000. If a database server is found, Setup will only add a single database called 'sx'.



If you are updating from a previous version of our software or if you already have another one of our products, you should do a backup of your database ('sx') before proceeding.

1. Log on to the computer where MSDE/SQL Server is running. The account you use must have:
 - > Administrative rights
 - > Access to SQL Server or MSDE
2. Close all programs running on the computer.
3. Insert the Sanctuary CD in your DVD/CD drive. Run the SETUP.EXE file located on the \SERVER\DB folder.
4. Setup.exe will install, if required, MSI version 2.0. When this is complete, the *Welcome* dialog is displayed. Starting with Windows 2000 SP3, the operating system includes a copy of MSI v2.0. Click NEXT to continue.
5. The next dialog displays the License Agreement. Copyright and international treaties protect Sanctuary software.

Read the license agreement carefully and, providing you agree with its



conditions, click **I ACCEPT THE TERMS IN THE LICENSE AGREEMENT**, next click **OK**, and then **NEXT**.

If you do not agree with it, click on the **CANCEL** button to exit without installing your Sanctuary software.

6. Choose the destination folder and click **NEXT**. By default, the application is installed in `C:\PROGRAM FILES\SECUREWAVE\SANCTUARY` folder.
7. Click **INSTALL** to perform the setup. This will take less than 2 minutes, depending on the hardware. The SQL script is run and the database created. Once completed, the final screen appears.
8. Click **FINISH** to close the Installation Wizard.

The SecureWave Database installation is described in detail in *Chapter 2: Installing the Database Components* on page 33.

Part 3: Installing the SecureWave Application Server

The SecureWave Application Server (SXS) handles client logons and is the only component that connects to the database.



SecureWave Application Server (SXS) should not be installed on Windows XP operating systems.

To install the SecureWave Application Server:

1. Log on to the computer that is going to hold the SecureWave Application server component. The account you use must have:
 - > Administrative rights
 - > Access to SQL Server or MSDE
2. Close all programs running on the computer.
3. Insert the Sanctuary CD in your DVD/CD drive. Run the `SETUP.EXE` file located in the `\SERVER\SXS` folder. Setup.exe will install, if required, MSI version 2.0. Once done, the *Welcome* dialog is displayed. Click **NEXT** to continue.
4. The next dialog displays the License Agreement.

Copyright and international treaties protect Sanctuary software. Read the license agreement carefully and, providing you agree with its conditions, click on **I ACCEPT THE TERMS IN THE LICENSE AGREEMENT** button.



If you do not agree with it, click on the CANCEL button to exit without installing your Sanctuary software.




A valid license should already exist on your computer to proceed with the installation process at this step. The program will refuse to install SecureWave Application Server if you do not have a valid license.

5. Choose the destination folder and click NEXT. By default, the application is installed in C:\PROGRAM FILES\SECUREWAVE\SANCTUARY folder. Some components are always installed on the %SystemRoot%\system32 directory and a %SystemRoot%\xsdata directory is always created.
6. The SecureWave Application Server requires a user account to run. Use a domain account (any domain user; an administrative account is not required) if you plan to use your Sanctuary software in a domain environment. Use a local account if you plan to administrate any number of computers in a workgroup.



Figure 5: SecureWave Application Server user account

Domain accounts should be entered as DOMAIN\User while local accounts should be prefixed by the computer name (e.g. COMPUTER\User).

 *If you are planning to install several SecureWave Application Servers – each one of them on a different machine, including the SecureWave Sanctuary Database Server – using Workgroups instead of Domains, there is NO domain administrator account to create a trusted database connection between them. In this case, the connection to your Database Server is done using Windows Authentication instead of SQL Authentication, thus, the communication fails if the Administrator's names and passwords are not the same on each one of these machines. You should always use the same Administrator's name AND password for all SXS and DB servers in this kind of scenario.*

7. You are asked to which SQL Server instance the SecureWave Application Server should connect. Type the machine name, or the virtual server name in case of a cluster server. If the database is not on a default instance, suffix the name with a backslash and the SQL Server instance name where you installed the Sanctuary 'sx' database.



Figure 6: Database server installation



The syntax you should use to enter the name of your database server depends on where you installed your database. Here is a summary of the different cases:

Database server	The database is created in the default instance	The database is created in a Named instance
The database is on the local computer	ServerName / leave the field blank	ServerName\InstanceName
The database is on another server	ServerName	ServerName\InstanceName
The database is on a cluster (local or remote)	VirtualServerName	VirtualServerName\InstanceName

Table 1: Database server name syntax

8. Click NEXT to continue.

You will be prompted for the folder where the SecureWave Application Server log files are to be stored. Setup suggests a directory named DataFileDirectory under the system's drive root. A permanent network share should be used when planning to use more than one SecureWave Application Server, as all servers need to write to the same, shared, directory. On the other hand, for evaluation purposes a local directory is better.






If you are planning to use a shared directory, you should apply the required NTFS and share permissions with full access at least for the account under which the 'SecureWave Application Server' runs.



Figure 7: Data file directory




9. Specify the directory, by clicking CHANGE if necessary, and click NEXT.

-  *Do not use Novell Shares for the DataFileDirectory. Please see Appendix H: Using Novell shares for your DataFileDirectory for more information.*
-  *Always use a UNC (Universal/Uniform Naming Convention) path name, e.g. \\server\volumedirectory. Do NOT use a mapped drive.*
-  *If you are installing Sanctuary Device Control and do not have a Certification Authority installed, you will see a warning message.*

10. You are now asked what kind of protocol the application server should use: the standard one used to communicate with older clients or a new, improved protocol, that can only communicate with clients from v3.1 or later. Deactivate this option if you are installing the server in an environment that has older client driver. If this is a new installation, leave the option activated. This dialog is only displayed if you have a valid Sanctuary suite license (Sanctuary Server Edition, Sanctuary Terminal Service Edition, and Sanctuary Custom Edition).
11. The next screen allows you to import SecureWave File definitions. You should import these files only if you are planning to install and use Sanctuary suite (Sanctuary Server Edition, Sanctuary Custom Edition, and Sanctuary Terminal Services Edition). These files contain the required information needed by the program to authorize running OS files. See *Appendix I: Importing file definitions during setup* on page 179 for more information. This is a time consuming operation, choose only the ones you need. Click on NEXT.
12. Finish the installation. The final dialog indicates that the installation has been successfully completed.

You should have a running server connected to a local database at this stage.

-  *After the installation of the server side components and before rolling out any client in a production environment, it is strongly recommended to generate a key pair to sign the communication between server(s) and clients. Please refer to Chapter 9: Using the Key Pair Generator on page 99 for more information about this topic.*

Chapter 3: Installing SecureWave Application Server on page 41 describes in detail the SecureWave Application Server installation.



Part 4: Installing the Sanctuary Management Console

The Sanctuary Console is the application that you use to manage your Sanctuary suite. You can install it on as many computers as you wish.

Follow these steps to install the Sanctuary Console:

1. Log on to the computer in which you are installing the Sanctuary Console.
2. Close all programs running on the computer.
3. Insert the Sanctuary CD in your DVD/CD drive. Run the `SETUP.EXE` file located in the `\SERVER\SMC\SDC` or `\SERVER\SMC\SAC` folder (depending on the components you are installing). `Setup.exe` installs, if required, MSI version 2.0. The *Welcome* dialog is displayed when this is completed.
4. Click **NEXT** to continue. The next dialog displays the License Agreement.

Copyright and international treaties protect Sanctuary software. Read the license agreement carefully and, providing you agree with its terms, click **I ACCEPT THE TERMS IN THE LICENSE AGREEMENT** to proceed with the setup.

If you do not agree with its conditions, click on the **CANCEL** button to exit without installing your Sanctuary product.





*The license agreement is copied with the program. If you want to review it later, select 'License agreement' from the **START → PROGRAMS → SANCTUARY DEVICE CONTROL** (or the component you are installing) menu.*

5. Leave all settings unchanged and click **NEXT** in the *Custom Setup* screen. The setup will install the Sanctuary Console and the Sanctuary Client Deployment tool. By default, the application is installed in `C:\PROGRAM FILES\SECUREWAVE\SANCTUARY DEVICE CONTROL\` (or the name of your corresponding software) folder.
6. Complete the installation. The final dialog indicates if the installation has been completed successfully. Click **FINISH** to close the dialog and end the procedure.

By default, only users who are members of the *Administrators* group of the computer running the SecureWave Application Server can connect via the Sanctuary Console. You should specify who can manage and define Sanctuary's policies using the *User Access Manager* dialog available from the Sanctuary Console *Tools* menu. Please refer to the *Administrator's Guide* for further information.



 *It is strongly recommended to install the Sanctuary Client on all computers having the Sanctuary Device Control Console. If you do not install the client on the administrator's computer, it is not possible to use media encryption or authorize multi-sessions DVD/CDs with the Media Authorizer. Please refer to Chapter 5: Installing the Sanctuary Client on your guest computers on page 63 for more details.*

 *It is strongly recommended to install the Sanctuary Client on all computers having the Sanctuary Server Edition Console. If you do not install the Sanctuary Client on the administrator's computer, it is not possible to authorize local files. Please refer to Chapter 5: Installing the Sanctuary Client on your guest computers on page 63 for more details.*

Chapter 4: Installing the Sanctuary Console on page 57 describes in detail the Sanctuary Console installation.

Part 5: Installing the Sanctuary Client Driver

The Sanctuary Client is the software used to manage the devices or authorize software execution on the client(s) computer. You can install it individually in each machine to be protected (see *Chapter 5: Installing the Sanctuary Client on your guest computers* on page 63) or – in large organizations, or when you cannot visit each client computer (server) individually – using our unattended client installation software described in *Chapter 10: Unattended Client Installation* on page 103.

Part 6: Testing your installation

The final step of this process is to test your installation before defining your policies and deploying all your clients. Please refer to *Chapter 7: Testing your Sanctuary Device Control installation* on page 81 and *Chapter 8: Testing your Sanctuary installation* on page 89 for further instructions.



Installing Sanctuary in a Workgroup

If, on the other hand, you are installing Sanctuary in a workgroup network instead of a domain, you must perform a manual synchronization using each computer Administrator's account. This is the only way that the SecureWave Application Server can read the Security Identified (SID) of every workstation. You will also need to open the correct firewall ports if using Windows XP with SP2 (or Windows 2003 SP1 if the firewall is enabled) and disable the Simple File Sharing feature (if enabled) on the workstations you wish to synchronize.

Furthermore, if you are planning to install several SecureWave Application Servers – each one of them on a different machine, including the Database Server – using Workgroups instead of Domains, there is NO domain administrator account to create a trusted database connection between them. In this case, the connection to your Database Server is done using Windows Authentication instead of SQL Authentication; thus, the communication fails if the Administrator's names and passwords are not the same on each one of these machines. You should always use the same Administrator's name AND password for all SXS and DB servers in this kind of scenario.



To install on a workgroup, follow the steps outlined on the *Installing all server components onto a single computer* section on page 22.



Chapter 2: Installing the Database Components

The information in this chapter applies to all Sanctuary software suite products.

This chapter explains how to install the SQL Engine and SecureWave Sanctuary Database (sx). While *Chapter 1: Installing Server Side Components* gives you an overview of the entire setup, this section focuses exclusively on the database requirements as well as in additional information not provided in that chapter.

-  *Although you can use Windows XP for the database or/and console, you cannot use it for the SecureWave Application Server (or client component in the case of Sanctuary Server Edition). If you are planning to spread Sanctuary components among several machines, one of them in an XP operating system – database and/or management console –, you should read carefully Appendix E: Installing Sanctuary on Windows XP SP2/2003 SP1 on page 155 before proceeding*
-  *If you are updating from a previous version of our software or if you already have another one of our products, you should do a backup of your database ('sx') before proceeding.*

Choosing a SQL engine

The database used by Sanctuary software requires a Microsoft SQL Server 7 compatible database server. This can be SQL Server 2000, SQL Server 2005, or MSDE 2000.

The database server you choose depends on the size of your implementation and the one you currently use. MSDE is certainly sufficient for installations of up to 200 (Sanctuary Device Control) or 50 (Sanctuary Suite) connected Sanctuary clients. Please note that there are inherent limits when using MSDE:

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



MSDE may be an attractive option for those sites that do not already use SQL Server. Because it is available free of charge, it eliminates the expense of purchasing the SQL Server.

We recommend using a full-blown SQL Server at larger, small, and medium size sites if it is already installed.

SQL Server is always mandatory for sites serving 200 or more connected Sanctuary clients. See our online knowledgebase at <http://www.SecureWave.com> for more details on MSDE vs SQL Server limitations.

If you begin using MSDE, you can migrate to SQL Server at a later date, should this be necessary.

Sanctuary setup includes MSDE 2000 SP4.



We strongly recommend downloading and applying the latest SQL Server / MSDE service packs from www.microsoft.com before putting the system in production. Be aware that the service pack for Microsoft SQL Server cannot be applied to a MSDE database; MSDE requires specific service packs. Make sure you download the appropriate file. The MSDE version present on the Sanctuary Suite CD is MSDE 2000 SP4 English US.

Before you install

Before you begin installing the required Database, you must make sure that the computer meets the minimum requirements. See *Appendix B: Detailed System Requirements* on page 141 for details.

Part 1: Install the SQL database engine



This part of the setup will install MSDE 2000. You can skip this step if you already have MSDE 2000 or SQL Server 2000/2005 running on a machine that will be used to host the Sanctuary Device Control database.

1. Log on to the computer that is going to hold the SQL Database engine. You must use an account with administrative rights.
2. Close all programs running on the computer.




3. Insert the Sanctuary CD in your DVD/CD drive. Run the `RUN.VBS` file located on the `\SERVER\MSDE` folder on the installation CD. The only dialog for this installation is displayed.



Figure 8: SA Account password

4. Enter a password of your choice. This is required to access the MSDE 2000 engine and is required by the Microsoft MSDE 2000 SP4 engine setup routine. It is used for the "sa" account of the MSDE database. Read the HTML document `Server\MSDE\ReadmeSql2k32desksp4.htm` for further details about MSDE 2000. The installation will not continue unless you enter a password.
5. After entering a password, click OK to continue the installation.

The MSDE installation will finish without further user interaction or notification.

 *If you already have MSDE installed, you will see the following error message:*

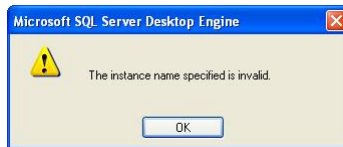




Figure 9: Error message when MSDE is already installed

 *Make sure that the TCP/IP protocol is enabled for your MSDE database. You can use the 'SvrNetCN.exe' tool that you can find in the 'Microsoft SQL Server' folder under 'Program files' to check/enable/disable protocols.*

 *You should activate the Server service before trying to install MSDE on your machine. This is especially true for Novell users that do not necessary need this service running on their machines*



Part 2: Install the SecureWave Sanctuary Database

The Database component requires a Microsoft SQL Server 7 compatible database server. This can be SQL Server 2000, SQL Server 2005, or MSDE 2000. If a database server is found, setup will add a single database called 'sx'.

1. Log on to the computer where MSDE/SQL Server is running. The account you use must have:
 - > Administrative rights
 - > Access to SQL Server or MSDE
2. Close all programs running on the computer.
3. Insert the Sanctuary CD in your DVD/CD drive. Run the SETUP.EXE file located on the \SERVER\DB folder.
4. Setup.exe will install, if required, MSI version 2.0. When this is complete, the *Welcome* dialog is displayed.



Figure 10: SecureWave Sanctuary Database installation: first step

5. Click NEXT to continue.



The setup will not install automatically MSI 2.0 nor will generate a log file if it is launched running the db.msi file instead of the setup.exe file. The log file may be important in case of troubleshooting and when contacting SecureWave Support.



The next dialog displays the License Agreement.

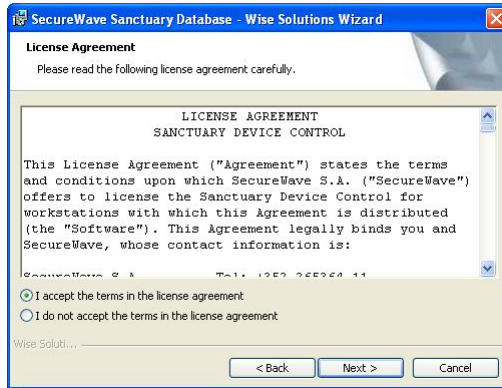


Figure 11: SecureWave Sanctuary Database installation: license agreement

Copyright and international treaties protect Sanctuary software.

6. Please read the license agreement carefully and, providing you agree with its conditions, click the **I ACCEPT THE TERMS IN THE LICENSE AGREEMENT** button to continue the installation process. The next dialog is displayed.

If you do not agree with it, click on the **CANCEL** button to exit without installing your SecureWave Sanctuary Database.

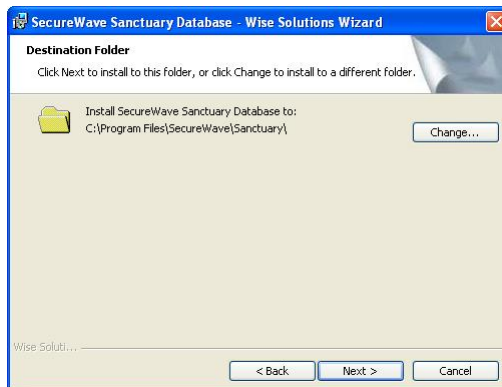


Figure 12: SecureWave Sanctuary Database installation: destination folder



7. Choose the destination folder (clicking **CHANGE**, if necessary) and then click **NEXT**. By default, the application will be installed in the `C:\PROGRAM FILES\SECUREWAVE\SANCTUARY` folder.
8. If you have several instances of the database installed, you are asked to select one:

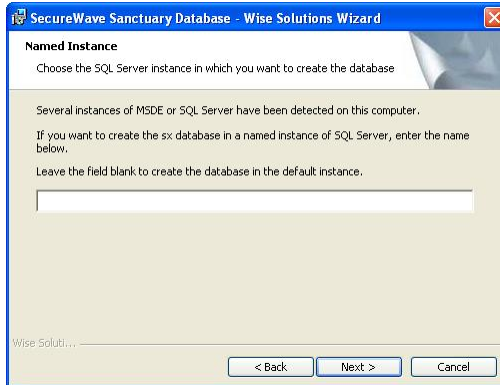


Figure 13: SecureWave Sanctuary Database installation: select SQL instance

9. Setup is ready to start the installation:

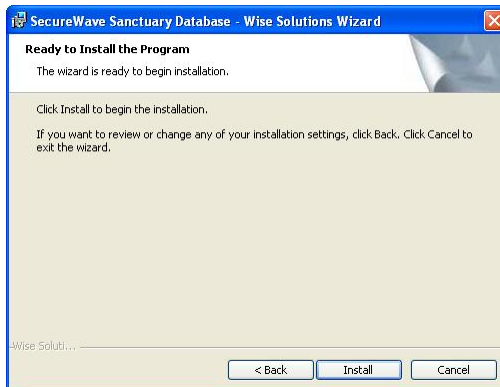


Figure 14: SecureWave Sanctuary Database installation: final step

Click on the **INSTALL** button to perform the setup. This will take less than 2 minutes, depending on the hardware.



10. The SQL scripts are run and the database created. Once completed, the final screen is displayed:

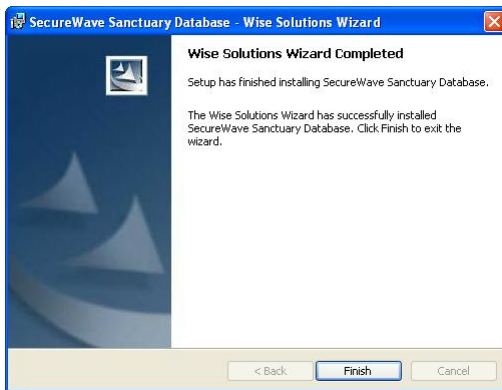


Figure 15: SecureWave Sanctuary Database installation: ending the installation wizard

11. Click on the **FINISH** button to close the wizard.




Chapter 3: Installing SecureWave Application Server

The information in this chapter applies to all Sanctuary software suite products.

This chapter explains how to install the SecureWave Application Server on the computers that are going to be servers for the application. While *Chapter 1: Installing Server Side Components* gives you an overview of the entire setup process, this section focuses exclusively on the *SecureWave Application Server*, providing you with additional information not available in that chapter.

When installing the SecureWave Application Server some other tools are also copied to your hard disk. The installed tools are:

- > The SXS Sanctuary Application Server
- > The Key Pair Generator
- > The SXDomain Tool

 *Although you can use Windows XP for the database or/and console, you cannot use it for the Application Server (or client component in the case of Sanctuary Server Edition). If you are planning to spread Sanctuary components among several machines, one of them in an XP operating system – database and/or management console –, you should read carefully Appendix E: Installing Sanctuary on Windows XP SP2/2003 SP1 on page 155 before proceeding.*

Before you install

Before you begin installing SecureWave Application Server:

- > Make sure that the computer meets the minimum requirements (see *Appendix B: Detailed System Requirements* on page 141 for details)
- > You must have already installed the database on the computer that is to hold your information (see *Chapter 2: Installing the Database Components* on page 33 for details)
- > Make sure that Microsoft Data Access Components (MDAC), version 2.6 SP1 or later, is installed



If the server setup cannot find the MDAC component on your computer, it will prompt you to download it from Microsoft web site <http://www.microsoft.com/data/>. You must restart the setup after the MDAC installation.

MDAC enables computers to connect to SQL Server and SQL Desktop Engine (MSDE) databases. As MDAC is language-dependent, it is mandatory that you install the correct language version for your operating system.



If you experience database connectivity problems when installing the SecureWave Application Server, you should re-install MDAC on the computer hosting the SecureWave Application Server.

- > Ensure the TCP/IP protocol is installed. TCP/IP is required so that the Sanctuary Client Drivers running on the client computers can communicate with the SecureWave Application Server. The Setup program does not check this prerequisite.
- > Make sure that the computer onto which SecureWave Application Server is installed has a fixed IP address. This is recommended as the Sanctuary Client Driver uses this address to connect to the SecureWave Application Server. You need at least one valid IP address. DHCP (Dynamic Host Configuration Protocol) and server names can be used, provided that the DNS (Domain Name Resolution) is set up correctly.
- > The SXS server(s) must be able to do a fully qualified domain name resolution of the clients it is going to manage – you have to setup the mechanism to translate the clients' names into an IP address.
- > Create or use an existing account to be used by the SecureWave Application Server service¹. Setup will automatically grant this account the privilege to log on as a service².



The service account must have the relevant permissions to read domain information, if any, from the Windows SAM (Security Account Management) database. One solution is to make the SXS service account a member of the Domain Users group.

¹ We will refer to this account as the Service Account

² User right: *Act as part of the operating system.*



If you are installing the program on a computer that is a member of a workgroup (wired to other computers but not member of a domain) you may need to use an account with Administrative privileges to connect to the database. Using a non-privileged account requires that the Setup process adds Access Control Entries (ACEs) for the user and to several directories as well as granting the account the rights to connect and use the database.

- > Make sure that the SecureWave Application Server service account has the right to access the database. If the database and SecureWave Application Server are installed on the same computer, there will be no need to create such access, as it will be granted by our Setup. However, when the database and SecureWave Application Server run on two different computers, you must grant the service account the rights to connect and use the database. You can use the Microsoft SQL Server Enterprise Manager to grant domain users the right to log in and use the database (available with SQL Server only). If running MSDE, you will have to use the GRANTDB.EXE command line application for every service account you will use. The grantdb.exe file can be found in the \BINTOOLS folder of your SecureWave CD.



SecureWave Application Server uses Windows Authentication mode to connect to the database. Start the "Enterprise Manager" provided with SQL Server, select your database server, expand this branch of the tree, and check the "Security" node. This section holds the Login definitions. By default, BUILTIN\Administrators have access. During Setup, the account under which the Application Server runs is granted access to the database (if the database and the application server are on the same machine). If the database and the application server are not on the same machine, then you have to use grantdb.exe to allow that account access to the database.

- > Get a license for your Sanctuary product. The license information is stored in a file called *SecureWave.lic*. The file is required to install SXS and without it, the installation will fail. The file contains details of the licenses you have purchased, for example the number of server and client copies. If you have purchased one of our Sanctuary suite products, this file is sent to you by email. If you are evaluating the products, then you can obtain an evaluation license by registering on the SecureWave website www.SecureWave.com. From there, select the corresponding product page, and then select Evaluation Request. Fill out the Evaluation License Request form. Once you have a copy of the license file, save it into the %SYSTEMROOT%\SYSTEM32 directory.
- > It is recommended that the computer(s) running SecureWave Application Server also has a system clock synchronization mechanism to match that of the



computer running the database. You can use Windows Time Service (W32Time, based on Simple Network Time Protocol or SNTP) to maintain date and time synchronization for computers running Windows 2000 or later.

The installation procedure

The SecureWave Application Server handles client logons and is the only component that connects to the database.

1. Log on to the computer that is going to hold the SecureWave Application server component. The account you use must have:
 - > Administrative rights
 - > Access to SQL Server or MSDE
2. Close all programs running on the computer.
3. Insert the Sanctuary CD in your DVD/CD drive. Run the SETUP.EXE file located on the \SERVER\setup folder.

Setup.exe will install, if required, MSI version 2.0. When this is done, the *Welcome* dialog is displayed.



Figure 16: SecureWave Application Server installation: first step

4. Click on the NEXT button to continue.



The Setup will not automatically install MSI 2.0 nor will it generate a log file if it is launched running the db.msi file instead of the setup.exe file. The log file may be important in case of troubleshooting and when contacting SecureWave Support.

The next dialog displays the License Agreement.



Figure 17: SecureWave Application Server installation: license agreement

Copyright and international treaties protect Sanctuary software.

Please read the license agreement carefully and, providing you agree with its conditions, click the **I ACCEPT THE TERMS IN THE LICENSE AGREEMENT** to continue the Setup process. The next dialog is displayed.

If you do not agree with it, click on the **CANCEL** button to exit without installing your Sanctuary product.

5. In the next step, the presence of a valid license file is checked. If the setup program cannot find one, an error message is displayed. If you, have a license file and see this message, verify the name (securewave.lic) and then copy it to the %SYSTEMROOT%\SYSTEM32 folder.



Figure 18: SecureWave Application Server installation: no license found

If the license file was altered in any way (e.g. due to an email filter introducing linefeed characters or translating foreign characters) the following error message is displayed:

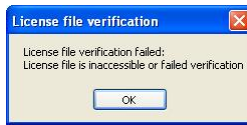


Figure 19: SecureWave Application Server installation: invalid license

In this case, verify your email client settings or contact SecureWave's technical support team to obtain a new license file.



The program will refuse to install SecureWave Application Server if you do not have a valid license.

If the server is being installed on a Windows 2003 SP1, Setup will have to adapt Windows settings to allow RPC communication between the Sanctuary Console and the SecureWave Application Server. Please refer to *Appendix E: Installing Sanctuary on Windows XP SP2/2003 SP1* on page 155.

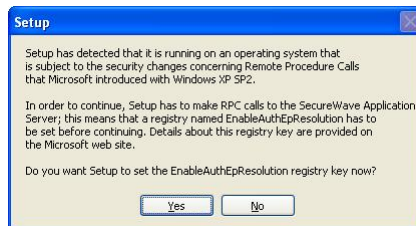


Figure 20: SecureWave Application Server installation: Remote Procedure Calls warning

6. In the next dialog choose the destination folder (clicking CHANGE, if necessary) and then click NEXT. By default, the application will be installed in C:\PROGRAM FILES\SECUREWAVE\SANCTUARY folder. Some components



are always installed on the %SystemRoot%\system32 directory and a %SystemRoot%\xsdata directory is always created.

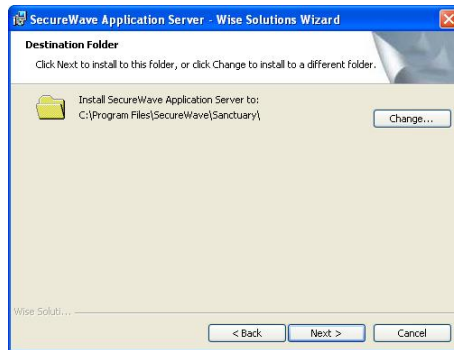


Figure 21: SecureWave Application Server installation: destination folder

7. The SecureWave Application Server requires a user account to run. Use a domain account (any domain user; an administrative account is not required) if you plan to use Sanctuary in a domain environment. Use a local account if you plan to manage several computers in a workgroup.



Figure 22: SecureWave Application Server installation: service account

Domain accounts should be entered as DOMAIN\User while local accounts should be prefixed by the computer name (e.g. COMPUTER\User).



Setup will verify the validity of the password. You must precede the user name with the domain or workstation name and a backslash (\). The account you enter must have full access to the database and the computer containing the DataFileDirectory where the SecureWave Application Server log files are stored.



Before attempting to connect to the remote server, you must grant the service account the right to connect and use the database. You must, therefore, log on to the computer where the SQL Server or MSDE server is running and grant the user the necessary rights either by means of the SQL Server Enterprise Manager or using the grantdb.exe utility located in the \BIN\TOOLS folder of the SecureWave CD. Local users should be mirrored (same user name and password on both servers).

8. SecureWave Application Server needs to know to which SQL Server instance it should connect. Type the name of the machine or the virtual server name in case of a cluster server. If the database does not reside on a default instance, you should suffix the name with a backslash and the SQL Server instance name where you installed the Sanctuary Device Control 'sx' database.



Figure 23: SecureWave Application Server installation: database server



9. Click on the NEXT button to continue.

The syntax used to enter the name of your database server depends on where you installed the database. Here is a summary of the different cases:

Database server	The database is created in the default instance	The database is created in a Named instance
The database is on the local computer	ServerName / leave the field blank	ServerName\InstanceName
The database is on another server	ServerName	ServerName\InstanceName
The database is on a cluster (local or remote)	VirtualServerName	VirtualServerName\InstanceName

Table 2: Database server name syntax

10. You are next prompted for the folder where the *SecureWave Application Server* log, shadow, or/and scan files are to be stored. Setup will suggest a directory named DataFileDirectory under the system's drive root. A permanent network share is to be used when planning to have more than one *SecureWave Application Server*. All servers need to write to the same, shared, directory. For evaluation purposes, use a local directory.



Figure 24 : SecureWave Application Server installation: data file directory



You should pay special attention to the network share security (ACL) and Directory NTFS permissions. Limit access to the server service account and optionally to some administrators. You will also need to consider those members of the 'Power Users' group.

- If you wish to change the directory location or if you are installing more than one *Application Server*, select a shared network folder by clicking on the CHANGE button. Locate the path you wish to use for the DataFileDirectory:

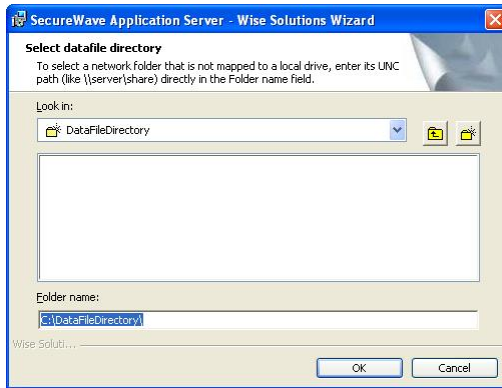


Figure 25: SecureWave Application Server installation: change destination folder



Always use a UNC (Universal/Uniform Naming Convention) path name, e.g. \\server\volume\directory. Do NOT use a mapped drive.

You receive the following warning if you set the log files folder on a local drive:



Figure 26: SecureWave Application Server installation: warning message when setting the log files folder to a local drive

If you are installing Sanctuary Device Control and do not have a Certification Authority installed, you will see a warning message:



Figure 27: SecureWave Application Server installation: no Certification Authority found

12. You are now asked what kind of protocol the application server should use: the standard one used to communicate with older clients or a new, improved protocol, that can only communicate with clients from v3.1 or later. Deactivate this option if you are installing the server in an environment that has older client driver. If this is a new installation, leave the option activated.



Figure 28: SecureWave Application Server installation: protocol selection dialog

13. The setup program then offers you the option to import SecureWave File Definitions (SFD files). You should import these files only if you are planning to install and use Sanctuary suite (*Sanctuary Server Edition*, *Sanctuary Custom Edition*, and *Sanctuary Terminal Services Edition*). These files contain the required information needed by the program to authorize running OS files. See *Appendix I: Importing file definitions during setup* on page 179 for more information. Choose only the ones you need and click on NEXT.



Figure 29: SecureWave Application Server installation: import SecureWave File Definitions

Setup is now ready to install the Application Server Component.

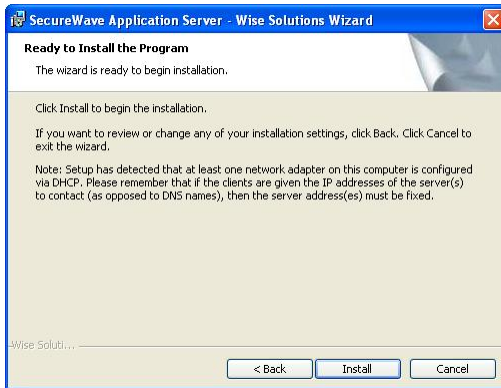


Figure 30: SecureWave Application Server installation: final stage

14. Click on the **INSTALL** button to proceed. You can see a warning message if you do not use a fixed IP address.
15. Setup then gathers information about the domain structure. It retrieves the names of the domain users and groups from the domain controller. This may take several minutes (up to half an hour), depending on the size of the domain and connection speed. The following dialog is displayed:

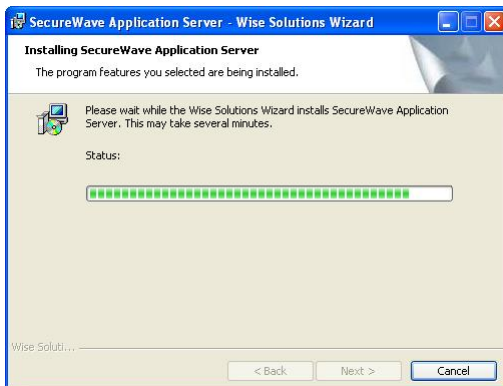


Figure 31: SecureWave Application Server installation: installation

The final dialog indicates that the installation has been successfully completed.



Figure 32: SecureWave Application Server installation: finishing the installation

16. Click on the FINISH button to close the wizard.

You should have a running server connected to a database at this stage.



After installing the server side components, and before rolling out any client in a working environment, we strongly recommend to generate a key pair to sign the communication between server(s) and clients. Please refer to Chapter 9: Using the Key Pair Generator on page 99 for more information about this topic.



Upgrading from a previous SecureWave Application Server version

If you are upgrading the SecureWave Application Server instead of making a "clean" installation, the dialogs and steps change from those found in the first section of this chapter as depicted in the following steps.

1. Log on to the computer where the SecureWave Application Server component is installed.
2. Close all programs running on the computer and stop the SXS service (`c>Net Stop SXS`).
3. Insert the Sanctuary CD in your DVD/CD drive. Run the `SETUP.EXE` file located on the `\SERVER\sxs` folder.

The *Welcome* dialog is displayed informing you that a previous version of the server is already installed and there will be an upgrade.



Figure 33: SecureWave Application Server upgrade: first step

4. Click on the `NEXT` button to continue. You are now asked what kind of protocol the application server should use: the standard one used to communicate with older clients or a new, improved protocol, that can only communicate with clients from v3.1 or later. Deactivate this option if you are installing the server in an environment that has older clients. If you are also upgrading ALL your clients to this new version, leave the option activated.



Figure 34: SecureWave Application Server upgrade: protocol selection dialog

5. The setup program has now all the necessary elements to begin the upgrade process.



Figure 35: SecureWave Application Server upgrade: protocol selection dialog

Click on the Upgrade button to begin the process.


The program verifies you license and RPC protocol (as described in *step 5* of the previous section; page 45)



Chapter 4: Installing the Sanctuary Console

The information in this chapter applies to all Sanctuary software suite products.

This chapter explains how to install the *Sanctuary Console* used to configure permissions to all the devices and/or executables of your organization, and carry out day-to-day administrative tasks and procedures.

 *You should read carefully the Appendix E: Installing Sanctuary on Windows XP SP2/2003 SP1 on page 155 before installing this component on a computer with this operating system and service pack.*

When installing the console you also install:


- > The *Client Deployment Tool* (see *Chapter 10: Unattended Client Installation* on page 103) to deploy client silently

If you are installing Sanctuary Console:

- > The *Svolbro.exe* program (described on *Chapter 7* of the *Administrator's Guide*) needed for one of our USB key encryption methods

If you are installing Sanctuary Server Edition or Sanctuary Custom Edition:

- > The *Authorization Wizard* (described on *Chapter 5* of the *Administrator's Guide*) to search executable files, create their hashes, and include them in the database
- > The *Versatile File Processor Tool* (described on *Chapter 14* of the *Administrator's Guide*) to scan files
- > The *Sanctuary Authorization Service* (described on *Chapter 14* of the *Administrator's Guide*) to monitor changes and create updates (using Microsoft's SUS or WSUS)

 *The actual screenshots presented in this chapter may differ slightly, depending on the component you are installing, from the ones you actually see throughout the installation process. This is only true for the screen titles. For example, Sanctuary Application Console instead of Sanctuary Device Console.*



Before you install

Before you begin the installation of the Sanctuary Console, you must:

- > Ensure that the computer(s) meet the minimum requirements. See *Appendix B: Detailed System Requirements and Limitations* on page 141 for details.
- > Ensure that the *SecureWave Sanctuary Database* and *SecureWave Application Server* have been installed, either on this computer or on other computers within your network. Refer to the previous chapters.

The installation procedure

To install the *Sanctuary Console*, follow these steps:

1. Log on with an account that has administrative privileges in the computer in which you are installing the Sanctuary Console.
2. Close all programs running on the computer.
3. Insert the *Sanctuary CD* in your DVD/CD drive. Run the SETUP.EXE file located on the \\SERVER\SMC\SDC or \\SERVER\SMC\SAC (depending on the component you are installing) folder.



Figure 36: Sanctuary Console installation: first step

4. The next dialog displays the License Agreement.



Figure 37: Sanctuary Console installation: license agreement

Copyright and international treaties protect Sanctuary software.

5. Please read the license agreement carefully and, providing you agree with its stipulations, click I ACCEPT THE TERMS IN THE LICENSE AGREEMENT to continue the setup process.

If you do not agree with it, click on the CANCEL button to exit without installing your Sanctuary product.



The license agreement text is installed with the program. If you want to review it later, select 'License agreement' from the START → PROGRAMS → SANCTUARY DEVICE CONTROL (or the corresponding program installed) menu.

You are then given the choice of changing the destination directory, and other features – making a complete or custom installation.



Figure 38: Sanctuary Console installation: custom setup

The Sanctuary Console allows you to configure, manage, and monitor permissions to devices/executables. You use the Sanctuary Client Deployment tool to deploy silently clients on a group of computers. Select the features you want.

6. If you decide to modify the default installation location, click on the CHANGE button and select a local path to install the components and documentation. By default, the files are copied to the %PROGRAMFILES%\SECUREWAVE\SANCTUARY DEVICE CONTROL\ or %PROGRAMFILES%\SECUREWAVE\SANCTUARY APPLICATION CONTROL\ directory – depending on the installed components.

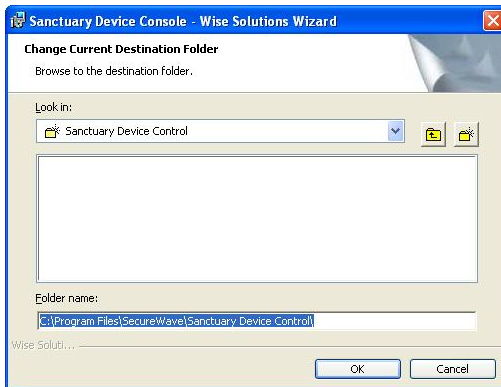


Figure 39: Sanctuary Console installation: modify destination folder



If you click **CHANGE**, select a local path to install the components and documentation, and click **OK** to continue the installation.

7. Now Setup is ready to install the files.

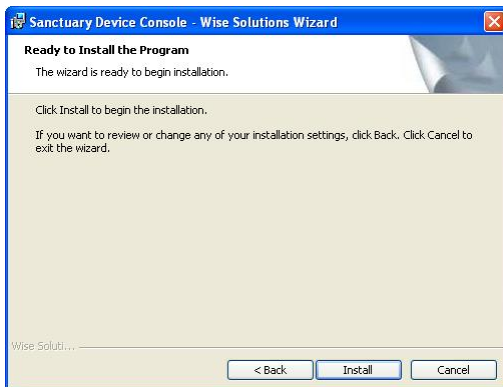


Figure 40: Sanctuary Console installation: ready to install

8. Click on the **INSTALL** button to start the process. The whole operation will take about 2 minutes depending on the components selected and the hardware used.
9. If the computer is running Windows XP SP2 or Windows 2003 SP1, Setup will have to adapt Windows settings to allow RPC communication between the Sanctuary Console and the SecureWave Application Server. Please refer to *Appendix E: Installing Sanctuary on Windows XP SP2/2003 SP1* on page 155.

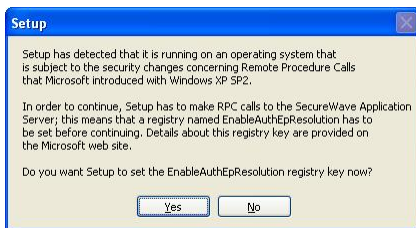


Figure 41: Sanctuary Console installation: Remote Procedure Calls warning

10. Click on **Yes** to continue.



The final dialog indicates that the installation has been completed successfully.

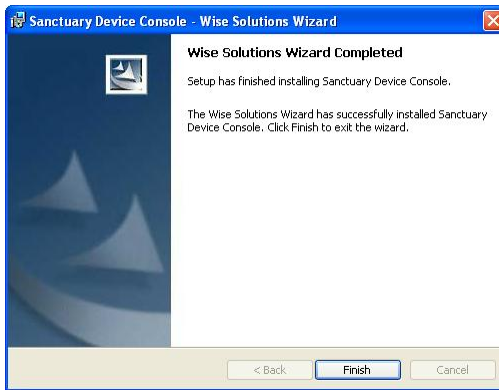


Figure 42: Sanctuary Console installation: finishing the installation

11. Click on the FINISH button to close the dialog and end the procedure.

By default, only users that are members of the Administrators group of the computer running the SecureWave Application Server can connect via the Sanctuary Console. You should define who can manage and define policies by selecting *User Access* from the *Tools* menu of the Sanctuary Console. Please refer to the *Administrator's Guide* for further information.



If you are installing Sanctuary Device Control, it is strongly recommended that you also install the Sanctuary Client on all computers having the Sanctuary Console. If you do not install it on the administrator's computer, it will not be possible to use media encryption or to authorize multi-sessions DVDs/CDs with the Media Authorizer. Please refer to Chapter 5: Installing the Sanctuary Client on your guest computers on page 63 for more details.



Chapter 5: Installing the Sanctuary Client on your guest computers

The Sanctuary Client is the software used to manage the devices/applications on the client computer/servers. This chapter explains how to install it on the client computers you want to manage when you only have a few computers in your system or for testing purposes. To deploy our client in large organizations, or when you cannot visit each computer individually, we recommend using our specialized software tool, described in *Chapter 10: Unattended Client Installation*.



You should carefully read Appendix E: Installing Sanctuary on Windows XP SP2/2003 SP1 on page 155 before installing this component on computers that use this operating system and service pack. Although you can use Windows XP for the database and console, you cannot install Sanctuary Server Edition's client on it. We do not support Windows XP or Windows 2000 Pro for Sanctuary Server Edition (client component).

System requirements

System requirements can be divided into what is needed for the overall system and what is needed for each client computer.

Requirements for the overall system

Before you install the Sanctuary Client on a client computer, you must:

- > Ensure that the SecureWave Sanctuary Database, SecureWave Application Server, and Sanctuary Console are already installed on their respective computers.
- > Make sure that the domain information stored in the database is up to date. If necessary, update it using the *Tools* → *Synchronize Domain Members* menu in the Sanctuary Console.
- > Define the appropriate, or at least minimum, policies that are to be used by the clients. Failing to do so WILL result in users being denied access to their executable files (event the operating system, blocking the user from his machine) and/or devices connected to their computers. If you are using Sanctuary Server Edition or Sanctuary Custom Edition, verify, in particular – in



the *Default Options* dialog of the console – that the *Blocking Mode* option is set to *Non Blocking Mode*.

Requirements for the client computer

Make sure that the computer meets the minimum hardware and software requirements. See *Appendix B: Detailed System Requirements* on page 141 for details.



If the target computers have been installed using prepared hard-drive images (for example using Symantec Ghost, Powerquest Driveimage, etc.) please make sure that every machine has received a different SID (Security Identifiers) and name before starting the deployment. You can use GhostWalker.exe, SidChanger.exe, etc., to do this.

Please refer to the Administrator's Guide for a detailed procedure on how to include the Sanctuary Client driver in a prepared hard-drive image.



Although the installation dialog only lets you input three SXS servers, you can easily add more if needed. You can also change how the SXS server(s) is selected – round-robin vs. random pick. All this is done by modifying certain options in the console or registry keys. Please see Sanctuary Client registry keys on page 148 and Load balancing methods on page 72 for more details. You can “push” these modifications to all clients using Group Policies with ADM templates.

The installation procedure

The first step in this procedure is to decide whether you want or not to import the company's permissions and policies as an independent file during the installation process. If you do want to import them during the client installation, you first need to export them. This export is done to a special file called *policies.dat* that should be located in the same directory as the MSI installation file package. The files needed to install the client are located in the client folder of your installation CD. You can copy them to a convenient location on your hard disk. Proceed with the installation steps as described below reading carefully step 6: Providing the SecureWave Application Server address.

Please consult the *To export and import permission settings* section of the *Administrator's Guide* for more information on how to export your settings to a file.



This 'import file' is particularly useful when doing client installations on machines that are not actually connected to the network or that cannot communicate with the SecureWave Application Server.

To install the Sanctuary Client on your client computers, follow these steps on each client computer:

1. Log on to the client computer with administrative rights.
2. Close all programs running on the computer.
3. Select the CLIENT folder on the Sanctuary CD or navigate to the network shared drive where the Sanctuary Client setup files are located. Run the SETUP.EXE file. The Setup program launches the MSI installer and you can see the *Welcome* dialog:

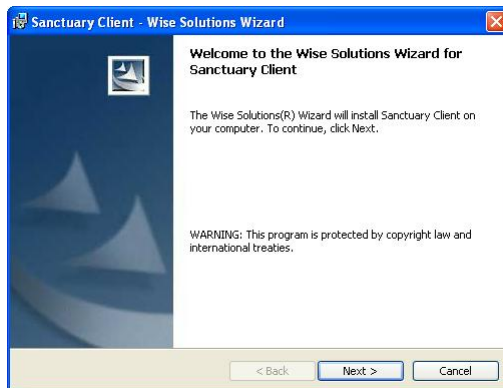


Figure 43: Sanctuary Client: first step

Click on the NEXT button to continue.

4. The next dialog displays the *License Agreement*. Copyright and international treaties protect Sanctuary software.



Click on the TEST button to check that the Sanctuary Client can establish a connection with the SecureWave Application Server(s) listed. A test is considered successful if the computer is online, a SecureWave Application Server could be contacted, and the key pair match is correct.

There are two different cases:

- You specify a correct address for the Sanctuary Application Server. This address is validated and, if correct, the setup continues. All permissions for the client are retrieved from the server(s) specified in this dialog.
- You specify a momentary unavailable address, invalid address, or no address at all. The setup continues after warning you. You can use this mode to deploy the client on machines that are not currently connected to the Sanctuary Application Server, but you want or need to apply predefined permissions (devices and/or executables) that should be immediately activated after the setup ends. In this latter case, you also need to generate the *policies.dat* file. If this file is not available, the default built-in restrictive settings are applied.

SXS address	Import file (Policies.dat)	Resulting action
Valid and reachable	Not present	The settings are taken from the server
Valid and reachable	Present	The settings are taken from the server
Valid but not reachable; no address provided; invalid address	Not present	The settings are the predefined ones (most restrictive – see notes and warning below) until a server can be contacted and the permissions updated
Valid but not reachable; no address provided; invalid address	Present	The settings are taken from the file until a server can be contacted and the permissions updated

Table 3: Server address and import file relationship

By default, the driver will randomly choose an available server to work with. This setting allows the load to be shared between the available SecureWave Application Servers. If a server is unavailable, the driver will pick up another one from the list and try to connect to it.



You can also choose to contact the servers sequentially in the order you enter them. This setting is particularly adapted to configurations that have a primary SecureWave Application Server and a backup one. The driver will connect preferably to the primary SecureWave Application Servers, that is, the first one on the list. In the case where it is not available, the driver will try to connect to the next one on the list.



If you are installing Sanctuary Device Control and there is no SecureWave Application Server to contact or exported policies, the most restrictive policies apply, the client shows no permissions at all even when some devices have predefined restricted permissions – for example, read/write permissions for the PS/2 port. See Chapter 3 of the Administrator's Guide for a list of the predefined permissions when first installing the program).



If there is no SecureWave Application Server to contact or exported policies and you are installing Sanctuary Server Edition or Sanctuary Custom Edition, the default built-in restrictive settings are applied and the user would NOT be able to log or run applications. Only Administrators can log on and run all programs except those installed by the user.

7. Choose between spreading the load through all selected servers (random load balancing occurs) or selecting them in the order provided in the fields by activating/deactivating the *Select a server at random to spread the load* option.
8. Click on the NEXT button to proceed. The server address is verified but you can still continue if it is invalid or unspecified:

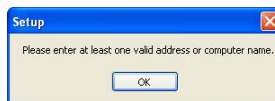


Figure 46: Sanctuary Client: no address specified



Figure 47: Sanctuary Client: no valid address specified or cannot contact server



Figure 48: Sanctuary Client: test failed

9. In the next step you are prompted for the target directory. You normally will accept the proposed one. Click on the NEXT button to continue.

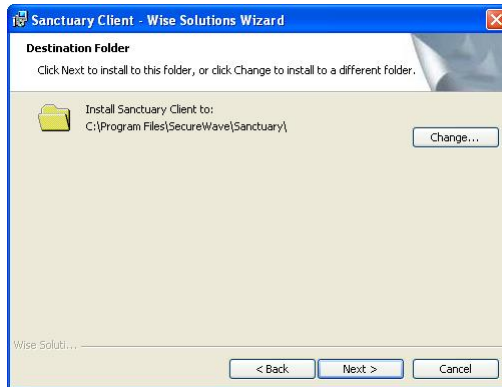


Figure 49: Sanctuary Client: change the target directory

10. You can now select the way the uninstall process is controlled:



Figure 50: Sanctuary Client: how will the program appear on the Windows' Add Remove Program dialog



Select the first option so that the program is not listed on Windows' *Add Remove Programs* dialog. Select the second one to show the program but not a REMOVE button.

11. On the next step, the program is ready to be installed:

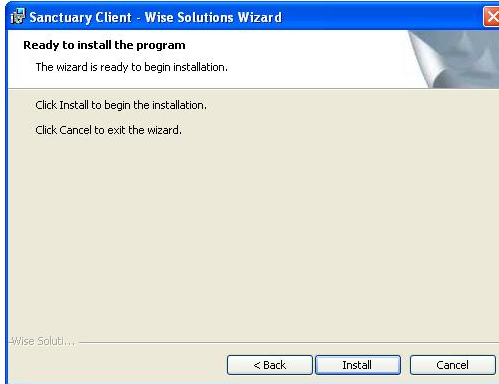


Figure 51: Sanctuary Client: the installation process is ready to start

Click on the **INSTALL** button to proceed. The setup will take about 2 minutes depending on the hardware in use.

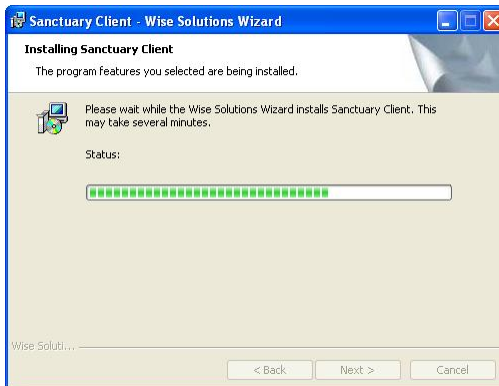


Figure 52: Sanctuary Client: the installation progress



12. Click **FINISH** to close the dialog and complete the procedure.

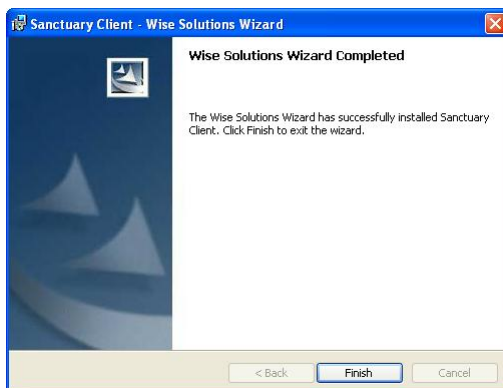


Figure 53: Sanctuary Client: finishing the installation process

The Sanctuary Client setup prompts you to reboot since its driver should start before all those already installed for your devices.

13. Click **Yes** to restart the computer.

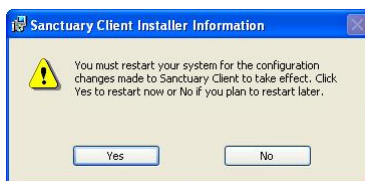


Figure 54: Sanctuary Client: restarting the computer

You can also see this dialog if there is no import file and you did not provide a server address:

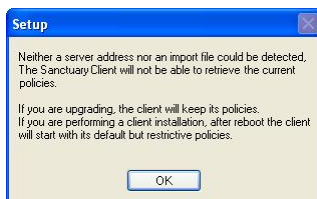


Figure 55: Sanctuary Client: no import file and no server address specified



Unattended installation of the Sanctuary Client

Once you have installed and tested your Sanctuary software configuration on a few computers, you will want to deploy it on all or most of the computers on your network. See *Chapter 10: Unattended Client Installation* on page 103 for details on how to do this without having to physically visit each client computer and run the Setup program.

Uninstalling the Sanctuary Client

At any time after installing Sanctuary Client, you can uninstall it from the client computer. If you used Group Policy to do an unattended installation, then you must also use it to uninstall the client(s).

You can use the Sanctuary Client Deployment tool to do an unattended install/uninstall of the client package. See *Using the Sanctuary Client Deployment tool to install the Clients* on page 111.

If the client was installed manually, then select *Add/Remove Programs* from the Windows Control Panel, and choose *Sanctuary Client* from the list of installed programs. The Setup program launches and uninstalls Sanctuary Client. You must reboot the computer once finished.



If a network shared disk was used during the initial installation, and this disk is no longer available during uninstall, the MSI program may ask specifically for the original setup file location before it can continue. A workaround solution for this problem is to copy the original MSI setup file on the local hard drive, then point the MSI uninstaller towards this file. You can remove the MSI setup file from the local hard drive once the client is deleted.

Load balancing methods

What is load balancing

When you have two or more application servers in your network, it is necessary to distribute the charge so that both of them work in a more or less “balanced” state. This creates a load balance condition distributing processing activity evenly so that no single server is overwhelmed. Load balancing is especially important



when it is difficult to predict the number of requests that will be issued to a server.

Round robin is a load balancing technique that works on a rotating basis – working in a loop fashion.

How does round robin DNS works?

When there is a request to a DNS server, configured in a round-robin fashion, it will resolve the name to one of the available IP addresses stored in its table in a rotated order. This redirects the request to one of the Application servers of a group.

As an example and using *Figure 1* as reference, when the first request arrives at the DNS server, it returns IP address # 192.168.1.1, the first machine. On the second request, IP address # 192.168.1.2. And so on. Assuming that we only have three servers defined in the DNS table, on the fourth request, the first IP address is returned once more.

Using the above DNS round robin schema, all of the requests to SecureWave Application Servers have been evenly distributed among all of the machines in the cluster. Therefore, using the DNS round robin method of load balancing, all of the nodes in the cluster are exposed to the clients.

Advantages of DNS Round Robin

Although very easy to implement, round robin DNS has some drawbacks, such as inconsistencies in the online DNS tables when remote servers go unpredictably down. However, this technique, together with other load balancing and clustering methods, can produce good solutions in many situations.

The main advantages of DNS round robin are:

- > Inexpensive and easy to set up. The system administrator only needs to make a few changes in the DNS server to support round robin. Clients are not even aware of the load-balancing scheme they are using.
- > Simplicity. You can add or remove servers as you go. All clients are identically installed using only one DNS alias provided as a SecureWave Application Server. When some of these servers are added or moved, you only need to edit one DNS table; not to modify registry settings.

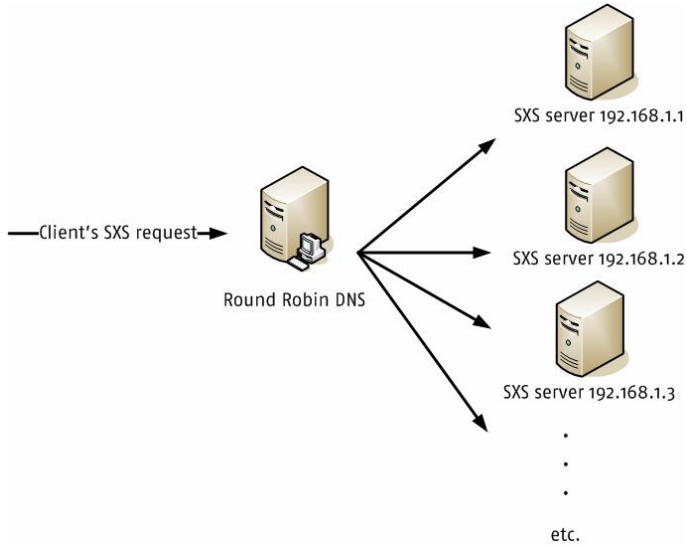


Figure 56: Round Robin DNS schema



Windows 2000 has some bugs related to DNS round robin. Applying the latest patches solves them.



Chapter 6: The Authorization Service tool

The information in this chapter applies only to the Sanctuary Suite (Sanctuary Server Edition, Sanctuary Custom Edition, and Sanctuary Terminal Services Edition)

Software Update Services (SUS) assists Microsoft Windows administrators with the distribution of security fixes and critical update releases provided by Microsoft. SUS is like running a Windows Update service inside your own network. SUS is used to distribute official updates to Microsoft Windows 2000, Microsoft Windows XP and Microsoft 2003 computers, including servers and desktops.

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

What is the Sanctuary Authorization Service tool?

You can use *Sanctuary Authorization Service* (AuthSrv.exe) to monitor changes on the approved and synchronized files done by SUS or WSUS, and process them, when needed, using our *Versatile File Processor Tool* – 'FileTool.exe' explained in *Chapter 14* of the *Administrator's Guide*. The goal of this process is a 'zero' administration effort. All Microsoft Authorized updates and fixes are automatically approved, their Hash created, and the database updated. Please see the configuration details in *Chapter 14* of the *Administrator's Guide*.



Notice that we do support neither Outlook Express nor Internet Information Server (IIS) as clients for sending email messages. If there is already an account in these types of clients, the SMTP IP address is transferred directly to the AuthSrv configuration. Furthermore, the 'LoadConfiguration' registry key parameter is always set to '3' (see the Administrator's Guide).



Installation

The installation of the Authorization Service Tool (AuthSrv.exe) is done through a setup Wizard. To install the tool follow these steps:

1. Localize and run the installation wizard on the Sanctuary Server Edition CD (server\AuthSrv\Setup.exe). The welcome screen is shown:



Figure 57: Sanctuary Server Edition installation: welcome screen

2. Click on the NEXT button. The next screen shows the License Agreement that you must accept before clicking on NEXT.
3. In the next screen, you need to key in the user's name and password, the SecureWave Application Server IP or name and the default port to communicate with it. Click on NEXT to continue.



Figure 58: Sanctuary Server Edition installation: configuration screen



4. Configure the options of the next screen to suit your needs. If you activate the e-mail option, the setup wizard proceeds to configure your mail services in the next screen. Click on the **Next** button to proceed.



Figure 59: Sanctuary Server Edition installation: option screen

5. If you choose the e-mail option in the previous step, you now have to configure it. Fill in all the corresponding fields. The program creates a test e-mail. If the send action is successfully finished, you get a message informing you that the test has been sent and everything is working correctly. Click on the **Next** button.

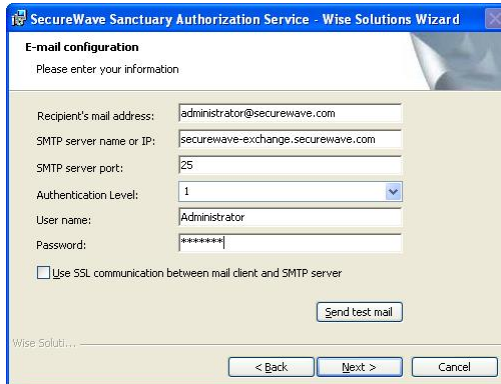


Figure 60: Sanctuary Server Edition installation: e-mail configuration screen

6. In the next screen, you are given the chance to change the installation directory (the program proposes c:\Program Files\SecureWave\Sanctuary). Change or accept by clicking on **Next**.

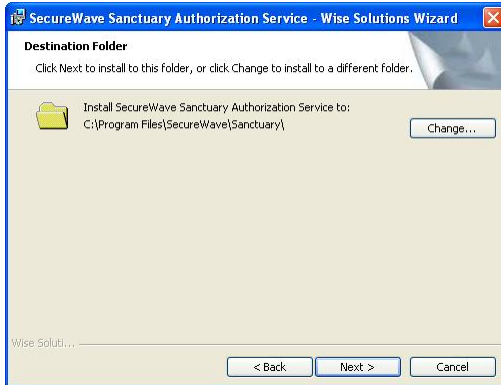


Figure 61: Sanctuary Server Edition installation: choose installation directory

7. The final summary screen is shown. You are now ready to install the program. Click on **INSTALL** to proceed, **BACK** to change options, or **CANCEL** to stop the setup. You will see the progress window and the final screen. Click on the **FINISH** button to close the setup window.

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

The tool waits until:

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

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

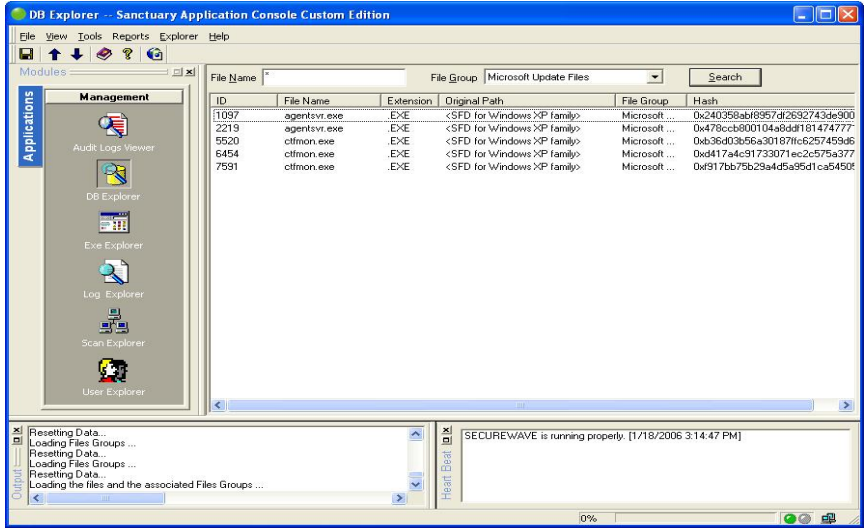


Figure 62: Sanctuary Server Edition initial scan



Chapter 7: Testing your Sanctuary Device Control installation

The information in this chapter applies only to Sanctuary Device Control.

This chapter details how to quickly test all of the Sanctuary Device Control key functions. You should refer to the Sanctuary Device Control Administrator's guide for details on how to configure the program.


After reading through and carrying out the steps in the following sections, you should have a basic understanding of how Sanctuary Device Control works and how to apply and revoke permissions in your production environment.



In this chapter, we named the workstation (client) computer in all the examples of the following sections as WKS and the server as SRV. We assume that all server-side components are installed on SRV and that the client-side components are installed on WKS. Furthermore, we assume that you have launched the Sanctuary Console on SRV and connected to the SecureWave Application Server.

Permissions

They allow permanent access to devices for users or groups on any computer. You should refer to the *To assign default permissions to users and groups* section in *Chapter 3: Using the Device Explorer* of the Sanctuary Device Control Administrator's Guide.

1. Put a CD in the DVD/CD reader of WKS.
2. Choose one user (let us call him 'Dummy'); log on WKS with the 'Dummy' account. If you try to browse the DVD/CD, you get an "Access Denied" message. You are not authorized to access this device.
3. Click on the 'Device Explorer' icon: . The central panel of the window contains a tree with 'Default Settings' as the topmost item. Expand this branch using the + key of your numeric keyboard or click on the + sign in front of the item.
4. Right click on the DVD/CD-ROM item and choose *Permissions* (or use the CTRL+D shortcut key).




5. In the *Permissions* dialog, choose **Add**. Type 'Dummy' in the *Name* field or click on the **SEARCH** button, find the user and then click on **OK**.
6. Back in the *Permissions* dialog, select the **READ** checkbox and click on the **OK** button.
7. In the **TOOLS** application menu, choose **SEND UPDATES TO ALL COMPUTERS**.

You have now given the user 'Dummy' read-only access to the DVD/CD drive on any computer he may be logged onto.

If you are logged on WKS with the 'Dummy' account, a popup appears in the system tray icon bar notifying you of the new rights that you have been granted. You can double-click on the Sanctuary Device Control icon to have a summary of all rights that apply to you. You can now read any DVD/CD-ROM.

Temporary permissions

Temporary permissions allow access to devices for users or groups on a specific computer for a limited period. You can refer to *Assigning temporary permissions to users* in *Chapter 3: Using the Device Explorer* of Sanctuary Device Control *Administrator's Guide* for more details.

1. Put a floppy disk in the floppy reader of WKS.
2. Choose one user (let us call him 'Dummy'), log on WKS with the 'Dummy' account. If you try to browse the floppy, you get an "Access Denied" message. You are not authorized to access this device.
3. Click on the 'Device Explorer' icon: . The central panel of the window contains a tree with 'Microsoft Windows Network' as the topmost item of one of the branches of the tree. Right click on it and choose **INSERT COMPUTER** (or use the **CTRL+A** shortcut key).
4. In the *Select Computer* dialog, choose **Add**. Type 'WKS' in the *Name* field or click on the **SEARCH** button, find the computer and then click on **OK**.
5. WKS appears in the tree, expand this branch. Use the **+** key of your numeric keyboard or click on the **+** sign in front of the item.
6. Right click on the **Floppy Disk Drives** item and choose **TEMPORARY PERMISSIONS**. A Wizard is launched.
7. Add 'Dummy' as user, choose **WRITE** on the next page. This will also select the **Read** option. Apply the permission for 5 minutes in the last page of the wizard.




8. Back in *Device Explorer*, right click on 'WKS', choose SEND UPDATES TO WKS.

Now you have given 'Dummy' read/write access to the floppy disk drive of WKS for the next 5 minutes.

If you are logged on WKS with the 'Dummy' account, a popup appears in the system tray icon bar notifying you of the new rights that you have been granted. You can double-click on the Sanctuary Device Control icon to have a summary of all rights that apply to you. You can now copy files to the floppy. The floppy drive will be automatically locked again after 5 minutes.

Scheduled permissions

Scheduled permissions allow access to devices for users or groups on all or specific computer following a pre-defined calendar. Please refer to *To assign scheduled permissions to users and groups in Chapter 3: Using the Device Explorer of Sanctuary Device Control Administrator's Guide* for more details.

1. Put a floppy disk in the floppy drive of WKS.
2. Choose one user (let us call him 'Dummy'), log on WKS with the 'Dummy' account. If you try to browse the floppy, you get an "Access Denied" message. You are not authorized to access this device.
3. Click on the *Device Explorer* icon: . The central panel of the window contains a tree with 'Default Settings' as the topmost item. Expand this branch using the + key of your numeric keyboard.
4. Right click on the Floppy Disk Drive item and choose *Add Schedule* (or use the CTRL+N shortcut key).
5. In the *Choose User* dialog, click on the ADD button. Type 'Domain Users' in the *Name* field and click on the SEARCH button and then on OK.
6. Back in the *Choose User* dialog, click on NEXT.
7. In the *Choose Permission* dialog, select the READ checkbox . Click on the NEXT button.
8. In the *Choose Timeframe* dialog, select all checkboxes except Saturday and Sunday. Leave the default hours, click on NEXT and then on FINISH.
9. In the TOOLS application menu choose SEND UPDATES TO ALL COMPUTERS.

Now you have given all members of the 'Domain Users' group read-only access to the floppy disk drive from Monday to Friday on any computer they may be logged onto.




If you are logged on WKS with the 'Dummy' account or any other Domain User, a popup appears in the system tray icon bar notifying you of the new rights that you have been granted through 'Domain Users'. You can click on the Sanctuary Device Control icon to have a summary of all rights that apply to you. Providing that you are on the schedule that has been chosen, you get a read-only access to the floppy.



Scheduled rights and temporary permissions only work properly when the different computer clocks are synchronized. Bear this in mind when using Sanctuary Device Control in multiple time zones.

CD authorization

This functionality lets you give access only to authorized DVD/CD-ROMs to users or groups. You can refer to *Chapter 6: Using the Media Authorizer* and *Chapter 7: Accessing encrypted media outside of your organization* in *Sanctuary Device Control Administrator's Guide*.


1. Put a DVD/CD-ROM (in this example, we will use the Microsoft Office CD) in the CD drive of WKS.
2. Choose one user (let us call him 'John'), log on WKS with the 'John' account. If you try to browse the CD, you get an 'Access Denied' message. You are not authorized to access this device.
3. Click on *Media Authorizer* icon: . Put the Microsoft Office CD in the SRV DVD/CD-ROM drive. Click on **ADD DVD/CD** button. In the *Media Name* dialog, type in a meaningful name (we use Microsoft Office CD in this case), click **OK**.
4. Select the Microsoft Office CD on the upper pane of the window. Click on the **ADD USER** button and select a domain user from the *Select Group, User, Local Group, Local User* dialog; for our example we will call this user 'John'. This allows you to grant John access to the Microsoft Office CD.
5. In the **TOOLS** application menu, choose **SEND UPDATES TO ALL COMPUTERS**.


Logged on WKS with 'John' account, if you put Microsoft Office CD in the drive, you now have access. Access to any other DVD/CD will be denied.



Shadowing

This functionality allows you to get a copy of what your users have copied to their devices. You can refer to *Chapter 4: Using the Log Explorer* in Sanctuary Device Control *Administrator's Guide*.

1. On SRV, launch the *Sanctuary Device Console* in the Sanctuary Device Control program group.
2. Go to the Device Explorer module () and select the *Floppy Disk Drives* in the *Default Settings* section. Right-click and choose *Shadow* or use the CTRL+W shortcut key.
3. In the *Choose User* dialog, click the ADD button and search for a known user. In this example, we use Marketing. Then click OK.
4. Click the NEXT button and activate the *Enabled* option. Click on NEXT and then on FINISH.
5. In the TOOLS application menu, choose SEND UPDATES TO ALL COMPUTERS.
6. Give 'Marketing' read/write access to the floppy as explained above.
7. Log on any computer (WKS in our case) with the 'Marketing' account. If you double-click on the Sanctuary Device Control icon in the Tray icon bar, you will see that there is a Read/Write access to the floppy and that shadowing is enabled for this device.
8. Copy some files to the floppy.
9. On SRV, use the *Default Options* item of the *Tools* menu and check that the *Centralized Device Control Logging* is enabled. Click on the *Log Explorer* module of the *Sanctuary Device Console*.
10. From the EXPLORER menu, choose FETCH LATEST LOG FILES.
11. In the *Select computer* dialog, enter WKS then click OK.

If you click on the SEARCH button, the files that have been copied to the floppy by 'Marketing' appear in the list. You will notice a clip  symbol to the right of the shadowed file. A right click on the file allows you to view, save, or open its content.




The shadowing rule only works in one direction. Files that are copied from the floppy to the hard disk are NOT shadowed.



Shadowing can also be set on a per-computer basis.

Auditing

With Auditing, a record of all actions made by Sanctuary Device Control administrators is taken. You can refer to *Chapter 6: Using the Audit Logs Viewer* in Sanctuary Device Control *Administrator's Guide*.

1. Click on the *Audit Logs Viewer* icon: .
2. Adjust the dates if necessary.
3. Click SEARCH.

You will see a record of each relevant action taken by the Sanctuary Device Control administrators. For example, you can find out when and which administrator granted a user access to some devices.

Reporting

For full details, you can refer to *Chapter 11: Reports* in Sanctuary Device Control *Administrator's Guide*.

User Permissions:

1. From the Sanctuary Device Console *Reports* menu, choose *User Permissions*.
2. In the *Select Domain User or Group* dialog, enter 'Dummy', and click SEARCH.
3. Click OK.

You receive a report with all rights that apply to 'Dummy'. This is useful when you want to check the privileges that apply to a specific user (local permissions are not included.)

Device Permissions:

- > From the *Reports* menu, simply choose *Device Permissions*.

You get a per device list of access permissions.



Computer permissions:

1. From the Reports menu, choose Computer Permissions.
2. In the *Select Computer(s)* dialog, enter 'WKS'.
3. Click OK.

You get a per computer list of access. This is useful when you want to know the rights that have been defined on one specific computer.

Summary

Administration of a Sanctuary Device Control installation is relatively easy assuming policy definition has been achieved at the beginning of the process.

Detailed explanations of all the functionalities of Sanctuary Device Control are available in the *Administrators Guide*.




Chapter 8: Testing your Sanctuary installation

The information on this chapter applies only to the Sanctuary Suite (Sanctuary Server Edition, Sanctuary Custom Edition, and Sanctuary Terminal Services Edition).

This chapter details how to quickly test all key functions of your Sanctuary suite installation. You should refer to the Sanctuary Suite Administrators' guide for details on how to configure it.

After reading through and carrying out the steps in this section, you should have a basic understanding of how Sanctuary works and how to authorize/revoke permissions to run applications in your production environment.


 *In this chapter, we named the workstation (client) computer in all the examples of the following section as WKS and the server as SRV. We assume that all server-side components are installed on SRV and that the client-side components are installed on WKS. Furthermore, we assume that you have launched the Sanctuary Console on SRV and connected to the SecureWave Application Server.*

Performing an initial scan

An initial scan allows you to quickly populate the database with the files required to operate the client computer. All files not included in the database will be denied execution as being unknown. Please refer to *Chapter 5: Building a list of executable files to be managed* in the *Sanctuary Suite Administrator's* guide.

To do this initial scan, follow these steps:

Creating a Scan Template


1. Click on the *Scan Explorer*  icon in the Sanctuary Management Console.
2. Select **PERFORM NEW SCAN** from the bottom right side of the main screen.
3. In the next window, select **CREATE NEW TEMPLATE**, this will allow you to select which files and drives you would like to scan.



4. Type the name for the new template. For this example, we will use 'Scan One'.
5. Click on ADD button to insert a rule for the scanning procedure.
6. Select the drive on which you would like to carry out the scan. Type in the drive letter and path where your operating system is installed. We will use C:\ for this example. Leave the pattern as default '*'. Check the INCLUDE SUBDIRECTORIES option. If you do not activate this option, only the c:\ directory will be scanned, letting out crucial files that reside in the OS installation directory. Do not forget to also check the SCAN EXECUTABLE option.
7. Click OK and SAVE to preserve your newly created template.

Utilizing your new Template

In order use your scan, you will now need to select a client computer on which to run it.

1. In the *Perform New Scan* dialog, still open after creating the template of the previous section, click on the ellipsis  button – or type in a name – to select a client on which to carry out the scan. If you close the dialog after step 7, open it again by clicking on the PERFORM NEW SCAN button and select the 'Scan one' scan. If you use the ellipsis button or if you type a wrong or partial name, a new search dialog opens – *Select Computer* – where you can select the correct computer.
2. Once you select the desired computer, click on the START SCAN button.

You need to define a comment to identify this scan. The scan will run to full completeness, giving you a status notification at the *Output* window (located at the bottom left of the main screen). Scanning an entire hard drive will take several minutes.

If you do not see the *Output* window, open it by using the OUTPUT item of the VIEW menu.

Authorizing your new file hashes

Once the scan is completed, you will need to authorize the new hashes to a File Group. This is done by first viewing the scan you have created.

1. Click on the SELECT SCANS button located on the bottom right part of the main window and select the scan in the SHOW SCANS MADE FROM TEMPLATE field by name (typing or selecting from the pull-down list 'Scan one'). You will notice that this will also fill the SECOND SCAN section below. This is




used when two (or more) scans exist in the database allowing you to compare them.

2. Once the scan is displayed, select all the unknown files. Unknown files are shown as <not authorized>.
3. Once the files are selected, right click on them and then on the *ASSIGN TO FILE GROUPS* contextual menu item. You will be presented with a new dialog, click on *FILE GROUPS* button.
4. In the next window, click on the *ADD FILE GROUP* button to create a new file group. Create a group called 'My Files'.
5. Once the group created, the *Assign Files to File Groups* dialog shows. At this stage, if you import known file definitions for your Operating System, you should see that many files actually have a File Group suggestion. You need to manually assign those file for which the system makes no suggestion to the newly created 'My Files' file group. Once finished, click on the OK button.
6. The files are added to the database and are now ready to be used in the *User Explorer* and *DB Explorer* module to manage and authorize.

Authorizing Files

Now that you have a file group ('My Files'), which has been populated by the *Scan Explorer*, you need to grant users the right to use these files on their server. Notice that each file only needs to be scanned once to add its hash to the database. The following steps demonstrate how to add files to the Domain Users group. You can also refer to *Chapter 8: Assigning access permissions to users and groups* in the *Sanctuary Server Edition Console Administrator's* guide.

1. Click on the *User Explorer*  icon in the Sanctuary Console.
2. In the central panel of the window, you will see the various user groups, domains, and common user groups (highlighted in red). Only those Users/Groups/Computers/Domains that have File Groups directly/indirectly assigned are shown. Click on the Users/Groups/Computers/Domains check boxes to further filter your search. You can add objects by typing the name or searching with the *ADD* button. These groups have common SID's amongst all computers, hence their existence at the top of the list. You can authorize your *My Files* file group to everyone if you want any user to use files on a desktop. We will be giving access to the Domain Users.



3. The right upper and lower panels will show you the directly, indirectly and non-authorized file groups.
4. Once the Domain Users group is selected, choose 'My Files' file group from the *Not Unauthorized* panel list and click on the AUTHORIZE button located below the panel. The file group moves to the *Authorized* panel list.
5. Changes made only modify the database and have no effect on the client side. To inform your clients, select the *Send Updates to All Computers* or *Send Updates to item* from the *Tools* menu. This will push the new information to all drivers or a specific computer on the network so that your new settings take effect immediately.

A number of File Groups have been created when importing the known file definitions. We suggest that you make the following assignments:

<i>File group</i>	<i>Recommended assignment(s)</i>
Boot Files	LocalSystem, network service, local service
all File Groups (except Common Files, Logon Files and Boot files)	Administrators
Common Files	Everyone
Logon Files	Everyone
Securewave support files	Everyone
Accessories	Everyone

Table 4: Recommended File group assignments

Files can also be authorized by using the *EXE Explorer* module. This module allows an administrator to browse a CD-ROM drive on a particular computer to permit users to run specific files from a CD.

Try to log on a machine with the client installed

If you logon in a computer (for example, with a user called 'Dummy'), you can, normally, execute all programs because they have been previously authorized following the steps of the preceding sections.



If you logon to a machine and receive a message saying that an application or DLL is denied or that it is not a valid Windows image, you probably forgot to fill up the database with some files or did not authorize them. Launch once more the 'Sanctuary Console' and select the 'Log Explorer' module from the side bar. Select 'Fetch New Log' from the 'Explorer' menu, and choose the machine. If you do not remember the name or you want to




search for it, use the SEARCH button, select it and then click on the OK button. Back in the 'Log Explore', click on SEARCH. The program will give you a list of files. All files not assigned to a File Group are identified as '<Not authorized>' in the File Group column. All files not authorized, directly or indirectly through Domain groups, to the user are either identified as 'Access denied', 'ok-non-BlockUser', or 'ok-nonBlocking'. If you double click on those files, the 'Assign Files to a File Group' dialog opens. You can choose to create a new group by clicking on FILE GROUPS button. You must then proceed to associate the files to the corresponding File Group (use the 'Suggested File Group' drop-down list, and click on OK). Activate the 'User Explorer' module on the left side bar and grant 'Dummy', 'LocalSystem', and 'Administrators' the access to your new 'File Group'. Please refer to the corresponding Administrator's Guide.

Auditing

There are two types of auditing carried out within Sanctuary Console: a review of the Audit Logs of administrative actions and an analysis of the execution logs of client actions. You can refer to the corresponding *Administrator's guide* for a full description. The two types of information are viewed with the *Audit Logs Viewer* and the *Log Explorer* modules.

Audit Logs Viewer

The *Audit Logs Viewer*  displays the administrative audit trail. You have options for selecting dates, author, target, computer, user, and action to view the audit information. The resulting list, after clicking the SEARCH button, would look like this:

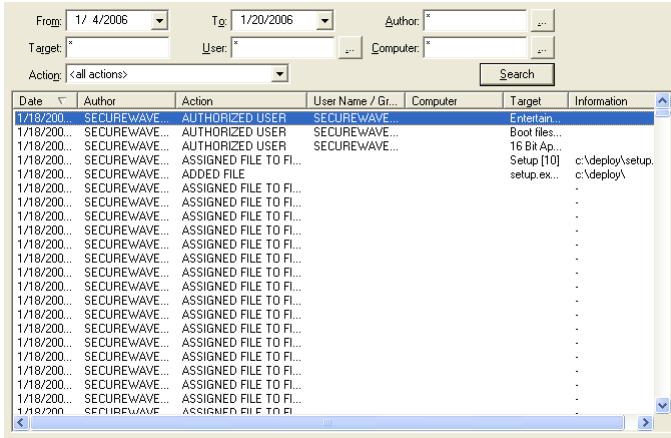



Figure 63: Audit Log Viewer module – main window

Please refer to the corresponding *Administrator's guide* for a full description.

Log Explorer

The *Log Explorer*  is the module that consolidates all logging information sent from the clients. Within this view, you can analyze which files users have been using, track access denied messages, and see if any users have been trying to run files unknown to the system on any of the clients.

You can apply various filters within the Log Explorer module to utilize its full capabilities. You can see an example screen on *Figure 63*.

Logs are sent as per the defined options from the Sanctuary Clients to the SecureWave Application Server. You may retrieve the latest logs from any client by using the *Fetch New Log* dialog located on the *Explorer* menu.

Please refer to the corresponding *Administrator's guide* for a full description.




Hash	File Name	File Path	Traced On	Transferred	User Name	Computer
28D06725A...	HprRes.dll	C:\Program Files\HyperSnap-DX 5	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...
BAB80963F...	Itelx10N.dll	C:\Program Files\HyperSnap-DX 5	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...
6D9015A19...	Itelg10N.dll	C:\Program Files\HyperSnap-DX 5	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...
41A179AE...	Itelw10n.dll	C:\Program Files\HyperSnap-DX 5	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...
CB6252E7A...	ItelS10n.dll	C:\Program Files\HyperSnap-DX 5	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...
A028027FE...	Itelmg10n.dll	C:\Program Files\HyperSnap-DX 5	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...
C178A2073...	Itelrn10n.dll	C:\Program Files\HyperSnap-DX 5	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...
6BD555717...	ItelI0n.dll	C:\Program Files\HyperSnap-DX 5	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...
87C35D9E8...	sqlmangr.FLL	C:\Program Files\Microsoft SQL Serv...	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...
12D487D0...	sqlsvc.FLL	C:\Program Files\Microsoft SQL Serv...	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...
B3DD94C1...	sqlseid.DLL	C:\Program Files\Microsoft SQL Serv...	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...
7EE01E2CF...	sqlsvc.DLL	C:\Program Files\Microsoft SQL Serv...	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...
97C969404...	w95scm.DLL	C:\Program Files\Microsoft SQL Serv...	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...
077E78509...	sqlmangr.exe	C:\Program Files\Microsoft SQL Serv...	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...
6E8352AE5...	HprSnap5.exe	C:\Program Files\HyperSnap-DX 5	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...
DE8E6C69...	igfres.dll	C:\WINDOWS\system32	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...
6C3F8EE67...	idfxhk.dll	C:\WINDOWS\system32	1/18/2006 12:4...	1/19/2006 4:23...	SECUREW...	WORKGRO...

Figure 64: Log Explorer example data window

Database Exploration

You can use the *DB Explorer* module of the Sanctuary Console to explore your database. This module was created to allow administrators to move files between File Groups in the database. To create additional File Groups follow these steps (you can refer to the corresponding *Administrator's guide* for full details):

1. Use the *DB Explorer* module  of the Sanctuary Console. The main window of this module is empty.
2. Type a file name or file group in the corresponding field) you can use wildcards) and click on the SEARCH button.
3. Click the *File Name* header to sort the database by that column.
4. Locate an executable(s) in the 'My Files' File Group by typing the name (or part of it) in the corresponding field and clicking on SEARCH. This file group was created following the steps outlined at previous sections of this chapter. Select one or more files assigned to that group.
5. Right click on the selected file(s) and choose the *Assign to File Group* item. The *Assign Files to File Groups* dialog opens.
6. Click on the FILE GROUPS button. Click the on the ADD FILE GROUP button and create a group named 'Other Files'. Click on the OK button to close the dialog.




7. Once the group is created, click on **CLOSE**.
8. Select the file and click on the arrowhead at the right of the *Suggested File Group* field. Select the newly created 'Other Files' file group.
9. Click on the OK button. You can now see that the file belongs to 'Other Files' file group.
10. Changes made only modify the database and have no effect on the client. To inform your clients, select the *Send Updates to All Computers* or *Send Updates to item* from the *Tools* menu. This will push the new information to all drivers or a specific computer on the network so that your new settings take effect immediately.
11. If you logon to the machine with the 'Dummy' account, you cannot execute the authorized file since it has been assigned to the 'Other Files' file group. The user has not been granted the rights to use those files. You can authorize the use of the 'Other Files' file group by using the *User Explorer* module. Do not forget to use the *Send Updates to All Computers* command. 'Dummy' will then be able to use the file(s).

As you can see from the previous example, it is easy to use the *DB Explorer* module. You can also select multiple files and assign them to a file group in the same way.

Local Authorization

Local Authorization provides the means to delegate to users the right and ability to locally authorize those applications not been centrally authorize. The user can then use that software locally. This provides users with the flexibility to run a particular program required to carry on doing business.

1. Click on the *User Explorer*  icon in the Sanctuary Console.
2. Select the *Default options* item of the *Tools* menu. The *Default Options* dialog opens.
3. Choose the *Computer* tab, and verify that the *Local Authorization* option is *Enabled* (default value). You can also use this option to disable local authorization on all computers. Click on the OK button to close the dialog.
4. Back in the *User Explorer*, click on the *Users* checkbox and select the user 'Dummy'. If it is not in the list, use the **ADD** button to insert him or type his name, or part of it, on the *Users, Groups, Computers, and*



Domains field. Right-click on the user's name and select the *Options* item from the popup menu to open the corresponding dialog.

5. Configure the *Blocking mode* option to *Ask user for *exe only* and click OK.
6. Changes made only modify the database and have no effect on the client. To inform your clients, select the *Send Updates to All Computers* or *Send Updates to* item from the *Tools* menu. This will push the new information to all drivers or a specific computer on the network so that your new settings take effect immediately.

Proceed to logon on the server with the 'Dummy' account. If you now attempt to execute an application not centrally authorized, you receive an alert message explaining that you are about to run an application that has not been authorized. The dialog shows detailed information about the application that is about to run.

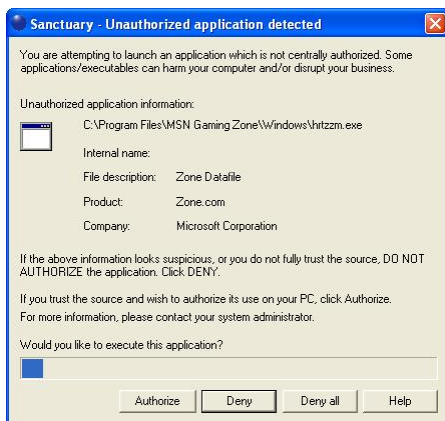


Figure 65: Local authorization dialog

- > If you are not sure that the application source is a trusted one, click on **DENY** preventing its execution (default behavior). You are prompted again next time this application tries to run.
- > You can click on **DENY ALL** if you do not want to receive execution notifications again. This setting can be reverted using Sanctuary's tray icon contextual menu.
- > If you click on **AUTHORIZE**, the application executes. This authorize the program locally only for that specific computer.



Once an application has been locally authorized, there is no way to block this program from the console. You should delete the local Sanctuary settings – as an administrator – to reset this condition.

A progress bar appears at the bottom of the dialog. The file is denied and the dialog closed if you do not respond within the timeout period.

7. All local authorization decisions are logged centrally. The administrator can monitor them using the *Log Explorer* module. He can also decide to centrally authorize those locally authorize applications. This operation will allow all selected users to run a given application.

Summary

Administration of a Sanctuary installation is relatively easy assuming policy definition has been achieved at the beginning of the process.

Detailed explanations of all the functionalities of your Sanctuary solution are available in the corresponding *Administrators Guide*.




Chapter 9: Using the Key Pair Generator

The information in this chapter applies to all Sanctuary software suite products.




To accompany the Sanctuary Console, SecureWave provides the Key Pair Generator. This is a utility that you can use to create a key pair that is used to assure the integrity of the communication between the Application Server and the clients.

Introduction

The Key Pair Generator is used to create a key pair. The SecureWave Application Server uses an asymmetric encryption system to communicate with the Sanctuary Clients. The SecureWave Application Server and kernel clients contain a default embedded key pair that is suitable for evaluation purposes only.

-  *In a production environment, create your own key pair BEFORE deploying the Sanctuary Client on the first client computer. You can do so using the Key Pair Generation utility.*

If you are using *Sanctuary Device Control*:

-  *NEVER change the key pair after having added some encrypted removable media in the Media Explorer. If you do so, your users will not be able to access their encrypted media anymore.*
-  *These keys are used to protect the communication between the SecureWave Application Server and the client computers. They play also a role in the media encryption process but they are not media encryption keys.*
-  *It is recommended that you install and publish a Microsoft CA on you Active Directory structure before trying to encrypt a removable device.*



Starting the key pair generator

1. Navigate to the PROGRAM FILES\SECUREWAVE\ SANCTUARY\SXTTOOLS directory, found on the machine where the Sanctuary Application Server is installed.
2. Run the KEYGEN.EXE tool.

The *SecureWave Key Pair Generator* dialog is displayed.

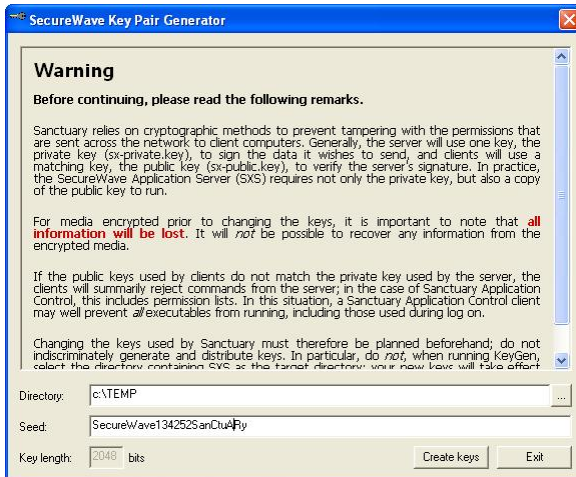


Figure 66: Key pair generation: first step

Generating a key pair

1. Select a temporary directory where the private and public key files are going to be saved.
2. Enter any random text into the *Seed* edit field. This is used to initiate the random number generator. This field may also be left blank.
3. Click on GENERATE. The key pair is generated. A dialog similar to the following one is displayed:



Figure 67: Key pair generation: final message

4. Click Ok.

Deploying the key pair

The key pair can now be distributed. Copy the private key file “sx-private.key” and the public key file “sx-public.key” to the computer(s) running SecureWave Application Server, under the %SYSTEMROOT%\SYSTEM32 directory. Alternatively, they can also be put on a removable drive or DVD/CD.

The SecureWave Application Server, *only* when starting up, will check for the key pair in the following locations:

1. The directory where the SecureWave Application Server executable is (usually %SYSTEMROOT%\SYSTEM32).
2. The SXS server’s private directory (%SYSTEMROOT%\SXSDATA).
3. All removable drives and DVDs/CDs in alphabetical order.

The search will stop at the first valid key pair.



When a new key pair has been generated to replace an existing one, you must stop and restart the SXS service before the newly generated keys will be taken into account. The SXS Service can be started and stopped through the Windows Services Panel or using a command line (`net stop sxs ; net start sxs`).



If the key pair is neither in %SYSTEMROOT%\SYSTEM32 nor %SYSTEMROOT%\SXSDATA, physical access to the servers running the SecureWave Application Server should be strictly controlled because a rogue administrator could replace the key pair by inserting a removable media with a different key pair.

When SecureWave Application Server starts and cannot find the key, it writes an event to the event log and uses the default key pair set provided by SecureWave. This message does not correspond to a system malfunction, it indicates that all



components work with default keys and this is not recommended for obvious security reasons.

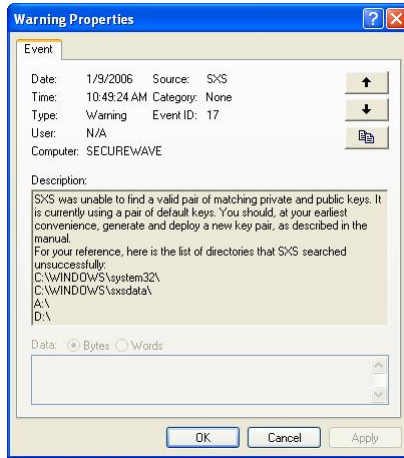


Figure 68: SXS did not find the public-private key pair

ONLY the public key file `sx-public.key` should then be deployed to all client computers by means of the Sanctuary client setup. You should copy the Client folder from the product media to a network share and copy the `sx-public.key` into this folder. Setup will detect that a new public key is present and will copy it to the target computer.



For machines that already have Sanctuary Clients installed, copy the public key file (NOT the private key file) to the %SYSTEMROOT%\SXDATA directory of the client computer (typically C:\WINNT\SXDATA). Afterwards, logoff or reboot to receive the new settings signed with the matching key pair.



Chapter 10: Unattended Client Installation

The information in this chapter applies to all Sanctuary software suite products.

Once you have installed and tested your Sanctuary configuration on a few computers, you may want to deploy it on all or most of the computers on your network. If you have a large number of computers to manage, this is much simpler with an unattended installation.

This chapter explains how to install the Sanctuary Client using MSI technology (at least version 2.0 of the MSI Installer must be installed to do this, Windows 2000 SP3 includes MSI 2.0) and optionally Windows 2000/2003 Group Policy.



If you prefer to use another deployment tool, you should be aware that some of them, by design limitations or errors in their configuration, do not do a completely 'silent' installation and sometimes fail since they are waiting for user input.



If you are installing Sanctuary Device Control or Sanctuary Custom Edition on Windows XP SP2 machines, you need to open certain blocked ports to be able to do an unattended client installation. Refer to Appendix F: Opening firewall ports for client deployment on page 163 for more details.



You cannot install Sanctuary Server Edition's client on Windows XP or Windows 2000 Pro machines.



Although the installation dialog only lets you input three SXS servers, you can easily add more if needed. You can also change how the SXS server(s) is selected – round-robin vs. random pick. All this is done by modifying certain options in the console or registry keys. Please see Sanctuary Client registry keys on page 148 and Load balancing methods on page 72 for more details. You can “push” these modifications to all clients using Group Policies with ADM templates.



Installing Sanctuary Client: MST file generation



You can refer directly to the Sanctuary Client Deployment help for more details.

1. On the administrator's machine, select *Sanctuary Client Deployment* from the **START** → **PROGRAMS** → **SANCTUARY DEVICE CONTROL** (or the corresponding program's name) menu. The following dialog appears on first use.

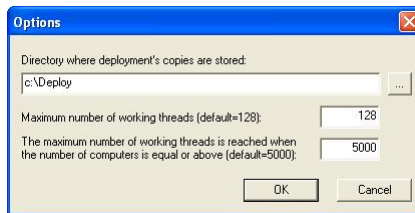


Figure 69: Sanctuary client deployment: first start-up

2. Choose a folder where you would like to store all the deployment packages. You can modify this setting by using the *Options* entry of the *Packages* menu at a later point in time. Do not change other settings.



Do not specify the root directory of the system drive or any other directory where existing files already reside or might be created by other applications.



If the deployment tool is installed on different machines, you might want to specify a shared directory where all instances of the deployment tool can access the company packages.

3. Click OK. The following dialog appears:

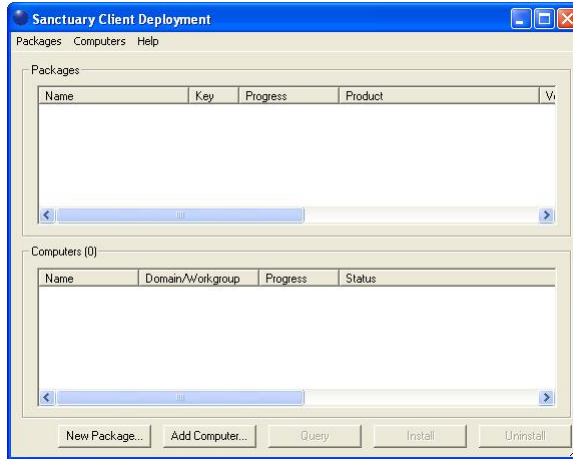


Figure 70: Sanctuary client deployment: packages and computers

4. From the *Packages* menu, select *New*. The following dialog is displayed.

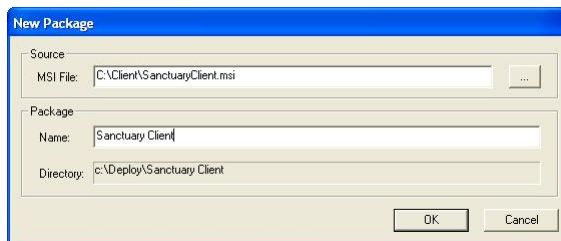



Figure 71: Sanctuary client deployment: new package

5. Click the ellipsis () button to select an MSI file, typically from the CLIENT folder of the CD-ROM. Type in the name you wish to give to the package. Take note of the directory, we will refer to it as the Deployment package folder (C:\DEPLOY in this example).
6. Click OK. The installation files are copied in a subfolder of the destination directory as defined in point 1 (C:\DEPLOY in our example). Then the *Options – SecureWave Installation Transform* dialog appears as shown below.

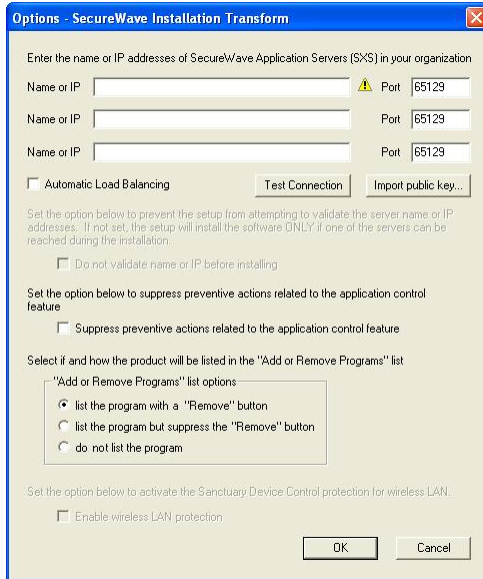



Figure 72: Sanctuary client deployment: application server IP or name

You can see two grayed-out options that are only valid if you are installing older versions of our client:

DO NOT VALIDATE NAME OR IP BEFORE INSTALLING. Used to give a Server address or name that is not available at the moment but will be accessible afterwards.


ENABLE WIRELESS LAN PROTECTION. An option available in older clients (v2.8 and before) that has now been superseded by permissions rules.


 *Despite our Client Deployment Tool supports installing older version of our client – which still supported Windows NT4 – this tool itself will not work with this operating system.*


7. Click **IMPORT PUBLIC KEY**.

Select the `sx-public.key` file located in the `%SYSTEMROOT%\SYSTEM32` folder of the *SecureWave Application Server* machine.



-  *If you do not find a `sx-public.key` file in the `%SYSTEMROOT%\SYSTEM32` or the `%SYSTEMROOT%\XSDATA` folders of the SecureWave Application Server, it means that your installation is using default keys. You should not deploy the clients in a production environment without having generated your own set of keys. Please refer to Chapter 9: Using the Key Pair Generator on page 99 for more details. Keep in mind that replacing an existing set of keys or implementing customized keys in an environment where encrypted media – if you are using Sanctuary Device Control – are already in use will prevent access to those media altogether.*

 -  *Although not recommended, it is possible to deploy the clients on test environments without a customized set of keys. If you do not want to generate custom keys, simply skip this step.*

 -  *The Sanctuary Clients can now be deployed without specifying a server address(s) that can immediately be validated: the server at the provided address(s) is contacted during the actual setup to make sure the client can communicate with it. If this communication is not achieved, the installation is aborted unless the 'Serverless Mode' option is selected. See next step for more information.*
8. Enter the fully qualified domain names or IP addresses of the SecureWave Application Servers to which these clients will attempt to connect, using the *Name or IP* fields. If alternative port numbers are required for these connections, then also type in the modified port numbers. If you do not specify any fully qualified domain name or address, you are installing in 'SERVERLESS MODE'. While using this mode, the installation routine will not abort if it cannot reach one of the application servers. Alternatively, if you do not leave them empty, at least one of them must be contactable for the installation to continue; the install will rollback if all connection attempts fail. When installing in 'Serverless mode', you can also control policies by exporting them to a special file (`polices.dat`) and you must also include the license file. See *The installation procedure* on page 64 for details.



When proceeding without specifying servers, you get the following warning message:

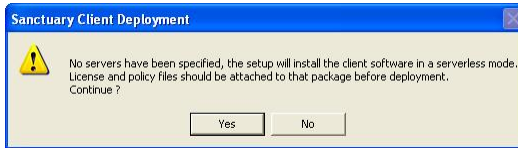


Figure 73: Message when installing in “Serverless mode”

9. Choose whether to select the *Automatic Load Balancing* checkbox. If you select this option, the Sanctuary Client driver attempts to contact one of the servers listed in a random manner. Alternatively, if you leave *Automatic Load Balancing* unchecked, the Sanctuary Client driver attempts to contact the application servers in the order they are listed.
10. Click on the TEST CONNECTION button to verify the fully qualified domain names or IP Addresses you have entered. A confirmation or failure dialog box is displayed. In the case of failure, check the error message for further details about the possible cause of failure (e.g. key pair mismatch, DNS resolution). Here are some:

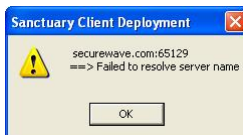


Figure 74: Message when the connection test fails

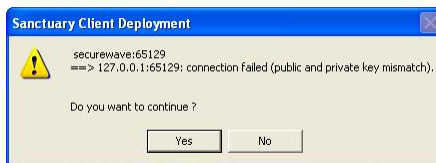


Figure 75: Message when the connection test fails (key related)

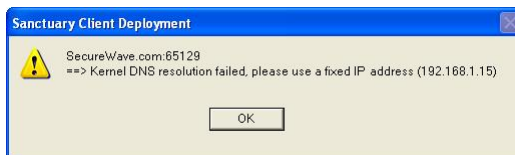


Figure 76: Message when the Kernel DNS resolution fails



Figure 77: Message when the connection test succeeds

Click OK to clear the message

11. Select those options controlling how the client driver is shown in the *Add or Remove Programs* Windows' dialog:

SUPPRESS PREVENTIVE ACTIONS...: Since the client software depends on the licenses you own, it is possible to completely block a computer if you do not export correctly the policies ("serverless" installation) or define them beforehand. This is especially true when installing our Sanctuary suite and not authorizing those files belonging to the operating system. To avoid this block out, the program first verifies if there is an update from Sanctuary Device Control to Sanctuary Suite and that this action does not blocks the machine. If this is the case, the installation will not proceed and will roll back. Use this option if you do not want this check done and you are sure that you have correctly defined the policies.

LIST THE PROGRAM WITH A "REMOVE" BUTTON – The program is listed in the "Add or Remove Programs" Windows' dialog in the 'standard' way; it will include a *Remove* button.

LIST THE PROGRAM BUT SUPPRESS THE "REMOVE" BUTTON – The program is listed in the "Add or Remove Programs" Windows' dialog but will not include a *Remove* button.

DO NOT LIST THE PROGRAM – The program will not appear in the "Add or Remove Programs" Windows' dialog.

12. Click on the OK button to close the dialog.

The new package appears in the Sanctuary Client Deployment packages list:

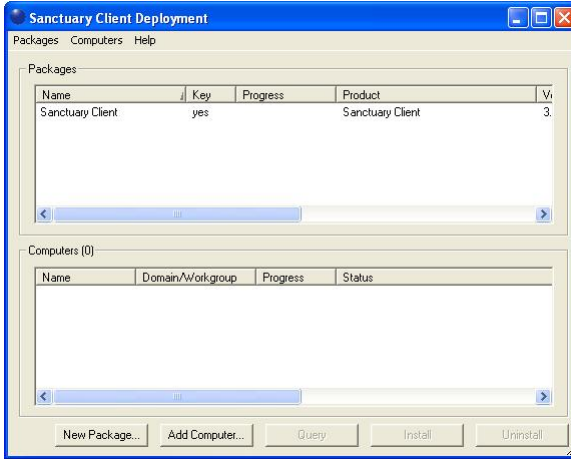


Figure 78: Sanctuary client deployment: new package

A small file called 'Sanctuary Client.MST' is created in the Deployment package folder (C:\DEPLOY in our example). Select *Options* from the *Packages* menu to check the location of the Deployment package folder on your installation. The specified directory contains subdirectories corresponding to the packages you have just created.

You can see the options of each generated package in the main window:

Name	Key	Progress	Product	Version	Server(s)	Last deployment	License	Policies
Marketing Remote	yes		Sanctuary Client	3.2	securewave:65129		no	yes
Sales Restricted	yes		Sanctuary Client	3.2		Install - 01-11-2006 14h37m19s	yes	no
Sanctuary Client	yes		Sanctuary Client	3.2			no	no

Figure 79: Sanctuary client deployment: package option



If the public key or license (in the case of an installation without servers), is not included in the package, it is displayed, as shown above, with an orange background to warn you. If there is no orange background, the key and license, if applicable, are present and the package is ready to be deployed. It is not recommended to deploy packages without a public key – or license – in a production network.



Using the Sanctuary Client Deployment tool to install the Clients

The Sanctuary Client Deployment tool has been designed to allow you to deploy silently the Sanctuary Clients on a list of machines.

Once the Deployment package has been created as explained in *Installing Sanctuary Client: MST file generation* on page 103, you can start the deployment, using the following procedure:



You can refer directly to the Sanctuary Client Deployment help for more details.

1. Select *Sanctuary Client Deployment* from the *Start → Programs → Sanctuary Device Control* (or corresponding program's name) menu.

The *Sanctuary Client Deployment* dialog is displayed:

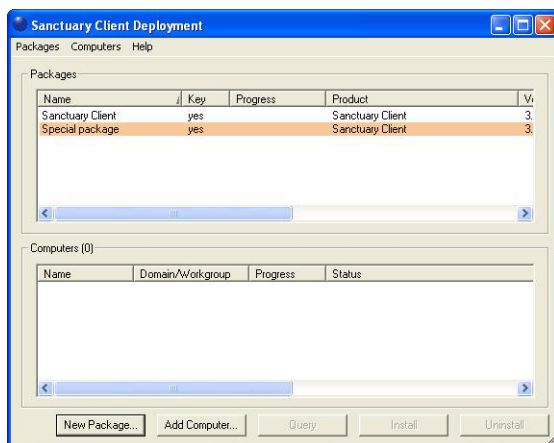


Figure 80: Sanctuary client deployment: first screen



If the public key or license (in the case of an installation without servers), is not included in the package, it is displayed, as shown above, with an orange background to warn you. If there is no orange background, the key and license, if applicable, are present and the package is ready to be deployed. It is not recommended to deploy packages without a public key – or license – in a production network.



2. Click on the **ADD COMPUTER** button. One of the following dialogs appears, depending on your operating system:

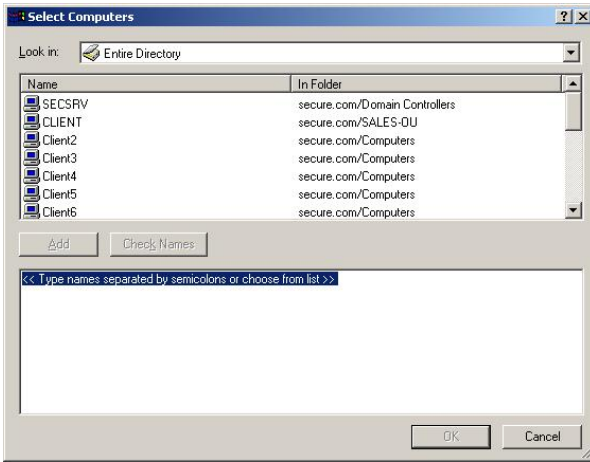


Figure 81: Sanctuary client deployment: select computer dialog (sample a)



Figure 82: Sanctuary client deployment: select computer dialog (sample b)

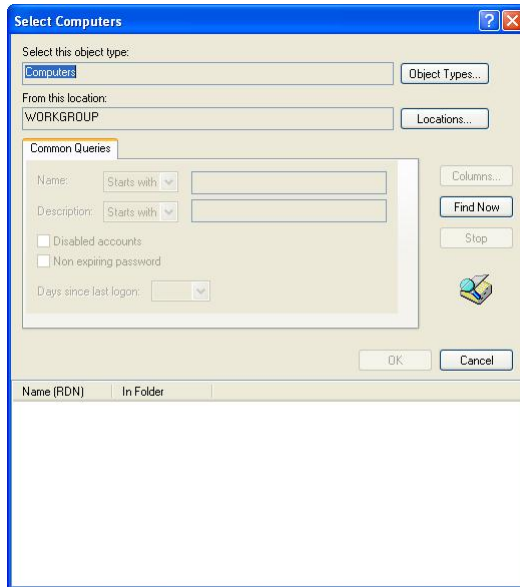


Figure 83: Sanctuary client deployment: advanced select computer dialog

You can also do a Drag & Drop between the external Microsoft Windows Network (from the My Network Places icon) selection dialog.

3. Select the domain you want to search. Then highlight or type in the names of the computers you want to add to the list. You can type in multiple names using a semicolon character ";" to separate computer names.
4. Once you have selected the computers you want to add to the list, click OK. The selected computers are now listed in the *Sanctuary Client Deployment* dialog, as shown below.

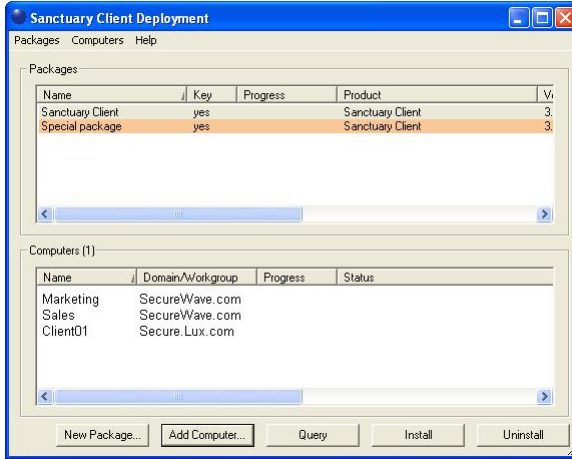


Figure 84: Sanctuary client deployment: selected computer(s)



If the current or newer version of the client is already installed on a machine you select, it will not be re-installed.

5. Select a register from the *Packages* list.
6. You can optionally select a subset of machines from the *Computers* list.
7. Click **INSTALL** to start the deployment.
8. If the installation requires a reboot of the client computers, the *Install/Uninstall/Reboot Options* dialog is displayed. Select the options that you decide are appropriate and then click **OK**.

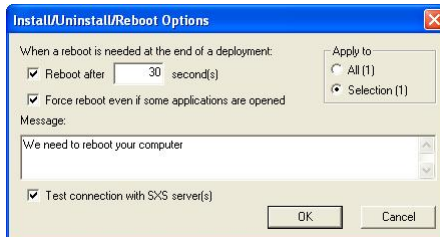


Figure 85: Sanctuary client deployment: reboot options

You can choose to require a reboot of the client computers after a defined period. You can also enter a text to be displayed to your users.

If a subset of machines was selected from the *Computers* list, the *Apply to* options allow you to choose if you want to target only the selected set of computers (*Selection*) or the complete list (*All*).

The *Test connection with SXS servers* option allows you to verify that the application servers defined in the package are up and running before proceeding to the deployment on the client computers. It is a safe precaution to check this option unless you want to do an installation with no servers – optionally controlling the policies with the *policies.dat* file. See *The installation procedure* on page 64 for more information



If the clients are installed while the SecureWave Application Servers are unavailable, they will not be able to obtain the permissions – unless they are included with policies.dat – and access to the applications/devices will be refused.



By default the client computers are not rebooted at the end of the client installation to avoid interference with the users. However, the client installation requires a reboot – even though the client is installed, it only delivers complete functionality after a reboot. The client un-installation also requires a reboot – the client driver stays active until the computer is rebooted.

When you have clicked OK, the *Sanctuary Client Deployment* dialog is displayed indicating the progress of each client installation.

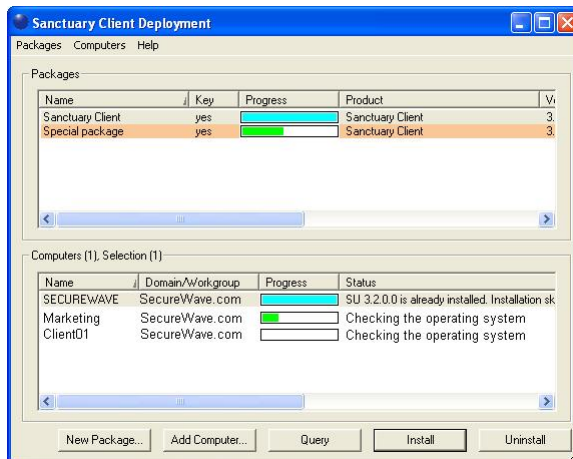


Figure 86: Sanctuary client deployment: installation progress



9. During the deployment, the dialog displays the status for each computer. The progress of the deployment is shown on the status bar, and the color of the progress bar indicates different conditions of the task as shown in the following table:





Color		Description
Turquoise		Task completed successfully.
Green		Task in progress with no warning.
Yellow		Task in progress or completed with warnings.
Red		Task in progress or stopped with an error.

Table 5: Task progress color code

The status column gives you information on the deployment progress for every machine. It reports the error or the warning message when the deployment did not succeed. If the error message reported does not allow you to find the cause of the problem (unknown error, hexadecimal error code – often 0x00000643), highlight the computer in the list and select *Open Last Log* from the *Computers* menu – or from the contextual menu. The MSI verbose setup log file displayed should contain information on why the setup was aborted and rolled back. You can contact SecureWave's Technical Support Department for further help in analyzing the log file.

Here are some common mistakes to avoid:

- Trying to deploy a client package with a different *sx-public.key* file than the SecureWave Application Server (Unspecified error)
- Trying to deploy a package while the SecureWave Application Server is offline or cannot be contacted (firewall, wrong IP address) or/and you did not export permissions in *policies.dat*
- Trying to deploy a package on a machine where the client has just been removed without a reboot in between. You must reboot the client machines after uninstalling

The dialog also displays a progress bar for the package being deployed. This progress bar has a mix of green, turquoise, yellow, and red indicating the clients at the various stages of deployment. The progress bar color changes to Turquoise when all tasks are completed successfully as shown. The dialog will eventually have all progress bars filled with diverse colors depending on the result of the different tasks.

When the deployment to a client computer is complete, it displays a *System Shutdown* dialog if necessary, as shown below. The message displayed is the one you typed on the *Install/Uninstall/Reboot Options* dialog.

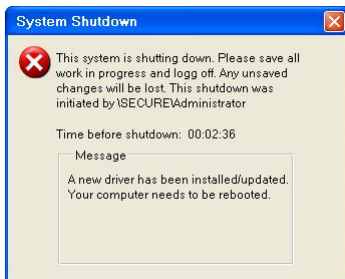


Figure 87: Sanctuary client deployment: shutdown dialog in client computers

Using the command-line to install the Clients

If you already own a software deployment tool that you want to use instead of using our visual interface, follow these steps:

1. Create a Deployment package as explained in *Installing Sanctuary Client: MST file generation* on page 103.
2. Copy the whole Deployment package folder to a local directory on the server (referred to as `DEPLOY`) from which the client is to be deployed. This directory should normally contain at least one file with the `msi` extension, one file with the `mst` extension, one `sx-public.key` file, one or several files with a `cab` extension, and some other files.
3. You can install the Sanctuary Client on a list of computers by using your favorite software deployment tool to run this command-line:

```
Msiexec /i "Sanctuary Client.msi" /qn TRANSFORMS="Sanctuary Client.MST" /L*v %TMP%\setupclt.log
```

 *The command above should be typed all on one line.*



Using Windows Group Policy to install the Clients

The following procedure describes implementing a computer based Group Policy for all computers in the secure.com domain. Group Policies can be applied to Site, Domains, or Organizational Units depending your requirements, and the types of computers they contain.

This example is used for demonstration purposes only and its application (domain or Organizational Unit or site) will differ according to individual requirements. The *Group Policy Management Console* (GPMC) has superseded the *Active Directory Users and Computers* dialog for Windows 2003 and XP (see following image).

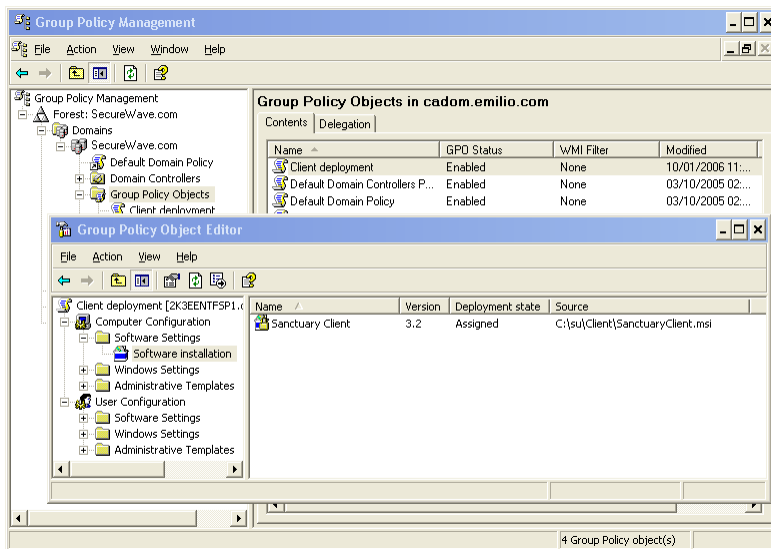


Figure 88: Using the Group Policy Management Console to install clients



As with all major changes to Group Policy, it is recommended that any new Policy or changes to existing ones are tested on a development Organizational Unit first before implementing in a production environment.

1. Create a Deployment package as explained in *Installing Sanctuary Client: MST file generation* on page 103.



2. Copy the whole Deployment package folder to a local directory on the server (referred to as `DEPLOY`) from which the client is to be deployed. This directory should normally contain at least one file with the `msi` extension, one file with the `mst` extension, one `sx-public.key` file, one or several files with a `cab` extension and some other files.
3. Select *Programs* → *Administrative Tools* menu to display the *Active Directory Users and Computers* dialog.

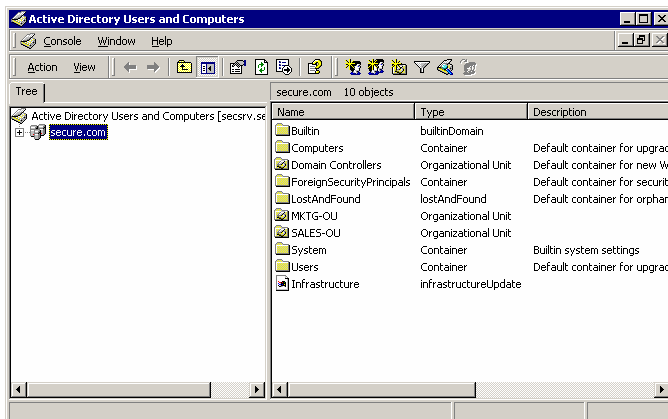


Figure 89: Deployment package using group policies: select active directory

4. Right-click the Domain (or Organizational Unit) and select *Properties*.
5. Select the **GROUP POLICY** tab.

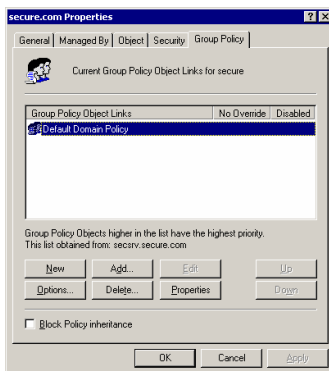


Figure 90: Deployment package using group policies: select group policy



6. Click **NEW** to create a new Group Policy, and click **EDIT**.
7. Expand *Software Settings*.

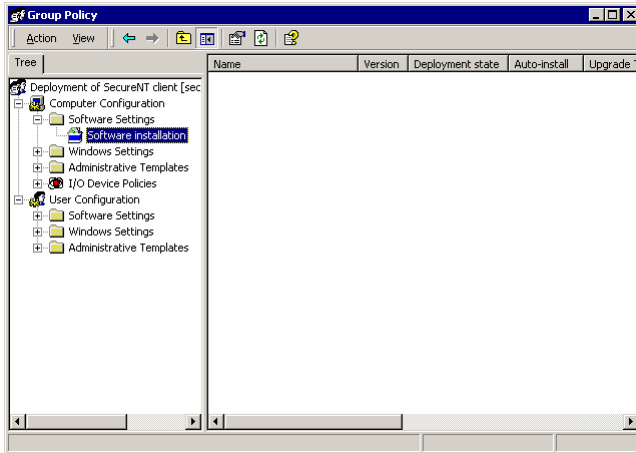


Figure 91: Deployment package using group policies: software installation

8. Right-click **SOFTWARE INSTALLATION** and select *New* → *Package*
9. Browse to **Deploy**, and select *Sanctuary Client.msi*, then click **OPEN**.
10. In the *Deploy Software* dialog box, select *Advanced published or assigned* and click **OK**.

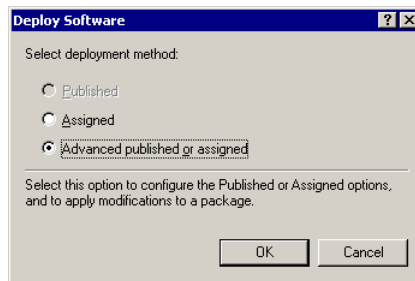


Figure 92: Deployment package using group policies: deployment type

11. Accept the default name of 'Sanctuary Client'. Click on the *Deployment* tab. Ensure *Assigned* is selected.

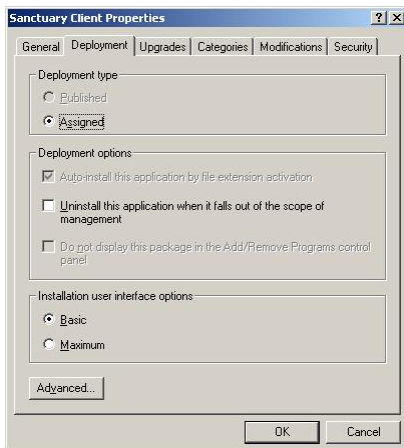


Figure 93: Deployment package using group policies: deployment options

12. Display the *Modifications* tab and click **Add**.
13. Browse to `Deploy\Sanctuary Client.mst`. Click **Open**.
14. Click **OK**.

A new computer-based policy that will install the Sanctuary Client driver with the configuration settings chosen as described above will be installed for all computers at boot up time (prior to client logon). A reboot will be required after installation before the software becomes fully effective.



Chapter 11: Using the SXDomain Command-line Tool

The information in this chapter applies to all Sanctuary software suite products.

This chapter explains how you can synchronize domain information with that contained in the SecureWave Sanctuary Database.

Introduction

The SXDomain command line tool is an alternative to the Add Domain / Synchronize Domain items in the *Tools* menu on the Sanctuary Console. It is used for the following purposes.

- > To add new domains to the list of those managed by Sanctuary
- > To add and update information about users, groups and computers in a domain already managed by Sanctuary
- > To add/synchronize local users and groups
- > To add/synchronize computers that are part of a workgroup.

SXDomain.exe can be found within the following directory:

'C:\Program Files\SecureWave\Sanctuary\SXTools'

(Assuming that you installed the Sanctuary software under 'C:\Program Files'.)

Use the command prompt to run the file from this directory.

The SXDomain parameters

The SXDomain command line should be entered as follows:

```
SXDomain [-s servername] domain1 [domain2 ...]
```

The parameters in this command line are defined below:



Parameter	Description
<code>-s servername</code>	The fully qualified domain name or IP address of the computer on which SXS is running.
<code>-i</code>	Instructs the utility to read domain names to add or synchronize from standard input stream.
<code>-e</code>	Instructs the utility to write the domain names that could be neither added nor synchronized to standard error stream.
<code>-u username</code>	The user name used to authenticate on the remote computer.
<code>-p password</code>	Password. SXDomain will prompt you for one if not supplied.
<code>-q</code>	Do not prompt for user name or password if cannot authenticate.
<code>domain</code>	The name of the domain(s) or computer(s) that you want to add or refresh.

Table 6: SXDomain parameters

Examples

For the following examples:

- > `SXS_SERVER` is the name of the computer running SecureWave Application Server.
- > `CLIENT` is the name of the computer running Sanctuary Client.

To refresh the domain information for the domain `DOMAIN`, use the following command.

```
SXDOMAIN -s SXS_SERVER DOMAIN
```

To refresh details of the local users of the computer `CLIENT`: (which can be a domain controller in case it does not show up after its domain was added)

```
SXDOMAIN -s SXS_SERVER CLIENT
```

To refresh details of the local users of the computer `CLIENT`, where `CLIENT` is part of a workgroup rather than a domain. The username and password of the computer's local administrator should be used in the command.

```
SXDOMAIN -s SXS_SERVER -u username -p password CLIENT
```



*Windows XP has by default the "Simple file sharing" option set. This option essentially turns the computer into "anonymous access only", preventing SXS to retrieve its local users. If it is set, turn it off using the **TOOLS** → **OPTIONS** dialog of the Windows Explorer.*

To synchronize a number of domains you can enter the names into a text file (one name per line of text) and supply it as input to the utility as shown below.

```
SXDOMAIN -s SXS_SERVER -i < mydomains.txt
```

You can also redirect the names of any domain that failed to synchronize to a file by means of the standard error stream.

```
SXDOMAIN -s SXS_SERVER -i -e < mydomains.txt > error_list.txt
```

Scheduling domain synchronizations

You can schedule domain synchronizations with your favorite task scheduler. Here is a procedure using the Windows Tasks Scheduler.

In the `C:\PROGRAM FILES\SECUREWAVE\SANCTUARY\SXTTOOLS DIRECTORY`, you should create a batch file `sxsynch.bat` containing the following line:

```
CMD /C SXDOMAIN -s SXS_SERVER -i -e < mydomains.txt >
error_list.txt
```

The `mydomains.txt` file holds the names of the domains to synchronize (one name per line of text). The list of domains that failed to synchronize is redirected to the `error_list.txt` file.

1. Go to the *Control Panel*, choose *Scheduled Tasks* and then *Add Scheduled Tasks*. The following screen is displayed.



Figure 94: Scheduled task: first step



2. Click NEXT.
3. In the following screen, click BROWSE and select the `sxsync.bat` file:



Figure 95: Scheduled task: select program

4. In the next two screens, choose the desired period:



Figure 96: Scheduled task: select period (1/2)



Figure 97: Scheduled task: select period (2/2)



5. Once you choose the period, specify an account that has rights to use the Sanctuary Console. This is the account that will run the `sxdomain` command:



Figure 98: Scheduled task: select account

6. Click **FINISH** to end the Wizard:



Figure 99: Scheduled task: ending the wizard



It is important to synchronize domains in order to have 'fresh' information available. If you do not do this in a regular basis, you could have bad surprises when some users or domains do not appear in your database.



Chapter 12: Registering your Sanctuary Product

The information in this chapter applies to all Sanctuary software suite products.

This chapter explains what happens when you register your Sanctuary product. It provides examples of information contained in a typical license file.

Licensing

Each Sanctuary Server has a license file that specifies whether you have a valid copy of one or several of our Sanctuary programs: Sanctuary Server Edition, Sanctuary Device Control, etc. Depending on the type of license, your client computers will show or not those options appropriate to each one of the installed programs. The following image was taken in a network that has Sanctuary Device Control and Sanctuary Custom Edition installed.

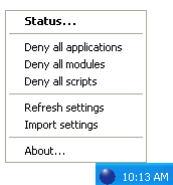


Figure 100: Client's options when several Sanctuary products are installed

If the license information changes – expires, a new product of our suite is added, etc. – the client would be informed and its options changed accordingly.

This section describes how to obtain a license, its location, and format.

Obtaining a license

Evaluation license

You can obtain an evaluation license by registering on the SecureWave website www.SecureWave.com. From there, select the product page for the Sanctuary product you want, and then select *Evaluation Request*. Fill out the Evaluation License Request form. Once your request is approved, you will receive a copy of the license file – save it into the %SYSTEMROOT%\SYSTEM32 directory.



An evaluation license provides you with the full functionalities of Sanctuary software, but with the following limitations:

- > A running duration of one month
- > No more than 10 SecureWave Application Servers can be installed in parallel
- > No more than 100 client computers can be administered

Full license

When you purchase one of our Sanctuary products, a new license key will be sent to you by e-mail. This license key will be specifically configured to conform to the license you have purchased. You do not need to uninstall the software when switching from an evaluation license to a full license. The Application Server (SXS) will use the new license file within an hour. If you want SXS to use the new license file immediately, you should restart the SXS service on every application server machine where the new license file was copied.

License file location

When you receive the license file, copy it to the %SYSTEMROOT%\SYSTEM32 folder of each computer that will run SecureWave Application Server (SXS). It is *not* required to be present on client machines.

License file format

A Sanctuary license file consists essentially of a series of name and value pairs, one per line.

You find, among others, the following important information in your license file:

Key	Value
<i>ProjectName</i>	Identifies the software product for which the license is valid.
<i>ExpiryDate</i>	Validity of the license file.
<i>LicensedClients</i>	Number of clients that can be registered in the Database. This corresponds to the sum of the number of computers where Sanctuary Clients are used.
<i>LicensedSessions</i>	This limits the number of sessions that SXS will allow. Exceeding this limit only causes warnings to be displayed. A session, in this context, refers to a 'logon session'. Such a logon session is created for every interactive logon of a user on a Sanctuary protected computer. Logon sessions are also created for services that run under a 'real' user account (as opposed to LocalSystem), and under certain



Key	Value
	circumstances by some server programs (mail, web, FTP servers, etc.).
<i>LicensedServers</i>	Number of instances of SXS that may be run at the same time. SXS refuses to start if it detects a number of already running SXS instances exceeding this limit.
<i>ProductName</i>	The full name of the product for which the license was created.
<i>ClientName</i>	The name of the customer to whom the product was licensed.
<i>GeneratedOn</i>	The date on which the license was created. Useful if you are unsure when to renew your maintenance contract.
<i>Serial#</i>	The serial number of this license.
<i>LicensedTo</i>	The name and/or email address of the person to whom the license was issued.

Table 7: License file format



Modifications to a license file – even just changing or adding a comment or blank line – could result in refusing access to devices and programs in your client computers.

Every computer protected by Sanctuary Client registers itself in the online table of the SecureWave Application Server during the boot sequence of the client. Counting these entries gives the number of 'clients'. This licensing mode is ideal for corporate environments where there is essentially one user per computer.

In ASP and Terminal Services environments, one computer may support hundreds of users. In these situations, the license is expressed in terms of 'sessions', a session being created when a user logs on and removed when a user logs off. Inaccuracies are created by services (programs that run unattended in the background), if the administrator has configured them to run with the identity of a regular user instead of LocalSystem, and by server software that verifies the identity of its users by simulating a logon. An example would be IIS with password protected pages. In addition to that, users may create additional sessions through the use of secondary logon services ('runas' command in Windows 2000/XP/2003).

In either case, SecureWave adjusts the actual license limits to account for those requirements.



License-related SXS actions at start-up

On start up, SXS immediately verifies the license file. If any of the following conditions is true, SXS quits directly:

- > The license is invalid (has been tampered with or is missing).
- > The project name is invalid.
- > The product expiry date has been surpassed
- > The number of licensed servers has been exceeded

No other license related conditions cause SXS to refuse to start.

License-related SXS actions while running

Once every hour, or thereabouts, SXS verifies the license file. This means that an upgrade to a more permissive license is done by simply copying the new license file over the old one.

SXS terminates if the license file is missing, has been tampered with, the project name is invalid, or the expiry date is exceeded for more than seven days.

If any of the following license-related conditions are true, SXS logs a message when running interactively:

- > The expiry date has passed
- > The *LicensedCPUs* value is less than the number of processors installed in the computer
- > The *IPAddress* key does not list at least one IP address belonging to the computer
- > The *LicensedClients* value has been exceeded
- > The *LicensedSessions* value has been exceeded
- > The *LicensedServers* value has been exceeded



License-related Client actions

The client applies licensed Sanctuary policies immediately even if they have not been correctly configured or defined. For example, if no proper application permissions have been set in Sanctuary Custom Edition, the client blocks all attempt to execute programs in the machine, even the logging program, with fatal consequences. Not configuring device permissions for Sanctuary Device Control will apply the most restrictive policy: no access to external devices.

An upgrade may surprise your clients when you install a license for several products but only one is active. The client shows 'unused' options.

Likewise, the client will cease to apply Sanctuary policies if not licensed. This will affect only those customers violating the license, but can also be a result of incorrect license management and can represent a security risk for your organization.



Appendix A: Troubleshooting

The information in this appendix applies to all Sanctuary software suite products.

This appendix provides answers to some of the problems users may encounter during setup and initial operations.

The Administrator's Guide also provides further troubleshooting techniques.

Contacting SecureWave Support

If you have a problem not covered by this guide, then you can contact SecureWave Technical Support by sending an email to support@SecureWave.com. Make sure that you include the following information:

1. A description of the problem, as complete as possible, including details of the circumstances when the problem occurred. Please visit our Knowledgebase on www.SecureWave.com to get more details on how to obtain the necessary technical information.
2. The exact version of the Sanctuary product you are using. This can be found if you open the Sanctuary Console, select the *Help* menu, and then select *About*. You can copy the "Version information" directly from the dialog and paste it into your email.

Troubleshooting Tips

Check that SecureWave Application Server is running

You may need, from time to time, to ensure that the SecureWave Application Server is running. This task can be achieved in a number of ways as shown below:

1. Using `SC.EXE` from the resource kit.

`SC.EXE` allows you to query the status and configure systems services.

```
C:\>sc query sxs
```

```
SERVICE_NAME: sxs
                TYPE               : 10  WIN32_OWN_PROCESS
                STATE                : 4   RUNNING
```

```
(STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
                WIN32_EXIT_CODE      : 0   (0x0)
```



```
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT         : 0x0
WAIT_HINT          : 0x0
```

2. Using the 'services' control panel applet.

Under Windows 2003, select *Start* → *Programs* → *Administrative Tools* → *Services*. Under Windows 2000, select *Start* → *Control panel* and choose *Administrative Tools* and then *Services*. Scroll down the list to SXS and check its status.

3. Using the Sanctuary Console.

A simple method to check that the server is running properly is to use the Sanctuary Console and try to connect to the server in question.

Client driver ignores updates from server

There can be a number of causes of this problem:

1. Mismatched keys between the server and the client.
2. Server not running (or not reachable).
3. IP address of server has changed.
4. Client computer not in the server's online table.

Looking at each cause in turn:

1. The key pair generation should be carried out only once to ensure that there is only one key pair in the company as the files look identical and they can easily be mixed up. If the public key on the client does not match the private key on the server then all updates will be ignored. The safest solution is to use on the client a copy of the `sx-public.key` file that is on the `%SYSTEMROOT%\SYSTEM32` of the computer running the SecureWave Application Server.
2. The server may not be running and the client loads cached data from its local cache. Check that the SecureWave Application Server is running.
3. If you change the IP address of the server and fail to update the clients then they will not be able to pick up any changes from the server. There are a number of solutions:
 - > Set the address back to what it was when you first installed the Sanctuary component



- > Change the client's IP address located in the 'Servers' registry key (see Appendix C)
- > The key can also be changed at logon with group policies or by setting the *SecureWave Application Server Address* field in *Default Options*, from the *Tools* menu in the Sanctuary Console



The Default Options dialog applies to all computers. You could also make changes to the registry and set directly the key to hold more than one address (one per SecureWave Application Server).

4. When the computer is not in the SXS online table, the easiest way to correct this is to ask the client to logoff and logon again on his computer. If this does not work, he can eventually reboot his computer. If this does not work, it means that there are most probably communication problems between the server and the client.



You can use the application called `PingSXS.exe` that is located in the `BINTools` subfolder of the Sanctuary CD. Running this application on the client would tell you more information on what goes wrong.

5. Check if the firewall is not blocking the required ports – especially if you install one of the allowed components in Window XP or 2003 SP1. Please read section *Appendix E: Installing Sanctuary on Windows XP SP2/2003 SP1* on page 155 for more information.

Database backup

This section lists important points about carrying out a database backup with Microsoft SQL Server and MSDE.

Microsoft SQL Server backup

- > You can refer to Microsoft SQL Server documentation for guidelines on how to backup a database.
- > Ensure that your backup software is capable of performing live Microsoft SQL Server database backups before attempting a live backup. Please consult your backup documentation regarding live SQL backups. If your backup software is capable of performing live Microsoft SQL Server database backups, it is most probably also capable of performing live MSDE backups.
- > Ensure that both 'sx' and 'master' databases are backed up.



- > If the backup software cannot handle live SQL backups, then an SQL dump to disk of the databases 'sx' and 'master' can be performed, and then archived onto tape (or other backup media) as part of the regular server backup. Please refer to the following *MSDE 2000 backup* section.

MSDE 2000 backup

The Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) is a data engine built and based on core SQL Server technology. It does not have its own user interface (UI) or tools. It is built into the SecureWave Application Server Setup and is redistributed royalty-free. As it does not have its own tools for backup, unlike Microsoft SQL Server, we recommend the use of a script-based solution for the backups.

1. Before you start the backup, stop the SecureWave Application Server(s):

```
net stop sxs
```

2. As MSDE 2000 does not ship with any UI interface, `osql.exe` is the only available tool for running SQL queries against the database.

The files and paths to be backed up (mdf path, ldf path) can be determined by running the following SQL query against the sx database. Save the following script as Files.sql

```
USE sx
GO
SP_HELPFILE
GO
```

3. Run the following command:

```
Osql -E -d master -s ^| -w 1000 -i Files.sql -o Output.txt
```

4. Open the Output.txt file produced by this command. It contains the locations of the DB files (sx.mdf and sx.ldf). Usually, these are located in:

```
C:\Program Files\Microsoft SQL Server\MSSQL\data\sx.mdf
C:\Program Files\Microsoft SQL Server\MSSQL\data\sx.ldf
```

5. Detach the sx database from the database engine. Save the following script as Detach.sql

```
USE master
GO
SP_DETACH_DB 'sx'
GO
```



6. Run the following command:

```
Osql -E -d master -s ^| -w 1000 -i Detach.sql -o Output.txt
```

If the following error message is produced in `Output.txt`, then it usually means that some SecureWave Application Servers (sxs) services were not stopped:

```
Server: Msg 3701, Level 16, State 1, Line 1  
Cannot detach the database 'sx' because it is currently in  
use.
```

7. Once the database is detached, you can copy the files `sx.mdf` and `sx.ldf` to the backup media.

8. Once the files are copied, you can attach the `sx` database to the database engine. Save the following script as `Attach.sql`:

```
USE master  
GO  
SP_ATTACH_DB 'sx', 'mdf path', 'ldf path'  
GO
```



'mdf path' and 'ldf path' are the full pathnames obtained in step 4.



The `SP_ATTACH` line should be in one complete line.

9. Run the following command:

```
Osql -E -d master -s ^| -w 1000 -i Attach.sql -o Output.txt
```

10. Restart the `sxs` service:


```
net start sxs
```




SecureWave Application Server backup

The backup of the application server is straightforward. Backup the following files, directories and registry keys:

1. The public and private keys: `sx-private.key` and `sx-public.key`. These are located in either `%SYSTEMROOT%\SYSTEM32` or `%SYSTEMROOT%\SXSDATA`
2. The license key `SecureWave.lic`. This is located in either `%SYSTEMROOT%\SYSTEM32` or the directory where `SXS.EXE` is located.
3. The `datafile` directory. Its location can be determined from the value of the registry parameter:
`HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\SXS\PARAMETERS\`
`"DATAFILEDIRECTORY"`
4. The registry key with all its associated values:
`HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\SXS\`
5. The contents of the directory `%SYSTEMROOT%\SXSDATA`.

 *This list does not include SecureWave application binaries since these can be reinstalled for the original CD if corrupted or lost.*

 *The storage*. * files, found in the `%SYSTEMROOT%\SXSDATA` directory, can be discarded without backup (they are regenerated each time the SXS service starts).*



Appendix B: Detailed System Requirements and Limitations

The information in this appendix applies to all Sanctuary software suite products unless otherwise specified.

This appendix specifies the minimum system requirements for the different computers used in a Sanctuary implementation and details the limitations of installing the Sanctuary Clients on Terminal Servers and Citrix environments.



Windows NT4 is no longer supported. SecureWave Application Server's client cannot be installed on Windows XP or Windows 2000 Pro.

System requirements

The following table specifies the minimum system requirements for the different computers used in a Sanctuary implementation.

	SecureWave Application Server	Database	Admin Tools	Client
Operating system:	Windows 2000 (Service Pack 4 or later) Server or Windows Server 2003	Windows 2000 (Service Pack 3 or later) Server or Professional, Windows XP Professional, Windows Server 2003	Windows 2000 (Service Pack 3 or later) Server or Professional, Windows XP Professional, Windows Server 2003	¹ Windows 2000 (Service Pack 3 or later) Server or Professional (not for Sanctuary Server Edition), Windows XP Professional (not for Sanctuary Server Edition), Windows Server 2003
Hard disk space:	5 Mb free disk space for program files and 15 Mb for the installation	5 Mb free disk space for program files, 40 Mb for the installation, and 20 Mb+ for data (depends on the number of users)	10 Mb free disk space for program files and 15 Mb for the installation	2 Mb free disk space for program files and 15 Mb for the installation
Memory:	128 Mb (256 Mb recommended)			

¹ There are limitations to the installation of the Sanctuary Client on Terminal Server, as described in the next section.



	SecureWave Application Server	Database	Admin Tools	Client
Display resolution:	Not applicable		1024x768	Not applicable
File System	NTFS			
Other:	MDAC V2.6 SP1.	Microsoft SQL Server 2000/2005 or MSDE 2000 (requires IE 5.0 or later) MDAC V2.6 SP1.	Internet Explorer 5.0 or later. Adobe PDF Reader v5.0 or later to consult the on-line manuals.	
Novell		LDAP and NDAP (for workstation objects synchronization)		Novell – and optionally ZENworks – client

Table 8: System requirements



If you plan to use encrypted devices – when installing Sanctuary Device Control –, you will need Active Directory and DNS installed and properly configured. The Microsoft Certificate Authority must be installed, properly configured, and published.



You can find the LDAP and NDAP components required for Novell synchronization in the installation CD or in Novell’s Web site.



For the Database installation, we strongly recommend that you install the latest Service Packs. You should not bring a database into use without installing at least MSDE 2000 or SQL 2000 SP4. Otherwise, your database is not protected against the slammer worm.

Sanctuary Device Control

Terminal services limitations

The Terminal Services administration mode and the remote desktop functionality allow access to computers remotely. This section details how the Sanctuary Client enforces security when devices are accessed remotely.

Sanctuary Device Control normally applies the permission of the user accessing the device, be it a remote user or the user working interactively with the computer. This is the case for the device classes for which the device access is performed in the context of the user who initiated the access: BlackBerry (USB), DVD/CD (READ



access), Com, LPT (NOT when used for printing), Palm OS Handheld Devices (USB), Removable, Tape, Unauthorized Encrypted Media, Windows CE Devices (USB).

Certain kinds of device access are not performed in the context of the user who initiated the access. Instead, a proxy that normally has privileged access to the system (a service or a driver) carries them out. DVD/CD WRITING is one example; there are a few other ones: modems, scanners, smart card readers, printers (either USB or connected to the LPT port) and unknown devices.

When the Sanctuary Client detects such 'proxy' access, it tries to determine the identity of the user who initiated the access. This is done successfully when there is only one interactive user.

When there is one interactive user and one remote user on the same computer (i.e., when there are more than one logon sessions with different session IDs), the client cannot determine reliably the identity of the user that initiated the access. In such conditions and only for the DVD/CD burning, modems, scanners, smart card readers, printers (USB or LPT) and unknown devices classes, the Sanctuary Device Control will deny all proxy access. It means for example that the users will not be able to write DVDs/CDs when somebody accesses their machine remotely even if both the interactive user and the remote user have a Read/Write access to the DVD/CD drive. The user accessing the machine remotely will not be able to write DVDs/CDs either.

The RunAs command limitations

There is a situation similar to the Terminal Services issue when using the RunAs Commands or equivalent. This type of command is often used in logon scripts.

Certain kinds of device access are not performed in the context of the user who initiated the access. Instead, a proxy that normally has privileged access to the system (a service or a driver) carries them out. DVD/CD WRITING is one example; there are a few other ones: modems, scanners, smart card readers, printers (either USB or connected to the LPT port) and unknown devices.

When the Sanctuary Client detects such 'proxy' access, it tries to determine the identity of the user who initiated the access. This is done successfully when there is only one interactive user. The user cannot be determined when there are active RunAs logon sessions.

When the Sanctuary client detects RunAs logon sessions, and only for DVD/CD burning, modems, scanners, smart card readers, printers (USB or LPT) and unknown devices classes, the RunAs Logon sessions are mapped to the interactive logon session with the same session ID. Thus, all RunAs processes will have exactly the same access as the interactive user who launched them. Using the RunAs command to change the level of access to these devices is not possible.



Example 1: Bill has no access to DVD/CD. John has Read/Write access to DVD/CD. If Bill uses a RunAs command to run the DVD/CD burning software under the credentials of John he will NOT be able to create new CDs. Bill will have to log off and log on as John to create new DVDs/CDs. Writing a DVD/CD requires a proxy, it is subject to the limitation described in this section.



The DVD/CD writing requires a proxy and is subject to the RunAs limitation, whereas reading a DVD/CD is not.

Example 2: Bill has no access to the Floppy. John has Read/Write access to the Floppy. If Bill uses a RunAs command to run the Windows File Explorer under the credentials of John he will be able to read and write to the Floppy. Indeed, access to the Floppy is done without a proxy. The limitation described in this section does not apply.



Appendix C: Registry Keys

The information in this appendix applies to all Sanctuary software suite products.

SecureWave Application Server registry keys

The following table contains details of each registry key entry used for SecureWave Application Server (SXS). All the SecureWave Application Server entries are of type REG_SZ (= string value). The entries in the following table are found within the following key:

`HKLM\system\CurrentControlSet\services\sxs\parameters`

Key Name	Description	Default
AdoVersion*	A string representing the version of ADO objects to use. Default: "". For Windows 2000, try ".2.5". Note that the leading dot must be present, unless an empty string is given.	""
Concurrency*	How many running threads are allowed by the IOCP. "0" (zero) means "auto" and is equivalent to one thread per CPU. Minimum: 0; maximum: MaxThreads.	"0"
CommVer	The application server (SXS) uses this key to determine which communication protocol version it should use. "0" (zero) indicates that there are still older version of the client in use (prior to v3.1) while "1" is used when the installation only has clients v3.1 or later.	"1"
DataFileDirectory	The base directory under which SXS will store data files (log files, for instance). If multiple SXS servers are in use, their DataFileDirectory entries must all resolve to the same directory on disk. This is the directory created during the Database setup process.	"."
DbConnectionCount	The number of database connections in the connection pool.	"20"
DbConnectionString	Driver, server, database, and either a trusted connection, or username and password. Default value is as follows. "Provider=sqloledb;Data Source=;Initial Catalog=sx;Trusted_Connection=yes;"	See Description cell
DbInitializationDelay*	Number of seconds that SXS will wait before contacting the SQL Server	"300"
Debug*	If "yes" or "1" and if SXS runs as a service, it will attempt to launch a debugger and attach it to itself.	"no"
Log file name	Gives the name of the log file written if "Log to file" is true.	"sxs.log"



Key Name	Description	Default
Log to console	If "yes" or "1", sends debug messages to the console, if any.	"no"
Log to dbwin	If "yes" or "1", sends debug messages to Dbwin32.	"no"
Log to file	If "yes" or "1", sends debug messages to the log file (see the Log file name entry).	"no"
LogMonitorDlls	Not used for SDC. Key used by <i>Spread Check</i> . If configured, it would also monitor the spread of DLLs that have been authorized implicitly in the <i>DLL don't care</i> mode. If not configured, only applications and explicitly authorized DLLs are monitored. Please see <i>Chapter 3</i> of the Administrators' Guide for more details	"no"
LogMonitorResetOptions	Not used for SDC. Controls whether the global user option is set to blocking mode when the alert is generated; if "no", SXS only issues a message in the event log; if "yes", it issues the same message, sets and pushes the option, and then issues another event log message informing if the set+push was successful.	"yes"
LogMonitorPeriod	Not used for SDC. Period, in seconds, between two checks.	"300"
LogMonitorThreshold	Not used for SDC. Number of distinct users that must execute the same locally authorized executable for an alert to be issued.	"10"
MaxSockets*	The maximum number of TCP connections that are allowed at any one time. The length of the listen queue backlog imposes an additional constraint. This queue holds connection requests that cannot be accepted because SXS is momentarily busy or because it has reached the limit imposed by MaxSockets. SXS always sets the length of the listen queue backlog to the maximum (5 on Home/Professional editions of Windows, 200 or more on the Server editions). Note that this entry does not control connections to the RPC server in SXS; see "MaxRpcCalls" for that. Minimum: 1; maximum: 50000 (arbitrary).	"5000"
MaxThreads*	The total number of worker threads at the disposal of the IOCP. Minimum: 1; maximum: 64 (MAXIMUM_WAIT_OBJECTS).	"64"
Port	The TCP port on which the socket-based SXS server listens for new connections. Minimum: 1; maximum: 65534. This affects only client drivers. The port used by the RPC server (for administration clients) is controlled by the "Protocols" setting. Minimum: 1; maximum: 65534.	"65129"
Products	Internal use. Do not modify.	3



Key Name	Description	Default
RpcProtectionLevel	<p>Determines whether the RPC server will require RPC clients to identify (authenticate). Valid levels are:</p> <p>"0": Instructs the OS to pick a protection level. At the time of this writing, this is equivalent to "2".</p> <p>"1": No protection. Should not be used except for testing.</p> <p>"2": The client's identity is verified when he connects to SXS. RPC messages are vulnerable to tampering and man-in-the-middle attacks.</p> <p>"3": For the connection-oriented protocols (TCP, for instance), same as "4". For connectionless protocols (UDP), this level ensures that a client's connection cannot be hijacked at the request level.</p> <p>"4": Examines client credentials not only once per request (like "3") but with every single packet.</p> <p>"5": Like "4", with added cryptographic signing of every packet to defend against tampering.</p> <p>"6": Like "5", but also encrypts data in both directions.</p> <p>Recommended setting: at least "5". Note that any setting except "0" requires that the client be in the same domain as the server, or in a domain that is trusted by the server's domain.</p>	"6"
SndPort	The TCP port on which the Sanctuary Client is expected to listen. If absent or zero, 33115 is used. Minimum: 1; maximum: 65534.	"33115"
SxdConnectTimeoutMSec	The time, in milliseconds, that SXS will wait for the Sanctuary Client to accept a TCP connection. It is useful to keep this time as low as possible, but not so low as to impede connectivity. In a lightly loaded LAN, one second (1000 ms) should be quite ample. The value should be between 500 and 120,000 ms if it is out of these limits, the default value (5,000 ms) is used instead.**	"5000"
SxdPort	The TCP port on which the Sanctuary Client's built-in server is expected to listen. If absent or zero, 33115 is used. Minimum: 1; maximum: 65,534.	"33115"
VerboseSyncLogging	If set to "yes", the SecureWave Application Server will log all the important attributes of the objects that it retrieves during a domain synchronization. In order to see the results in the sxs log file, the Log to file value must be set to "yes". If the Log to file value is already set to "yes", you do not need to restart the SXS service to take the VerboseSyncLogging Value into account. You should not set this option to "yes" permanently for performance reasons.	"no"




Key Name	Description	Default
 Keys whose names are marked with an asterisk * should not be modified except under the supervision of SecureWave Support personnel.		
** See note on next section.		

Table 9: Application Server registry keys (1/2)

The entries in the table below are found within the following key:

HKLM\system\CurrentControlSet\Services\EventLog\Applications\sxs

Key Name	Description	Default
EventMessageFile	Path and file name of SXS.EXE	
TypesSupported	Supported message for the event log. 0x10 for AUDIT_FAILURE and 0x08 for AUDIT_SUCCESS (value is of type REG_DWORD). You can combine the values in a hexadecimal addition. The default value (0x1F) stands for: register all type of messages (error, warning, information, etc.): 0x00 Success 0x01 Error 0x02 Warning 0x04 Information 0x08 Success 0x10 Failure	0x1F

Table 10: Application Server registry keys (2/2)

Sanctuary Client registry keys

The changes to the registry values are only effective after a reboot of the client computer.

- > SCC – Sanctuary Command Control – is in charge of all communication between server and client(s). Its keys are located in:
 HKLM\system\CurrentControlSet\Services\scom\parameters

The following table contains details of each registry key entry for SCC:



Key Name	Type	Description	Default
ImportDir	REG_SZ	The directory used to import the encryption key.	C:\Program Files\SecureWave\Sanctuary\Import
LastShadowUploadTime	REG_SZ	Indicates the last time the shadow update was done. The update consists on copying the file data or name, depending on the shadowing rule, from the client computers.	
LastSxLogUploadTime	REG_SZ	Indicates the last time logs were transmitted.	
Log file name	REG_SZ	Gives the name of the log file written if "Log to file" is "yes".	"scomc.log"
Log to console	REG_SZ	If "yes" or "1", sends debug messages to the console, if any.	"no"
Log to dbwin	REG_SZ	If "yes" or "1", sends debug messages to Dbwin32.	"no"
Log to file	REG_SZ	If "yes" or "1", sends debug messages to the log file (see below).	"no"
Servers	REG_SZ	A list of SXS server names or IP addresses, separated by spaces. A port number may be specified for any server by appending a colon and the port number to the name/address of the server (e.g. "10.34.22.16:65129 sxs.example.com:65130").	Those defined during the client installation
LastSeenComputerName	REG_SZ	Internal use. Do not modify.	
ServersOverride	REG_SZ	Internal use. Do not modify.	
HID*	REG_SZ	Internal use. Do not modify.	
FirstServer (optional)	REG_DWORD	If this is greater than or equal to the number of IP addresses in the list located on the Servers key, Sanctuary Client will pick a random server from the list. Otherwise, it uses this value as a zero-based index into the list. If a server cannot be contacted, the next one is used, in a round-robin	



Key Name	Type	Description	Default
		fashion.	
HistoryPeriodSecs (optional)	REG_DWORD	Internal use. Do not modify.	
ShadowDirHistory (optional)	REG_BINARY	Internal use. Do not modify.	
Debug (optional)	REG_DWORD	Use for debugging purposes	3 (you must reboot in order to make it work)

Table 11: Client registry keys (1/2)

- > WLD is the Sanctuary Client's white list driver name. Its keys are located in: `HKLM\system\CurrentControlSet\services\sk\parameters`

The following table contains details of the major registry key entries for SK.

Key Name	Type	Description	Default value
Enum	Subkey	Contains device list	
Limits	Subkey	Copy limit settings (UpdateTime, CachedSize, etc.)	
EventLog	REG_DWORD	Internal use. Do not modify.	
FileLog	REG_DWORD	Internal use. Do not modify.	
Classes	REG_DWORD	Contains device names and permissions	
HistoryPeriodSecs	REG_DWORD	Internal use. Do not modify.	
ShadowDirHistory	REG_BINARY	Internal use. Do not modify.	
Debug	REG_DWORD	Use for debugging purposes	3 (reboot to activate)
Security	Subkey	Internal use. Do not modify.	
ComputerName	REG_SZ	Internal use. Do not modify.	

Table 12: Client registry keys (2/2)



Appendix D: Upgrading from previous versions


The information in this appendix is product specific.


If you are upgrading from an older version of Sanctuary Device Control, you should be aware that the upgrade process should always be done in this order:

1. Stop the SXS service.
2. Update the Database in your SQL server (SQL Server 7, SQL Server 2000, MSDE 1.0, or MSDE 2000).
3. Update all the SecureWave Application Server.
4. Update the SecureWave Management Console.
5. Finally, update all your clients.

 *Old SecureWave Management Consoles will simply refuse to communicate with a more recent SecureWave Application Server.*

 *A client update requires a reboot.*

 *If you update from older versions of Sanctuary, but you keep the old clients, application control permissions are NOT sent to them. You must consider updating these older clients as soon as possible.*

 *You must stop SecureWave Application Server(s) – using 'net stop SXS' from the command line prompt – BEFORE updating the database.*

To summarize, the upgrade is done in two broad phases: first, upgrade all server-side components – during this first phase, the new server-side components will have to work with the old client versions; second, deploy the new client upgrade packages – the client deployment phase may be organized in batches and may take several days to complete.

The server-side components have not been designed to communicate with old clients. You should also update them.



Sanctuary Device Control

Sanctuary installation routines can upgrade from Sanctuary Device Control version 2.8 and above. If you are running an older version, you should first uninstall the program completely before deploying the new server and client components.

✍ The server addresses you set on the Default Options dialog (Default & Computer options) are not kept if you are updating from Sanctuary Custom Edition v2.8. You should change them back to the correct value after installing this new version. See Chapter 8: Setting and changing options on the Administrator's Guide for more information on how to change these options.

Sanctuary Server Edition

Sanctuary installation routines support upgrading from SecureEXE 2.7.6. If you have a previous version, you should first uninstall it completely before deploying the new server and client components.

Upgrading SecureEXE Clients

You can upgrade the SecureEXE Client driver to Sanctuary Server Edition doing one of the following:

- > Running the SETUP.EXE file from the CLIENT folder of the Sanctuary Server Edition CD-ROM.
- > Deploying the SANCTUARY CLIENT.MSI and a SANCTUARY CLIENT.MST files as described in *Chapter 10: Unattended Client Installation* on page 103.
- > Running the Setup in command-line mode. Refer to *Chapter 10: Unattended Client Installation* on page 103 for more details on how to create a transform file (.mst extension):

```
msiexec /i "Sanctuary Client.msi" /qn TRANSFORMS="Sanctuary  
Client.MST" /L*v %TMP%\setupclt.log
```



Upgrading Server-side components

1. If you have installed the SecureWave Application Server on a different computer than the database, it is important that you stop the SXS service on that computer before upgrading:

```
net stop sxs
```

2. Run the `SETUP.EXE` file located on the `\SERVER\DB` folder on the computer where you installed the SecureWave Database.



You should do a database backup before proceeding with an update.

3. Run the `SETUP.EXE` file located on the `\SERVER\SXS` folder on the computer(s) where you installed the SecureWave Application Server.
4. Run the `SETUP.EXE` file located on the `\SERVER\SMC` folder on the computer(s) where you installed the SecureWave Management Console. Sanctuary Device Control will replace the SecureWave Management Console by the Sanctuary Device Control Console.



It is very important that you upgrade first the database, then the application servers and finally the Management tools. Furthermore, always upgrade server-side components before upgrading the clients.



Appendix E: Installing Sanctuary on Windows XP SP2/2003 SP1

The information in this chapter applies to all Sanctuary software suite products.

By default, Windows Firewall is enabled on computers that are running Windows XP SP2 or Windows 2003 SP1. Windows Firewall closes ports such as 33115 and 65129 that are used by Sanctuary Clients and Application Server to communicate over TCP. Sanctuary Clients that are trying to connect to the SecureWave Application Server will not be able to connect until an exception is set in Windows Firewall.

With these Service Packs, a number of changes have been made in the Remote Procedure Call (RPC) service that help make RPC interfaces secure by default and reduce the attack surface of Windows XP/2003. Sanctuary Consoles installed on Windows XP/2003 trying to connect to the SecureWave Application Server will not be able to do so unless the appropriate options are set.

Connection between SecureWave Application Server and the database

The SecureWave Application Server uses the MDAC (Microsoft Data Access Components) to connect to SecureWave Sanctuary Database.

ADO (Microsoft ActiveX Data Objects), the technology used by the Application Server, relies on a protocol called Tabular Data Stream (TDS). By default, TDS uses port 1433 for incoming database traffic.

When the Sanctuary Database is installed on a Windows XP SP2/2003 SP1 computer, make sure that the TCP port 1433 is opened. Please refer to *Configuring the firewall* on page 160 for details on how to configure Windows XP/2003.

You can preset the TDS port to another one during SQL Server setup (when you select the *Select Network Protocols* option). After you have installed SQL Server, you must rerun the setup program and select the *Change Network Support* option to change the TDS port.



If you want to use another port instead of the standard one (1433), you need to create an Alias. To do this, follow these steps:

1. Use the Client Network Utility command found in the *Start* → *Programs* → *Microsoft SQL Server* menu.
2. The *SQL Server Client Network Utility* dialog is displayed.
3. Choose the *Alias* tab.
4. Click on the Add button. The *Add Network Library Configuration* dialog opens.
5. Type in a name in the '*Server Alias*' field. If you are using Network Libraries, select the *TCP/IP* option.
6. Type in the *Server name* and change the port in the lower field (*Pipe name*) located on the right panel of the dialog (*Connection parameters*).
7. Click on the OK button to close the dialog and accept the new Alias.

During the setup process, you will need to provide this Alias instead of the SQL server name.

You can find more details, in the Microsoft knowledge base article "How Windows XP Service Pack 2 (SP2) Affects SQL Server and MSDE", available at Microsoft's Web site.

Connection between the console and the Application Server

A number of changes have been made in the Remote Procedure Call (RPC) service for Windows XP SP2/2003 SP1 that help make RPC interfaces secure by default and reduce the attack surface of Windows XP/2003. The most significant change is the addition of the *RestrictRemoteClients* registry key. This key modifies the behavior of all RPC interfaces on the system and, by default, eliminates remote anonymous access to RPC interfaces, with some exceptions.

The Sanctuary Console uses the RPC protocol to connect to the SecureWave Application Server.



Step 1: Configuring a fixed port on the Server

By default, SecureWave Application Server uses dynamic ports for the RPC communication with the Console. The ports change every time the Application Server is started, making it impossible to configure the firewall.

In order to be able to configure the firewall, it is mandatory to instruct the Application Server to use a fixed port. To do this, open *RegEdit* and set the following entry:

Key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\sxs\parameters

Name: Protocols

Type: REG_SZ

Value: "ncacn_ip_tcp[1234]"

1234 represents the fixed TCP port number that you want to use for the communication between the Consoles and the Application Server.

You should restart the SecureWave Application Server for the setting to take effect (net stop sxs / net start sxs)

Step 2: Opening the port on the Server Firewall

On the computer where the console is installed, open the chosen ports on the firewall. If you have the console installed on Windows XP/2003, please refer to *Configuring the firewall* on page 160 for more details.

Connecting to the Server using the fixed port

In the *Connect* dialog of the Sanctuary Console, specify the fixed port to use to communicate with the server, such as: secsrv.secure.com[1234]

Connecting using the Endpoint Mapper

If you do not want to specify the fixed port in the *Connect* dialog of the Sanctuary Console, it is possible to instruct the Console to retrieve the port in use directly from the Endpoint Mapper on the SecureWave Application Server.

In Windows XP SP2 or Windows 2003 SP1, by default, the RPC Endpoint Mapper interface (port 135) is not accessible anonymously. This is a significant security improvement, but it changes the task of resolving an endpoint.



Currently, an RPC client that attempts to make a call using a dynamic endpoint will first query the RPC Endpoint Mapper on the server to determine to which endpoint it should connect. This query is performed anonymously, even if the RPC client call is, itself, done using RPC security.

Anonymous calls to the RPC Endpoint Mapper interface will fail by default on Windows XP SP2 or Windows 2003 SP1 because of the default value for the RestrictRemoteClients key.

This makes it necessary to modify the RPC client runtime to perform an authenticated query to the Endpoint Mapper. If the EnableAuthEpResolution key is set on the client, the RPC client runtime will use NTLM to authenticate to the Endpoint Mapper.

Setting the EnableAuthEpResolution Registry Key will instruct the Sanctuary Console to use NTLM to authenticate to the Endpoint mapper and obtain what endpoint it should connect to on the Application Server.

You may also experience some authentication problems when running the Console on a computer with Windows XP SP2 or Windows 2003 SP1. The console displays an access denied popup message even when the correct credentials are specified. To fix this, the following key must be set on the Windows XP SP2 or Windows 2003 SP1 machines running the Sanctuary Console:

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\RPC

Name: "EnableAuthEpResolution"

Type: REG_DWORD

Value: 0x00000001

and

Name: "RestrictRemoteClients"

Type: REG_DWORD

Value: 0x00000000

Please follow this link for more details on those settings:

http://msdn.microsoft.com/security/productinfo/XPSP2/networkprotection/enable_authep_resolution.aspx

and



<http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/sp2netwk.mspx>



The Sanctuary Console setup will propose to create this key if it does not exist.



Operating systems prior to Windows XP SP2/2003 SP1 do not support the "EnableAuthEpResolution" key.

Summary

Connection string to use in the Sanctuary Console	Port to open on the SecureWave Application Server firewall	Protocols registry key on the SecureWave Application Server
MyComputer.MyDomain.com[1234]	1234	ncacn_ip_tcp[1234]
MyComputer	1234 + 135	ncacn_ip_tcp[1234]

Replace "1234" with the actual port you want to use for the communication between the Sanctuary Console and the SecureWave Application Server

Table 13: Communication ports in Windows XP

Connection between the client and the SecureWave Application Server

If you install the SecureWave Application Server and the client(s) on different machines, and you have a firewall between them (including Windows XP firewall, if applicable), the communication between them can be blocked.

The default ports used for the communication between the drivers and SecureWave Application server are the following ones:

- > The SecureWave Application Server listens on port TCP 65129
- > The Sanctuary Client listens on port TCP 33115

Please refer to the next section, *Configuring the firewall*, for details on how to configure Windows XP/2003.



The ports used for the communication between the client and the SecureWave Application Server can be configured. See SecureWave Application Server registry keys on page 145 and Sanctuary Client registry keys on page 148.

Configuring the firewall

With Windows XP SP2, the integrated firewall is enabled by default. You can also activate it on Windows 2003 SP1. Here is a procedure to open a TCP port on the firewall:

1. Click **START**, and then click **RUN**.
2. In the *Run* dialog box, type `Firewall.cpl`, and then click **OK**.
3. On the *Exceptions* tab, click **ADD PORT**.
4. In the *Port number* box, type the number of the port to open (33115 and 65129), and then click the **TCP** button.
5. In the *Name* box, type a name for the port, and then click **OK**. The new service is displayed on the *Exceptions* tab.
6. To enable the port, click to select the check box next to your new service, and then click **OK**.



The Installation Wizard proposes to open these ports for you during the setup phase even if they are already opened.



Another way of configuring your firewall is by using Windows' *Netsh* command. To open a port using this command:

1. Click **START**, and then click **RUN**.
2. In the *Run* dialog box, type `netsh firewall set portopening TCP 33115 ENABLE`, and then click **OK**. In this example, we use port 33115. You will also need to open port 65129.

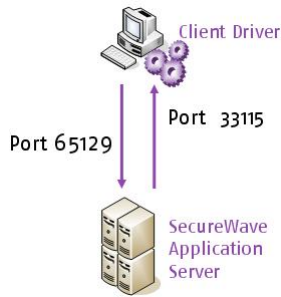


Figure 101: Communication ports between SXS and the client driver



Appendix F: Opening firewall ports for client deployment

The information in this chapter applies to all Sanctuary software suite except for Sanctuary Server Edition (the client cannot be installed on Windows XP nor Windows 2000 Pro computers).

Microsoft Windows XP SP2 enables the Windows Firewall by default. While this firewall configuration helps secure your system, it can also prevent legitimate software from interacting with the computer.

Many NetBIOS and DirectHost services, such as our deployment tool, rely upon a combination of TCP and UDP network ports, specifically TCP 139, TCP 445, UDP 137, and UDP 138. These services are installed by default on Windows NT 4.0 and Windows 2000 systems, as well as domain-joined Windows XP systems.

With the advent of Windows XP SP2 these services are, by default, no longer available to remote systems. This firewall denies access to these services and prevents connections to all network ports. The defaults settings prevent our installation tool to connect to the remote computers.

With the methods described in this chapter, you can preserve system security while deploying our software in your organization.

You can apply these necessary firewall settings on a computer-by-computer basis, or via an Active Directory domain group policy as explained in the following sections.

To manually open the ports in a computer-by-computer basis

1. *Start* → *Settings Control Panel* → *Windows Firewall* (or click *SECURITY CENTER* and then *WINDOWS FIREWALL*) and go to the *Exceptions* tab.

On this tab, you can choose to enable the *File and Print Sharing services* (as well as other listed services). By enabling File and Printer Sharing services, TCP ports 139 and 445, and UDP ports 137 and 138, you can install our client remotely using our deployment tool, while all other (non-selected) services are blocked.



If the computer resides on a remote IP subnet, you will need to edit the service and choose Subnet as the Scope.

2. Click OK to close the Windows Firewall control panel.
3. Restart the computer to enable these choices.

To open the ports in a computer-by-computer basis with a .bat file

Open your notepad or your favorite text processor and type or copy and paste the following lines:

```
netsh firewall set portopening protocol=UDP port=137  
name=SANCTUARY_UDP_137 mode=ENABLE profile=All
```

```
netsh firewall set portopening protocol=UDP port=138  
name=SANCTUARY_UDP_138 mode=ENABLE profile=All
```

```
netsh firewall set portopening protocol=TCP port=139  
name=SANCTUARY_TCP_139 mode=ENABLE profile=All
```

```
netsh firewall set portopening protocol=TCP port=445  
name=SANCTUARY_TCP_445 mode=ENABLE profile=All
```

Save and run on each machine.

To open the firewall ports via an Active Directory Group policy

While it is possible to open ports manually in a small network, this can also be achieved in a larger scale by centrally configuring the Windows firewall using Group Policy. When the XP SP2 machines log on to the network, they will inherit the customized Group Policies, thus opening the Windows Firewall ports required for remote deployment. This is the Microsoft recommended method to manage centrally Windows Firewall settings.

In the following steps, we will modify a domain group policy to open the needed ports:



To avoid compatibility problems ensure that the machine has the latest patches and service packs.



If you are using a Windows Server 2003 with Service Pack 1 computer joined to the domain:

1. Log on as domain administrator.
2. Download and install the .NET framework (required for the next step.)
3. Download and install the Microsoft Group Policy Management Console (GPMC) from Microsoft's Web site.

To create the Group Policy (GPO):

1. Open the Group Policy Management console (Start → Run → gpmc.msc)

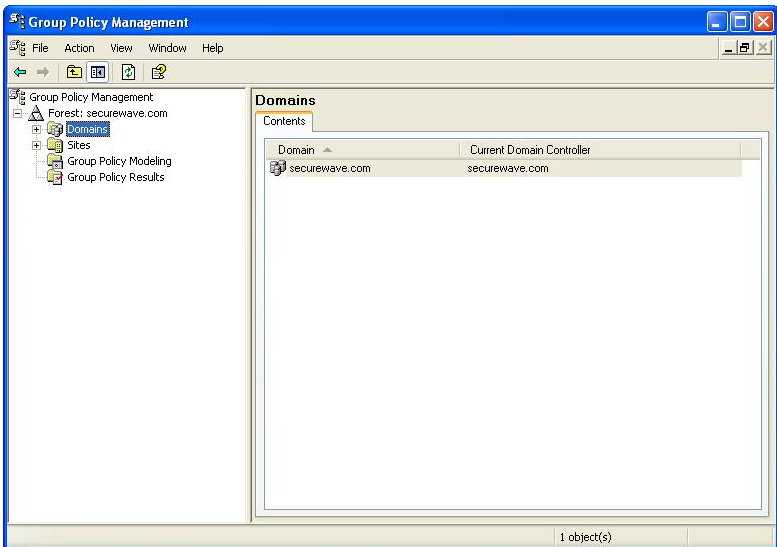


Figure 102. Open firewall ports: select domain and forest

2. Select the Forest and the Domain for which you wish to create a Windows Firewall Policy.
3. Right-click the entry for *Default Domain Policy* and select **E**dit.

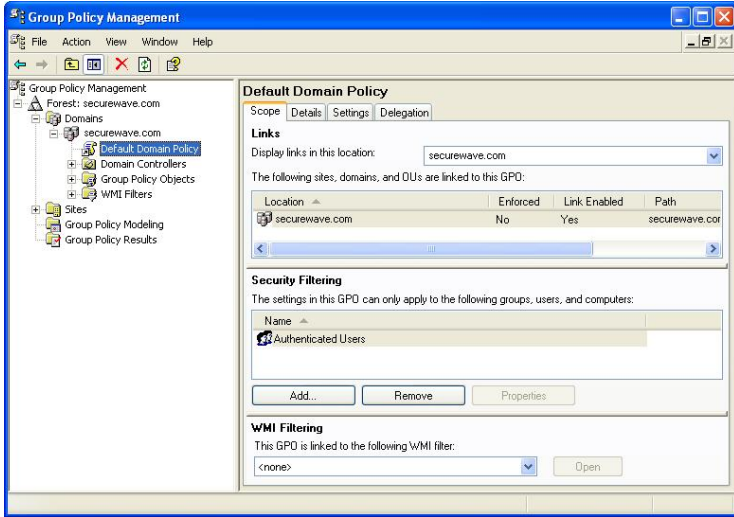


Figure 103. Open firewall ports: edit the Default Domain Policy

4. This will open a *Group Policy* window for the selected domain:

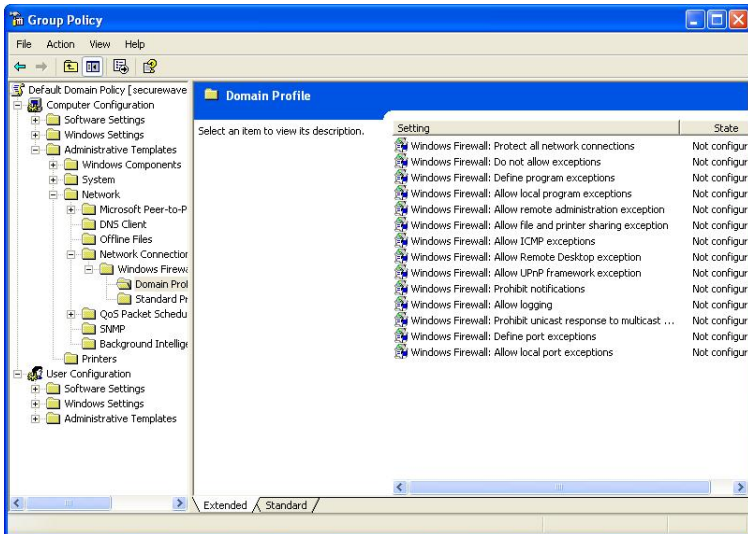


Figure 104. Open firewall ports: modify file and printer sharing exceptions



5. Expand the *Computer Configuration* tree and navigate to the *Administrative Templates* → *Network* → *Network Connections* → *Windows Firewall* → *Domain Profile* folder, as illustrated in the previous figure.

The simplest way to enable the ports used by our deployment tool is to enable the policy *Windows Firewall: Allow file and printer sharing exception*.

6. Right-click *Windows Firewall: Allow file and printer sharing exception* and select *Properties*. The following dialog appears:

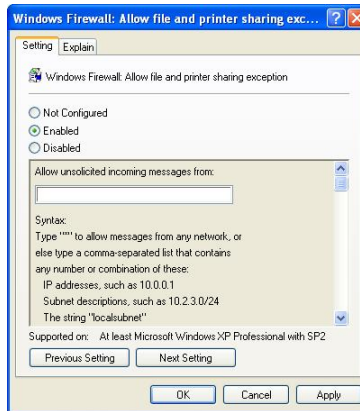


Figure 105. Open firewall ports: enable the required ports

7. Choose *Enabled* and then type *Localsubnet* in the *Allow unsolicited incoming messages from* field.
8. To save these settings click on the **APPLY** button and then on **OK**.

Enabling File and Printer Sharing access will open TCP ports 139 and 445, and UDP ports 137 and 138, making them available to other machines on the same local IP subnet. These machines will appear completely blocked for those systems outside of the local subnet.

To improve security

To enhance further the security, you can replace 'localsubnet' in step 7 of the preceding procedure with the specific IP address or addresses (comma separated) of the computers allowed to deploy the client.



Appendix G: Using your Sanctuary Synchronization Script for Novell: Quick Guide

The information in this chapter applies to all Sanctuary software suite except for Sanctuary Server Edition (the client cannot be installed on Windows XP nor Windows 2000 Pro computers).

Introduction

In this section, we guide you through a chronological order all the way through the installation and implementation process providing you with a quick reference list that summarizes all relevant steps

Step by step guide to install your Sanctuary Synchronization Script

Please follow these steps to quickly get up and running your Sanctuary Synchronization Script installation – your Novell server must be ready before proceeding:

1. Install the database server. This is the first component to install since Sanctuary solution uses this database to stock diverse information. You will need at least one database. The database is stored in a SQL server (full-blown version or MSDE, depending on your company's size). To install the database, see *Chapter 2: Installing the Database Components* on page 33.
2. The second component needed is the SecureWave Application Server (SXS). This component does the interface between the database and the client component and between the console – used to define/modify/delete/create permissions and rules – and the database. You need to install at least one and it can be on the same computer as the database. To install the application server, see *Chapter 3: Installing SecureWave Application Server* on page 41.
3. The third component is the console. Its purpose is to manage the definition, modification, deletion, and creation of permissions and rules. You can install the Console in the same machine as the database



and application server or in a different one. To install the console, see *Chapter 4: Installing the Sanctuary Console* on page 57.

4. One of your Windows client machines needs a Novell client and our synchronization script. This machine must already have Novell's LDAP and ActiveX NDAP installed (available on Novell's Web site or in the LDAP-NDAP\activex_ldap and LDAP-NDAP\activex_ndap directories of your installation CD). You can find the necessary synchronization script (NDSSync.vbs) in the Scripts directory.



Windows' Gateway Services for Netware (GSNW) is not sufficient to run the NDSSync.vbs synchronization script

5. Define simple permissions rules for the well-known accounts (Everyone, Local System, etc.) using the Console installed in step 3. See *Chapter 7: Testing your Sanctuary Device Control installation* on page 81
6. In the next step, you will need to install or deploy the clients through your network to start the protection process. To install a single client, run setup.exe located on the \CLIENT folder of your installation CD: to deploy several, consult *Chapter 10: Unattended Client Installation* and *Chapter 5: Installing the Sanctuary Client on your guest computers*.
7. Now you need to be sure that the clients are communicating with the SecureWave Application Server and the policies defined in step 4 are enforced.
8. Run the script (c:\>cscript.exe \path_to_folder\NDSSync.vbs Novell_Server_Tree) as an Administrator on the client machine defined in step 7. You can optionally add the SQL server parameters to the script: c:\>cscript.exe \path_to_folder\NDSSync.vbs Novell_Server_Tree [<SQL Server> [<SQL User Name> <SQL Password>]. You can run this script manually from time to time (if there are not too many changes in your eDirectory structure) or automatically using a scheduler software. See an example in *Scheduling domain synchronizations*.



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.
```

9. When the script finishes, open the Console. You can now select the user accounts, groups, workstations, and OUs when defining permissions. Create a simple Read permissions rule that applies to a device for a



specific user. For example, a 'Read only' permission that applies to the floppy disk drive. Send the updates to the client machines.

10. Test the enforcement of the new permissions rule defined in step 9.



If you use NDSSync.vbs script to connect to Sanctuary's Database from a remote computer, SQL Authentication is used. This is also the case when the database and console are installed on the same machine and you login as a different user. If you installed MSDE with our installation wizard, or manually using the Windows Authentication mode, the login options of the script cannot be used. In this case, it is impossible to synchronize Novell's eDirectory using user credentials different from those of the system administrator of the Database Server machine as NDSSync.vbs script parameters.



The following table summarizes the previous steps:

Step	Description	Purpose	Reference
1	Install the database	Store permissions, rules, and settings	<i>Chapter 2: Installing the Database Components</i>
2	Install the application server	Interface between database and clients/console	<i>Chapter 3: Installing SecureWave Application Server</i>
3	Install the console	Manage permissions, options, and rules	<i>Chapter 4: Installing the Sanctuary Console</i>
4	Install Sanctuary Synchronization script, a Novell client, and LDAP & NDAP on a Windows machine	Setup required to run Sanctuary Synchronization script	Administrator's Guide <i>Chapter 10, Chapter 11: Using the SXDomain Command-line Tool</i> , and Novell's guides
5	Define basic permissions	Be sure that everything is working correctly by defining some permissions for well-know groups	Administrator's Guide <i>Chapter 3, Chapter 7: Testing your Sanctuary Device Control installation</i>
6	Install clients	Begin the protection process	<i>Chapter 5: Installing the Sanctuary Client on your guest computers and Chapter 10: Unattended Client Installation</i>
7	Run Sanctuary Synchronization script	Convey all eDirectory information to the database	Administrator's Guide <i>Chapter 10 and Chapter 11: Using the SXDomain Command-line Tool</i>
8	Define new permissions for a Novell user in the console	Test	Administrator's Guide <i>Chapter 3</i>
9	Proceed to define all of your company's policies	Protect and enforce company's policies	Administrator's Guide

Table 14: Novell quick guide installation steps



Appendix H: Using Novell shares for your DataFileDirectory

The information in this chapter applies to all Sanctuary software suite except for Sanctuary Server Edition (the client cannot be installed on Windows XP nor Windows 2000 Pro computers).

DataFileDirectory access to a Novell share

When installing the SecureWave Application Server (SXS), the setup asks for a data file directory where all logs files are stored. It is possible to define such directory on a Novell server in the same way as it is done for a Windows server. To do this, SecureWave Application Server must meet two conditions:

- > It must be able to have create/read/write/erase access on the Novell share.
- > It should have a transparent authentication access to the Novell server

In this chapter, we explain how to create this shared directory to use it transparently in a Novell environment.

Transparent SXS authentication for Novell eDirectory

Due to the interaction between Novell eDirectory and Microsoft Windows (Active Directory or domain environment is not required in this case), it is possible to have a transparent authentication for the Application Server.

Window's user credentials (name and password) are, by default, passed to Novell as such. If the same username (including the same password) exists in Novell, this authentication process is transparent. If this is not the case, Novell rejects the user for all non-interactive processes. If the process is an interactive one, Novell will ask for a new authentication through the Novell Client for Windows.

In essence, the process consists in setting an account in Novell's eDirectory structure with the same name and password as in Windows (local or domain user). This account is going to be used by the SXS service.

We make these assumptions in the following procedure (which, of course, differs from your actual Novell installation):



- > The Novell server is called 'BOOGIE'
- > The Novell Tree is called 'SECUREWAVE'
- > The Novell Context is called 'TEST'
- > The Novell shared directory which will be used as DataFileDirectory for Sanctuary is called 'BOOGIE_MYDATA.TEST:DataFileDir' (which is located on server BOOGIE (context TEST) hosting a shared directory (MYDATA) which contains a subdirectory named 'DataFileDir')
- > The SecureWave Application Server account used in Windows is called 'sxs'
- > The shared folder and the 'sxs' account should already exist on the Novell eDirectory. Please refer to your Novell documentation for further details on how to create shares and users in Novell. The 'sxs' account on the Novell eDirectory should have, by default, no rights to any files or directories.

Follow these steps –in Novell v5.0 or later – to enable this transparent authentication:

1. Run, from a Windows machine with a Novell Client for Windows installed on it and logged on as a Novell administrator, the Netware Administrator tool – nwadmn32.exe –, located at BOOGIE\SYS\PUBLIC\WIN32\ on the Novell server.

Now search the user account (sxs) in the root of the context TEST, this account will be used to access the Novell share by SXS, as shown below:



Figure 106: Searching the account that SXS is going to use

Open the properties window for user 'sxs' (right click on the user and select *Details*).

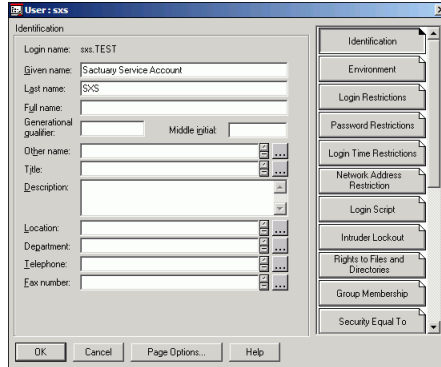


Figure 107: Properties of the Novell account used for the SXS service

2. Click on the **PASSWORD RESTRICTIONS** button located at the right panel of this window and activate the *Require a password* Option.

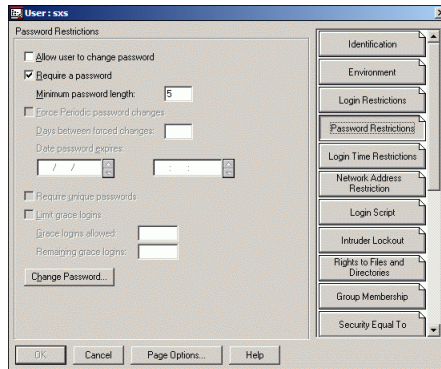


Figure 108: Password restrictions windows for the Novell user

Now click on the **CHANGE PASSWORD** button and use the **SAME** password and name as for its Windows counterpart.

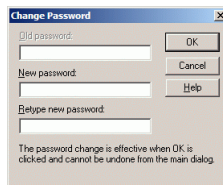


Figure 109: Change the password for the Novell user



- Now click on the RIGHTS TO FILES AND DIRECTORIES button located on the right panel of the properties window, click on FIND, and select the TEST context:

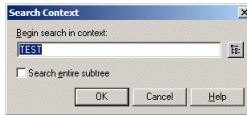


Figure 110: Selecting the context for the user's rights

You should now see a window similar to this one:

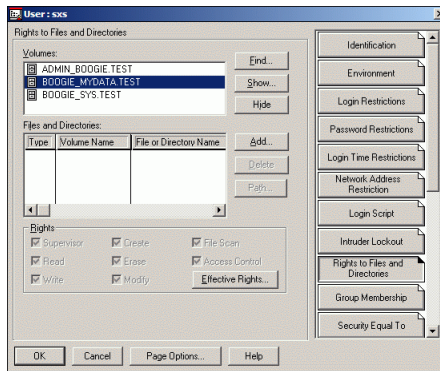


Figure 111: User rights for DataFileDirectory

Click on the ADD button and traverse the tree – starting from the context TEST – until you reach the location of the data file directory (= object) as show in the next two screenshots.

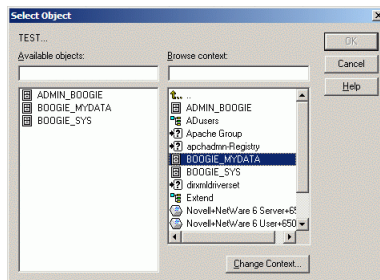


Figure 112: Selecting the data file directory location on the Novell file server (1/2)

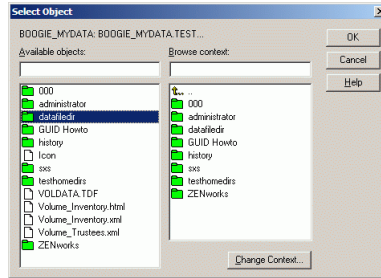


Figure 113: Selecting the data file directory location on the Novell file server (2/2)

Once this directory is selected, give the user the following rights to it:

Right	Purpose
READ	Needed by SXS for opening shadow files and logs
WRITE	Required by SXS to write to log files
CREATE	Needed by SXS to save fetched shadow files and create new logs
ERASE	Required by SXS when performing a database maintenance
MODIFY	Needed by SXS when temporary SXS files are converted into log files
FILE SCAN	Required at startup of SXS to enumerate the present shadow files and logs

Table 15: Novell user's rights



Appendix I: Importing file definitions during setup

The information in this chapter applies only to Sanctuary Server Edition & Sanctuary Custom Edition.

During the installation of SecureWave Application Server, you are offered the opportunity of importing SecureWave File Definitions (SFD). These definitions are sets of all the hashes of various operating systems files supported by Sanctuary. We recommend installing those of the operating systems/applications that you use. There are several reasons to do this:


- > Sanctuary will know all the files of the operating system. This means you do not have to manually create File Groups for the operating system files. You only have to add files to File Groups when you authorizing other applications.
- > SecureWave has already classified the operating system files into File Groups. This provides you with a 'standard' set that can be used as a starting point for further authorizations.
- > Importing file definitions makes your life easier when upgrading. As an example, the system already knows that `mfc42.dll` is assigned to the 'Windows Common' File Group. When you receive a new version of this file (e.g. when installing an operating system patch), the same File Group will automatically be suggested in the *Assign Files to File Group* dialog.
- > If you use SecureWave File Definitions, you can be sure that the operating system files were not tampered with before you had a chance to add them to the different File Groups using the Console.
- > The File Groups created while importing the SecureWave File Definitions during setup are automatically assigned to the Groups and Users who are most likely to need them when beginning your authorization work.


The next table summarizes the list of File Groups created and the Users and Groups to whom they are assigned during setup:




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

Table 16: Created file groups and assigned users

-  *If you do not import the File Groups during the setup but later using the Console, they are not automatically assigned to users.*

-  *Importing SecureWave File Definitions (SFD) can be a time-consuming task. To save yourself time, only import those ones that correspond to the versions of the operating systems you are currently using. DO NOT import SFD you do not need/use, they increase the file permissions packages and, thus, network traffic.*

-  *SFD files from older operating system versions are not imported during the installation. They must be manually imported.*



Appendix J: Using Sanctuary Server Edition with Sanctuary Device Control

The information in this chapter only applies when installing both products in your network.

Checking your database and application server version

If you are using another of our software on your machine, for example Sanctuary Device Control, you have to be sure that you are using the latest version of the SecureWave Application Server (SXS) and Database Server (SX) before proceeding with the installation. There are two distinctive cases:

1. The database and application server version are newer than that of the program you are trying to install.
2. The database and application server you are using are an old version and, thus, do not have the required functionalities.

The detection and installation is done in two steps. It is mandatory to complete them in this order:

1. Install the Database.
2. Install the Application server.

The installation routine refuses to install the components if the present database has a higher version number.

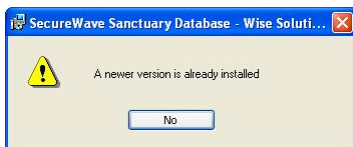


Figure 114: Message when trying to install an older database version

To verify your database version (only for your information or in case of a technical support call):

1. Open the Control Panel (Start → Settings → Control Panel).



2. Select *Add or Remove programs*.
3. Choose the SecureWave Sanctuary Database and then click on [*Click here for Support Information*](#). The *Support Info* dialog opens and you can see the database version:



Figure 115: Installed database version

If the setup detects that the version you have in your computer is older than the one to be installed, you see the following dialog when running the setup Wizard:

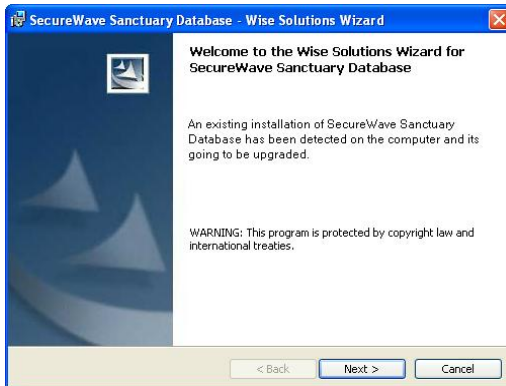





Figure 116: Installing a more recent database version

Remember that the SXS Service can be started and stopped through the Windows Services Panel or using a command line (`net stop sxs ; net start sxs`). The setup Wizard stops, updates, and starts the service automatically without your intervention only if the application server resides on the same machine as the database. If you are using several application serves, please stop their respective services manually before proceeding.

 *We recommend backing up your database before a new installation.*

 *If you update your database, you need, as well, to update your application server(s).*




 *If the database needs no update – you have a higher version –, just install your console and client(s).*

Checking your blocking options

When you are installing other products of our suite, the case we analyze in this chapter, you have to ensure that the computer and user/group 'Blocking Mode' option is set to the appropriate value. If this is not done, the Sanctuary Device Control setup cannot proceed, as it would be classified as an unknown executable that needs authorization. You will need to set this option for your Administrators and Local System and change it when you finish your Sanctuary Device Control installation and have authorized all your applications accordingly.

The process is the same no matter if you are dealing with a computer or a User/Group:

1. Install the SecureWave Management Console and go to the User Explorer module by clicking on its icon: .
2. Select *Default Options* from the *Tools* menu.
3. In the *Default Options* dialog box, click the *Computer* tab. The left panel shows all the available options. The right panel shows the current value for the selected option.
4. Select the *Blocking mode* in the left panel list, click on the *Not configured* option and change to *Non-blocking mode*. See a sample screen in *Figure 117*.

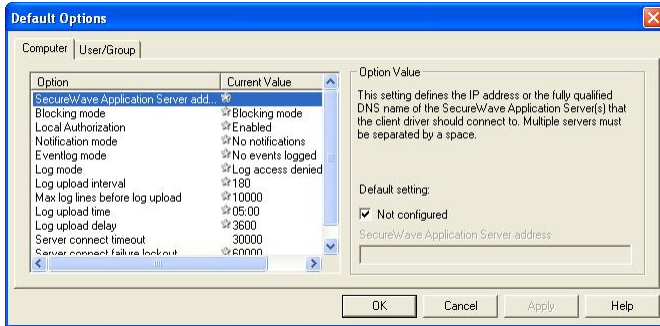


Figure 117. Default Computer Options

The tab chosen is *Computer* indicating that the options are not specific to a particular machine, but the defaults for all of them.



Glossary

ACE

Access Control Entries. An entry of the Access Control List (ACL). It contains a set of access rights and a security identifier (SID) identifying a trustee.

ACL

Access Control List. A list of security protections that apply to an object (file, process, event, or anything else having a security descriptor).

ADC

Advanced Data Connector. See RDC.

CAB

File extension for cabinet files, which are multiple files LZx-compressed into a single file and extractable with the extract.exe utility. Such files are frequently found on Microsoft software distribution packages.

Client Computer

The computers on your network that Sanctuary Device Control protects/controls.

Direct cable connection (DCC)

A RAS networking connection between two computers, or between a computer and a Windows CE/PPC-based device, which uses a serial or parallel cable directly connected between the systems instead of a modem and a phone line.

DNS

Domain Name System (also Service or Server). A service that translates common names (easy for human to remember) into IP addresses.

Executable Program

A computer program that is ready to run. The term usually applies to a compiled program translated into computer code in a format that can be loaded in memory and executed by a computer's processor.



FAT

The *File Allocation Table* defines a reserved zone on a magnetic media containing the list of clusters it occupies.

File Group

Organizational groups used to cluster authorized executable files. Files must be assigned to 'File Groups' before users can be granted permission to use them. You can choose to assign files to 'File Groups' from various modules throughout the Sanctuary Application Console Terminal, e.g. by double-clicking on a file in the *DB Explorer*, *EXE Explorer*, *Log Explorer* or *Scan Explorer*.

Hash

A complex digital signature calculated by Sanctuary Suite to uniquely identify each executable file that can be run. The hash is calculated using the SHA-1 algorithm that takes into account the entire contents of the file.

IOCP

I/O Completion Port.

MDAC

Microsoft Data Access Components. Required by Windows computers to connect to SQL Server and MSDE databases.

MSDE

Microsoft SQL Server Desktop Engine. Either MSDE 1.0 or MSDE 2000 can be used with Sanctuary Device Control.

MSI

Microsoft's Windows Installer engine (Sanctuary suite supports MSI from version 2.0 up to v3.1). It is also the extension of the file used by this component.

NTFS

New Technology File System offers several enhancements and advantages over older FAT systems. Among them, we can quote a superior architecture, support for larger files, enhanced reliability, automatic encryption and decryption, disk quota tracking and limiting, change journals, disk defragmenter, sparse file support, improved security and permissions, etc.



Private Key

One of two keys used in public key encryption. The user keeps the private key secret and uses it to encrypt digital signatures and to decrypt received messages.

Public Key

One of two keys in public key encryption. The user releases this key to the public, who can use it for encrypting messages to be sent to the user and for decrypting the user's digital signature.

RAS

Remote Access Services is a Windows' program that allows most of the available network facilities to be accessed over a modem link.

RDC

Remote Data Connector. Formerly known as *Advanced Data Connector*. Technology used in conjunction with ActiveX Data Objects (ADO) to retrieve a set of data from a database server.

RPC

Remote Procedure Call. A protocol that allows a computer program running on one host to run a subroutine located on another one. RPC is used to implement the client-server model of distributed computing.

SCC

Sanctuary Command Control. Component that is in charge of all communication between server and client(s).

SFD

SecureWave provides a number of pre-computed file hashes for most versions of suites and Windows Operating Systems, in several languages, and for all the available Service Packs. The file hashes are referred to as *SecureWave File Definitions* or SFD. They are installed during the setup, but you can import them as soon as SecureWave releases new ones. You can find the latest ones on our Web site.

SID

The *Security Identifier* is a unique alphanumeric character string that identifies each operating system and user in a network.



SQL Server

The industry standard database server, supported by Sanctuary Device Control. Either MSSQL 2000 or MSSQL 2005 can be used with Sanctuary Device Control.

SK

The Sanctuary Kernel Driver, the client component that runs as a kernel driver.

SMC

SecureWave Management Console. The console used to define the device permissions and default options. Its functions are described in the Administrator's Guide.

SUS

Software Update Services is a tool provided by Microsoft to assist Windows administrators with the distribution of security fixes and critical update releases.

SXS

SecureWave Application Server.

TCP/IP

The protocol used by the client computers to communicate with the SecureWave Application Servers.

UPC

Universal/Uniform Naming Convention. A path convention that originated in Unix and uses a \\server\volume\directory\file convention instead of arbitrary mapped letters to describe the actual location of a file or directory.

WINS

Windows Internet Naming Service. A system that determines the IP address associated with a particular network computer (called name resolution). WINS uses a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one.

WSUS

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



Index of figures

Figure 1: Trust relationships.....	16
Figure 2: Sanctuary's infrastructure	21
Figure 3: Sanctuary's setup	22
Figure 4: MSDE password setting	23
Figure 5: SecureWave Application Server user account	26
Figure 6: Database server installation.....	27
Figure 7: Data file directory	28
Figure 8: SA Account password.....	35
Figure 9: Error message when MSDE is already installed.....	35
Figure 10: SecureWave Sanctuary Database installation: first step.....	36
Figure 11: SecureWave Sanctuary Database installation: license agreement	37
Figure 12: SecureWave Sanctuary Database installation: destination folder	37
Figure 13: SecureWave Sanctuary Database installation: select SQL instance	38
Figure 14: SecureWave Sanctuary Database installation: final step	38
Figure 15: SecureWave Sanctuary Database installation: ending the installation wizard.....	39
Figure 16: SecureWave Application Server installation: first step.....	44
Figure 17: SecureWave Application Server installation: license agreement.....	45
Figure 18: SecureWave Application Server installation: no license found	46
Figure 19: SecureWave Application Server installation: invalid license	46
Figure 20: SecureWave Application Server installation: Remote Procedure Calls warning.....	46
Figure 21: SecureWave Application Server installation: destination folder	47
Figure 22: SecureWave Application Server installation: service account	47
Figure 23: SecureWave Application Server installation: database server.....	48
Figure 24 : SecureWave Application Server installation: data file directory	49
Figure 25: SecureWave Application Server installation: change destination folder	50
Figure 26: SecureWave Application Server installation: warning message when setting the log files folder to a local drive.....	50
Figure 27: SecureWave Application Server installation: no Certification Authority found	51
Figure 28: SecureWave Application Server installation: protocol selection dialog.....	51
Figure 29: SecureWave Application Server installation: import SecureWave File Definitions..	52



Figure 30: SecureWave Application Server installation: final stage	52
Figure 31: SecureWave Application Server installation: installation	53
Figure 32: SecureWave Application Server installation: finishing the installation	53
Figure 33: SecureWave Application Server upgrade: first step	54
Figure 34: SecureWave Application Server upgrade: protocol selection dialog	55
Figure 35: SecureWave Application Server upgrade: protocol selection dialog	55
Figure 36: Sanctuary Console installation: first step	58
Figure 37: Sanctuary Console installation: license agreement.....	59
Figure 38: Sanctuary Console installation: custom setup.....	60
Figure 39: Sanctuary Console installation: modify destination folder	60
Figure 40: Sanctuary Console installation: ready to install	61
Figure 41: Sanctuary Console installation: Remote Procedure Calls warning	61
Figure 42: Sanctuary Console installation: finishing the installation	62
Figure 43: Sanctuary Client: first step	65
Figure 44: Sanctuary Client: license agreement	66
Figure 45: Sanctuary Client: SXS name or address.....	66
Figure 46: Sanctuary Client: no address specified	68
Figure 47: Sanctuary Client: no valid address specified or cannot contact server.....	68
Figure 48: Sanctuary Client: test failed	69
Figure 49: Sanctuary Client: change the target directory.....	69
Figure 50: Sanctuary Client: how will the program appear on the Windows' Add Remove Program dialog	69
Figure 51: Sanctuary Client: the installation process is ready to start	70
Figure 52: Sanctuary Client: the installation progress	70
Figure 53: Sanctuary Client: finishing the installation process.....	71
Figure 54: Sanctuary Client: restarting the computer	71
Figure 55: Sanctuary Client: no import file and no server address specified	71
Figure 56: Round Robin DNS schema	74
Figure 57: Sanctuary Server Edition installation: welcome screen.....	76
Figure 58: Sanctuary Server Edition installation: configuration screen	76
Figure 59: Sanctuary Server Edition installation: option screen	77
Figure 60: Sanctuary Server Edition installation: e-mail configuration screen	77



Figure 61: Sanctuary Server Edition installation: choose installation directory 78

Figure 62: Sanctuary Server Edition initial scan 79

Figure 63: Audit Log Viewer module – main window 94

Figure 64: Log Explorer example data window..... 95

Figure 65: Local authorization dialog 97

Figure 66: Key pair generation: first step.....100

Figure 67: Key pair generation: final message 101

Figure 68: SXS did not find the public–private key pair..... 102

Figure 69: Sanctuary client deployment: first start–up.....104

Figure 70: Sanctuary client deployment: packages and computers.....105

Figure 71: Sanctuary client deployment: new package 105

Figure 72: Sanctuary client deployment: application server IP or name106

Figure 73: Message when installing in “Serverless mode”108

Figure 74: Message when the connection test fails.....108

Figure 75: Message when the connection test fails (key related).....108

Figure 76: Message when the Kernel DNS resolution fails.....108

Figure 77: Message when the connection test succeeds109

Figure 78: Sanctuary client deployment: new package..... 110

Figure 79: Sanctuary client deployment: package option..... 110

Figure 80: Sanctuary client deployment: first screen 111

Figure 81: Sanctuary client deployment: select computer dialog (sample a) 112

Figure 82: Sanctuary client deployment: select computer dialog (sample b)..... 112

Figure 83: Sanctuary client deployment: advanced select computer dialog..... 113

Figure 84: Sanctuary client deployment: selected computer(s).....114

Figure 85: Sanctuary client deployment: reboot options114

Figure 86: Sanctuary client deployment: installation progress.....115

Figure 87: Sanctuary client deployment: shutdown dialog in client computers 117

Figure 88: Using the Group Policy Management Console to install clients 118

Figure 89: Deployment package using group policies: select active directory119

Figure 90: Deployment package using group policies: select group policy119

Figure 91: Deployment package using group policies: software installation 120

Figure 92: Deployment package using group policies: deployment type 120



Figure 93: Deployment package using group policies: deployment options	121
Figure 94: Scheduled task: first step	125
Figure 95: Scheduled task: select program	126
Figure 96: Scheduled task: select period (1/2).....	126
Figure 97: Scheduled task: select period (2/2).....	126
Figure 98: Scheduled task: select account.....	127
Figure 99: Scheduled task: ending the wizard	127
Figure 100: Client's options when several Sanctuary products are installed	129
Figure 101: Communication ports between SXS and the client driver	161
Figure 102. Open firewall ports: select domain and forest	165
Figure 103. Open firewall ports: edit the Default Domain Policy.....	166
Figure 104. Open firewall ports: modify file and printer sharing exceptions	166
Figure 105. Open firewall ports: enable the required ports.....	167
Figure 106: Searching the account that SXS is going to use	174
Figure 107: Properties of the Novell account used for the SXS service	175
Figure 108: Password restrictions windows for the Novell user.....	175
Figure 109: Change the password for the Novell user	175
Figure 110: Selecting the context for the user's rights.....	176
Figure 111: User rights for DataFileDirectory	176
Figure 112: Selecting the data file directory location on the Novell file server (1/2)	176
Figure 113: Selecting the data file directory location on the Novell file server (2/2).....	177
Figure 114: Message when trying to install an older database version	181
Figure 115: Installed database version	182
Figure 116: Installing a more recent database version	182
Figure 117. Default Computer Options	184



Index of Tables

Table 1: Database server name syntax.....	28
Table 2: Database server name syntax	49
Table 3: Server address and import file relationship.....	67
Table 4: Recommended File group assignments	92
Table 5: Task progress color code.....	116
Table 6: SXDomain parameters.....	124
Table 7: License file format.....	131
Table 8: System requirements.....	142
Table 9: Application Server registry keys (1/2)	148
Table 10: Application Server registry keys (2/2).....	148
Table 11: Client registry keys (1/2).....	150
Table 12: Client registry keys (2/2)	150
Table 13: Communication ports in Windows XP	159
Table 14: Novell quick guide installation steps	172
Table 15: Novell user's rights.....	177
Table 16: Created file groups and assigned users	180



Index

A

ACE; 185
ACL; 185
ADC; 185
Additional Information; 7
ADO; 155
Anonymous access; 156
Auditing; 86
AuthSrv.exe; 75
Automatic Load Balancing; 108

B

Back-up; 137
Basic Security Rules; 17
 Access policy; 18, 20
 Administrative rights; 18
 BIOS password; 17
 Boot sequence; 17
 Firewalls; 19
 Hot fixes; 19
 NTFS partition; 18
 Password policies; 19
 Power users; 18
 Private and public key generation; 20
 Recovery console; 19
 Safe mode; 19
 Seal/chassis intrusion protection; 17
 Service packs; 19

C

Cab; 185
CD Authorization; 84
Client computer; 99, 102, 114, 116, 185
Cluster; 28, 49
Command-line; 117
Contact Information; 9

D

Database; 13, 14, 33, 34, 41, 43, 44, 48, 58, 63, 123, 130, 141
 Back-up; 137
 Engine; 23, 33, 34
Datafile Directory; 28, 49, 145
DbConnectionString; 145
Debug; 149
Deploy Software; 120
Direct cable connection; 185
DNS; 185
Drivelmage; 64

E

EnableAuthEpResolution; 158
Enterprise Manager; 43
Executable
 Program; 185
Explanation of Symbols; 8

F

FAT; 186
File definitions
 Importing; 179
File groups; 186
Firewall; 155, 159, 160
Firewall ports; 163
 Improve security; 167
 Open manually; 163
 Open using GPO; 164
 Open with a .bat file; 164
FirstServer; 149
Fixed Endpoints; 157

G

Generating a Key Pair; 100
Ghost; 64
Glossary; 185
GrantDB.exe; 43



Group Policy; 118

H

Hash; 186

Help menu; 135

I

Infrastructure; 20

Install/Uninstall/Reboot Options
dialog; 114, 116

Installing; 5, 10, 13, 31, 33, 41, 62, 63,
170, 172

 Sanctuary Console; 57

Instance; 27, 28, 48, 49

IOCP; 186

IpaqDetectDelay; 149

K

Key pair; 99, 100

 Generation; 41, 99

Key pair mismatch; 108

L

License; 45

 File; 43

 File format; 130

 File location; 130

Log; 149

 File name; 145, 149

 To console; 146, 149

 To file; 146, 147, 149

M

MDAC; 41, 42, 142, 155, 186

Microsoft Certificate Authority; 142

MSDE; 33, 34, 186

 Back-up; 138

MSI; 186

 File; 105

MsiExec; 117

MST File; 110

N

Named Instance; 28, 49

nscan_ip_tcp; 157

Novell; 169

 quick guide; 169

NTFS; 186

NTLM; 158

O

Organizational Unit; 118

P

Package; 105, 110, 111, 114, 116, 120

 Colors; 110, 111

 Warning; 110, 111

Packages menu; 105

Permissions; 81

policies.dat; 64, 107

Port; 146, 155

Power users; 18

Private Key; 187

Public key; 110, 111, 187

R

RAS; 187

RDC; 187

Reboot; 114, 116

Registering Sanctuary Device Control;
129

Registry Keys; 145

Reporting; 86

RestrictRemoteClients; 156

RPC; 155, 187

RunAs; 143

S

sa; 23, 35

Sanctuary Authorization Service tool;
75

Sanctuary Client; 5, 31, 42, 63, 64,
65, 67, 99, 102, 103, 108, 124, 133,
148, 160

Sanctuary Client Deployment; 111



- Dialog; 113, 115
- Sanctuary Console; 13, 30, 57, 58, 63, 99, 123, 135
- Sanctuary Device Control Client; 149
- Sanctuary Device Protection Module Driver; 188
- SCC; 148, 187
 - Sanctuary Command Control; 148, 187
- Scheduled Permissions; 83
- Scheduling domain
- Synchronizations; 125
- SecureNT; 151
- SecureWave Application Server; 13, 14, 25, 41, 42, 43, 48, 58, 63, 66, 67, 68, 99, 101, 106, 107, 130, 141, 145, 160, 188
 - Back-up; 140
 - Upgrading; 54
- SecureWave File Definitions; 179, 187
- SecureWave Installation Transform; 105
- Select computers; 114, 115
- Serverless mode; 107
- Servers; 149
- Server-side; 13, 22
- SFD; 179, 187
- SHA-1; 186
- Shadowing; 85
- SID; 185
- SID Server; 187
- SK; 188
- SMC; 188
- SndPort; 147
- SQL Server; 33, 34, 42, 43, 142, 145, 186, 188
- Support; 135
- SUS; 75, 188
- sx; 27, 48
 - Database; 24, 36
- SxdConnectTimeoutMSec; 147
- SXDomain*; 5, 41, 123
- SxdPort; 147
- SXS; 188
 - Account; 47
- Synchronize Domain Members; 147
- System Requirements; 14, 63, 141

- System Shutdown dialog; 116

T

- TCP; 155
- TCP/IP; 42, 188
- TDS; 155
- Temporary Permissions; 82
- Terminal Services; 142
 - Limitations; 142
- Testing; 81, 89
 - Authorizing; 90
 - Authorizing files; 91
 - Create template; 89
 - Initial scan; 89
 - Logging to a client; 92
 - Using a template; 90
- The RunAs command limitation; 143
- Troubleshooting; 135

U

- Unattended; 72, 103
- Uninstalling; 72
- UPC; 188
- Upgrade; 152, 153
- Using the Key Pair Generator; 99

V

- VerboseSyncLogging; 147
- VirtualServerName; 28, 49

W

- Windows 2003
 - SP1; 155
- Windows Authentication; 43
- Windows CE Devices; 149
- Windows Installer; 186
- Windows XP
 - SP2; 155
- WINS; 188
- Workgroup; 32
 - Installing Sanctuary in a; 32
- WSUS; 5, 75, 188

