SecureWave
Safeguarding Tomorrow

Sanctuary's Setup Guide

www.securewave.com

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SecureWave claims copyright in this program and documentation as an unpublished work, revisions of which were first licensed on the date indicated in the foregoing notice.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

Trademarks

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

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

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

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

You can contact our technical support team by calling:

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

or by sending an email to support@securewave.com

Published August 2007

Contents

About this guide

This guide explains in detail how to install all components of your Sanctuary solution. For a quick setup guide, consult the printed Sanctuary's Quick Setup and Configuration Guide.

> *Chapter 1: Installing Sanctuary's Components* shows you the basic Sanctuary architecture, security tips, and guides you through the process of installing the Sanctuary components.

> *Chapter 2: Installing the SecureWave Sanctuary Database* explains how to set up the database needed by Sanctuary.

> *Chapter 3: Installing the SecureWave Application Server* explains how to set up the component that serves as a link between the client driver and the database and/or the management console and the database.

> *Chapter 4: Installing the Sanctuary Management Console* explains how to set up the console used to administer Sanctuary.

> *Chapter 5: Installing the Sanctuary Client on your endpoint computers* guides you on how to set up the Sanctuary Client on the computers that will be protected by Sanctuary.

> *Chapter 6: The Authorization Service Tool* explains the setup procedures for the SUS/WSUS (Software Update Services & Windows Server Update Services) update partner tool used for our Sanctuary Application Control Suite programs (Sanctuary Application Control Server Edition, Sanctuary Application Control Custom Edition, and Sanctuary Application Control Terminal Services Edition).

> *Chapter 7: Using the Key Pair Generator* explains how to generate public and private keys before you deploy the Sanctuary Client to the machines you want to protect.

> *Chapter 8: Unattended Client installation* shows you how to deploy clients silently.

> *Chapter 9: Using the SXDomain Command line tool* explains how to synchronize information between the SecureWave Sanctuary Database and the domain controller.

> *Chapter 10: Registering your Sanctuary product* explains the Sanctuary licensing model.

> *Appendix A: Detailed system requirements and limitations* details the hardware and software you need for an optimum operation of the software.

> *Appendix B: Registry keys* provides detailed information about registry key settings for servers and clients.

> *Appendix C: Upgrading from old versions* explains how to upgrade from a previous version of Sanctuary Device Control and Sanctuary Application Control Suite.

> *Appendix D: Installing Sanctuary components on Windows XP SP2/2003 SP1* explains how to configure this system to work with Sanctuary programs.

> *Appendix E: Opening firewall ports for client deployment* covers how to open the required ports needed for the client deployment technique described in *Chapter 8: Unattended Client installation*.

> *Appendix F: Using the synchronization script for Novell* provides a quick setup guide for synchronizing Novell eDirectory objects to define device/application permissions.

> *Appendix G: 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.

> *Appendix H: Installing a Certificate Authority for encryption and TLS Communication* describes how to install a Microsoft Certificate Authority needed for client driver-SecureWave Application Server and intra-

SecureWave Application Server TLS communication. This authority is also needed if you plan to centrally encrypt removable devices (if using Sanctuary Device Control).

- *Appendix I: Importing file definitions during setup* includes necessary information to use the Standard File Definitions (SFD) for Sanctuary Application Control Suite programs during the setup phase.
- *Appendix J: Controlling administrative rights for Sanctuary's administrators* describes a file script used to set and control the rights to administer Organizational Units/Users/Computers/Groups in Active Directory.
- *Appendix K: Installation checklist* contains several tables to guide you through the initial setup process.
- 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, *Appendix I: Importing file definitions during setup* is only applicable if you installed *Sanctuary Application Control Suite*.

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

Product relevance of each chapter

All chapters contain information that is relevant to users of all Sanctuary products, apart from:

- *Chapter 6: The Authorization Service Tool*, which only contains information relevant to Sanctuary Application Control Suite programs (Sanctuary Application Control Server Edition, Sanctuary Application Control Terminal Services Edition, and Sanctuary Application Control Custom Edition).
- *Appendix I: Importing file definitions during setup*, which only contains information relevant to Sanctuary Application Control Suite programs (Sanctuary Application Control Server Edition, Sanctuary Application Control Terminal Services Edition, and Sanctuary Application Control Custom Edition).

Conventions

Notational conventions

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.*

Typographic conventions

The following typefaces are used 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.

For more information

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

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 Sanctuary.
- Our Knowledge Base (KB), with FAQ (Frequent Asked Questions) and practical information of your everyday use of Sanctuary solutions.

To contact us

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, email, or regular mail.

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

You can contact our technical support team by calling:

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

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

Alternatively, you can write to customer support at:

Atrium Business Park
23, rue du Puits Romain
L-8070 Bertrange
Luxembourg

Chapter 1: Installing Sanctuary’s Components

The information in this chapter is relevant to all Sanctuary products.

This chapter guides you through the procedure for installing the various Sanctuary components. You can find a complete description of the Sanctuary products in the Sanctuary's Architecture Guide.

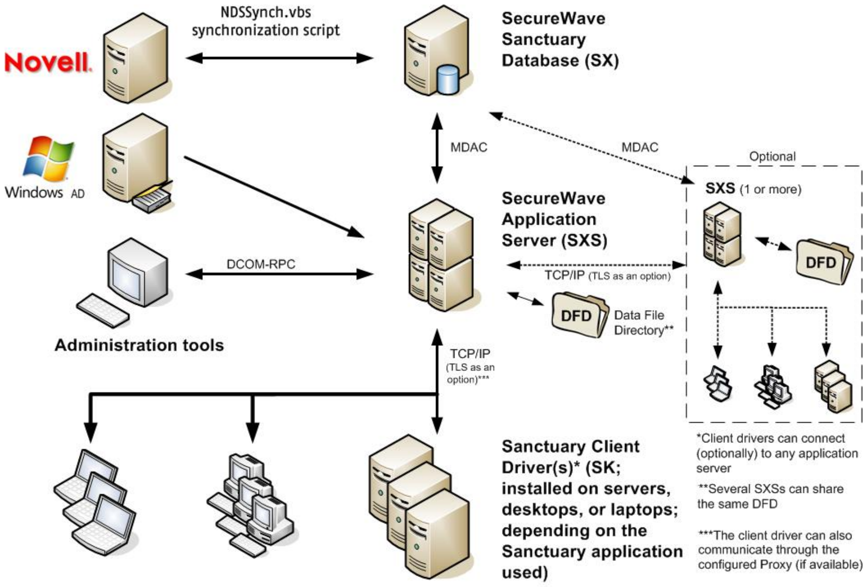
Sanctuary architecture

A Sanctuary solution includes the following four main components (for a full description see the *Sanctuary's Architecture Guide*):

- One SecureWave Sanctuary Database — This serves as the central repository of authorization information (devices/applications).
- One or more SecureWave Application Server with one or (optionally) more Data File Directory (DFD) — This is used to communicate between the SecureWave Sanctuary Database and the protected clients.
- The Sanctuary Client — installed on each computer you want to protect.
- Administrative tools — including the Sanctuary Management Console. This provides the administrative interface to the SecureWave Application Server. This interface, which can be installed on one or more computers, is used to configure the solution and perform a range of day-to-day administrative tasks.

An implementation can have more than one *SecureWave Application Server* and one *SecureWave Sanctuary Database* connected over a wide area. This means that Sanctuary can provide a resilient and scalable solution to your security issues.

The relationship between the Sanctuary components is represented in the following figure:



*Client drivers can connect (optionally) to any application server

**Several SXSs can share the same DFD

***The client driver can also communicate through the configured Proxy (if available)

Figure 1: Sanctuary’s architecture

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

We assume that the TCP/IP protocol is properly configured during the installation process described in this guide:

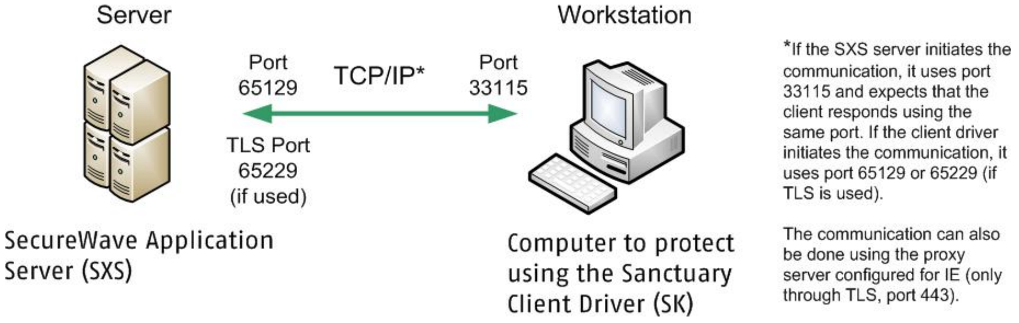

Server
Workstation
Port 65129
TCP/IP*
Port 33115
TLS Port 65229 (if used)
SecureWave Application Server (SXS)
Computer to protect using the Sanctuary Client Driver (SK)
*If the SXS server initiates the communication, it uses port 33115 and expects that the client responds using the same port. If the client driver initiates the communication, it uses port 65129 or 65229 (if TLS is used).
The communication can also be done using the proxy server configured for IE (only through TLS, port 443).

Figure 2: Sanctuary's setup

To install Sanctuary products

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

1. ***Decide whether you are going to use an extra encryption layer*** for Sanctuary Client Driver - SecureWave Application Server and intra-SecureWave Application Server communications or not. If you decide to use it, you need to install a Certificate Authority. This is also needed if you want to centrally encrypt removable media using *Sanctuary Device Control*. See *Transport Layer Security* on page 12*, Appendix H: Installing a Certificate Authority for encryption and TLS Communication* on page 129, and *Sanctuary Device Control Administrator's Guide*.

2. ***Install the SecureWave Sanctuary Database*** on the computer that is to hold authorization information for devices and/or executables, scripts and macros. You can find a detailed installation procedure explanation in *Chapter 2: Installing the SecureWave Sanctuary Database* on page 17.

3. ***Install the* SecureWave Application Server** on the computer or computers that serve as intermediates between the Sanctuary Client and the SecureWave Sanctuary Database, distributing the list of device/software permissions for each client computer and/or User/group. See *Chapter 3: Installing the SecureWave Application Server* on page 19.

4. ***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 *Chapter 4: Installing the Sanctuary Management Console* on page 36.

5. ***Generate the key pair*** that is used to sign/encrypt messages/media. See *Chapter 7: Using the Key Pair Generator* on page 59.

6. ***Install a Sanctuary Client and test the predefined permissions for devices and/or executables, scripts or macros***. You can install the client on the same machine that you are using for the *SecureWave Sanctuary Database*, *SecureWave Application Server*, and *Sanctuary Management Console* (some limitations apply). See *Chapter 5: Installing the Sanctuary Client on* your endpoint computers on page 41.

7. ***Define some test permissions*** for devices and/or executable files using the console installed on step 3 and test these on the client machine. See the *Sanctuary's Quick Setup and Configuration Guide*.

8. ***Define company's policies*** (permissions, rules, and settings). Determining and defining which users get access to which devices and/or executables, scripts and macros. This step is done before installing or rolling out any clients. Installing Sanctuary Clients without a good policy definition would result in a loss of productivity. Consult the Sanctuary Application Control Suite Administrator's Guide and/or Sanctuary Device Control Administrator's Guide for more information.

9. ***Plan the client installation strategy and deploy your clients*** in production machines to begin enjoying immediately the benefits of being protected by Sanctuary. See *Chapter 8: Unattended Client installation* on page 63.

10. ***Define a synchronization schema*** to be used for your Microsoft Domains or Novell eDirectory structure. See *Chapter 9: Using the SXDomain Command line* tool on page 85.

You can find a detailed explanation of the functions carried out by the various Sanctuary administration components in the Sanctuary Application Control Suite Administrator's Guide and/or Sanctuary Device Control Administrator's Guide. We recommend that you read these through thoroughly before starting the implement Sanctuary products.

At any time after installing the *SecureWave Sanctuary Database*, *SecureWave Application Server*, *Sanctuary Management 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. These are placed in %TMP% directory (of the user account who is doing the installation) and named sxdbi.log, setupcltsu.log, setupsmc.log, setupdb.log, and setupsxs.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.

You should resolve all hardware conflicts before installing Sanctuary solutions. You can use Windows’ Device Manager to troubleshoot and fix software-configurable devices. All hardware devices that use jumper pins or dip switches must be configured manually.

It is critical to determine the Policy Definition that is best for your organization. This is where you define which users get access to which devices and/or executables. This step must be done 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 or it could prevent users from accessing their devices. ***Define policies BEFORE installing any clients!***

Ghost image deployment

A common problem that administrators face is how to deploy a ‘standard’ computer to a new user or when upgrading to new hardware. They normally do this by installing all necessary software on a ‘fresh’ computer and then use ‘Ghost’ software to create an image of it. The administrator then imprints this image on all new computers.

The Sanctuary Client can be included in the ‘ghost ‘image. You can do this, using the following steps:

1. Install the Sanctuary Client on the machine to be 'ghosted', as you would do on any other client computer.
2. Change all drivers to start on demand mode. To do this, use Regedit to modify the following values found in `HKLM\System\CurrentControlSet\Services\`.

   `scomc: Start, REG_DWORD = 4`

   `sk: Start, REG_DWORD = 4`
3. Delete the value 'sk' in the registry key `HKLM\System\CurrentControlSet\Control\Class\{71A27CDD-812A-11D0-BEC7-08002BE2092F}\Upperfilters`.

   If this is not done, the client will not boot up.
4. Reboot the computer. The driver is installed but does not run.
5. In `HKLM\System\CurrentControlSet\Services\sk\Parameters` delete ALL entries that start with '`\SystemRoot\SxData\...`'.
6. In `HKLM\System\CurrentControlSet\Services\sk\Parameters` delete the 'DeviceIndex' key
7. In `HKLM\System\CurrentControlSet\Services\scomc\Parameters` delete the 'LastSeenComputerName' key.
8. Delete any keys (apart from default) that do not have a value set.
9. Delete all files in the %SystemRoot%\sxdata directory, apart from the public key file, sx-public.key.

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

When deploying the Ghost image:

1. Change the SID (which uniquely identifies the computer) and the name of the computer. This can be done using Ghostwalker or the freeware SIDchanger tool available from the SYSinternals website, www.sysinternals.com.

2. Change the starting mode of each driver back to its original state. To do this, use Regedit to modify the following values found in `HKLM\System\CurrentControlSet\Services\`.

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

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

3. Restore the registry key value 'sk' in `HKLM\System\CurrentControlSet\Control\Class\{71A27CDD-812A-11D0-BEC7-08002BE2092F}\Upperfilters`.

4. Reboot the ‘new’ computer.

Transport Layer Security

The Transport Layer Security (TLS) protocol (based on SSL — Secure Socket Layers) addresses security issues related to message interception during communication between hosts. The deployment of TLS, client and server side, is the primary defense against compromised clients or mixed networks where is possible to intercept transmitted messages.

TLS has specific advantages when addressing message security issues:

> The identities of peers can be authenticated using asymmetric or public key cryptography, allowing the safe exchange of encrypted information , coupled with a Certificate Authority (see *Appendix H: Installing a Certificate Authority for encryption and TLS Communication*). Clients can verify that the IP address and name are consistent with the DNS records, inhibiting ‘man in the middle’ and DNS ‘spoofing’ exploits.

> Message’s contents cannot be modified while en route between two TLS negotiated hosts. Either party has the ability of detecting TLS protocol violations.

However, there are also some disadvantages to using the TLS protocol:

> Cryptography, specifically when it involves public key operations, is CPU-intensive and using TLS may result in a performance loss. The level of performance loss depends on factors such as your environment, the total number of permissions required, if you want to use shadowing or not, and so on. Unfortunately, it is impossible to know beforehand how large the performance loss will be for your particular organization.

> A TLS environment requires maintenance — the system administrator must configure the system and manage certificates.

You should consider carefully whether your organization needs this extra security, i.e. if your company either uses sensitive data or has to meet certain security regulations.

Using TLS for client-SecureWave Application Server communication

There are two ways in which a Sanctuary Client can communicate with a SecureWave Application Server. It can use:

> *A Pull operation* in which the client driver establishes a connection with the server to:

- Obtain the most recent permission updates.
- Upload its log files.
- Upload its shadow files.

If using TLS protocol, the authentication and confidentiality of the data exchanged is guaranteed.

> A *Push operation* in which a SecureWave Application Server establishes a connection with the client to:

- Request a client driver to perform a scan.
- Request a client driver to upload its log file.
- Request the client driver to upload its shadow files.
- Request a client driver to contact the server to receive the latest permission updates.
- 'Ping' a client to update its client list or begin another communication or process.

Push messages are very limited and basic and therefore do not use TLS. SecureWave Application Server sends a short message informing the client to callback with an ID number, nothing else. This message, although not encrypted, is signed. The Sanctuary Client Driver then opens a connection channel with the SecureWave Application Server — either using TLS or not, as defined when installed — and sends back the ID number. The SecureWave Application Server(s) verify that there is a pending request for this communication and instruct the client driver what to do next.

The callback message (see also *Using TLS for the inter-SecureWave Application Server communication* on page *15*) is authenticated using the private/public key pair, which must be generated before installing client drivers. Messages are signed with the server private key and clients use the corresponding public key to guarantee that the messages come from genuine servers.

Since the messages exchanged with the server do not contain confidential data, there is no need to encrypt them, i.e. using TLS for push messages would not provide any significant benefits.

When the communication mode used is TLS, Sanctuary Client:

> Checks that the size of the package received is at least big enough to hold the server signature, rejecting any packages smaller than this minimum size.

> Rejects packages that are bigger than the maximum allowed size.

> Verifies the signature and integrity of the message, for the packages that have been accepted.

When a client driver receives a valid SecureWave Application Server command, it begins sending back the requested data through a TLS connection (if configured). This data can comprise:

> Scan results.

> Log files.

> Shadow files.

> Permission updates.

> 'Ping' information.

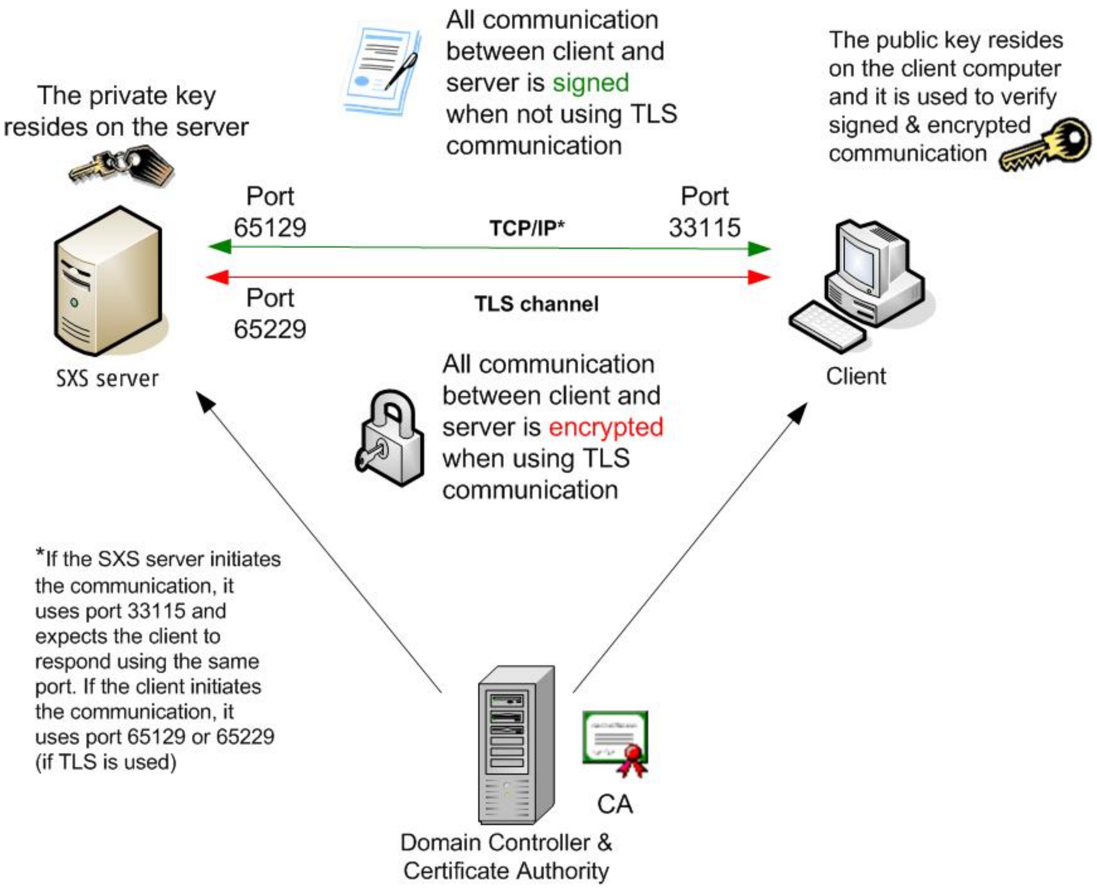
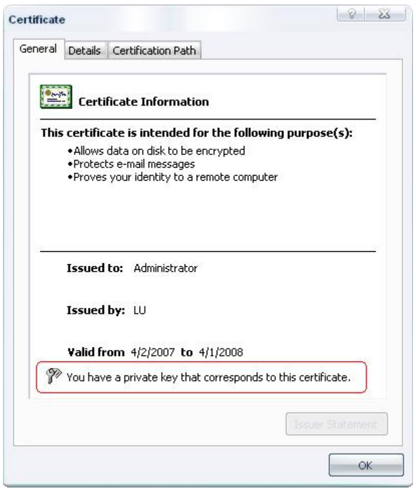

The private key resides on the server
All communication between client and server is signed when not using TLS communication
The public key resides on the client computer and it is used to verify signed & encrypted communication
Port 65129
TCP/IP*
Port 33115
Port 65229
TLS channel
SXS server
Client
All communication between client and server is encrypted when using TLS communication
*If the SXS server initiates the communication, it uses port 33115 and expects the client to respond using the same port. If the client initiates the communication, it uses port 65129 or 65229 (if TLS is used)
CA
Domain Controller & Certificate Authority

Figure 3: Sanctuary Client: Using the TLS protocol for client-SecureWave Application Server communication

If the program does not auto-generate the required certificate (by attempting to obtain it from the Certificate Authority) you can either try to import it or generate it with the Wizard. You must ensure that it is signed by a private key as shown in the following image:



Certificate Information

This certificate is intended for the following purpose(s):

- Allows data on disk to be encrypted
- Protects e-mail messages
- Proves your identity to a remote computer

Issued to: Administrator

Issued by: LU

Valid from 4/2/2007 to 4/1/2008

You have a private key that corresponds to this certificate.

Figure 4: Signed certificate

Using TLS for the inter-SecureWave Application Server communication

If your Sanctuary implementation contains several SecureWave Application Servers and uses distributed Data File Directories (DFD), then since confidential information is exchanged between these, it is a good idea to choose to use the TLS protocol when installing them. For example, if you plan to define read/write shadow rules (see the *Sanctuary Device Control Administrator's Guide* for a complete explanation), there could be a constant flow of shadowed files circulating between them. Using the TLS protocol option assures that data is encrypted.

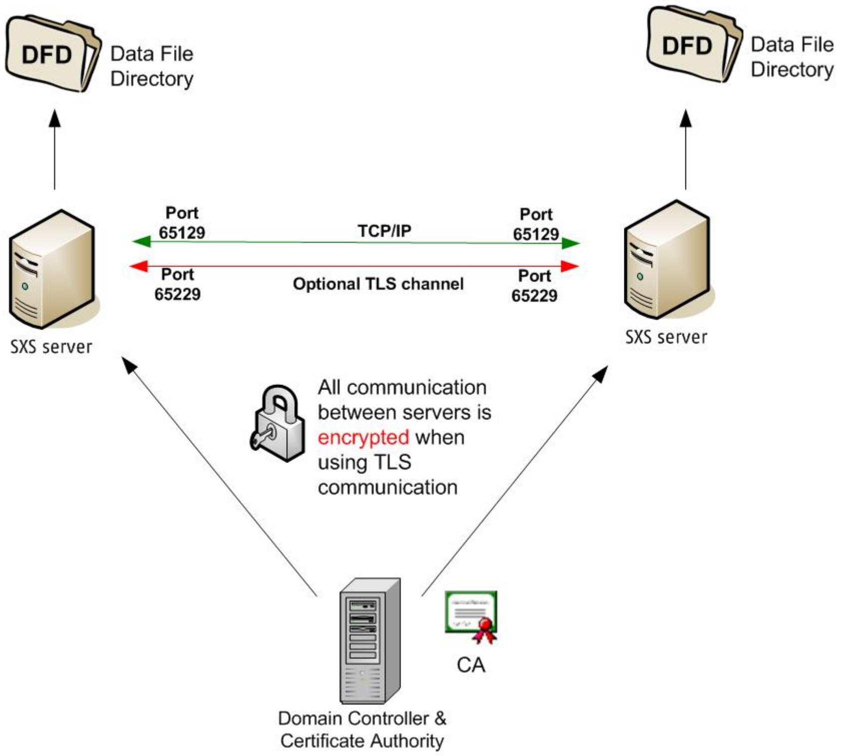


Figure 5: SecureWave Application Server: Using the TLS protocol for intra-SecureWave Application Server communication

SecureWave Application Server machines may have multiple DNS names and multiple certificates. The certificate selected by SecureWave Application Server must match the DNS name used by the Sanctuary Client and other SecureWave Application Servers when they communicate over secure TLS ports. These values can be manually overridden by modifying a registry key (see *Table 19* on page *100* for more information).

The value in 'ServerName' can be used to specify a fully qualified DNS name that SecureWave Application Servers register in the servers table and communicate to client drivers in callbacks. The value 'ServerCertSerial' is used to specify the serial number of the certificate that SecureWave Application Server should use for TLS communication. The format of this value is *exactly* the same as the one that SecureWave Application Server displays when a certificate is loaded, for example, 3738DCAE0003000001C0. (The MMC Certificates snap-in uses almost the same format, except it has blanks after every two digits. These blanks must NOT be specified for the SecureWave Application Server value.)

Server callback messages (see also *Using TLS for client-SecureWave Application Server communication* on page *12*) include the server's DNS name and port number(s). This ensures that the client only answers the particular contacting SecureWave Application Server even if the client has no prior information about it. The message also includes a timestamp, which prevents the client driver from replying to old requests.

What is a digital certificate?

A digital certificate is an electronic presentation card that establishes your identity and credentials when doing transactions over a channel. Certificates are issued by a Certification Authority. They contain, among other things:

- A digital signature, indicating which certificate-issuing authority generated them. This lets a recipient verify that the certificate is genuine.
- A public key, to be used for encrypting messages and digital signatures. All messages encrypted using the public key can be decrypted using the corresponding private key pair (see a complete description on *Sanctuary's Architecture Guide*).

Most certificates used today are based on the X.509 v3 certificate standard.

All messages encrypted using the public key can be decrypted using the corresponding private key pair (see a complete description on *Sanctuary's Architecture Guide*).

Typically, certificates also contain the following information:

- Certificate’s version and serial number.
- Signature algorithm.
- Validity (not before, not after).
- Authority and subject’s ID.
- Digital signature of the issuer, testifying the validity of the binding between the subject’s public key and the subject’s identifier information.

What is a Certificate Authority?

A Certificate Authority (CA) is an entity that issues and manages certificates in a network. As part of a public key infrastructure, a CA checks with a registration authority (RA) to verify the information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate stating that the public key contained in it belongs to the person, computer, or entity noted in the same certificate. The idea behind this security process is that the user trusts the CA and can verify its signature and can also corroborate that a certain public key belongs to whoever is identified in the certificate.

You either trust a CA or not. If you trust a CA, this means that you have confidence that it has proper policies in place when evaluating certificates requests. In addition to this, you also trust that the CA will revoke certificates that should no longer be considered as being valid, publishing an up-to-date CRL (Certification Revocation List).

Chapter 2: Installing the SecureWave Sanctuary Database

This chapter explains how to install the SQL Engine and *SecureWave Sanctuary Database* . Whereas *Chapter 1: Installing Sanctuary's Components* provides an overview of the entire setup, this chapter focuses exclusively on the database requirements. The information in this chapter is relevant to all Sanctuary software suite products.

💣 *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 Application Control 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 D: Installing Sanctuary components on Windows XP SP2/2003 SP1 *on page* 109 *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 take a backup of your database before proceeding.*

Choosing a SQL engine

The database used by Sanctuary software requires a Microsoft SQL Server database. This can be SQL Server 2000/2005, SQL Server 2005 Express Edition, or MSDE 2000.

The database server you choose depends on the size of your implementation and which, if any, of these Microsoft SQL Server databases you are currently using within your organization.

MSDE 2000 and SQL Server 2005 Express Edition are certainly sufficient for installations of up to 200 connected Sanctuary clients when you are using Sanctuary Device Control, or 50 Sanctuary clients when you are using Sanctuary Application Control Suite. Please note that there are inherent limits when using SQL Server 2005 Express Edition including:

> 4 GB Database size limit.

> No parallel processing of index operations.

> Only uses up to 1GB RAM.

> Only one CPU, no workload governor.

> No query analyzer.

SQL Server 2005 Express Edition may be an attractive option for sites that do not already use SQL Server. It is available free of charge, eliminating the expense of purchasing the SQL Server.

We recommend using a full-blown SQL Server at sites in which it is already installed. SQL Server should always be used for sites serving 200 or more connected Sanctuary clients.

See our online knowledgebase (at www.securewave.com) for advice about which Microsoft SQL Server database you should choose.

The Sanctuary Setup CD includes an installation of SQL Server 2005 Express Edition.

✍ *You can start using SQL Server 2005 Express Edition, and migrate to SQL Server later, should this be necessary. You cannot create a cluster using SQL Server 2005 Express Edition.*

✍ *To successfully install SQL Server 2005 Express Edition you must already have Microsoft's .Net Framework 2.0 and Windows Installer 3.1 (or later) installed on your machine.*

💣 *We strongly recommend downloading and applying the latest SQL Server service packs from www.microsoft.com before putting the system in production. Make sure you download the appropriate file. For example, service packs for Microsoft SQL Server cannot be applied to a MSDE 2000 database.*

Before you install

Before you start installing your database engine of choice, you must first check that the computer meets the minimum requirements. See *Appendix A: Detailed system requirements* on page *93* for details.

✍ *You must activate the 'Server' service (File and Print Sharing to Microsoft Networks) before attempting to install SQL Server on your machine. This is particularly important for Novell users who do not necessary already have this service running on their machines.*

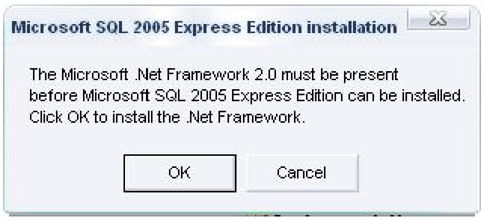
Stage 1: To install the SQL database engine

✍ *This procedure explains how to install SQL Server 2005 Express Edition. You can skip this stage if you already have MSDE 2000 or SQL Server 2000/2005 running on the machine that you want to host the SecureWave Sanctuary Database.*

1. Log on to the computer on which you want to install 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 and execute run.vbs located in the \SERVER\SQL2005 folder on the installation CD. The setup starts.

✍ *You must have Microsoft Installer v3.1 or later installed on your system. The setup prompts you to install this if you do not have it.*

✍ *If you do not have Microsoft's .Net Framework v2.0 (or later) installed on your computer, the following dialog is displayed:*



Microsoft SQL 2005 Express Edition installation

The Microsoft .Net Framework 2.0 must be present before Microsoft SQL 2005 Express Edition can be installed. Click OK to install the .Net Framework.

Figure 6: Installing SQL Server 2005 Express Edition, .Net not available

Click on OK and follow the instructions to install .Net Framework v2.0 (or later).

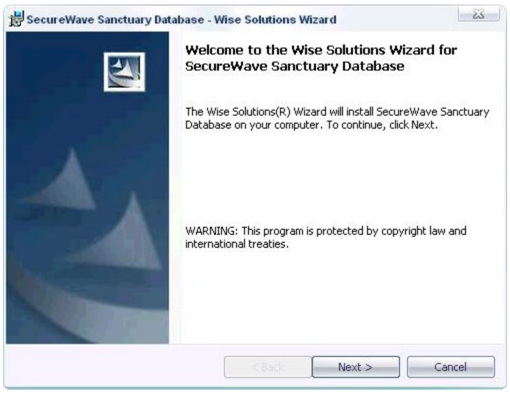
4. Read the End User License Agreement carefully and, providing you agree with its conditions, select the accept option and click on NEXT and INSTALL to continue the installation.

✍ *Make sure that the TCP/IP protocol is enabled for your SQL database. You can use the 'SQL Server Configuration Manager' tool in the 'Start ➔ Programs ➔ Microsoft SQL Server 2005' menu to check or manage protocols.*

Stage 2: To install the SecureWave Sanctuary Database

The Sanctuary database component requires a Microsoft SQL Server database. This can be SQL Server 2000/2005, SQL Server 2005 Express Edition, or MSDE 2000. If a database server is found, the setup adds a single database called ‘sx’.

1. Log on to the computer on which MSDE 2000/SQL Server is running. The account you use must have:
   - Administrative rights.
   - Access to SQL Server or MSDE 2000.
2. Close all programs running on the computer.
3. Insert the Sanctuary CD in your DVD/CD and run SETUP.EXE located on the \SERVER\DB folder.
4. The *Welcome* dialog is displayed.



SecureWave Sanctuary Database - Wise Solutions Wizard

Welcome to the Wise Solutions Wizard for SecureWave Sanctuary Database

The Wise Solutions(R) Wizard will install SecureWave Sanctuary Database on your computer. To continue, click Next.

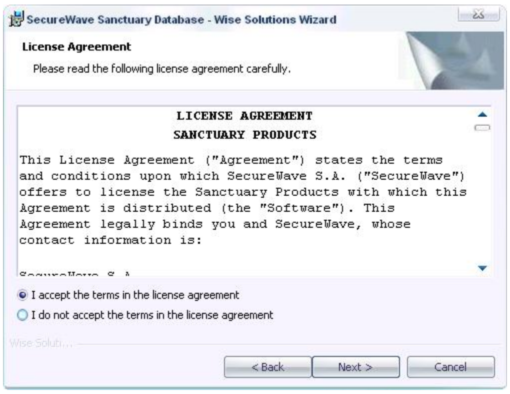
WARNING: This program is protected by copyright law and international treaties.

Figure 7: SecureWave Sanctuary Database installation: First step

5. Click on NEXT to continue.

The setup will not 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.

6. The next dialog displays the License Agreement.



SecureWave Sanctuary Database - Wise Solutions Wizard

License Agreement

Please read the following license agreement carefully.

LICENSE AGREEMENT

SANCTUARY PRODUCTS

This License Agreement ("Agreement") states the terms and conditions upon which SecureWave S.A. ("SecureWave") offers to license the Sanctuary Products with which this Agreement is distributed (the "Software"). This Agreement legally binds you and SecureWave, whose contact information is:

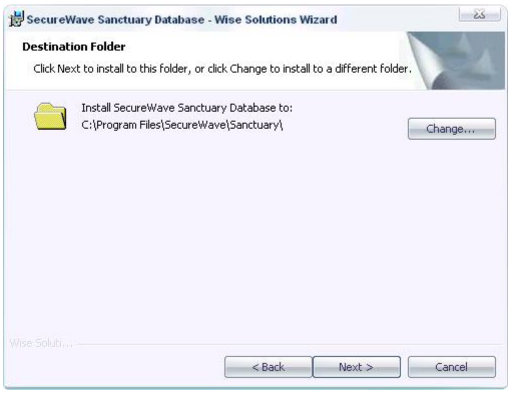
● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Figure 8: SecureWave Sanctuary Database installation: License agreement

7. Read the license agreement carefully and, providing you agree with its conditions, select the accept option and click on NEXT to continue the installation process.

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



SecureWave Sanctuary Database - Wise Solutions Wizard

Destination Folder

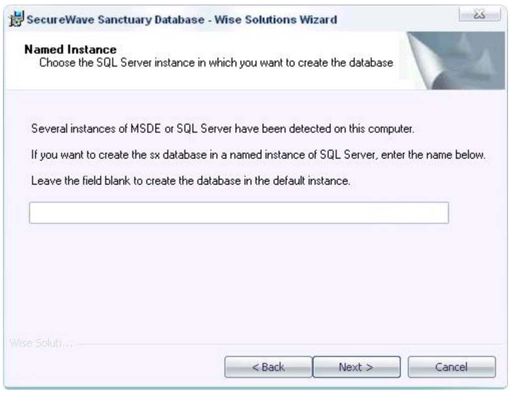
Click Next to install to this folder, or click Change to install to a different folder.

Install SecureWave Sanctuary Database to:
C:\Program Files\SecureWave\Sanctuary\

Figure 9: SecureWave Sanctuary Database installation: Destination folder

8. Choose the folder in which you want to create the SecureWave Sanctuary Database and click on NEXT. By default, the database is installed in the C:\Program Files\SecureWave\Sanctuary folder. To choose another location, click on CHANGE and browse to the folder you want.

9. If you already have several instances of the database engine on your computer, you are asked to select the one you want to use:



SecureWave Sanctuary Database - Wise Solutions Wizard

Named Instance

Choose the SQL Server instance in which you want to create the database

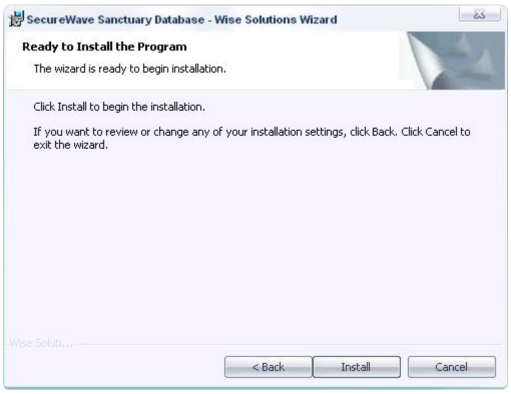
Several instances of MSDE or SQL Server have been detected on this computer.

If you want to create the sx database in a named instance of SQL Server, enter the name below.

Leave the field blank to create the database in the default instance.

Figure 10: SecureWave Sanctuary Database installation: Select SQL instance

The setup wizard is ready to start the installation:



SecureWave Sanctuary Database - Wise Solutions Wizard

Ready to Install the Program

The wizard is ready to begin installation.

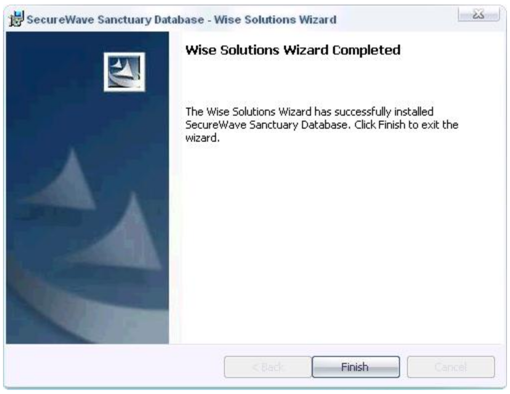
Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Figure 11: SecureWave Sanctuary Database installation: Final step

10. Click on the INSTALL button to perform the setup.

The SQL scripts run and the database is created. This process normally takes less than 2 minutes, depending on your hardware. Once completed, the final screen is displayed:



SecureWave Sanctuary Database - Wise Solutions Wizard

Wise Solutions Wizard Completed

The Wise Solutions Wizard has successfully installed SecureWave Sanctuary Database. Click Finish to exit the wizard.

Figure 12: SecureWave Sanctuary Database installation: Ending the installation wizard

11. Click on FINISH to close the wizard.

Database clustering

The *SecureWave Sanctuary Database* is the repository where all permissions and hashes (which define whether an application or device can be used or not) are stored. As an alternative to installing it on a single machine, you can choose to install SecureWave Sanctuary Database on a clustered server to provide a fault-tolerant system, as described below. Once you have at least two servers in a cluster with SQL working, you can proceed to install the database as described in the previous procedure.

What is database clustering?

A cluster is a group of computers, or nodes, which functions as a single system to provide high availability and fault tolerance. Database clustering is a failover technology. It ensures that the execution environment and services move to another computer in the cluster in case of a node failure, maximizing the database availability. (Database clustering does not provide scalability; It does not focus on performance or distributing the traffic to different servers.)

Terminology

Cluster: A group of computers configured to work together to serve clients in a similar fashion.

Node: Each server participating in a cluster is called a node.

Maximum # of nodes in a cluster: The maximum number of servers that can form a cluster. This is eight in Windows 2003 Enterprise, with at most 16 SQL instances.

Heartbeat: The nodes in a cluster remain in constant communication through the exchange of periodic messages called heartbeats.

Virtual IP (VIP): The client system communicates with the DB server using a virtual IP address. MSCS (Microsoft Cluster Service) takes care of redirecting the client request to the active server and hence the client does not have to worry about which server in a cluster is active.

MSCS (Microsoft Cluster Service): A Windows component, which once installed through the Control Panel, guides you through the steps needed to create a cluster service (cluadmin.exe).

Quorum: Physical disk where all configuration parameters are stocked. Without quorum the cluster cannot work — it must be a backup.

Failover: Capability to switch, automatically or manually, to a standby computer in a cluster. In normal situations, one (primary or active) computer provides the service while a second one (failover) is present to run the services if the primary fails.

Failback: Operation where a cluster is back and running after a failover. Control passes on to the active or primary computer of a cluster.

✍ *The same operating system must be installed on the nodes of a cluster database server.*

Requirements

Database clustering requires:

- At least two servers (up to the maximum that the operating system used in the cluster supports).
- Two network adapters per server — one to communicate with clients, the other one to communicate between the nodes that form the cluster (heartbeat). If only two computers are used, you can join them using a simple cross-link cable.
- A Shared Disk Array, SAN, or SCSI device to host the database.
- Microsoft Cluster Service (MSCS) to form the cluster. This is provided with Windows Operating Systems.
- One instance of SQL Server 2000/2005, including a SQL server, SQL server agent, and Full text search service.

To implement a database cluster

1. Define the cluster using Microsoft Cluster Service (MSCS). To do this, you need to name the cluster, add nodes to it, configure the network interfaces to define those that are public and those that are private (heartbeat), and, finally, test the cluster configuration.

MSCS provides three cluster models:

- **Single node server cluster** — This does not provide failover. This model is mainly used to organize resources on a server for administrative conveyance.
- **Single quorum** — This is the traditional cluster model. It maintains the cluster configuration data on a single cluster storage device connected to all nodes. For n-node clusters, the cluster is active until the last node in a cluster is working. Data is stored on a single cluster storage device (SCSI etc.). Data synchronization is not required. We recommend that you use a RAID solution for the cluster storage devices.
- **Majority node set** — Each node maintains its own copy of the cluster configuration data (quorum). More than half the nodes in a cluster must be running to keep the cluster working. This configuration is useful if you need to host applications that can failover, but where there is another, application-specific way, to replicate or mirror data between nodes.

Note that in Single Quorum model, there is only one copy of the database stored on a special hardware disk and hence issues like data synchronization never occur.

A typical cluster implementation is shown in the following image:

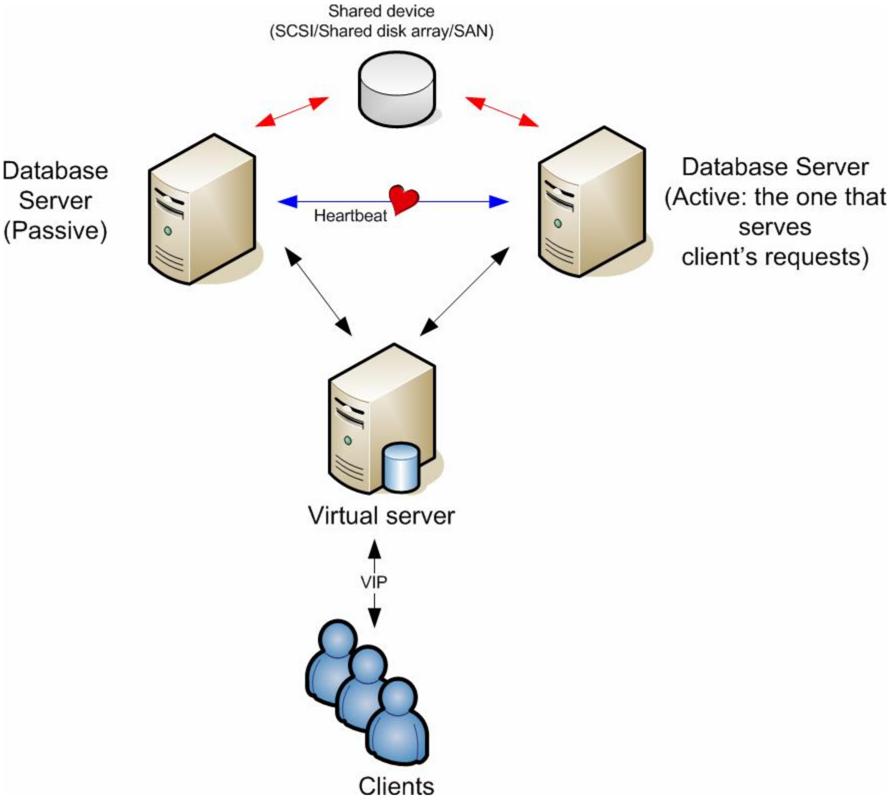

Shared device
(SCSI/Shared disk array/SAN)
Database Server (Passive)
Heartbeat
Database Server (Active: the one that serves client's requests)
Virtual server
VIP
Clients

Figure 13: SecureWave Sanctuary Database installation: Clustering

Every resource group is published in a virtual server, which is accessible to external clients via a unique IP address and name.

2. Install SQL Server, add this to the cluster to provide failback services, deploy SQL Server to all nodes and, finally, test your installation.

Items created during the SecureWave Sanctuary Database setup

During the SecureWave Sanctuary Database installation, the following items are created:

Item	***Purpose***	***Access***
Directory: %INSTALLDIR%\DB	Contains all SQL scripts needed by the SecureWave Application Server.	Full control for Administrators
Uninstall registry keys*	Helps delete the SecureWave Sanctuary Database.	n/a
*You can block the use of the RegEdit.exe program for all users by using our Sanctuary Application Control Suite.		

Table 1: Items created by the SecureWave Sanctuary Database installation

✍ *The %INSTALLDIR% directory points to the folder where the program was installed. It is usually C:\Program Files\SecureWave\Sanctuary, but can refer to another folder.*

Chapter 3: Installing the SecureWave Application Server

This chapter explains how to install the *SecureWave Application Server* on the computers that are going to be servers for the application. Whereas *Chapter 1: Installing Sanctuary's Components* provides an overview of the entire setup, this chapter focuses exclusively on the *SecureWave Application Server*. The information in this chapter is relevant to all Sanctuary software suite products.

When you install the SecureWave Application Server, a number of tools are copied to your hard disk. The installed tools are:

- The SecureWave Application Server.
- The Key Pair Generator.
- The SXDomain Tool.

> *Although you can use Windows XP for the SecureWave Application Server and/or Sanctuary Management Console, you should not use it for the SecureWave Application Server (or client component in the case of Sanctuary Application Control Server Edition). If you are planning to spread Sanctuary components among several machines, one of which has an XP operating system please read* Appendix D: Installing Sanctuary components on Windows XP SP2/2003 *SP1 on page* 109 *carefully before proceeding.*

Before you install

Before you begin installing the SecureWave Application Server, you must do the following:

- Make sure that the computer meets the minimum requirements (see *Appendix A: Detailed system requirements* on page *93* for details).
- Have the database already installed on the computer that is to hold your information (see *Chapter 2: Installing the SecureWave Sanctuary* Database on page *17* 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 prompts you to download it from Microsoft web site http://www.microsoft.com/data/. You must restart the setup after installing MDAC.*
>
> *MDAC enables computers to connect to SQL Server and SQL Desktop Engine 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, re-install MDAC on the computer hosting it.*

- Ensure that the TCP/IP protocol is installed. This is required so that the Sanctuary Client running on the client computer can communicate with the SecureWave Application Server. The setup program does not check this prerequisite.
- Ensure that the computer on which you want to install SecureWave Application Server 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.

- Ensure the SecureWave Application Server can do a fully qualified domain name resolution of the clients it is going to manage. You have to set up the mechanism to translate clients' names into IP addresses.
- Create or use an existing account to be used by the SecureWave Application Server service[1]. Setup automatically grant this account the rights to log on as a service[2]. You **MUST** use an account with local administration rights if you plan to use TLS protocol for Sanctuary Client Driver -SecureWave Application Server or intra-SecureWave Application Server communications. See *Transport Layer Security* on page *12* for more information.

  ✍ *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 SecureWave Application Server service account a member of the* ***Domain Users*** *group.*

  ✍ *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.*

  ✍ *Setup verifies the specified password/account before proceeding. Setup continues if it fails to verify the password but will be interrupted, and rollback, if the password cannot be validated when creating the server service.*

- 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 SecureWave Sanctuary 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 2000, you will have to use the grantdb.exe command-line application for every service account you will use. This can be found in the \BIN\TOOLS folder of your SecureWave CD.

  ✍ *grant.exe is not compatible with Microsoft SQL Server 2005 since it does not have the DMO object activated by default. You must install SQLServer2005_BC.msi, a backward compatibility package on Microsoft's Web site, as a short-term solution to this problem.*

  ✍ *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 holds the Login definitions. By default, BUILTIN\Administrators have access. If the SecureWave Sanctuary Database and the SecureWave Application Server are on the same machine the account under which the SecureWave Application Server runs is granted access to the database during setup. If the SecureWave Sanctuary Database and the SecureWave Application Server are on different machines, you must use grantdb.exe to allow the account to access the database.*

- Get a license for your Sanctuary product. The license information is stored in a file called *SecureWave.lic*. Your SecureWave Application Server installation will fail without it. 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 products, this file is sent to you by email. If you are evaluating a Sanctuary product, then you can obtain an evaluation license by registering on the SecureWave website (www.securewave.com), selecting the appropriate product page, and completing an Evaluation License Request form. Once you have a copy of the license file, save it into the %SYSTEMROOT%\SYSTEM32 directory. If your license has expired, SecureWave Application Server services do not start and a warning message is displayed.

  💣 *If you are using more than one SecureWave Application Server the same license file must be used on all the servers.*

[1] We will refer to this account as the Service Account

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

> (Optional). Check 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.

> Have a Certificate Authority installed and ready to provide your SecureWave Application Server machine with a valid certificate if you are planning to use TLS (Transport Layer Security) protocol to communicate between SecureWave Application Servers (if you are planning to install more than one) and/or SecureWave Application Server-client driver communications. See *Transport Layer Security* on page *12* and *Appendix H: Installing a Certificate Authority for encryption and TLS Communication* for more information.

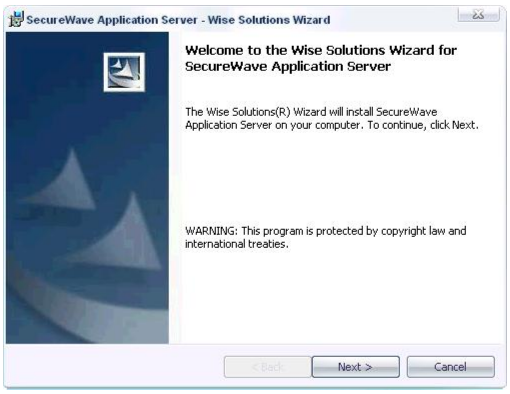
The decision to use or not TLS should not be taken lightly. Once you decide to use TLS for your client-SecureWave Application Server and/or intra-SecureWave Application Server communications and install Sanctuary in this mode, it is very difficult to roll this back and you will need to completely uninstall all Sanctuary's components and modify registry keys.

To install the SecureWave Application Server

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 2000.
2. Close all programs running on the computer.
3. Insert the Sanctuary CD in your DVD/CD drive and run setup.exe located in the \SERVER\SXS folder.

The *Welcome* dialog is displayed.



Welcome to the Wise Solutions Wizard for SecureWave Application Server

The Wise Solutions(R) Wizard will install SecureWave Application Server on your computer. To continue, click Next.

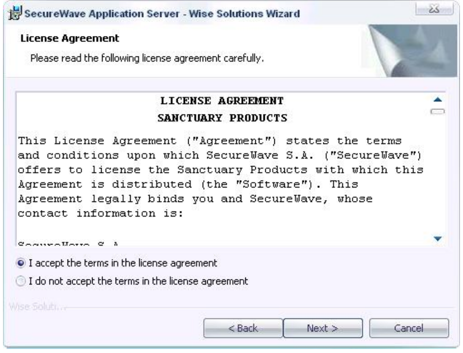
WARNING: This program is protected by copyright law and international treaties.

Figure 14: SecureWave Application Server installation: First step

4. Click on the NEXT button to continue.

The Setup does not 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.

The next dialog displays the License Agreement.



SecureWave Application Server - Wise Solutions Wizard

License Agreement

Please read the following license agreement carefully.

LICENSE AGREEMENT
SANCTUARY PRODUCTS

This License Agreement ("Agreement") states the terms and conditions upon which SecureWave S.A. ("SecureWave") offers to license the Sanctuary Products with which this Agreement is distributed (the "Software"). This Agreement legally binds you and SecureWave, whose contact information is:

SecureWave S.A.

● I accept the terms in the license agreement

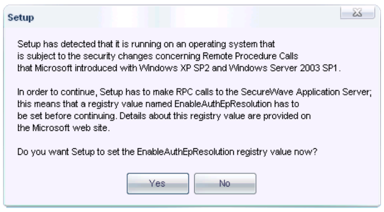
○ I do not accept the terms in the license agreement

Figure 15: SecureWave Application Server installation: License agreement

5. Read the license agreement carefully and, providing you agree with its conditions, select the accept option and click on Next to continue the installation process.

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

   If you are using an operating system subject to security changes concerning the RPC (Remote Procedure Call) protocol (Windows XP SP2 or Windows Server 2003 SP1 or SP2), the registry key ‘EnableAuthEpResolution’ must be changed:



Setup

Setup has detected that it is running on an operating system that
is subject to the security changes concerning Remote Procedure Calls
that Microsoft introduced with Windows XP SP2 and Windows Server 2003 SP1.

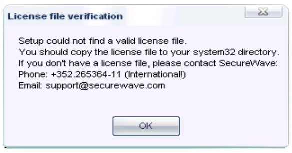
In order to continue, Setup has to make RPC calls to the SecureWave Application Server;
this means that a registry value named EnableAuthEpResolution has to
be set before continuing. Details about this registry value are provided on
the Microsoft web site.

Do you want Setup to set the EnableAuthEpResolution registry value now?

Figure 16: SecureWave Application Server installation: RPC warning

   See *Appendix D: Installing Sanctuary components on Windows XP SP2/2003 SP1* on page 109 for more information.

   The installation program checks for the presence of a valid license file is checked. If the setup program cannot find one or the file was altered in any way (e.g. due to an email filter introducing linefeed characters or translating foreign characters), an error message is displayed.



License file verification

Setup could not find a valid license file.
You should copy the license file to your system32 directory.
If you don't have a license file, please contact SecureWave:
Phone: +352.265364-11 (International!)
Email: support@securewave.com

Figure 17: SecureWave Application Server installation: No license found

6. If you have a license file and see an error message, check the name of the SecureWave.lic file and copy it to the %SYSTEMROOT%\SYSTEM32 folder.

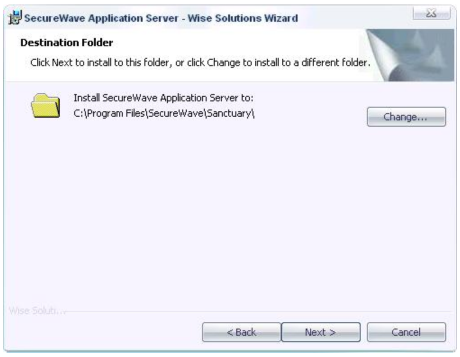
   If this does not resolve the problem, check your email client settings or contact SecureWave’s technical support team to obtain a new license file.

✍ *The program refuses to install SecureWave Application Server if it cannot find a valid license.*

💣 *If you are using more than one SecureWave Application Server the same license file must be used on all your servers.*

7. Choose the folder in which you want to install the SecureWave Application Server and click on Next. By default, the database is installed in the C:\Program Files\SecureWave\Sanctuary folder.

To choose another location, click on CHANGE and browse to the folder you want. Some components are always installed on the %SystemRoot%\system32 directory and a %SystemRoot%\sxsdata directory is always created.



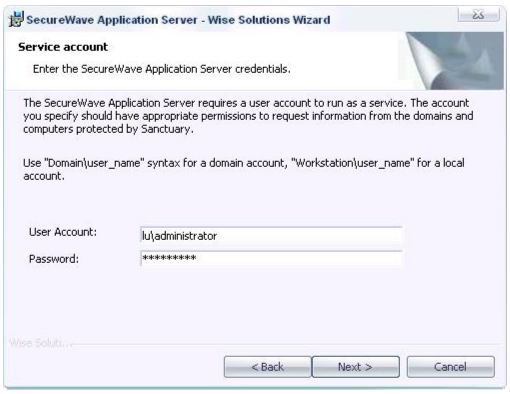
Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install SecureWave Application Server to:
C:\Program Files\SecureWave\Sanctuary\

Figure 18: SecureWave Application Server installation: Destination folder

8. Specify the user account you want to use to run the SecureWave Application Server. 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.



Service account

Enter the SecureWave Application Server credentials.

The SecureWave Application Server requires a user account to run as a service. The account you specify should have appropriate permissions to request information from the domains and computers protected by Sanctuary.

Use "Domain\user_name" syntax for a domain account, "Workstation\user_name" for a local account.

User Account: lu\administrator
Password: *********

Figure 19: SecureWave Application Server installation: Service account

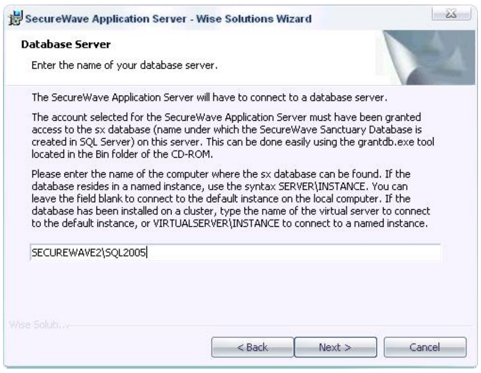
Domain accounts should be entered as DOMAIN\User while local accounts should be prefixed by the computer name (e.g. COMPUTER\User).

✍ *Setup checks 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, shadow and history files are stored.*

💣 *Before attempting to connect to a remote server, you must grant the service account the rights to connect and use the database. You must, therefore, log on to the computer where the SQL Server or Client 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).*

✍ *grant.exe is not compatible with Microsoft SQL Server 2005 since it does not have the DMO object activated by default. You must install SQLServer2005_BC.msi, a backward compatibility package on Microsoft's Web site, as a short-term solution to this problem.*

9. Specify the SQL Server instance that SecureWave Application Server should connect to. To do this, enter 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 SecureWave Sanctuary Database (sx)


SecureWave Application Server - Wise Solutions Wizard

Database Server

Enter the name of your database server.

The SecureWave Application Server will have to connect to a database server.

The account selected for the SecureWave Application Server must have been granted access to the sx database (name under which the SecureWave Sanctuary Database is created in SQL Server) on this server. This can be done easily using the grantdb.exe tool located in the Bin folder of the CD-ROM.

Please enter the name of the computer where the sx database can be found. If the database resides in a named instance, use the syntax SERVER\INSTANCE. You can leave the field blank to connect to the default instance on the local computer. If the database has been installed on a cluster, type the name of the virtual server to connect to the default instance, or VIRTUALSERVER\INSTANCE to connect to a named instance.

SECUREWAVE2\SQL2005

Figure 20: SecureWave Application Server installation: SecureWave Sanctuary Database server location

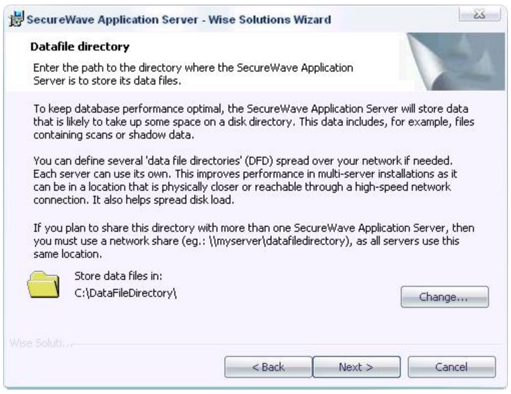
10. Click on NEXT to continue.

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

SecureWave Sanctuary Database server	The ***SecureWave Sanctuary Database*** is created in the default instance	The ***SecureWave Sanctuary Database*** is created in a Named instance
The database is on the local computer.	ServerName or 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

11. Choose the folder where you want the *SecureWave Application Server* log, shadow, or/and scan files are to be stored. Setup will suggest a directory named DataFileDirectory (DFD) under the system's drive root. You should use a permanent network share if you are planning to install more than one *SecureWave Application Server*. All servers can optionally write to the same, shared, directory or you can opt for having different ones for each server (see *Figure 1*). For evaluation purposes, use a single DFD in a local directory.


SecureWave Application Server - Wise Solutions Wizard

Datafile directory

Enter the path to the directory where the SecureWave Application Server is to store its data files.

To keep database performance optimal, the SecureWave Application Server will store data that is likely to take up some space on a disk directory. This data includes, for example, files containing scans or shadow data.

You can define several 'data file directories' (DFD) spread over your network if needed. Each server can use its own. This improves performance in multi-server installations as it can be in a location that is physically closer or reachable through a high-speed network connection. It also helps spread disk load.

If you plan to share this directory with more than one SecureWave Application Server, then you must use a network share (eg.: \\myserver\datafiledirectory), as all servers use this same location.

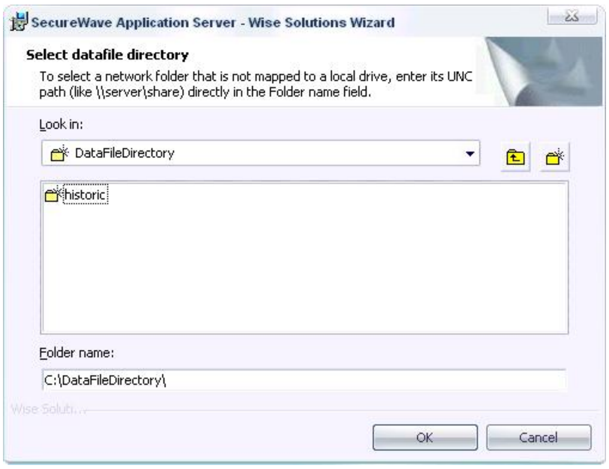
Store data files in:
C:\DataFileDirectory\

Figure 21 : SecureWave Application Server installation: Data file directory

✍ *You can have several ‘data file directories’ (DFD, see Figure 1) defined and spread over your network to be used by the SecureWave Application Server(s). Each server can use its own. This improves performance in multi-server installations as each server can be configured to store its data files in a location that is physically closer, or reachable through a high-speed network connection. It also helps spread disk load, as each defined directory only contains part of the files. Note that it is still possible for more than one server to use the same DFD, all servers can still access all data files — it does not matter if only one or multiple directories are used, when a server does not find a file in its defined directory, it requests a copy from a server having access to it.*

💣 *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 the members of the ‘Power Users’ group.*

12. If you want to change the directory location or if you are installing more than one *SecureWave Application Server*, select a shared network folder. To do this, click on CHANGE and locate the path you want to use for the DataFileDirectory:



Select datafile directory

To select a network folder that is not mapped to a local drive, enter its UNC path (like \\server\share) directly in the Folder name field.

Look in: DataFileDirectory

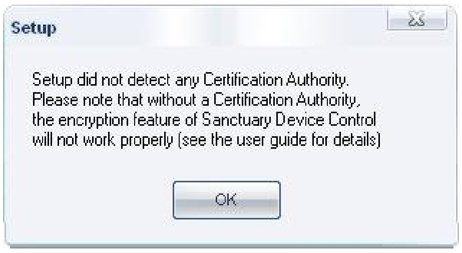
historic

Folder name: C:\DataFileDirectory\

Figure 22: SecureWave Application Server installation: Change destination folder

✍ *Always use a Universal/Uniform Naming Convention (UNC) path name, for example, \\server\volume\directory. Do NOT use a mapped drive.*

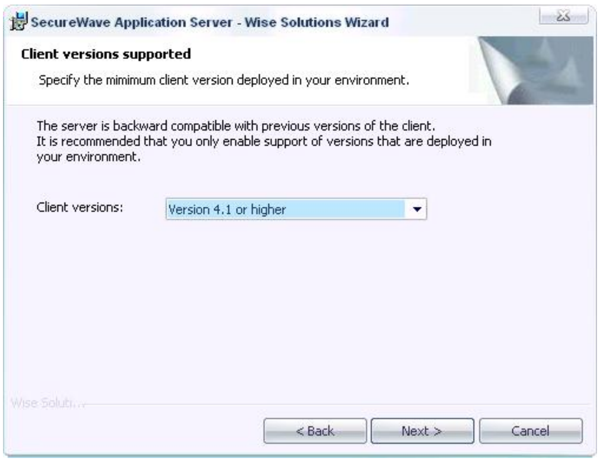
If you are installing Sanctuary Device Control and do not have a Certification Authority installed, the following warning message is displayed:



Setup did not detect any Certification Authority.
Please note that without a Certification Authority,
the encryption feature of Sanctuary Device Control
will not work properly (see the user guide for details)

Figure 23: SecureWave Application Server installation: No Certification Authority found

13. Specify the protocol that SecureWave Application Server should use. You can either choose the standard one, used to communicate with older clients, or the improved protocol, which includes optional TLS protocol that only works with the latest client version. Select from the list the type of client you already have installed. If this is a new installation, select the latest version.



SecureWave Application Server - Wise Solutions Wizard

Client versions supported

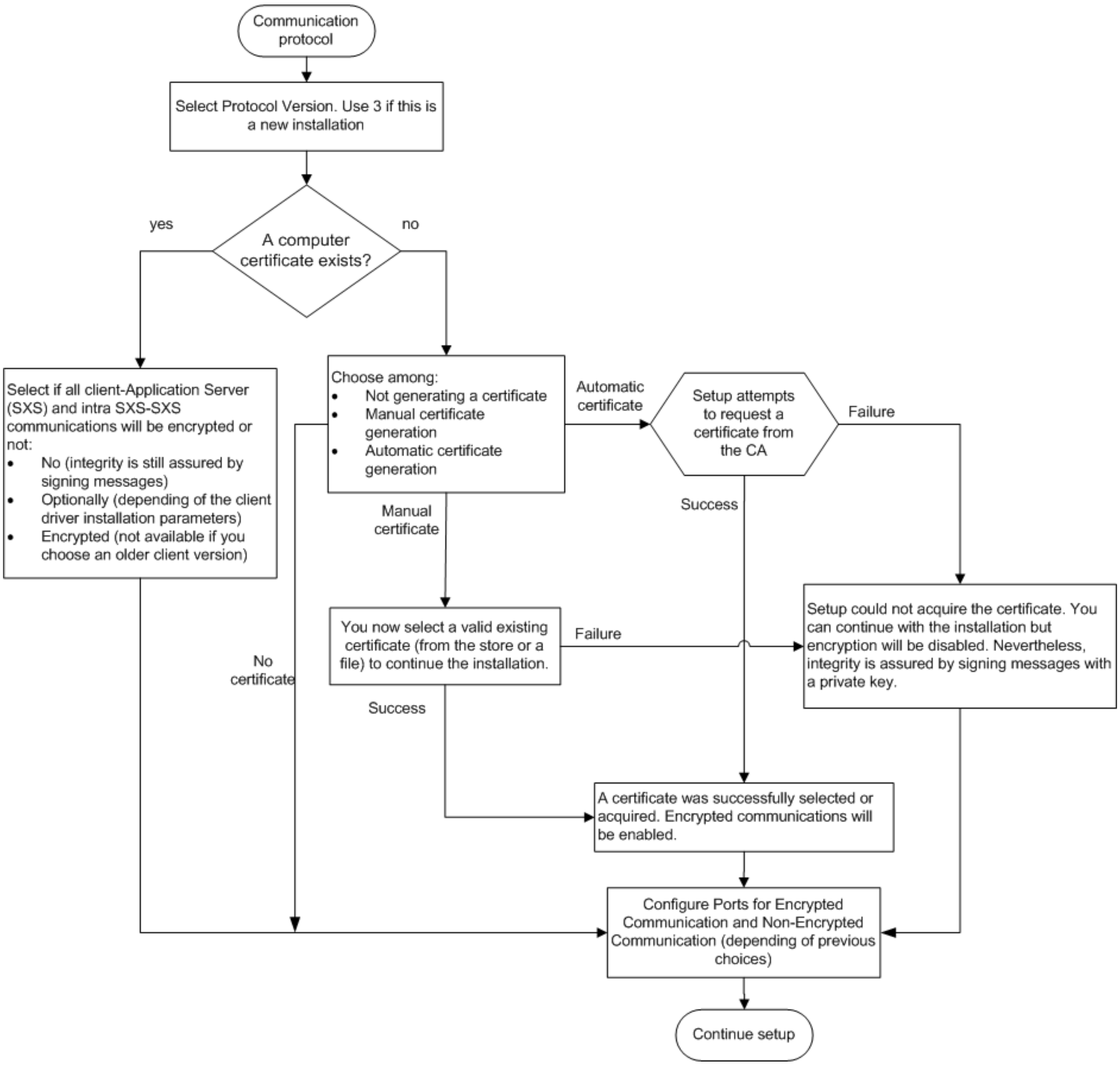
Specify the mimimum client version deployed in your environment.

The server is backward compatible with previous versions of the client.
It is recommended that you only enable support of versions that are deployed in your environment.

Client versions: Version 4.1 or higher

Figure 24: SecureWave Application Server installation: Protocol selection dialog

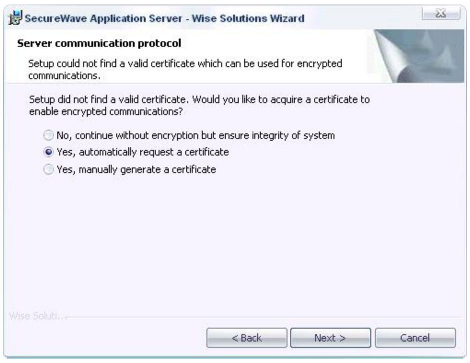
14. For the rest of the installation, follow flowchart below (especially if you choose the latest version of the client):



Communication protocol
Select Protocol Version. Use 3 if this is a new installation
A computer certificate exists?
yes
no
Select if all client-Application Server (SXS) and intra SXS-SXS communications will be encrypted or not:
• No (integrity is still assured by signing messages)
• Optionally (depending of the client driver installation parameters)
• Encrypted (not available if you choose an older client version)
Choose among:
• Not generating a certificate
• Manual certificate generation
• Automatic certificate generation
Automatic certificate
Setup attempts to request a certificate from the CA
Failure
Success
Manual certificate
No certificate
You now select a valid existing certificate (from the store or a file) to continue the installation.
Failure
Success
Setup could not acquire the certificate. You can continue with the installation but encryption will be disabled. Nevertheless, integrity is assured by signing messages with a private key.
A certificate was successfully selected or acquired. Encrypted communications will be enabled.
Configure Ports for Encrypted Communication and Non-Encrypted Communication (depending of previous choices)
Continue setup

Figure 25: SecureWave Application Server installation: Protocol selection flowchart

The following screens may appear, depending of the options selected (as stated in the flowchart depicted in *Figure 25*):



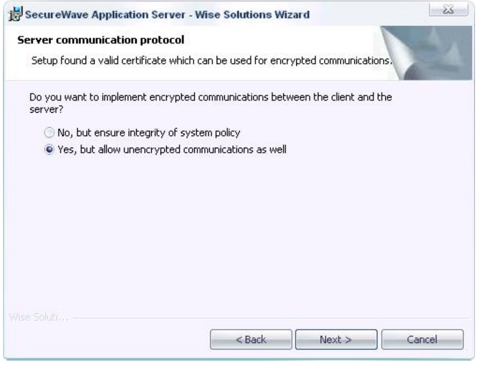
Server communication protocol

Setup could not find a valid certificate which can be used for encrypted communications.

Setup did not find a valid certificate. Would you like to acquire a certificate to enable encrypted communications?

○ No, continue without encryption but ensure integrity of system
● Yes, automatically request a certificate
○ Yes, manually generate a certificate

Figure 26: SecureWave Application Server installation: No certificate



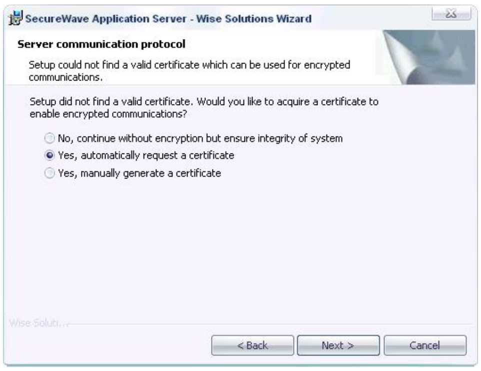
Server communication protocol

Setup found a valid certificate which can be used for encrypted communications.

Do you want to implement encrypted communications between the client and the server?

○ No, but ensure integrity of system policy
● Yes, but allow unencrypted communications as well

Figure 27: SecureWave Application Server installation: Valid certificate, old clients



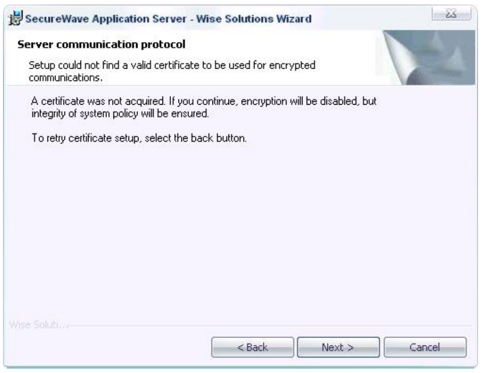
Server communication protocol

Setup could not find a valid certificate which can be used for encrypted communications.

Setup did not find a valid certificate. Would you like to acquire a certificate to enable encrypted communications?

○ No, continue without encryption but ensure integrity of system
● Yes, automatically request a certificate
○ Yes, manually generate a certificate

Figure 28: SecureWave Application Server installation: Valid certificate new clients



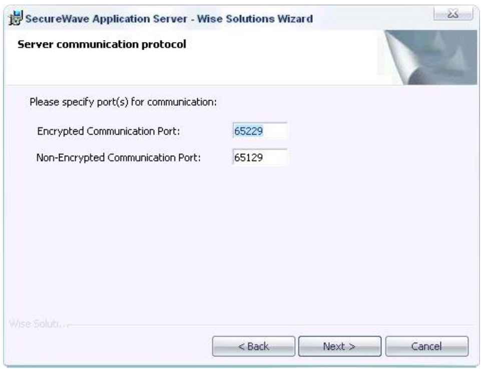
Server communication protocol

Setup could not find a valid certificate to be used for encrypted communications.

A certificate was not acquired. If you continue, encryption will be disabled, but integrity of system policy will be ensured.

To retry certificate setup, select the back button.

Figure 29: SecureWave Application Server installation: Could not retrieve or generate a valid certificate



Server communication protocol

Please specify port(s) for communication:

Encrypted Communication Port: 65229

Non-Encrypted Communication Port: 65129

Figure 30: SecureWave Application Server installation: Communication port configuration

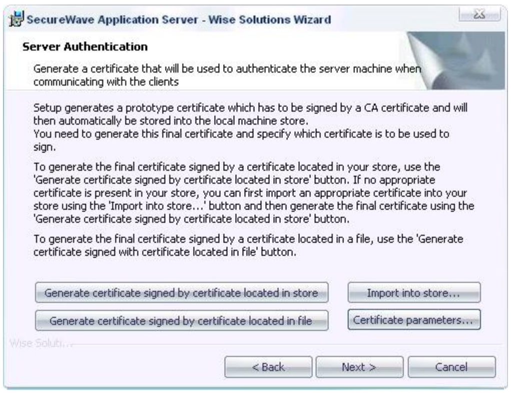
✍ *You should only configure the 'Communication Port' fields when the proposed ones are used by another software application or blocked for security reasons.*

✍ *The parameters selected in the previous dialogs should also be used if you are installing more than one SecureWave Application Server. See Using TLS for the inter-SecureWave Application Server communication on page 15 for more information.*

✍ *For a detailed manual tuning, see Table 20 & Table 21 on page 100.*

When the *Automatic request certificate* option is selected, the program attempts to obtain a valid certificate by requesting it to the Certificate Authority. If this fails, the installation can continue but communication's encryption is deactivated. Nevertheless, integrity is assured by signing the messages with a private key (see *Chapter 7: Using the Key Pair Generator* on page *59*).

If you select the manual option, a new dialog opens where you are invited to select the location where a valid machine certificate can be found — you must already have a Certificate Authority installed or the required certificate at hand. See *Appendix H: Installing a Certificate Authority for encryption and TLS Communication* on page *129* for more details. The available options are the same ones described for the client installation (found on page *42*).


SecureWave Application Server - Wise Solutions Wizard
Generate certificate signed by certificate located in store
Import into store...
Generate certificate signed by certificate located in file
Certificate parameters...
Wise Soluti...
< Back
Next >
Cancel

Server Authentication

Generate a certificate that will be used to authenticate the server machine when communicating with the clients

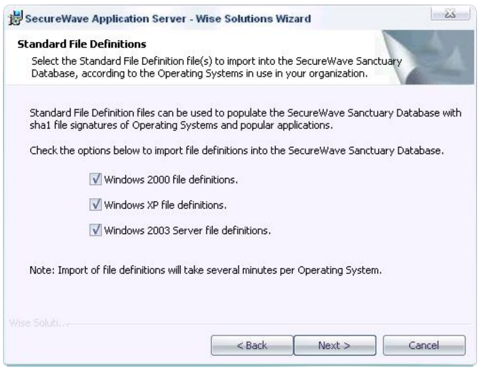
Setup generates a prototype certificate which has to be signed by a CA certificate and will then automatically be stored into the local machine store.
You need to generate this final certificate and specify which certificate is to be used to sign.

To generate the final certificate signed by a certificate located in your store, use the 'Generate certificate signed by certificate located in store' button. If no appropriate certificate is present in your store, you can first import an appropriate certificate into your store using the 'Import into store...' button and then generate the final certificate using the 'Generate certificate signed by certificate located in store' button.

To generate the final certificate signed by a certificate located in a file, use the 'Generate certificate signed with certificate located in file' button.

Figure 31: SecureWave Application Server installation: Server authentication certificate location

15. Choose which Standard File Definitions files you want to import, if you have a Sanctuary Application Control Suite (Sanctuary Application Control Server Edition, Sanctuary Application Control Terminal Services Edition, or Sanctuary Application Control Custom Edition) license. These files contain the information required by the program to authorize all the OS files. See *Appendix I: Importing file definitions during setup* on page *135* for more information. Select the operating systems that you need (only) and click on NEXT.



Standard File Definitions

Select the Standard File Definition file(s) to import into the SecureWave Sanctuary Database, according to the Operating Systems in use in your organization.

Standard File Definition files can be used to populate the SecureWave Sanctuary Database with sha1 file signatures of Operating Systems and popular applications.

Check the options below to import file definitions into the SecureWave Sanctuary Database.

☑ Windows 2000 file definitions.

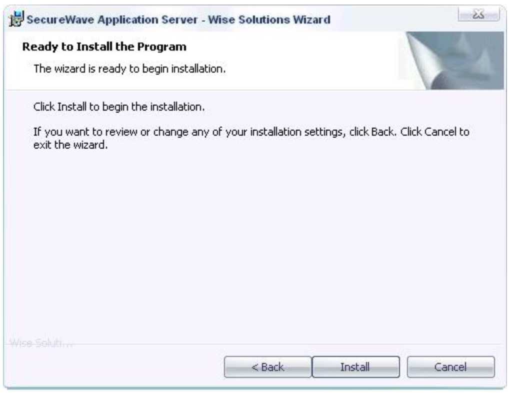
☑ Windows XP file definitions.

☑ Windows 2003 Server file definitions.

Note: Import of file definitions will take several minutes per Operating System.

Figure 32: SecureWave Application Server installation: Import Standard File Definitions

Setup is now ready to install the SecureWave Application Server Component.



Ready to Install the Program

The wizard is ready to begin installation.

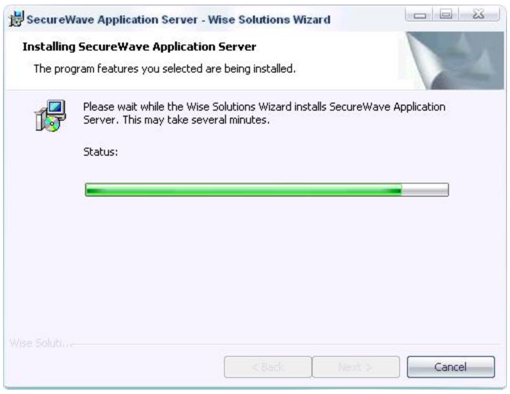
Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Figure 33: SecureWave Application Server installation: Final stage

16. Click on INSTALL to proceed. A warning message is displayed if you are not using a fixed IP address.

    Setup 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.



Installing SecureWave Application Server

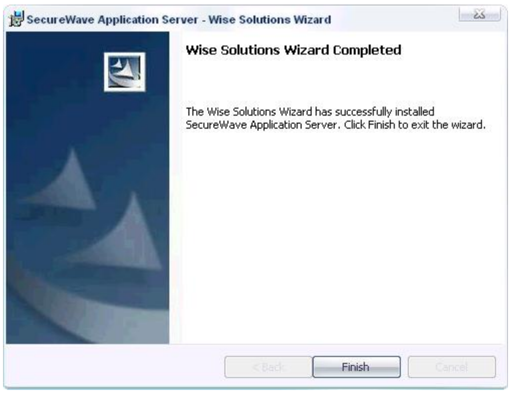
The program features you selected are being installed.

Please wait while the Wise Solutions Wizard installs SecureWave Application Server. This may take several minutes.

Status:

Figure 34: SecureWave Application Server installation: Installation

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



Wise Solutions Wizard Completed

The Wise Solutions Wizard has successfully installed SecureWave Application Server. Click Finish to exit the wizard.

Figure 35: SecureWave Application Server installation: Finishing the installation

17. Click on FINISH to close the wizard.

You should now have a working *SecureWave Application Server* connected to the *SecureWave Sanctuary Database*.

✍ *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. See Chapter 7: Using the Key Pair Generator on page* 59 *for more information.*

Items created during SecureWave Application Server setup

During the SecureWave Application Server installation, the setup creates the following items:

Item	*Purpose*	*Access*
Directory: C:\DataFileDirectory	Directory where the SecureWave Application Server logs, and shadow files are stored.	Full control for Administrators.
Directory: %INSTALLDIR%\SXTools	Folder where the FileTool, KeyGen, and SXDomain auxiliary tools are placed. You can find a full description of these tools in the corresponding administrator's guide and in this setup guide.	Full control for Administrators, Read/Execute for authenticated users.
Directory: %INSTALLDIR%\SSF	Contains all SecureWave Application Server EXE and DLL files.	Full control for Administrators, Read/Execute for authenticated users.
Uninstall registry keys*	Registry keys created to help delete the SecureWave Application Server.	n/a
Registry keys*: HKLM\system\CurrentControlSet\services\sxs\parameters	See *Appendix B: Registry keys* on page *97* for a complete description.	n/a
*You can block the use of the RegEdit.exe program for all users by using our Sanctuary Application Control Suite.		

Table 3: Items created by the SecureWave Application Server installation

✍ *The %INSTALLDIR% directory points to the folder where the program was installed. It is usually C:\Program Files\SecureWave\Sanctuary, but can refer to another folder.*

Chapter 4: Installing the Sanctuary Management Console

This chapter explains how to install the *Sanctuary Management Console* used to configure permissions to all the devices and/or executables that your organization uses. It is also used to carry out day-to-day administrative tasks and procedures. The information in this chapter is relevant to all Sanctuary software suite products.

You should read Appendix D: Installing Sanctuary components on Windows XP SP2/2003 SP1 on page 109 carefully before installing this component on a computer with this operating system and service pack.

When installing the Sanctuary Management Console you also install some or all of the following, depending on the type of license you have purchased:

> The *Client Deployment Tool* (see *Chapter 8: Unattended Client installation* on page 63) to deploy clients silently.

> The *Svolbro.exe* program (see description in the *Sanctuary Device Control Administrator's Guide*) needed for one of our USB key encryption methods.

> The *Authorization Wizard* (see description in the *Sanctuary Application Control Suite Administrator's Guide*) to search for executable files, create their hashes, and include them in the database.

> The *Versatile File Processor Tool* (see description in the Sanctuary Application Control Suite Administrator's Guide) to scan files.

If you are using Sanctuary Application Control Suite, you should also consider installing the Authorization Service (see the Sanctuary Application Control Suite Administrator's Guide) to monitor changes and create updates (using Microsoft's SUS or WSUS)

Before you install

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

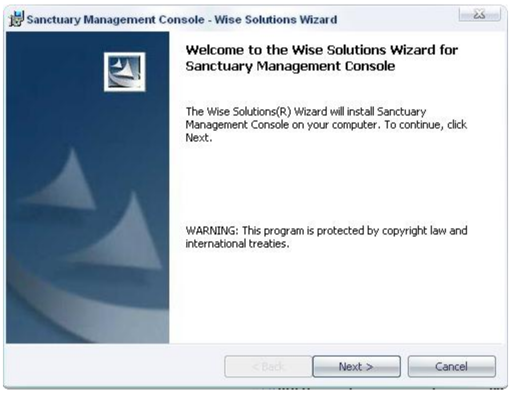
> Ensure that the computer(s) meet the minimum requirements. See *Appendix A: Detailed system requirements and limitations* on page *93* for details.

> 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.

To install the Sanctuary Management Console

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

1. Log on with an account that has administrative privileges in the computer in which you are installing the Sanctuary Management Console.
2. Close all programs running on the computer.
3. Insert the *Sanctuary CD* in your DVD/CD drive and run setup.exe located in the \Server\smc folder.



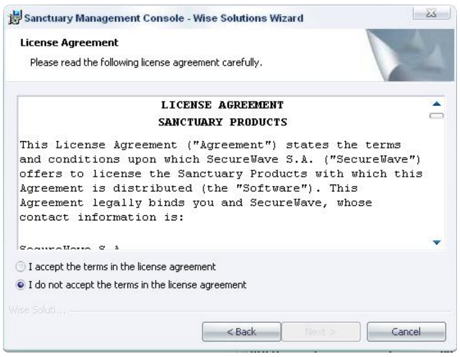
Welcome to the Wise Solutions Wizard for Sanctuary Management Console

The Wise Solutions(R) Wizard will install Sanctuary Management Console on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Figure 36: Sanctuary Management Console installation: First step

The next dialog displays the License Agreement.



License Agreement

Please read the following license agreement carefully.

```
                LICENSE AGREEMENT
               SANCTUARY PRODUCTS

This License Agreement ("Agreement") states the terms
and conditions upon which SecureWave S.A. ("SecureWave")
offers to license the Sanctuary Products with which this
Agreement is distributed (the "Software"). This
Agreement legally binds you and SecureWave, whose
contact information is:

SecureWave S.A.
```

○ I accept the terms in the license agreement

● I do not accept the terms in the license agreement

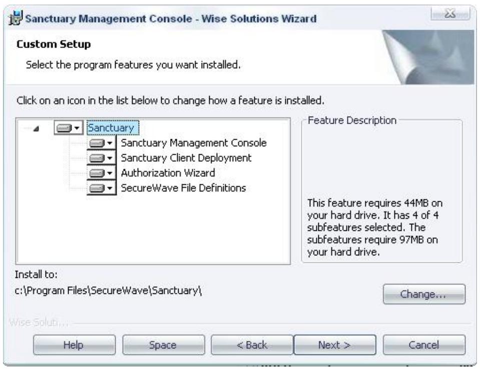
Figure 37: Sanctuary Management Console installation: License agreement

4. Read the license agreement carefully and, providing you agree with its conditions, select the accept option and click on NEXT 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 menu.*

5. Choose the destination directory, and other features — making a complete or custom installation.


Sanctuary Management Console - Wise Solutions Wizard
Sanctuary
Sanctuary Management Console
Sanctuary Client Deployment
Authorization Wizard
SecureWave File Definitions
Feature Description
Change...
Wise Soluti...
Help
Space
< Back
Next >
Cancel

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

This feature requires 44MB on your hard drive. It has 4 of 4 subfeatures selected. The subfeatures require 97MB on your hard drive.

Install to:
c:\Program Files\SecureWave\Sanctuary\

Figure 38: Sanctuary Management Console installation: Custom setup

✍ *The Sanctuary Management Console allows you to configure, manage, and monitor permissions to devices/executables. You use the Client Deployment tool to deploy silently clients on a group of computers. The Authorization Wizard allows administrators to quickly identify and authorize executables. File Definitions let you rapidly populate your database with signatures of all the files needed for running your operating systems.Select the features you want.*

If you decide to modify the default installation location, click on CHANGE and select a local path to install the components and documentation. By default, the files are copied to the %ProgramFiles%\SecureWave\Sanctuary\Console directory.

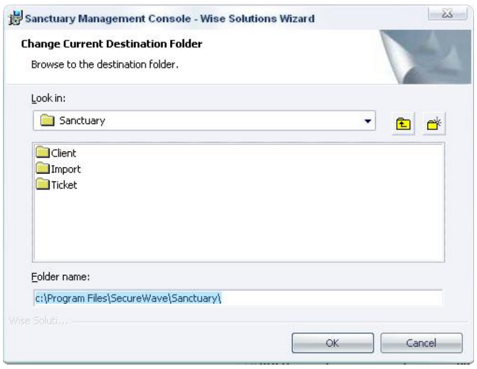
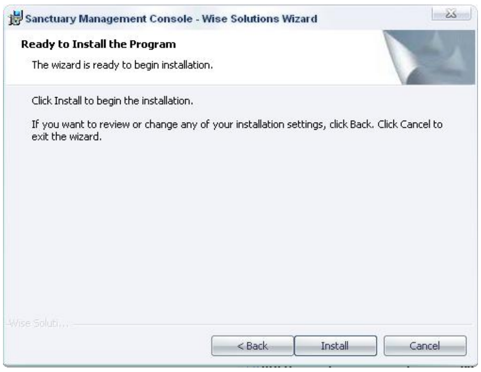

Sanctuary Management Console - Wise Solutions Wizard
Change Current Destination Folder
Browse to the destination folder.
Look in:
Sanctuary
Client
Import
Ticket
Folder name:
c:\Program Files\SecureWave\Sanctuary\
Wise Soluti...
OK
Cancel

Figure 39: Sanctuary Management Console installation: Modify destination folder

6. Click on OK to continue the installation.

Now Setup is ready to install the files.


Sanctuary Management Console - Wise Solutions Wizard
Ready to Install the Program
Wise Soluti...
< Back
Install
Cancel

The wizard is ready to begin installation.

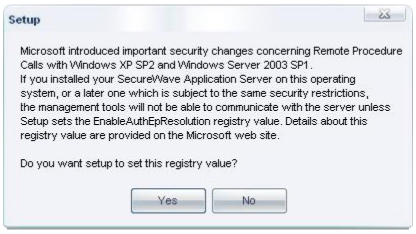
Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Figure 40: Sanctuary Management Console installation: Ready to install

7. Click on INSTALL to start the installation process. This takes approximately 2 minutes, depending on the components selected and the hardware used.

8. If the computer is running Windows XP SP2 or Windows 2003 SP1, click on YES to continue. In this case, Setup needs to adapt the Windows settings to allow RPC communication between the Sanctuary Management Console and the SecureWave Application Server. See *Appendix D: Installing Sanctuary components on Windows XP SP2/2003* SP1 on page *109*.

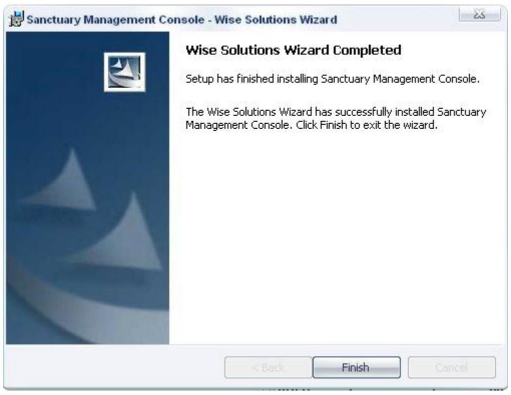


Microsoft introduced important security changes concerning Remote Procedure Calls with Windows XP SP2 and Windows Server 2003 SP1.
If you installed your SecureWave Application Server on this operating system, or a later one which is subject to the same security restrictions, the management tools will not be able to communicate with the server unless Setup sets the EnableAuthEpResolution registry value. Details about this registry value are provided on the Microsoft web site.

Do you want setup to set this registry value?

Figure 41: Sanctuary Management Console installation: Remote Procedure Calls warning

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



Wise Solutions Wizard Completed

Setup has finished installing Sanctuary Management Console.

The Wise Solutions Wizard has successfully installed Sanctuary Management Console. Click Finish to exit the wizard.

Figure 42: Sanctuary Management Console installation: Finishing the installation

9. 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 Management Console. You should define who can manage and define policies by selecting *User Access* from the *Tools* menu of the Sanctuary Management Console. See the relevant *Administrator's Guide* for further information.

✍ *If you are installing Sanctuary Device Control, we strongly recommend that you also install the Sanctuary Client on all computers having the Sanctuary Management Console. If you do not install it on the administrator's computer, it is not possible to use media encryption or to authorize multi-sessions DVDs/CDs with the Media Authorizer. See Chapter 5: Installing the Sanctuary Client on your endpoint computers on page 41 for more details.*

Items created during Sanctuary Management Console setup

During the Sanctuary Management Console installation, the setup creates the following items:

Item	*Purpose*	*Access*
Directory: %INSTALLDIR%\Console	Contains all Sanctuary Management Console EXE and DLL files.	Full control for Administrators, Read/Execute for authenticated users.
Directory: %SYSTEMROOT%\Help	Sanctuary Management Console help files.	Full control for Administrators, Read/Execute for authenticated users.
Uninstall registry keys*	Registry keys created to help delete the Sanctuary Management Console.	n/a
Shortcuts	All Windows' *Start*➔*Programs* menu shortcuts.	n/a
*You can block the use of the RegEdit.exe program for all users by using our Sanctuary Application Control Suite component.		

Table 4: Items created by the Sanctuary Management Console installation

✍ *The %INSTALLDIR% directory points to the folder where the program was installed. It is usually C:\Program Files\SecureWave\Sanctuary, but can refer to another folder. %SYSTEMROOT% is usually C:\Windows.*

Chapter 5: Installing the Sanctuary Client on your endpoint computers

The Sanctuary Client is the software used to manage the devices and/or applications on the endpoint computer/servers. This chapter explains how to install the Sanctuary Client on the endpoints 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 8: Unattended Client installation*.

The Sanctuary Client communicates with the SecureWave Application Server(s) to retrieve application/device control policies. This is done using a TCP/IP connection with a signed or encrypted communication — depending on the installation options. If this connection cannot be established using the Fully Qualified Domain Names (FQDN) or IP addresses, the driver tries to use the Proxy configured for Internet Explorer — if available – to locate a valid SecureWave Application Server. See Sanctuary's Architecture Guide for more info on how to configure this proxy connection.

Please read Appendix D: Installing Sanctuary components on Windows XP SP2/2003 SP1 on page 109 carefully 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 the Sanctuary Application Control Server Edition client on it. We do ***not*** *support Windows XP or Windows 2000 Pro for Sanctuary Application Control Server Edition (client component).*

Sanctuary Client is not supported on Windows 2003 Server (32- and 64-bit).

Please disable Windows' System Restore feature before installing the client. If you try to roll back to a previous state after installing the Sanctuary Client, the system becomes unstable. This is a System Restore design limitation since it will not reinstate all files completely. Be aware that System Restore is not a substitute for uninstalling a program.

System requirements

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

Overall system requirements

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

- Ensure that the *SecureWave Sanctuary Database*, *SecureWave Application Server*, and *Sanctuary Management 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 Management 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 Application Control Server Edition or Sanctuary Application Control Custom Edition, confirm that the *Blocking Mode* option is set to *Non Blocking Mode*, in the *Default Options* dialog of the console.
- If you have already installed the client driver and want to uninstall/ modify/ repair it, issue an 'Endpoint Maintenance Ticket', using the management console, and copy it to the required directory. Please consult

your corresponding *Administrator's Guide* and *Uninstalling* the Sanctuary Client on page *50* for more information. If you are using our client deployment tool, you only need to specify a valid SecureWave Application Server address from where the ticket is obtained.

> If you are planning to use the TLS protocol for your client driver, have a valid certificate issued by your Certificate Authority installed and configured (as explained in the *Appendix H: Installing a Certificate Authority for encryption and TLS Communication*).

💣 *The decision whether or not to use encrypted communications (TLS protocol) should not be taken lightly. Once you decide to use TLS for your Sanctuary Client Driver -SecureWave Application Server and/or intra-SecureWave Application Server communications and install Sanctuary in this mode, it is very difficult to roll this back: You must completely uninstall all Sanctuary's components and modify registry keys.*

Client computer requirements

Make sure that the computer meets the minimum hardware and software requirements. See *Appendix A: Detailed system requirements* on page *93* 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 a different name before starting the deployment. You can use GhostWalker.exe, SidChanger.exe, etc., to do this.*

✍ *Although the installation dialog only lets you input three SecureWave Application Servers, you can easily add more if needed. You can also change how the SecureWave Application Server(s) is selected — round robin vs. random pick. All this is done by modifying certain registry keys. See Sanctuary Client registry keys on page 102 and Uninstalling the Sanctuary Client on page 50 for more details. You can 'push' these modifications to all clients using Group Policies with ADM templates.*

✍ *The setup also lets you retrieve a 'Maintenance ticket' from the SecureWave Application Server (see the relevant Administrator's Guide). This is only done if a communication between them exists. If the 'client hardening' is enabled — the uninstall process allows you to choose how to deactivate it.*

To install Sanctuary Clients

The first step in this procedure is to decide whether or not you want to import the company's permissions and policies as an independent file during the installation process. If you 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. You should also include the public key — not the private one — in this directory. Proceed with the installation steps as described below carefully reading step 7: Providing the SecureWave Application Server address.

✍ *The policies.dat file should be accessible to the installation program. Be aware that if you place it in a network share — only valid for Active Directory environments —the computer account must have access to it through LocalSystem.*

See the *To export and import permission settings* section of the relevant *Administrator's Guide* for more information about how to export your settings to a file.

The *policies.dat* '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.

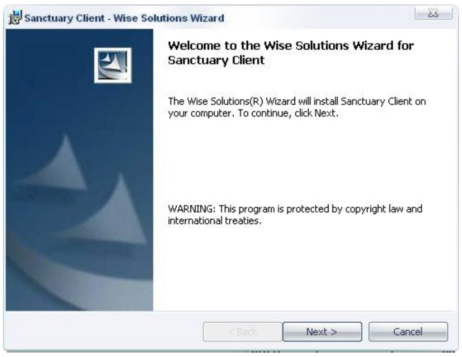
In the next step you must specify whether or not you are using TLS protocol for Sanctuary Client Driver - SecureWave Application Server communications. If using TLS, all transmissions are fully encrypted. If the TLS is not selected, all communications are signed using the key pair previously generated. See *Chapter 7: Using the Key Pair Generator* on page *59* for more information about how to create these keys.

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

1. Log on to the client computer using an account that has 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, and run the setup.exe file.

If you are installing the Sanctuary Client on a Vista machine with Vista's UAC (User Account Control) functionality turned on, you must use setup.exe (not Control Panel ➔ Add/Remove Programs) otherwise the operation will fail.

The Setup program shows the *Welcome* dialog:



Sanctuary Client - Wise Solutions Wizard

Welcome to the Wise Solutions Wizard for Sanctuary Client

The Wise Solutions(R) Wizard will install Sanctuary Client on your computer. To continue, click Next.

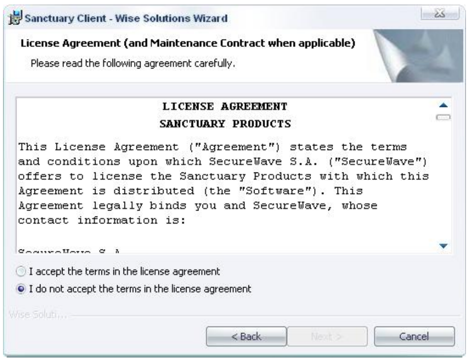
WARNING: This program is protected by copyright law and international treaties.

Figure 43: Sanctuary Client: First step

4. Click on NEXT to continue.

You cannot carry out maintenance if you do not first issue an 'Endpoint maintenance ticket' or relax the client security settings using the management console. See Uninstalling the Sanctuary Client on page 50 for more information.

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



Sanctuary Client - Wise Solutions Wizard

License Agreement (and Maintenance Contract when applicable)

Please read the following agreement carefully.

```
LICENSE AGREEMENT
SANCTUARY PRODUCTS

This License Agreement ("Agreement") states the terms
and conditions upon which SecureWave S.A. ("SecureWave")
offers to license the Sanctuary Products with which this
Agreement is distributed (the "Software"). This
Agreement legally binds you and SecureWave, whose
contact information is:

SecureWave S.A.
```

○ I accept the terms in the license agreement

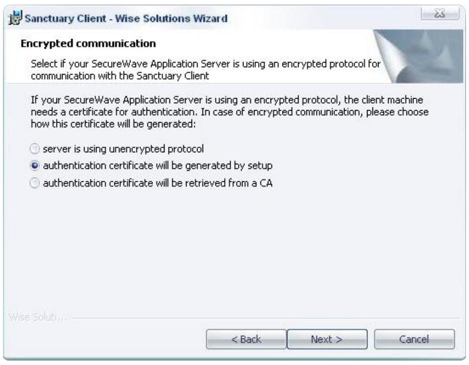
● I do not accept the terms in the license agreement

Figure 44: Sanctuary Client: License agreement

5. Read the license agreement carefully and, providing you agree with its conditions, select the accept option and click on NEXT and INSTALL to continue.

   If you do not agree with its stipulations, click on the CANCEL button to exit without installing the Sanctuary Client.

6. Specify whether or not you want the Sanctuary Client Driver to use the TLS protocol to communicate with SecureWave Application Server (see *Transport Layer Security* on page *12*).



Sanctuary Client - Wise Solutions Wizard

Encrypted communication

Select if your SecureWave Application Server is using an encrypted protocol for communication with the Sanctuary Client

If your SecureWave Application Server is using an encrypted protocol, the client machine needs a certificate for authentication. In case of encrypted communication, please choose how this certificate will be generated:

○ server is using unencrypted protocol
● authentication certificate will be generated by setup
○ authentication certificate will be retrieved from a CA

Figure 45: Sanctuary Client: Communication protocol

You can install the Sanctuary Client installation in one of three modes:

- ‘Server is using unencrypted protocol’ — No TLS.
  All communication between Sanctuary Client Driver and SecureWave Application Server(s) is not encrypted but is signed using the private key. This is, essentially, a legacy communication protocol and not recommended for high security installations.
- ‘Authentication certificate will be generated by setup’ — Manual mode using TLS communication.
  The administrator generates and provides the machine certificate that is used in all communications. All communication between Sanctuary Client Driver and SecureWave Application Server(s) is encrypted. This mode is used when there is no Certification Authority installed in the network or the CA cannot be reached when doing the client driver installation. The machine certificate has to be created by a user (usually the administrator) who already possesses a certificate that can be issued and who trusted as a root or intermediate Certificate Authority by the SecureWave Application Server. This authorized user has to be physically present at the machine to create the required certificate.
- ‘Authentication certificate will be retrieved form a CA’ — Automatic mode using TLS communication.
  The program attempts to obtain a valid computer’s certificate by requesting one from one of the selected Certificate Authorities. This certificate must be able to be issued and the CA trusted as a root or intermediate Certificate Authority by the SecureWave Application Server. All communication between Sanctuary Client Driver and SecureWave Application Server(s) is encrypted. You do not need a Certificate Authority at this point, but it is required when you first start the client(s), since the program requests a machine certificate. The user who has the rights to create machine’s certificates does not have to be physically present at the machine to do the installation if this mode is selected.

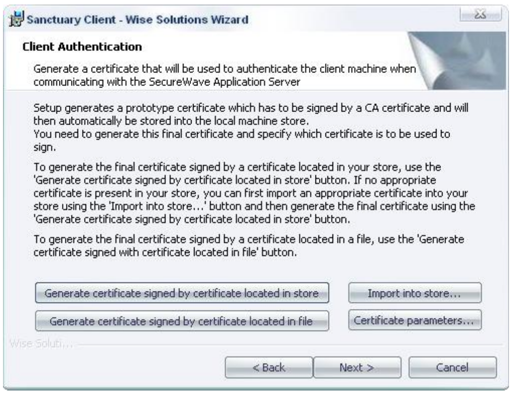
You should ALWAYS use automatic mode when your organization has already deployed a Certificate Authority infrastructure and the SecureWave Application Server and clients are part of it. In this case, deployment of Sanctuary Client Driver using TLS is completely transparent and requires no additional action.

We recommend you use the automatic mode in preference to all other methods for issuing valid certificates. If it is not possible to use this mode, then you should use the semi-automatic mode if you are using our Client Deployment Tool (see *Chapter 8: Unattended Client installation* on page *63*), and manual mode in all other cases.

Although you can select the port default values, you can always change them, if desired, to fine-tune the communication protocol by modifying the corresponding registry entries. See *Appendix B: Registry keys* on page *97* for more information.

Remember that you require a valid certificate on both machines (the one with SecureWave Application Server and the one with the Sanctuary Client Driver) in order to use a TLS channel that encrypts all communication. If you are not using TLS, all data transfer is signed with the private key generated before installing the first client. See *Chapter 7: Using the Key Pair Generator* on page *59* for more information about how to create these keys.

If selecting the second option, you should already have a valid machine certificate (i.e. not one that is revoked or has expired). The following screen is displayed, as:


Sanctuary Client - Wise Solutions Wizard
Client Authentication
Generate certificate signed by certificate located in store
Import into store...
Generate certificate signed by certificate located in file
Certificate parameters...
Wise Soluti...
< Back
Next >
Cancel

Generate a certificate that will be used to authenticate the client machine when communicating with the SecureWave Application Server

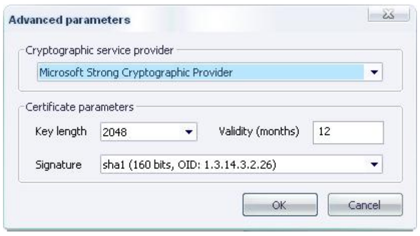
Setup generates a prototype certificate which has to be signed by a CA certificate and will then automatically be stored into the local machine store.
You need to generate this final certificate and specify which certificate is to be used to sign.

To generate the final certificate signed by a certificate located in your store, use the 'Generate certificate signed by certificate located in store' button. If no appropriate certificate is present in your store, you can first import an appropriate certificate into your store using the 'Import into store...' button and then generate the final certificate using the 'Generate certificate signed by certificate located in store' button.

To generate the final certificate signed by a certificate located in a file, use the 'Generate certificate signed with certificate located in file' button.

Figure 46: Sanctuary Client: Communication protocol

TLS protocol uses a certificate to encrypt messages sent over the channel. In this dialog, you can select the machine's certificate location and its parameters. When selecting the computer certificate's parameters you can choose the service provider, key length, validity and signature shown below:



Cryptographic service provider: Microsoft Strong Cryptographic Provider

Certificate parameters

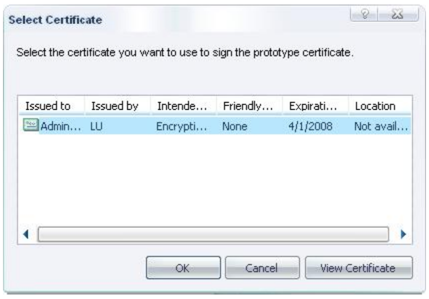
Key length: 2048

Validity (months): 12

Signature: sha1 (160 bits, OID: 1.3.14.3.2.26)

Figure 47: Sanctuary Client: Certificate's parameters

If you select Import into store, Windows' Certification Wizard opens to allow you to retrieve the computer certificate. All other options require a valid certificate to exist in a store (special location where the Certificate authority saves valid certificates) or directly in a file that is imported to the local certificate store. An administrator can generate a valid one using the MMC console (Start➔Run➔mmc.exe):

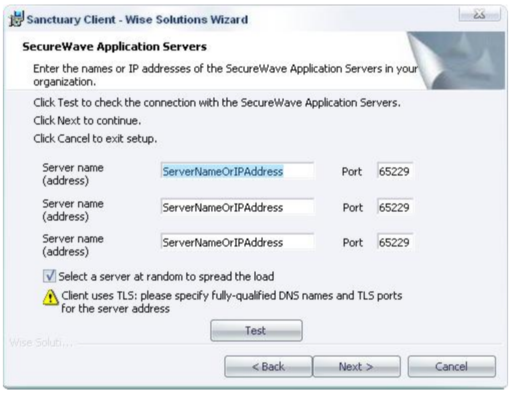


Select the certificate you want to use to sign the prototype certificate.

Issued to	Issued by	Intende...	Friendly...	Expirati...	Location
Admin...	LU	Encrypti...	None	4/1/2008	Not avail...

Figure 48: Sanctuary Client: Certificate's parameters

7. Enter the *Server name* of at least one SecureWave Application Server on your network. You can enter up to three server names during the setup and more afterwards in the client registry (see *Appendix B: Registry keys* on page *97* for details). The dialog accepts fully qualified domain names (FQDNs) or IP addresses. If you are using TLS protocol, you MUST specify fully qualified DNS names for the servers. You can also proceed without providing a server address.



Sanctuary Client - Wise Solutions Wizard

SecureWave Application Servers

Enter the names or IP addresses of the SecureWave Application Servers in your organization.

Click Test to check the connection with the SecureWave Application Servers.
Click Next to continue.
Click Cancel to exit setup.

Server name (address)	ServerNameOrIPAddress	Port	65229
Server name (address)	ServerNameOrIPAddress	Port	65229
Server name (address)	ServerNameOrIPAddress	Port	65229

☑ Select a server at random to spread the load

⚠ Client uses TLS: please specify fully-qualified DNS names and TLS ports for the server address

Figure 49: Sanctuary Client: SecureWave Application Server name or address

8. 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. The ports are different if you are using TLS (65229) or not (65129). If using TLS, there is a REQUEST CERTIFICATE button that is used to contact the Certificate Authority and ask for a valid computer certificate.

   There are three different cases:

   - You specify a correct address for the SecureWave Application Server. This address is validated and, if correct, the setup continues. All permissions for the client are retrieve form 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 Sanctuary Client on machines that are not currently connected to a SecureWave 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 (see your corresponding *Administrator's Guide*). If this file is not available, the default built-in restrictive settings are applied.
   - There is a valid server and the *policies.dat* file exists, policies are imported from this file.

SecureWave Application Server 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 policies.dat.
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 policies.dat file until a server can be contacted and the permissions updated.

Table 5: Server address and import file relationship

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

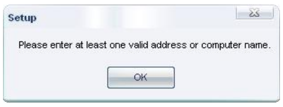
You can also choose to contact the servers sequentially in the order you enter them. This setting is ended for particularly adapted to configurations that have a primary SecureWave Application Server and a backup one. The driver connects to the primary SecureWave Application Server, that is, the first one on the list, unless this is not available, in which case the driver tries 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 to use, the most restrictive policies apply. The client has no permissions at all even when some devices have predefined restricted permissions, for example, read/write permissions for the PS/2 port. See the Sanctuary Device Control 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 to use and you are installing Sanctuary Application Control Suite, applications are NOT blocked until the first contact has been established.

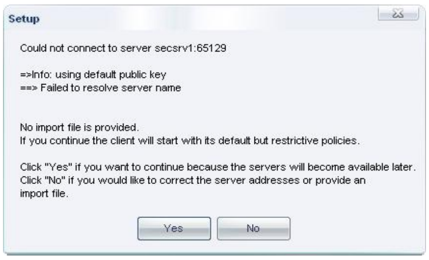
9. Choose between spreading the load through all selected servers (random load balancing) and selecting them in the order provided in the fields. To do this, activate (or deactivate) the *Select a server at random to spread the load* option.

10. Click on NEXT to proceed. The server address is validated, but you can still continue if it is invalid or unspecified:



Please enter at least one valid address or computer name.

Figure 50: Sanctuary Client: No address specified



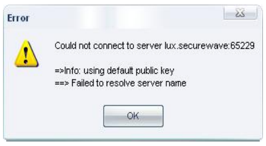
Could not connect to server secsrv1:65129

=>Info: using default public key
==> Failed to resolve server name

No import file is provided.
If you continue the client will start with its default but restrictive policies.

Click "Yes" if you want to continue because the servers will become available later.
Click "No" if you would like to correct the server addresses or provide an import file.

Figure 51: Sanctuary Client: No valid address specified or cannot contact server

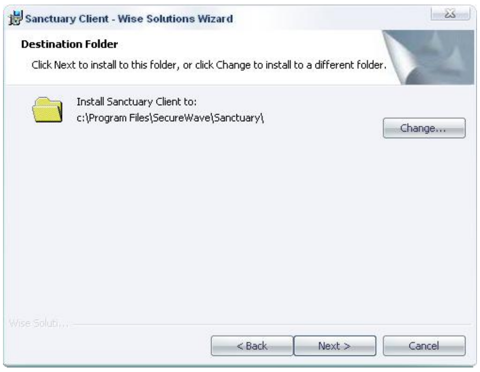


Could not connect to server lux.securewave:65229

=>Info: using default public key
==> Failed to resolve server name

Figure 52: Sanctuary Client: Test failed

11. Choose the target directory for the installation (typically the default one) and click on NEXT to continue.



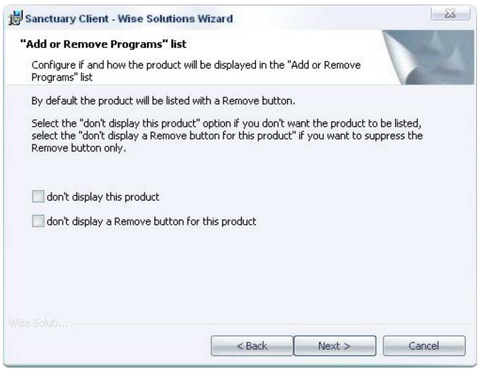
Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Sanctuary Client to:
c:\Program Files\SecureWave\Sanctuary\

Figure 53: Sanctuary Client: Change the target directory

12. Choose how the uninstall process is controlled. You can select the first option so that the program is not listed on Windows' *Add Remove Programs* dialog or select the second one to show the program in the list but not provide a REMOVE button:



Sanctuary Client - Wise Solutions Wizard

"Add or Remove Programs" list

Configure if and how the product will be displayed in the "Add or Remove Programs" list

By default the product will be listed with a Remove button.

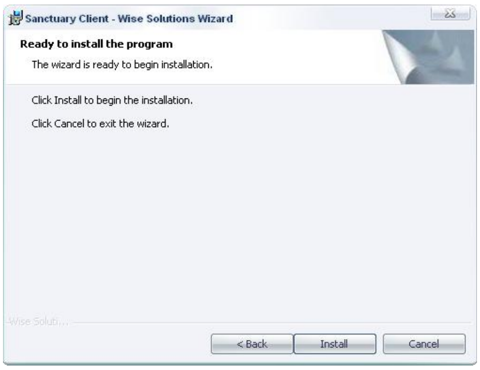
Select the "don't display this product" option if you don't want the product to be listed, select the "don't display a Remove button for this product" if you want to suppress the Remove button only.

□ don't display this product

□ don't display a Remove button for this product

Figure 54: Sanctuary Client: How will the program appear on the Windows' Add Remove Program dialog

The program is now ready to be installed:



Sanctuary Client - Wise Solutions Wizard

Ready to install the program

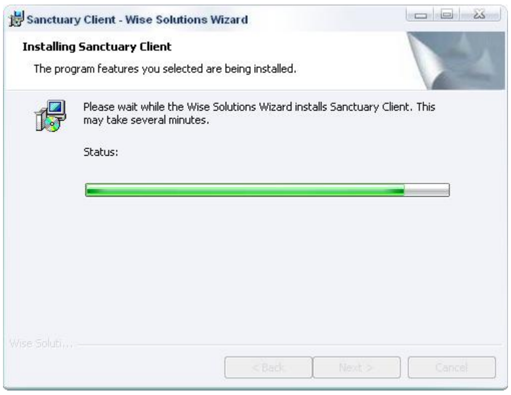
The wizard is ready to begin installation.

Click Install to begin the installation.

Click Cancel to exit the wizard.

Figure 55: Sanctuary Client: The installation process is ready to start

13. Click on INSTALL to proceed. The setup takes about 2 minutes, depending on the hardware in use.



Sanctuary Client - Wise Solutions Wizard

Installing Sanctuary Client

The program features you selected are being installed.

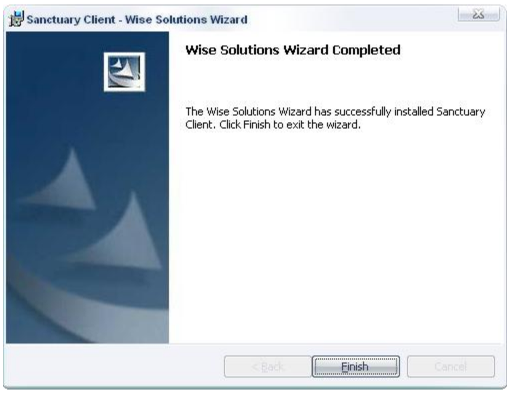
Please wait while the Wise Solutions Wizard installs Sanctuary Client. This may take several minutes.

Status:

Figure 56: Sanctuary Client: The installation progress

✍ *You may also see an error message if you are using Windows XP SP2 and the TCP port that the firewall blocks cannot be unblocked by the installation program.*

14. Click on FINISH to close the dialog and complete the procedure.

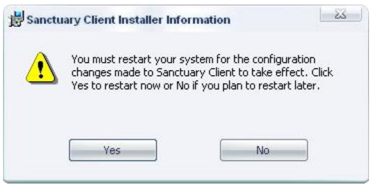


Wise Solutions Wizard Completed

The Wise Solutions Wizard has successfully installed Sanctuary Client. Click Finish to exit the wizard.

Figure 57: Sanctuary Client: FINISHING the installation process

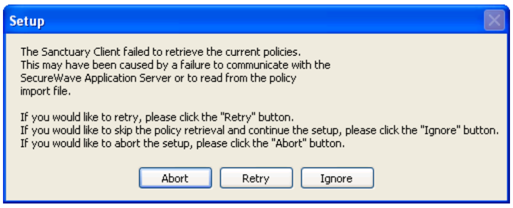
15. Reboot your computer when prompted to do so by the Sanctuary Client setup program. To do this, click on YES to restart the computer.



You must restart your system for the configuration changes made to Sanctuary Client to take effect. Click Yes to restart now or No if you plan to restart later.

Figure 58: Sanctuary Client: Restarting the computer

The following dialog is displayed if the policies file could not be retrieved or initialized. If you choose to ignore this situation, you risk blocking your machine since the most restrictive of all policies applies — i.e. no access at all.

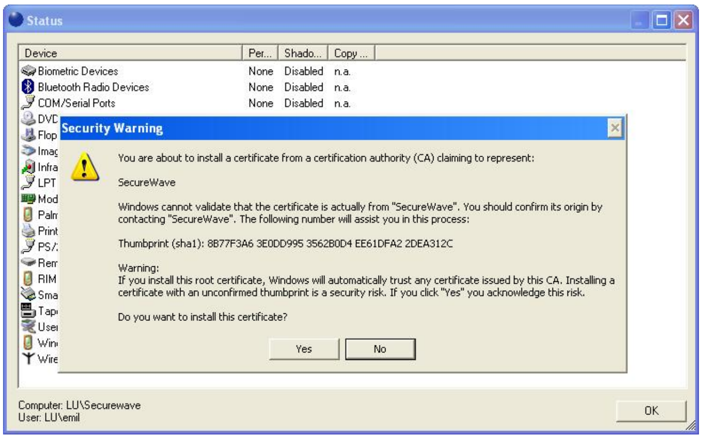


The Sanctuary Client failed to retrieve the current policies.
This may have been caused by a failure to communicate with the
SecureWave Application Server or to read from the policy
import file.

If you would like to retry, please click the "Retry" button.
If you would like to skip the policy retrieval and continue the setup, please click the "Ignore" button.
If you would like to abort the setup, please click the "Abort" button.

Figure 59: Sanctuary Client: No import file and no server address specified

After finishing the installation, you now have all the required components copied in the selected installation folder, several directories created, and all the required registry keys generated in the client machine.



Device	Per...	Shado...	Copy ...
Biometric Devices	None	Disabled	n.a.
Bluetooth Radio Devices	None	Disabled	n.a.
COM/Serial Ports	None	Disabled	n.a.
DVD			
Flop			
Imag			
Infra			
LPT			
Mod			
Palm			
Print			
PS/:			
Rem			
RIM			
Sma			
Tap			
User			
Win			
Wire			

You are about to install a certificate from a certification authority (CA) claiming to represent:

SecureWave

Windows cannot validate that the certificate is actually from "SecureWave". You should confirm its origin by contacting "SecureWave". The following number will assist you in this process:

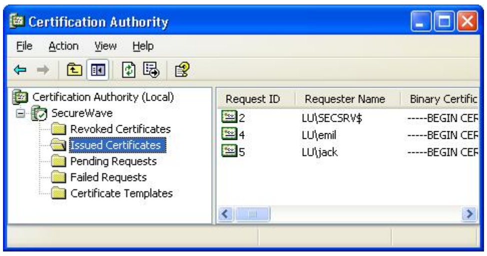
Thumbprint (sha1): 8B77F3A6 3E0DD995 3562B0D4 EE61DFA2 2DEA312C

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Computer: LU\Securewave
User: LU\emil

Figure 60: Sanctuary Client: Certificate generation and installation



Request ID	Requester Name	Binary Certific
2	LU\SECSRV$	-----BEGIN CER
4	LU\emil	-----BEGIN CER
5	LU\jack	-----BEGIN CER

Figure 61: Sanctuary Client: Certificate Authority issued certificates

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 8: Unattended Client installation* on page *63* for information about 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 Driver, you can uninstall it from the client computer. If you used Group Policy to do an unattended installation, then you can also use Group Policy to uninstall the client(s).

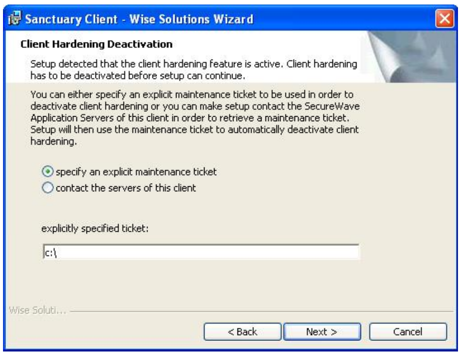
✍ *Uninstalling the Sanctuary Client Driver briefly disconnects the computer from the network. This behavior can cause problems if you are working in a remote connection or doing other remote tasks.*

You can use the Client Deployment Tool to do an unattended install/uninstall of the client package. See *Using the Sanctuary Client Deployment tool to install the Sanctuary* Client on page *71*.

If the client was installed manually, then select *Add/Remove Programs* from the Windows Control Panel, and choose *Sanctuary Client Driver* from the list of installed programs. The Setup program launches and uninstalls Sanctuary Client Driver. You must reboot the computer once finished. Remember that this option may or may not be present, depending on choices you made during the setup process.

⌛ *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.*

Since you are now in a highly secure environment, changes to the client and its components have to be done in an orderly fashion. Even if you are an administrator, the services, registry entries, and special directories of the client cannot be modified before taking some measures to certify that you have the right to do so.



Client Hardening Deactivation

Setup detected that the client hardening feature is active. Client hardening has to be deactivated before setup can continue.

You can either specify an explicit maintenance ticket to be used in order to deactivate client hardening or you can make setup contact the SecureWave Application Servers of this client in order to retrieve a maintenance ticket. Setup will then use the maintenance ticket to automatically deactivate client hardening.

● specify an explicit maintenance ticket
○ contact the servers of this client

explicitly specified ticket: c:\

Figure 62: Defining from where does the Sanctuary Client Driver gets its maintenance ticket

To uninstall the client you should either:

> Deactivate the ‘client hardening’ option using the management console.

> Generate an ‘Endpoint Maintenance Ticket’ that overrules the ‘client hardening option’.

If you chose to create and save an endpoint maintenance ticket, the client will search for it:

> On the same directory where the .msi package resides (‘default maintenance ticket’ called ‘ticket.smt’).

> In the ‘ticket’ directory which is created by the setup during the client installation (‘explicit maintenance ticket’).

> Request it from a SecureWave Application Server (the user must have valid credentials to do this) if you are using our client deployment tool.

Please consult your corresponding *Administrator’s Guide* or help file for a complete description on how to create an Endpoint Maintenance Ticket.

Load balancing methods

What is load balancing

When you have two or more SecureWave Application Servers in your network, it is necessary to distribute the processing activity evenly so that the SecureWave Application Servers work in a more or less ‘balanced’ state and 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.

One approach is to use a load balancing technique called round robin, which works on a rotating basis, i.e. in a loop.

How does round robin DNS works?

When a DNS server that is configured in a round robin fashion receives a request, it resolves 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 SecureWave Application Server in the 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 sent to SecureWave Application Servers have been evenly distributed among all of the machines in the cluster. 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 are unpredictably unavailable. 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 servers are added or removed, you only need to edit one DNS table, not to modify registry settings.

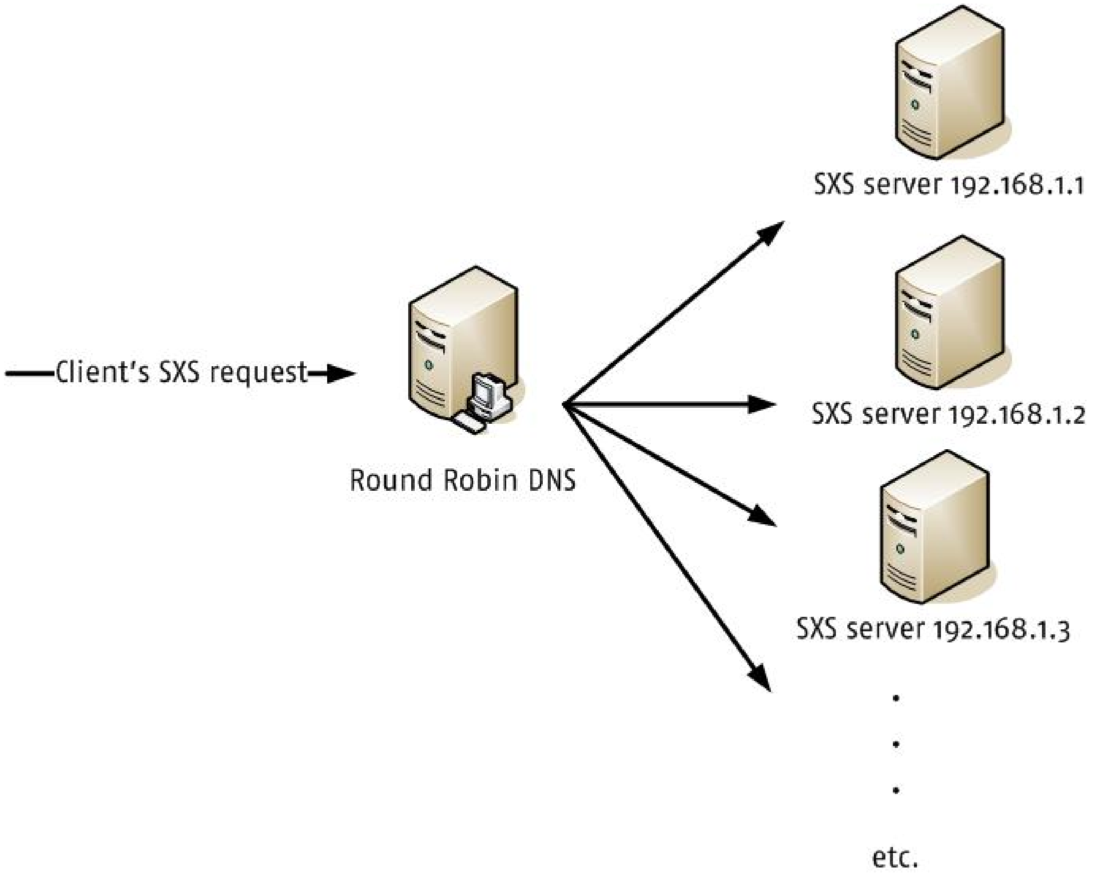


Figure 63: Round Robin DNS schema

✍ *Windows 2000 has some bugs related to DNS round robin. You must apply the latest patches solves them.*

Items created during the Sanctuary Client setup

When doing a Sanctuary Client installation, the setup creates the following items:

Item	***Purpose***	***Access***
Directory: %INSTALLDIR%\Client	Contains the Sanctuary Client and all required components.	Restricted access granted to Administrators and LocalSystem, read/execute access granted to Everyone. The security settings are propagated to child objects.
Directory: %INSTALLDIR%\Import	Used for a special file that is used to import permissions. This file is created by exporting permissions using the Sanctuary Management Console and has a two-week validity.	Read/write access granted to Everyone.
Directory: %INSTALLDIR%\Ticket	Where the endpoint maintenance ticket has to be copied in order to relax 'client hardening'.	Read/write access granted to Everyone.
Directory: %SYSTEMROOT%\SXData	Contains several files that are required for the program to work.	Restricted access granted to Administrators and LocalSystem. The security settings are propagated to child objects.
Directory: %SYSTEMROOT%\SXData\shadow	Contains the write/read shadow data (if necessary and defined by Sanctuary's Administrator).	Inherits its security settings from %SYSTEMROOT%\SXData.
Uninstall registry keys*	Registry keys created to help delete the SecureWave Application Server.	n/a
Registry keys*: HKLM\system\CurrentControlSet\Services\scomc\parameters — and — HKLM\system\CurrentControlSet\services\sk\parameters	Registry keys. See *Appendix B: Registry keys* on page *97*.	n/a

*You can block the use of the RegEdit.exe program for all users by using our Sanctuary Application Control Suite component.

Table 6: Directories created by a Sanctuary Client installation

✍ *The %INSTALLDIR% directory points to the folder where the program was installed. It is usually C:\Program Files\SecureWave\Sanctuary, but can refer to another folder.*

Chapter 6: The Authorization Service Tool

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

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.

The information in this chapter applies only to the Sanctuary Application Control Suite (Sanctuary Application Control Server Edition, Sanctuary Application Control Terminal Services Edition, or Sanctuary Application Control Custom Edition).

What is the Authorization Service Tool?

You can use *Authorization Service Tool* (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' (see the *Sanctuary Application Control Suite Administrator's Guide* for more information). The aim of this process is to require 'zero' administration effort, i.e. all Microsoft Authorized updates and fixes are automatically approved, their Hash created, and the database updated. See the configuration details in the *Sanctuary Application Control Suite Administrator's Guide*.

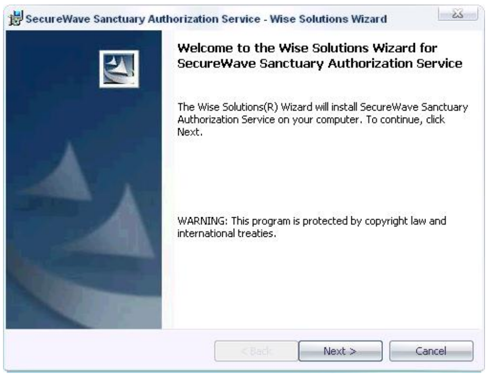
✍ *Notice that we do **not** support either Outlook Express or Internet Information Server (IIS) as clients for sending email messages. If there is already an account in these types of clients, the SMTP IP address is transferred directly to the AuthSrv configuration. Furthermore, the 'LoadConfiguration' registry key parameter is always set to '3' (see the Sanctuary Application Control Suite Administrator's Guide).*

✍ *SUS does not support Vista.*

To install the Authorization Service Tool

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 CD (server\AuthSrv\Setup.exe). The welcome screen is shown:



SecureWave Sanctuary Authorization Service - Wise Solutions Wizard

Welcome to the Wise Solutions Wizard for SecureWave Sanctuary Authorization Service

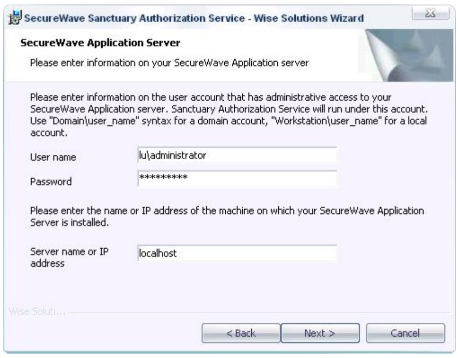
The Wise Solutions(R) Wizard will install SecureWave Sanctuary Authorization Service on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Figure 64: Authorization Service Tool installation: Welcome screen

2. Click on Next. The License Agreement is shown.
3. Read the license agreement carefully and, providing you agree with its conditions, select the accept option and click on Next.

   If you do not agree with its stipulations, click on the Cancel button to exit without installing the Authorization Service Tool.
4. Enter the user's name and password, the SecureWave Application Server IP or name and click on Next to continue.



SecureWave Sanctuary Authorization Service - Wise Solutions Wizard

SecureWave Application Server

Please enter information on your SecureWave Application server

Please enter information on the user account that has administrative access to your SecureWave Application server. Sanctuary Authorization Service will run under this account. Use "Domain\user_name" syntax for a domain account, "Workstation\user_name" for a local account.

User name: lu\administrator

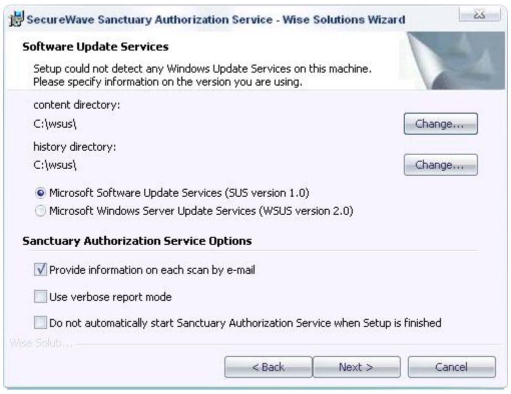
Password: *********

Please enter the name or IP address of the machine on which your SecureWave Application Server is installed.

Server name or IP address: localhost

Figure 65: Authorization Service Tool installation: Configuration screen

5. Configure the SUS and Authorization Service options to suit your requirements and click on Next.



SecureWave Sanctuary Authorization Service - Wise Solutions Wizard

Software Update Services

Setup could not detect any Windows Update Services on this machine.
Please specify information on the version you are using.

content directory:
C:\wsus\

history directory:
C:\wsus\

● Microsoft Software Update Services (SUS version 1.0)
○ Microsoft Windows Server Update Services (WSUS version 2.0)

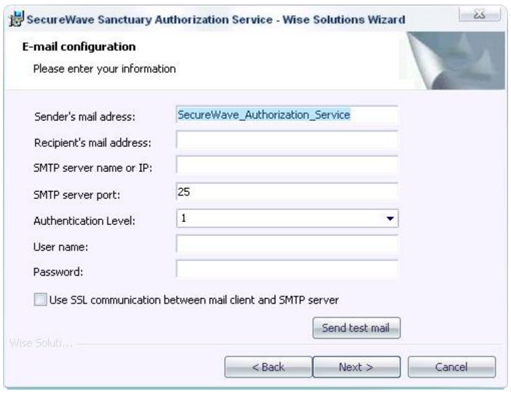
Sanctuary Authorization Service Options

☑ Provide information on each scan by e-mail
□ Use verbose report mode
□ Do not automatically start Sanctuary Authorization Service when Setup is finished

Figure 66: Authorization Service Tool installation: Option screen

6. If you selected the e-mail option in the previous step, configure this by completing the corresponding fields and click on Next.

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. .



SecureWave Sanctuary Authorization Service - Wise Solutions Wizard

E-mail configuration

Please enter your information

Sender's mail adress: SecureWave_Authorization_Service

Recipient's mail address:

SMTP server name or IP:

SMTP server port: 25

Authentication Level: 1

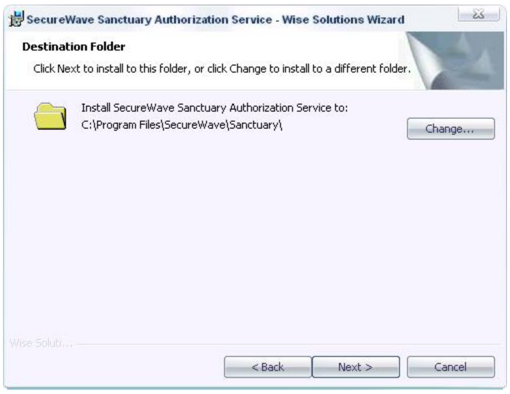
User name:

Password:

□ Use SSL communication between mail client and SMTP server

Figure 67: Authorization Service Tool installation: E-mail configuration screen

7. Accept or change the installation directory (the program proposes c:\Program Files\SecureWave\Sanctuary) and click on NEXT.



SecureWave Sanctuary Authorization Service - Wise Solutions Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install SecureWave Sanctuary Authorization Service to:
C:\Program Files\SecureWave\Sanctuary\

Figure 68: Authorization Service Tool installation: Choose installation directory

The final summary screen is shown. You are now ready to install the program.

8. Click on INSTALL, BACK to change options, or CANCEL to stop the setup. You will see the progress window and the final screen.

9. Click on the FINISH button to close the setup window.

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

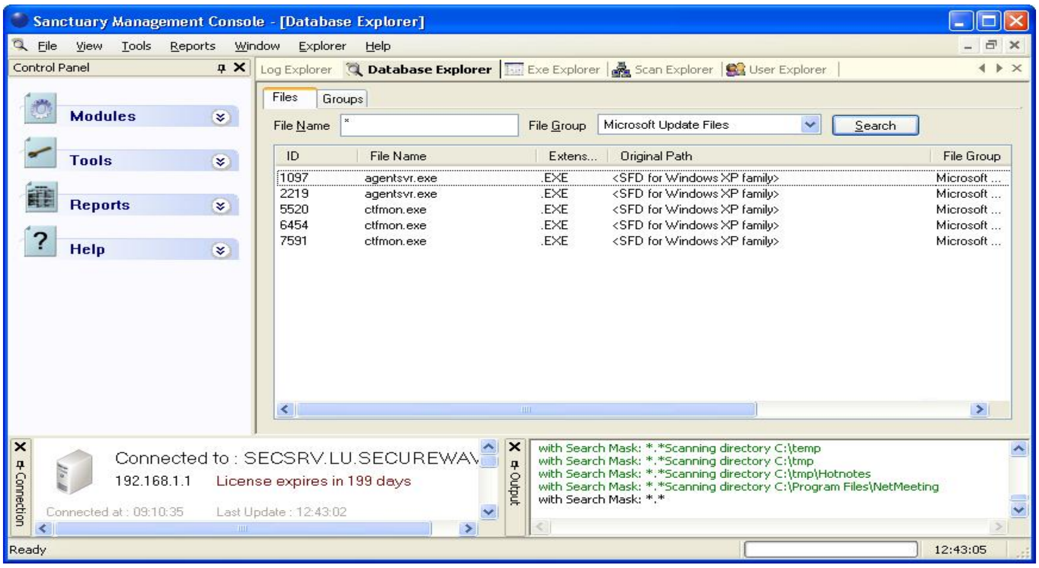
The tool waits until:

> A change is made in the default update folder by WSUS.

> The administrator approves the updates on the SUS console.

> Each hour.

> Once installed and loaded, you get a screen similar to that of *Figure 69* when choosing *Microsoft Update Files* in *File Group* field of the Database Explorer module of the console (assuming you have some update files ready to authorize):



Sanctuary Management Console - [Database Explorer]

File Name: *

File Group: Microsoft Update Files

ID	File Name	Extens...	Original Path	File Group
1097	agentsvr.exe	.EXE	<SFD for Windows XP family>	Microsoft ...
2219	agentsvr.exe	.EXE	<SFD for Windows XP family>	Microsoft ...
5520	ctfmon.exe	.EXE	<SFD for Windows XP family>	Microsoft ...
6454	ctfmon.exe	.EXE	<SFD for Windows XP family>	Microsoft ...
7591	ctfmon.exe	.EXE	<SFD for Windows XP family>	Microsoft ...

Connected to : SECSRV.LU.SECUREWAV
192.168.1.1 License expires in 199 days
Connected at : 09:10:35 Last Update : 12:43:02

```
with Search Mask: *.*Scanning directory C:\temp
with Search Mask: *.*Scanning directory C:\tmp
with Search Mask: *.*Scanning directory C:\tmp\Hotnotes
with Search Mask: *.*Scanning directory C:\Program Files\NetMeeting
with Search Mask: *.*
```

Ready 12:43:05

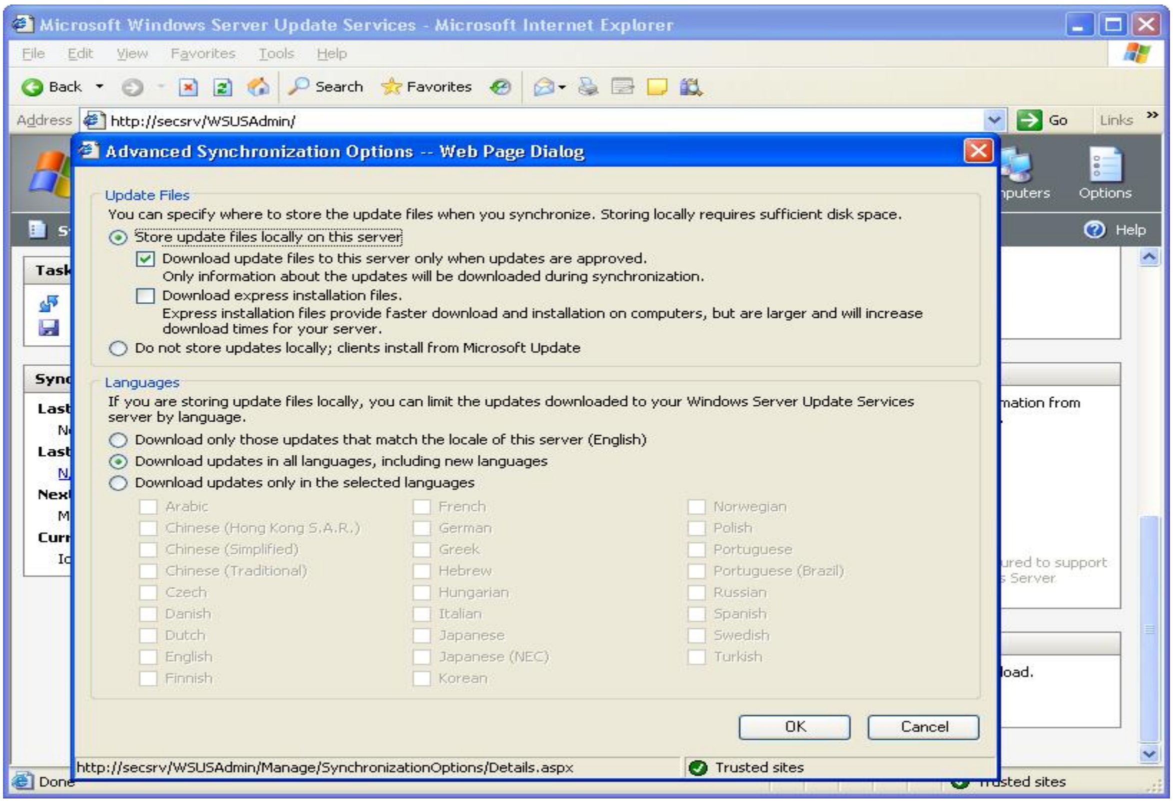
Figure 69: Authorization Service Tool initial scan

Configuring WSUS

Once the Authorization Service Tool has been installed, you must configure the WSUS system since this tool does not support express installation files. To do this:

1. Open Internet Explorer with your WSUS server active (http://<server_name>/WSUSAdmin).
2. On the WSUS console toolbar, click on OPTIONS, and then select SYNCHRONIZATION OPTIONS.
3. Under the UPDATE FILES AND LANGUAGES section, click on ADVANCED and accept the warning message by clicking on OK.
4. Deselect the *Download express installation files* checkbox.

If you want to reactivate them, follow the same procedure and click on the *Download express installation files* option.


Microsoft Windows Server Update Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://secsrv/WSUSAdmin/
Go Links
nputers Options
Help
Task
Sync
Last
Last
Next
Curr
mation from
ured to support
s Server
load.
Done
Trusted sites

Advanced Synchronization Options -- Web Page Dialog

Update Files

You can specify where to store the update files when you synchronize. Storing locally requires sufficient disk space.

● Store update files locally on this server

☑ Download update files to this server only when updates are approved.
Only information about the updates will be downloaded during synchronization.

□ Download express installation files.
Express installation files provide faster download and installation on computers, but are larger and will increase download times for your server.

○ Do not store updates locally; clients install from Microsoft Update

Languages

If you are storing update files locally, you can limit the updates downloaded to your Windows Server Update Services server by language.

○ Download only those updates that match the locale of this server (English)
● Download updates in all languages, including new languages
○ Download updates only in the selected languages

□ Arabic	□ French	□ Norwegian
□ Chinese (Hong Kong S.A.R.)	□ German	□ Polish
□ Chinese (Simplified)	□ Greek	□ Portuguese
□ Chinese (Traditional)	□ Hebrew	□ Portuguese (Brazil)
□ Czech	□ Hungarian	□ Russian
□ Danish	□ Italian	□ Spanish
□ Dutch	□ Japanese	□ Swedish
□ English	□ Japanese (NEC)	□ Turkish
□ Finnish	□ Korean	

http://secsrv/WSUSAdmin/Manage/SynchronizationOptions/Details.aspx Trusted sites

Figure 70: WSUS configuration

Chapter 7: Using the Key Pair Generator

To accompany the Sanctuary Management Console, SecureWave provides the Key Pair Generator. This utility is used to create a key pair to assure the integrity of the communication between the SecureWave Application Server and the Sanctuary Client. The information in this chapter is relevant to all Sanctuary products.

Introduction

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

💣 *In a production environment, you must create your own key pair **BEFORE** deploying the Sanctuary Client Driver on the first client computer. This is done using the Key Pair Generation utility.*

If you are using *Sanctuary Device Control:*

💣 ***NEVER** change the key pair after adding encrypted removable media in the Media Explorer. Doing so means that your users will no longer be able to access their encrypted media.*

💣 *Never change the key pair during a Sanctuary upgrade when client hardening is switched on, otherwise your upgrade will fail.*

✍ *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.*

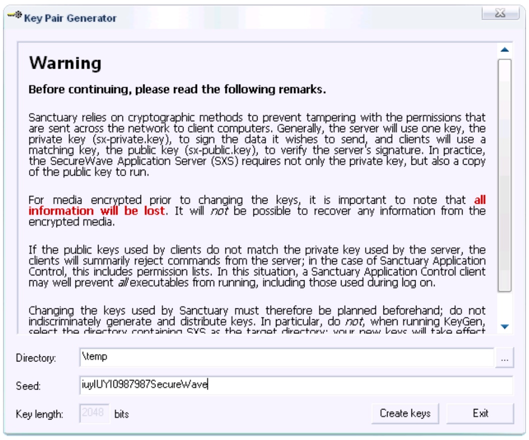
✍ *We recommend that you install and publish a Microsoft CA on you Active Directory structure before trying to encrypt a removable device.*

Starting the Key Pair Generator

1. Navigate to the Program Files\SecureWave\ Sanctuary\SXTools directory, found on the machine where the SecureWave Application Server is installed.

2. Run the keygen.exe tool.

   The *Key Pair Generator* dialog is displayed.



Key Pair Generator

Warning

Before continuing, please read the following remarks.

Sanctuary relies on cryptographic methods to prevent tampering with the permissions that are sent across the network to client computers. Generally, the server will use one key, the private key (sx-private.key), to sign the data it wishes to send, and clients will use a matching key, the public key (sx-public.key), to verify the server's signature. In practice, the SecureWave Application Server (SXS) requires not only the private key, but also a copy of the public key to run.

For media encrypted prior to changing the keys, it is important to note that **all information will be lost**. It will *not* be possible to recover any information from the encrypted media.

If the public keys used by clients do not match the private key used by the server, the clients will summarily reject commands from the server; in the case of Sanctuary Application Control, this includes permission lists. In this situation, a Sanctuary Application Control client may well prevent *all* executables from running, including those used during log on.

Changing the keys used by Sanctuary must therefore be planned beforehand; do not indiscriminately generate and distribute keys. In particular, do *not*, when running KeyGen, select the directory containing SXS as the target directory; your new keys will take effect

Directory: \temp

Seed: iuyIUYI0987987SecureWave

Key length: 2048 bits

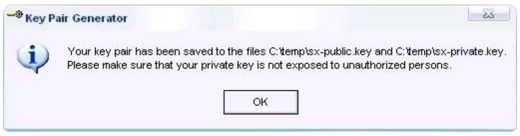
Figure 71: Key pair generation: First step

Generating a key pair

1. Select the temporary directory in which you want to save the private and public key files.

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:



Key Pair Generator

Your key pair has been saved to the files C:\temp\sx-public.key and C:\temp\sx-private.key. Please make sure that your private key is not exposed to unauthorized persons.

Figure 72: Key pair generation: Final message

4. Click on OK.

Deploying the key pair

The key pair can now be distributed. To do this, 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%\SXSdata directory. Alternatively, they can also be put on a removable drive or DVD/CD.

On startup the SecureWave Application Server checks for the key pair in the following locations:

1. The directory where the SecureWave Application Server executable is installed (usually %SYSTEMROOT%\SYSTEM32).

2. The SecureWave Application Server’s private directory, whose recommended location is %SYSTEMROOT%\SXSDATA.

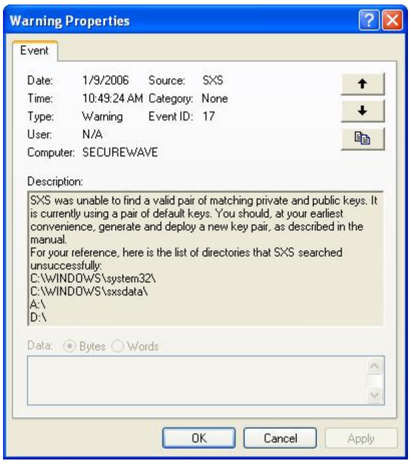
3. All removable drives and DVDs/CDs in alphabetical order.

The search stops at the first valid key pair.

✍ *When a new key pair is generated to replace an existing one, you must restart the SecureWave Application Server service in order to start using the newly generated keys. The SecureWave Application Server Service can be started and stopped through the Windows Services Panel or using a command line (net stop sxs and net start sxs).*

✍ *If the key pair is not in the %SYSTEMROOT%\SXSDATA directory, 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 on it.*

If 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. This is not recommended for obvious security reasons.



Date: 1/9/2006 Source: SXS
Time: 10:49:24 AM Category: None
Type: Warning Event ID: 17
User: N/A
Computer: SECUREWAVE

Description:

SXS was unable to find a valid pair of matching private and public keys. It is currently using a pair of default keys. You should, at your earliest convenience, generate and deploy a new key pair, as described in the manual.
For your reference, here is the list of directories that SXS searched unsuccessfully:
C:\WINDOWS\system32\
C:\WINDOWS\sxsdata\
A:\
D:\

Data: ● Bytes ○ Words

Figure 73: SecureWave Application Server did not find the public-private key pair

ONLY the public key file sx-public.key should 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 Client Driver installed, copy the **public** key file (NOT the private key file) to the %SYSTEMROOT%\SXDATA directory of the client computer (typically C:\WINDOWS\SXDATA). Afterwards, logoff or reboot to receive the new settings signed with the matching key pair.*

Chapter 8: Unattended Client installation

Once you have installed and tested your Sanctuary configuration on a few computers and are satisfied that you can administer it effectively, the next step is 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 made much simpler with an unattended installation. This is also the easiest way of ensuring that all computers have the correct package. In addition, you can use our tool to obtain a list of all machines that already have the client deployed.

This chapter explains how to install the Sanctuary Client using MSI technology and optionally Windows 2000/2003 Group Policy. The information in this chapter is relevant to all Sanctuary software suite products.

💣 *If you prefer to use a different 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 using encrypted communications using the automatic certificate generation mode, the client deployment task cannot be successfully completed unless you guarantee that the machine certificate file's properties (located at %SystemDrive%\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys) are 'Full Control for Administrators and LocalSystem' (the usual setting).*

💣 *Sanctuary Client is not supported on Windows 2003 Server (32- and 64-bit) machines.*

✍ *If you are installing Sanctuary Device Control or Sanctuary Application Control Custom Edition on Windows XP SP2 machines, you need to open certain blocked ports to be able to do an unattended client installation. See Appendix E: Opening firewall ports for client deployment on page 115 for more details.*

✍ *You cannot install Sanctuary Application Control Server Edition client on Windows XP or Windows 2000 Pro machines.*

✍ *Although the installation dialog only lets you input three SecureWave Application Servers, you can easily add more if needed. You can also change how the SecureWave Application Server(s) is selected — round robin vs. random pick. All this is done by modifying certain registry keys. See Sanctuary Client registry keys on page 102 and Uninstalling the Sanctuary Client on page 50 for more details. You can 'push' these modifications to all clients using Group Policies with ADM templates.*

✍ *The client setup package is available for 32-bit and 64-bit operating systems. If you create an installation package that includes the 32-bit client and try to install it on a machine with a 64-bit OS, the installation will fail and rollback. The same is true the other way around. If you are working on a mixed environment containing both 32-bit and 64-bit machines, you should create two distinctive installation packages, one for each type of OS.*

Even though you can use other deployment packages to install Sanctuary Client, our specialized silent unattended installation deployment tool offers you the advantage of doing (among other things):

> Port unblocking.

> Policy import.

> Standalone client installation and licensing.

- Import client communication layer parameters.
- Generated public key installation.
- Removal of obsolete data files.
- Client hardening detection and, if required, deactivation.
- Client communication layer's Windows Management Instrumentation (WMI) interface registration.
- Installation of WMI redistributable components.

The installation process is carried out in five stages:

1. The original client driver's setup MSI file is used as the base for a client deployment. This file is copied to whatever directory you choose when you first start the Sanctuary Client Deployment tool. After deciding on a name for your installation package, a new folder is created using this name. For example, if you want your installation packages to be located in a directory named 'Deploy' and the installation package name is 'Marketing', the program places the client MSI file in C:\Deploy\Marketing\.
2. After modifying the installation options, a new transform file (MST) is created in the installation package folder.
3. The license, policies (optionally), and public key files are copied (exported) to the same folder where the MSI and MST files resides.
4. The computer(s) on which the package will be installed are defined.
5. The deployment process is started.

What is an MSI file?

An MSI file is a database with relationally linked tables and a set of files either inside or accompanying it. This database contains information about what has to be done to the target machine in order to install the application.

The installation process itself is controlled by a list of 'Actions'. Several such lists are predefined in the MSI standard. These can be adjusted by 'Custom Actions', performing special tasks not covered by the normal MSI behavior. Custom actions can even launch scripts and executables to perform special installation tasks.

The actual installation process is performed by a special MSI installer service running on the computer. Because this service runs with system privileges, it has all the rights necessary to perform the installation. Depending on the local security policy, normal users can be granted the right to make the installer service install certain packages or even any package the user wants.

Creating a Transform file (MST) for an existing MSI file

Transform files are similar to MSI files but with a different file extension. They alter the installation process in order to encapsulate a set or required customizations. The contents of both MSI and MST files are merged together during the installation.

You can create MST files using a third party tool or directly with our Sanctuary Client Deployment tool.

Since there are so many variables to control in the client MSI file, we strongly recommend using the Sanctuary Client Deployment tool. In addition to the original MSI installation package, you now have an MST file with all necessary options to install on all your machines.

Prerequisites for creating a Sanctuary Client Deployment package

Before you create and install a deployment package, you must meet the following conditions:

> The administrator running the Sanctuary Client Deployment tool must be in the Local Administrators group on all targeted computers. You can also use the command 'net use \\<computer>' to log on as an administrator.

> You must synchronize the clocks of the different computers. 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 operating system where the deployment tool (Deploy.exe) is running must be Windows 2000 or Windows XP Professional.

> If you are running the deployment tool on Windows XP SP2, check Microsoft Knowledge base article 884020 (http://support.microsoft.com/default.aspx?scid=kb;en-us;884020 — Programs that connect to an IP address that are in the loopback address range) and, if necessary, install the provided patch.

> The deployment tool does not work under Windows NT4. Sanctuary is not designed to work on this operating system.

> If there is a firewall between the Sanctuary Client Deployment and the computer where you want to deploy the Sanctuary Client, open the following incoming ports on the client computers (see *Appendix E: Opening firewall ports for client deployment* on page *115*):

- TCP 33115.
- TCP: 139, 445 NetBIOS.
- UDP: 137, 138 Browsing.

> You must generate the key pair and have the public key available for the client. You also need the license file if you want to do a 'standalone installation' when using Sanctuary Device Control. If you plan to install on a client that does not have access to the SecureWave Application Server, you also need to export the policies to a special file, *policies.dat*, and place it in the same client installation package.

✍ *Installing a client using exported policies works well when policies.dat is placed locally in the same directory as setup.exe however if it is placed on a share you must change the security of the share directory so that computer accounts are able to access it.*

> If you have already installed the client driver and want to uninstall/ modify/repair it, you must first issue an 'Endpoint Maintenance Ticket' and copy it to the required directory. See the relevant *Administrator's Guide* for more information.

To install the Sanctuary Client Deployment tool

The *Sanctuary Client Deployment* tool is installed, among others tools, when setting up the *Sanctuary Management Console*. See *Chapter 4: Installing the Sanctuary Management Console* on page *37* for more information.

When considering the choice of the computer on which you install the Sanctuary Client Deployment tool and from which you start the deployment, consider the following:

> The deployment of the Sanctuary Client on a long list of computers may take some time. You cannot log off the computer during that period.

> The tool makes significant use of the network resources of the computer on which you are installed.

> You must **NEVER** interrupt an ongoing deployment.

To install packages

The installation process is carried out in the following two stages:

1. Create package(s).

The deployment tool allows you to select client installations (from the CD-ROM, LAN, or local drives). It makes a local copy of the client installation and displays the ‘Options – SecureWave Installation Transform’ dialog so that you can create an installation transform (.MST) linked to the MSI file.

✍ *An installation transform is a customization of the installation which predefines settings for the installed application. Having an installation transform allows the system administrator to apply identical settings to a group of client computers.*

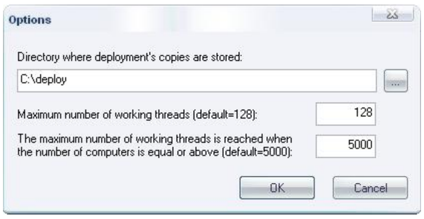
2. Install/Uninstall package.

To do this, select the package and target computer(s) to begin the (un)installation and set the reboot and configuration options. After this the deployment starts.

The following sections describe the installation process.

To install the Sanctuary Client: MST file generation

1. On the administrator’s machine, select *Sanctuary Client Deployment* from the Start → Programs → Sanctuary menu. The following dialog appears on first use.



Options

Directory where deployment's copies are stored:

C:\deploy

Maximum number of working threads (default=128): 128

The maximum number of working threads is reached when the number of computers is equal or above (default=5000): 5000

Figure 74: Sanctuary Client Deployment: First start-up

2. Choose the folder in which 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 may want to specify a shared directory where all instances of the deployment tool can access the company packages.*

3. Click on OK. The following dialog appears:

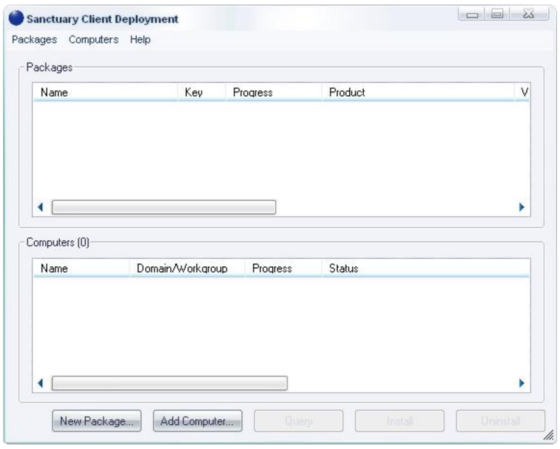
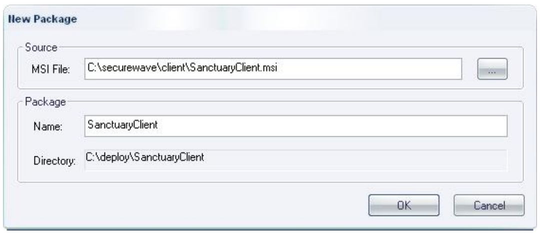


Figure 75: Sanctuary Client Deployment: Packages and computers

4. From the *Packages* menu, select *New* or click on NEW PACKAGE (located in the lower part of the window). The following dialog is displayed:



MSI File: C:\securewave\client\SanctuaryClient.msi

Name: SanctuaryClient

Directory: C:\deploy\SanctuaryClient

Figure 76: Sanctuary Client Deployment: New package

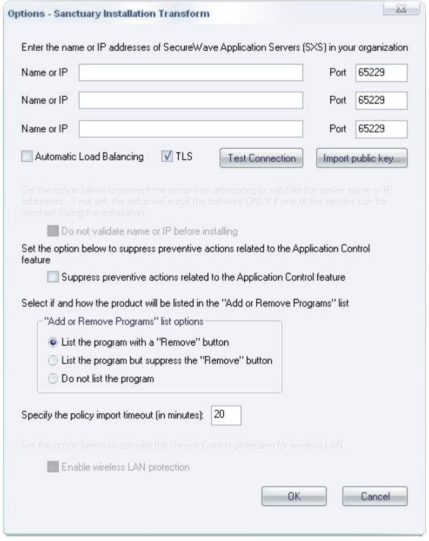
5. Click on the ellipsis ( ) button to select an MSI file, typically from the Client folder of the CD-ROM.

6. Enter the name you want to give to the package.

Do not use numbers in the form ###.###.###.### as they are interpreted as an IP address. Make a note of the directory (which we refer to as the Deployment package folder, C:\Deploy in this example).

7. Click on OK.

The installation files are copied to a subfolder of the destination directory as defined in step1 (C:\DEPLOY in our example). The *Options – SecureWave Installation Transform* dialog is displayed:



Enter the name or IP addresses of SecureWave Application Servers (SXS) in your organization

Name or IP: Port 65229

Name or IP: Port 65229

Name or IP: Port 65229

☐ Automatic Load Balancing ☑ TLS

Set the option below to prevent the setup from attempting to validate the server name or IP addresses. If not set, the setup will install the software ONLY if one of the servers can be reached during the installation.

☐ Do not validate name or IP before installing

Set the option below to suppress preventive actions related to the Application Control feature

☐ Suppress preventive actions related to the Application Control feature

Select if and how the product will be listed in the "Add or Remove Programs" list

"Add or Remove Programs" list options

● List the program with a "Remove" button
○ List the program but suppress the "Remove" button
○ Do not list the program

Specify the policy import timeout (in minutes): 20

Set the option below to activate the Device Control protection for wireless LAN

☐ Enable wireless LAN protection

Figure 77: Sanctuary Client Deployment: SecureWave Application Server IP or name

The two grayed-out options 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 currently available 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.

On the other hand, the SPECIFY THE POLICY IMPORT TIMEOUT (IN MINUTES) is only available for client version 3.2 or later.

💣 *Although the Client Deployment Tool supports installing an older version of our client on Windows NT4, the tool itself does not work with this operating system.*

8. Click on IMPORT PUBLIC KEY.
9. Select the sx-public.key file located in the %SYSTEMROOT%\SXSdata folder of the *SecureWave Application Server* machine.

💣 *If you do not find a sx-public.key file in the %SYSTEMROOT%\SYSTEM32 or the %SYSTEMROOT%\SXSData (recommended location) folders of the SecureWave Application Server, this means that your installation currently uses the default keys. You should not deploy the clients in a production environment without having generated your own set of keys. See Chapter 7: Using the Key Pair Generator on page 59 for more details. Bear in mind if you are using Sanctuary Device Control that replacing an existing set of keys or implementing customized keys in an environment where encrypted media are already in use prevents access to these media.*

✍ *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 Client 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 that the client can communicate with it. If this communication is not achieved, the installation is aborted unless the 'Serverless Mode' option is selected. See the following step for more information.*

10. Enter the fully qualified domain names or IP addresses of the SecureWave Application Server to which these clients attempts 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 a fully qualified domain name or address, the installation is done in 'SERVERLESS MODE'. While using this mode, the installation routine does not abort if it cannot reach a SecureWave Application Server. Alternatively, if these fields are not empty, at least one SecureWave Application Server 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 first exporting them to a special file (policies.dat) and you must include the license file. See *To install Sanctuary Client* on page 42 for details. If you are planning to do a client maintenance, it is important that the server(s) address are reachable since it is also used to retrieve the 'Endpoint Maintenance Ticket' needed to manage the client drivers and its associated directories and registry keys. Please consult your corresponding *Administrator's Guide* and *Uninstalling the Sanctuary Client* on page *50* for more information.

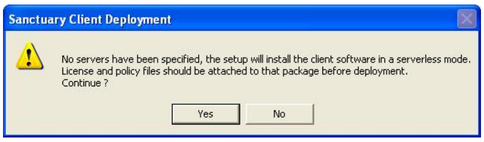
The following table shows all the possibilities:

Condition	***Result***
Valid server, no policies file present	Deploy succeeds using server information.
Valid server: a valid policies file is present	Deploy succeeds importing the policies file.
Invalid server, no policies file present	Deploy fails.
Invalid server, a valid policies file is present	Deploy succeeds importing the policies file (as soon as a server becomes available, it is used as the permissions/authorization source).
No server found, no	Deploy succeeds enforcing Sanctuary Device Control permissions

policies file present	starting with the built-in restrictive policies (a valid Sanctuary Device Control only license file has to be placed along with the .msi package) ➔ 'Standalone Installation'.
No server found, a valid policies file is present	Deploy succeeds importing the policies file ➔ 'Serverless Installation'.

Table 7: Deployment result depending if server and/or policies file is present or not

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


Sanctuary Client Deployment

No servers have been specified, the setup will install the client software in a serverless mode.
License and policy files should be attached to that package before deployment.
Continue ?

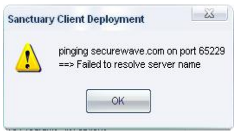
Figure 78: Message when installing in 'Serverless mode'

11. Choose whether to select the *Automatic Load Balancing* checkbox. If you select this option, the Sanctuary Client attempts to contact one of the servers listed in a random manner. Alternatively, if you leave *Automatic Load Balancing* unchecked, the Sanctuary Client attempts to contact the SecureWave Application Server in the order in which they are listed.

12. Choose whether or not the client uses TLS protocol to communicate with the SecureWave Application Server. See *Transport Layer Security* on page *12* for more information.

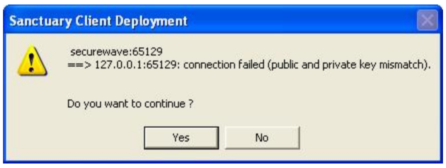
13. Click on TEST CONNECTION to verify the fully qualified domain names or IP Addresses you have entered. A confirmation or failure dialog box is displayed.

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) and click on OK to continue. Here are some:


Sanctuary Client Deployment

pinging securewave.com on port 65229
==> Failed to resolve server name

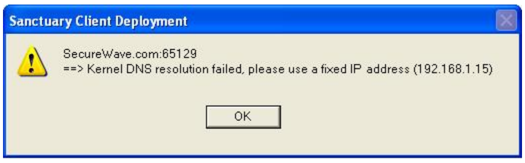
Figure 79: Message when the connection test fails


Sanctuary Client Deployment

securewave:65129
==> 127.0.0.1:65129: connection failed (public and private key mismatch).

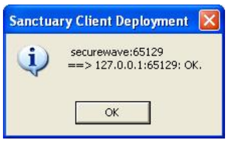
Do you want to continue ?

Figure 80: Message when the connection test fails (key related)


Sanctuary Client Deployment

SecureWave.com:65129
==> Kernel DNS resolution failed, please use a fixed IP address (192.168.1.15)

Figure 81: Message when the Kernel DNS resolution fails


Sanctuary Client Deployment

securewave:65129
==> 127.0.0.1:65129: OK.

Figure 82: Message when the connection test succeeds

14. Select the options that control how the client driver is shown in the *Add or Remove Programs* (Programs and Features in Windows Vista) Windows' dialog and the policy file timeout. The following options can be chosen:

    > 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 Application Control 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 Application Control Suite and that this action does not blocks the machine. If this is the case, the installation will not proceed and rolls 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' (Programs and Features in Windows Vista) Windows' dialog in the 'standard' way, and it will include a *Remove* button.

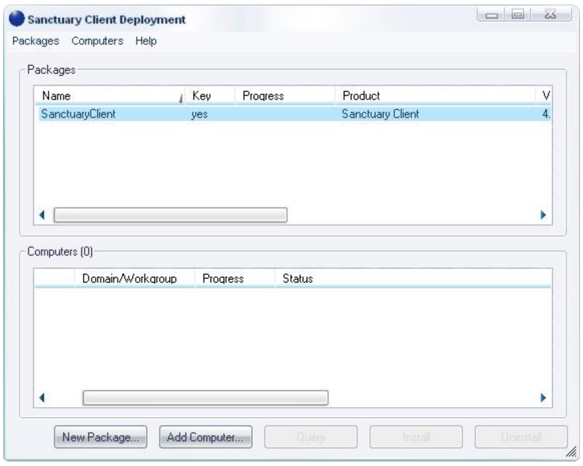
    > LIST THE PROGRAM BUT SUPPRESS THE 'REMOVE' BUTTON – The program is listed in the 'Add or Remove Programs' (Programs and Features in Windows Vista) Windows' dialog but will not include a *Remove* button.

    > DO NOT LIST THE PROGRAM – The program will not appear in the 'Add or Remove Programs' Windows' (Programs and Features in Windows Vista) dialog.

    > SPECIFY THE POLICY IMPORT TIMEOUT (IN MINUTES) (only available for client version 3.2 or later) - set how many minutes should elapse before the program will consider the policy file as out of date. Type any value between 20 and 600 minutes (10 hours).

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

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

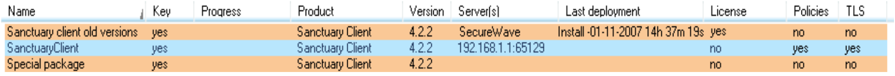


Name	Key	Progress	Product	V
SanctuaryClient	yes		Sanctuary Client	4.

Figure 83: 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	TLS
Sanctuary client old versions	yes		Sanctuary Client	4.2.2	SecureWave	Install -01-11-2007 14h 37m 19s	yes	no	no
SanctuaryClient	yes		Sanctuary Client	4.2.2	192.168.1.1:65129		no	yes	yes
Special package	yes		Sanctuary Client	4.2.2			no	no	no

Figure 84: Sanctuary Client Deployment: Package option

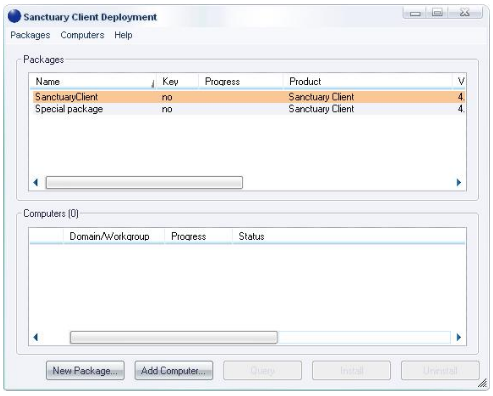
✍ *If any of the public key, policies file, or license (in the case of an installation without servers), are not included in the package, they are displayed, as shown above, with an orange background as a warning. If there is no orange background, the key, policies file, and license, if applicable, are present and the package is ready to be deployed. We recommend you do not deploy packages without a public key — or license — in a production network. The license file is only required when doing a 'Standalone installation'.*

Using the Sanctuary Client Deployment tool to install the Sanctuary Client

The Sanctuary Client Deployment tool is designed to allow you to silently deploy the Sanctuary Client on a list of machines. Once the Deployment package has been created, you can start the deployment, using the following procedure:

1. Select *Sanctuary Client Deployment* from the *Start* → *Programs* → *Sanctuary* menu.

   The Sanctuary Client Deployment dialog is displayed:



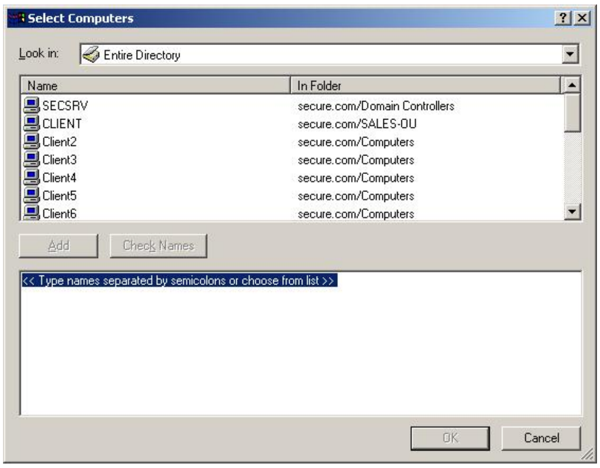
Name	Key	Progress	Product	V
SanctuaryClient	no		Sanctuary Client	4.
Special package	no		Sanctuary Client	4.

	Domain/Workgroup	Progress	Status

Figure 85: Sanctuary Client Deployment: First screen

✍ *If any of the public key, policies file, or license (in the case of an installation without servers), are not included in the package, they are displayed, as shown above, with an orange background as a warning. If there is no orange background, the key, policies file, and license, if applicable, are present and the package is ready to be deployed. We recommend you do not deploy packages without a public key — or license — in a production network. The license file is only required when doing a 'Standalone installation'.*

2. Click on ADD COMPUTER (located in the lower part of the window) or select *Computer* → *Add* from the menu bar. One of the following dialogs is displayed, depending on your operating system:

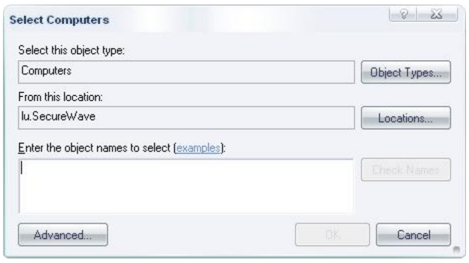


Look in: Entire Directory

Name	In Folder
SECSRV	secure.com/Domain Controllers
CLIENT	secure.com/SALES-OU
Client2	secure.com/Computers
Client3	secure.com/Computers
Client4	secure.com/Computers
Client5	secure.com/Computers
Client6	secure.com/Computers

<< Type names separated by semicolons or choose from list >>

Figure 86: Sanctuary Client Deployment: Select computer dialog (Sample a)

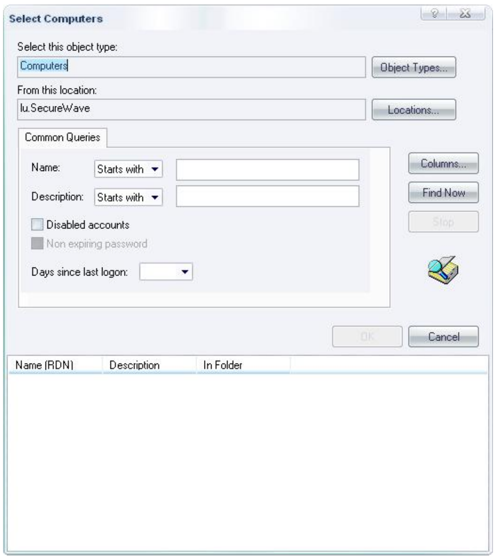


Select this object type: Computers

From this location: lu.SecureWave

Enter the object names to select (examples):

Figure 87: Sanctuary Client Deployment: Select computer dialog (Sample b)



Select this object type: Computers

From this location: lu.SecureWave

Name: Starts with

Description: Starts with

□ Disabled accounts

□ Non expiring password

Days since last logon:

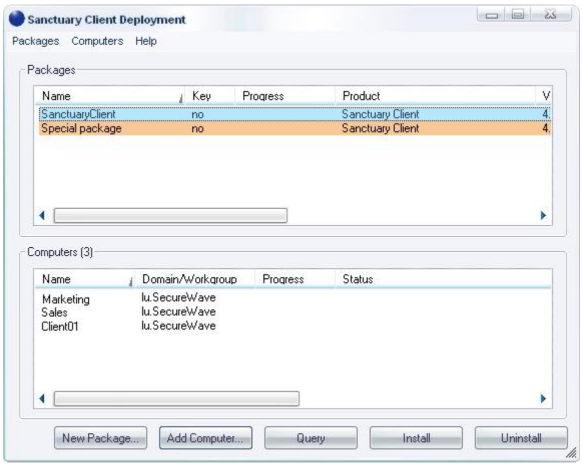
Name (RDN)	Description	In Folder

Figure 88: Sanctuary Client Deployment: Advanced select computer dialog

✍ *You can also Drag and Drop between the external Microsoft Windows Network (from the My Network Places icon) selection dialog.*

3. Select the domain you want to search and highlight (or enter) 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 on OK. The selected computers are now listed in the Sanctuary Client Deployment dialog, as shown below.



Packages

Name	Key	Progress	Product	V
SanctuaryClient	no		Sanctuary Client	4.
Special package	no		Sanctuary Client	4.

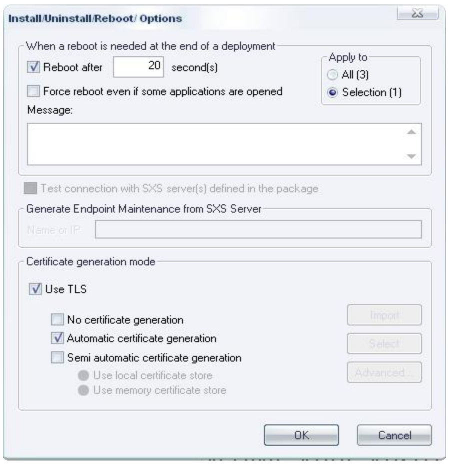
Computers (3)

Name	Domain/Workgroup	Progress	Status
Marketing	lu.SecureWave		
Sales	lu.SecureWave		
Client01	lu.SecureWave		

Figure 89: Sanctuary Client Deployment: Selected computer(s)

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

5. Choose whether or not the client will be communicating with the SecureWave Application Server(s) using TLS protocol (see *Transport Layer Security* on page 12) and select the reboot options.



Install/Uninstall/Reboot/ Options

When a reboot is needed at the end of a deployment

☑ Reboot after 20 second(s)

☐ Force reboot even if some applications are opened

Message:

Apply to

○ All (3)

● Selection (1)

☐ Test connection with SXS server(s) defined in the package

Generate Endpoint Maintenance from SXS Server

Name or IP:

Certificate generation mode

☑ Use TLS

☐ No certificate generation

☑ Automatic certificate generation

☐ Semi automatic certificate generation

● Use local certificate store

● Use memory certificate store

Figure 90: Sanctuary Client Deployment: Selecting the TLS protocol

To select TLS protocol, right click on a computer name and select CHANGE TLS MODE ((or select it from the *Computers* menu).

When selecting the *Semi-automatic certificate generation*, you have the same options as those described for the client installation (described on page *42*):

- Import — to place the machine certificate in the computer's store.
- Select — to choose a certificate from the computer's store.
- Advanced — to set the certificate's cryptographic signature and parameters.

You must already have a Certificate Authority installed or the required computer certificate at hand. See Appendix H: Installing a Certificate Authority for encryption and TLS Communication on page 129 for more details.

Remember that you also need an 'Endpoint maintenance ticket' if you are updating clients that require this type of permissions to be modified or updated. See your corresponding Administrator's Guide for a full description.

6. Select a register to install from the *Packages* list.

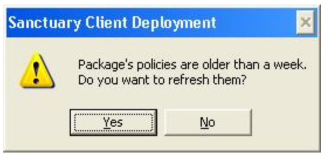
7. Optionally select a subset of machines where the package will be installed from the *Computers* list.

8. Click on INSTALL to start the deployment.

Sanctuary's administrator can decide to use a policy file, *policies.dat,* to export permissions to clients that are not connected, or cannot contact, to a server during the installation. See the *To export and import permission settings* section of the relevant *Administrator's Guide* for more information about how to export your settings to a file.

✍ *Installing a client using exported policies works well when policies.dat is placed locally in the same directory as setup.exe however if it is placed on a share you must change the security of the share directory so that computer accounts are able to access it.*

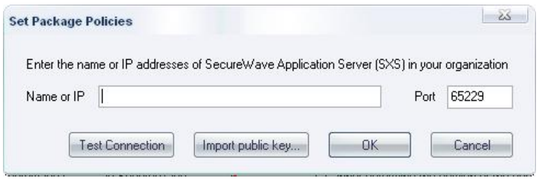
If the exported policy file was created more than a week ago, you get the following message:



Package's policies are older than a week.
Do you want to refresh them?

Figure 91: Sanctuary Client Deployment: Refreshing old policies file

You can choose to either refresh the file or deny this request. If you choose to update these policies, you need to provide a SecureWave Application Server valid address or name:



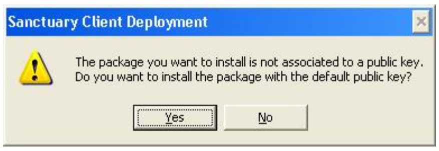
Enter the name or IP addresses of SecureWave Application Server (SXS) in your organization

Name or IP:

Port: 65229

Figure 92: Sanctuary Client Deployment: Refreshing policies file

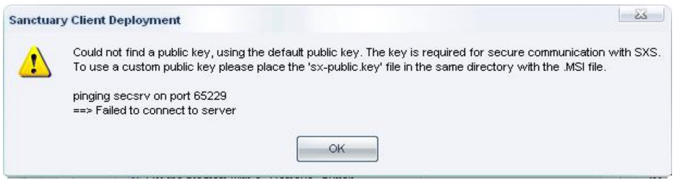
A similar scenario happens when you are not using a public key but are using the default one provided with the installation for testing purposes. Remember that it is not secure to communicate in a working environment with the default key; You should always generate a key pair when you install Sanctuary in a production machine. See *Chapter 7: Using the Key Pair Generator* on page *59* for more information.



The package you want to install is not associated to a public key.
Do you want to install the package with the default public key?

Figure 93: Sanctuary Client Deployment: Missing public key during client deployment (1/2)

You can choose not to associate a public key pair with your client deployment (not recommended, see previous paragraph). If you click on TEST CONNECTION in the *Set Package Policies* dialog and you have not yet generated a public-private key pair, the following warning is displayed:



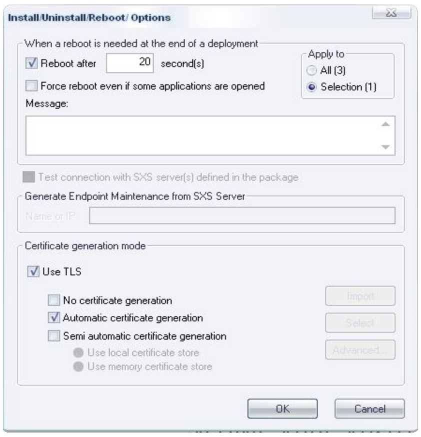
Could not find a public key, using the default public key. The key is required for secure communication with SXS.
To use a custom public key please place the 'sx-public.key' file in the same directory with the .MSI file.

pinging secsrv on port 65229
==> Failed to connect to server

Figure 94: Sanctuary Client Deployment: Missing public key during client deployment (2/2)

You can also choose to import the public key — you should already have generated the key pair at this point. In this case, you should choose the file using Windows' *Open* dialog. Remember that you can always select to keep this file in an external device for added security.

9. If the installation requires rebooting the client computers, the *Install/Uninstall/Reboot Options* dialog is displayed. If this is the case, select the appropriate options and click on OK. These options correspond to those already selected when creating the package.



Install/Uninstall/Reboot/ Options

When a reboot is needed at the end of a deployment

☑ Reboot after 20 second(s)

□ Force reboot even if some applications are opened

Message:

Apply to

○ All (3)

● Selection (1)

■ Test connection with SXS server(s) defined in the package

Generate Endpoint Maintenance from SXS Server

Name or IP:

Certificate generation mode

☑ Use TLS

□ No certificate generation

☑ Automatic certificate generation

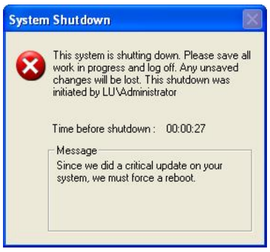
□ Semi automatic certificate generation

● Use local certificate store

● Use memory certificate store

Figure 95: 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.



System Shutdown

This system is shutting down. Please save all work in progress and log off. Any unsaved changes will be lost. This shutdown was initiated by LU\Administrator

Time before shutdown : 00:00:27

Message

Since we did a critical update on your system, we must force a reboot.

Figure 96: Sanctuary Client Deployment: Forced reboot message

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* SecureWave Application Servers option allows you to verify that the SecureWave Application Server defined in the package is 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. See *To install Sanctuary Client* on page *42* for more information.

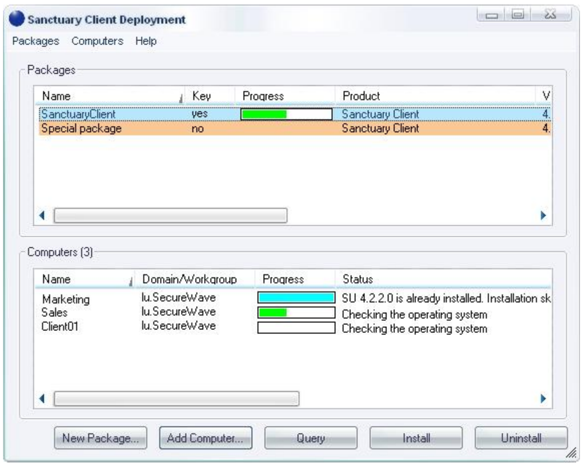
Specify the server name from where the ‘Endpoint Maintenance Ticket’ can be retrieved. If left empty, you must copy this ticket manually to the required directory (normally c:\Program Files\Sanctuary\Ticket) before you can add/modify/delete any client’s component (including directories and registry keys). See *Uninstalling the Sanctuary Client* on page *50* and your corresponding *Administrator’s Guide* for more information.

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

By default 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 remains active until the computer is rebooted.*

✍ *If the endpoint maintenance ticket cannot be retrieved from a server, you must copy it manually to each machine. You cannot modify/change/delete the client components (including directories and registry keys) if this maintenance ticket is not present (unless you deactivate the 'client hardening' options, see your corresponding Administrator's Guide for more information). The client is installed using the 'Disabled' option for 'Client hardening'.*

10. Click on OK. The *Sanctuary Client Deployment* dialog is displayed indicating the progress of each client installation.



Name	Key	Progress	Product	V
SanctuaryClient	yes	🟩	Sanctuary Client	4.
Special package	no		Sanctuary Client	4.

Name	Domain/Workgroup	Progress	Status
Marketing	lu.SecureWave	🟦	SU 4.2.2.0 is already installed. Installation sk
Sales	lu.SecureWave	🟩	Checking the operating system
Client01	lu.SecureWave	□	Checking the operating system

Figure 97: Sanctuary Client Deployment: Installation progress

During 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 explained in the following table:

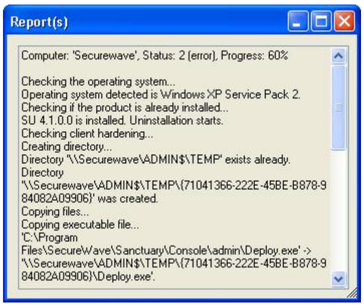
Color		Description
Turquoise	🟦	Task completed successfully.
Green	🟩	Task in progress with no warning.
Yellow	🟨	Task in progress or completed with warnings.
Red	🟥	Task in progress or stopped with an error.

Table 8: Task progress color code

The status column gives you information about 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 context menu. The MSI verbose setup log file displayed should contain information about why the setup was aborted and rolled back. You can contact SecureWave's Technical Support Department for further help in analyzing the log file.

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. The dialog eventually has all progress bars filled with diverse colors depending on the result of the different tasks.

You can also right click on the machine name and use the PROGRESS menu item to view information about the progress of the deployment:



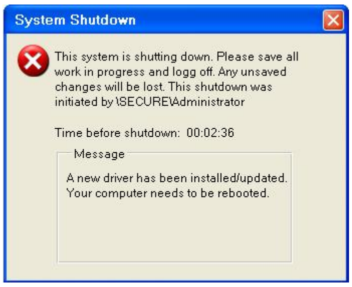
```
Computer: 'Securewave', Status: 2 (error), Progress: 60%

Checking the operating system...
Operating system detected is Windows XP Service Pack 2.
Checking if the product is already installed...
SU 4.1.0.0 is installed. Uninstallation starts.
Checking client hardening...
Creating directory...
Directory "\\Securewave\ADMIN$\TEMP' exists already.
Directory
"\\Securewave\ADMIN$\TEMP\{71041366-222E-45BE-B878-9
84082A09906}' was created.
Copying files...
Copying executable file...
'C:\Program
Files\SecureWave\Sanctuary\Console\admin\Deploy.exe' ->
"\\Securewave\ADMIN$\TEMP\{71041366-222E-45BE-B878-9
84082A09906}\Deploy.exe'.
```

Figure 98: Sanctuary Client Deployment: Installation progress dialog

Here are some common mistakes to avoid:

- Trying to deploy a client package with an sx-public.key file that does not correspond to the key on 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* (except when you are trying to do a ‘Serverless’ installation).
- Trying to deploy a package on a machine where the client has just been removed and the machine has not been rebooted since. You must reboot the client machines after uninstalling.

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.



System Shutdown

This system is shutting down. Please save all work in progress and logg off. Any unsaved changes will be lost. This shutdown was initiated by \SECURE\Administrator

Time before shutdown: 00:02:36

Message

A new driver has been installed/updated. Your computer needs to be rebooted.

Figure 99: Sanctuary Client Deployment: Shutdown dialog in client computers

Using the command line to install 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.
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 include the msi installation file and the public key file (sx-public.key).
3. Install the Sanctuary Client on a list of computers by using your chosen software deployment tool to run this command-line:

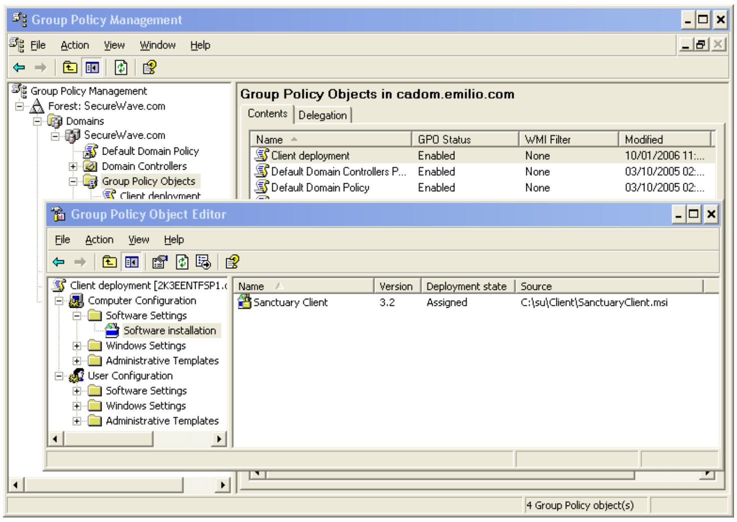
```
Msiexec /i "SanctuaryClient.msi" /qn TRANSFORMS="SanctuaryClient.mst" /L*v
%TMP%\setupcltsu.log
```

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

Using Windows Group Policy to install clients

You can implement 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.

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



Group Policy Objects in cadom.emilio.com

Name	GPO Status	WMI Filter	Modified
Client deployment	Enabled	None	10/01/2006 11:...
Default Domain Controllers P...	Enabled	None	03/10/2005 02:...
Default Domain Policy	Enabled	None	03/10/2005 02:...

Name	Version	Deployment state	Source
Sanctuary Client	3.2	Assigned	C:\su\Client\SanctuaryClient.msi

Figure 100: Using the Group Policy Management Console to install Sanctuary Client

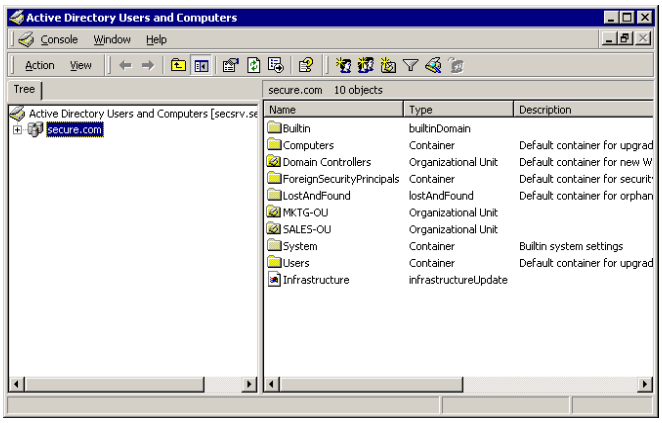
✍ *As with all major changes to Group Policy, it is recommended that any new Policy or changes to existing ones are tested on a development Organizational Unit first before implementing in a production environment.*

✍ *You should define the group policy package with the 'Run logon script synchronously' option activated. This will force a reboot. Beware that the client installation requires an extra reboot.*

1. Create a Deployment package.

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.

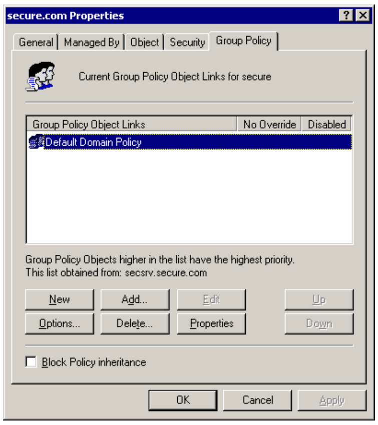

Active Directory Users and Computers
Console Window Help
Action View
Tree
Active Directory Users and Computers [secsrv.se
secure.com
secure.com 10 objects

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upgrad
Domain Controllers	Organizational Unit	Default container for new W
ForeignSecurityPrincipals	Container	Default container for securit
LostAndFound	lostAndFound	Default container for orphan
MKTG-OU	Organizational Unit	
SALES-OU	Organizational Unit	
System	Container	Builtin system settings
Users	Container	Default container for upgrad
Infrastructure	infrastructureUpdate	

Figure 101: Deployment package using group policies: Select active directory

4. Right-click on the Domain (or Organizational Unit) and select *Properties*.

5. Select the GROUP POLICY tab.



Current Group Policy Object Links for secure

Group Policy Object Links	No Override	Disabled
Default Domain Policy		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: secsrv.secure.com

□ Block Policy inheritance

Figure 102: Deployment package using group policies: Select group policy

6. Click on New to create a new Group Policy, and click on Edit.

7. Expand the *Software Settings* folder.

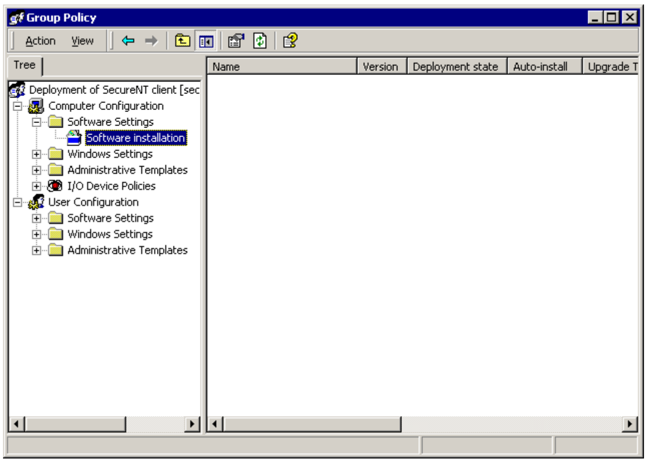
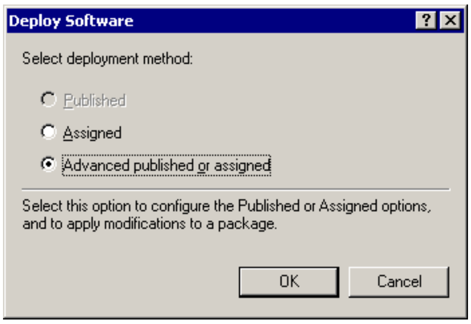


Figure 103: Deployment package using group policies: Software installation

8. Right-click on Software Installation and select *New* → *Package*.

9. Browse to Deploy, select *Sanctuary Client.msi*, and click on Open.

10. In the *Deploy Software* dialog box, select *Advanced published or assigned* and click on OK.



Select deployment method:

○ Published

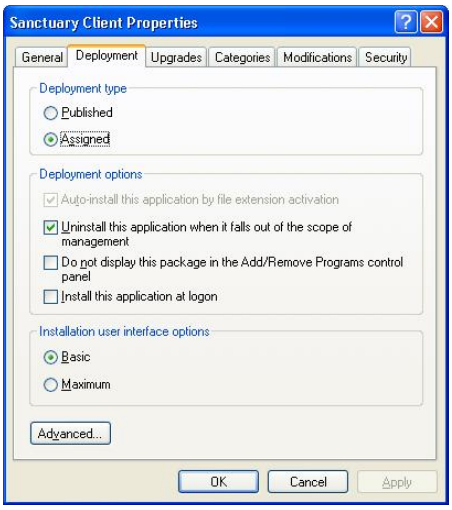
○ Assigned

● Advanced published or assigned

Select this option to configure the Published or Assigned options, and to apply modifications to a package.

Figure 104: Deployment package using group policies: Deployment type

11. Accept the default name of ‘Sanctuary Client’, click on the *Deployment* tab and ensure that *Assigned* is selected.



Deployment type

○ Published

● Assigned

Deployment options

☑ Auto-install this application by file extension activation

☑ Uninstall this application when it falls out of the scope of management

□ Do not display this package in the Add/Remove Programs control panel

□ Install this application at logon

Installation user interface options

● Basic

○ Maximum

Figure 105: Deployment package using group policies: Deployment options

12. Display the Modifications tab and click on Add.

13. Browse to Deploy\Sanctuary Client.mst.

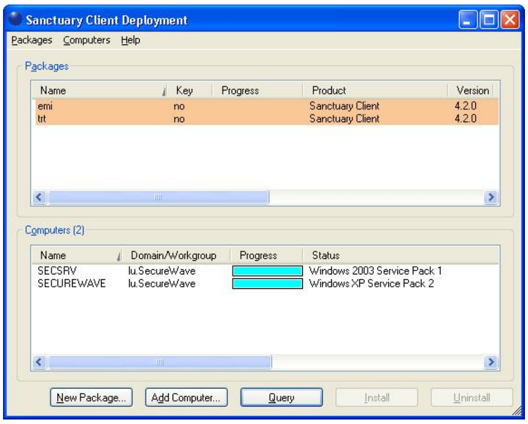
14. Click on Open.

15. Click on OK.

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

Querying the client status

Once you have installed the Sanctuary Client on some client computers, it is necessary to keep track of where and which packages are installed.



Packages

Name	Key	Progress	Product	Version
emi	no		Sanctuary Client	4.2.0
trt	no		Sanctuary Client	4.2.0

Computers (2)

Name	Domain/Workgroup	Progress	Status
SECSRV	lu.SecureWave		Windows 2003 Service Pack 1
SECUREWAVE	lu.SecureWave		Windows XP Service Pack 2

Figure 106: Manage deploy: Query

When you click on the QUERY button, the Sanctuary Client Deployment Tool reports which version of the MSI package is installed on each computer selected in the list. It also checks if all client drivers are still in place and running and reports the client operating system and version, if it is using TLS protocol or not, client hardening status, etc.

✍ *This allows you to detect, for instance, whether or not a user has the client installed on their machine but has disabled the drivers.*

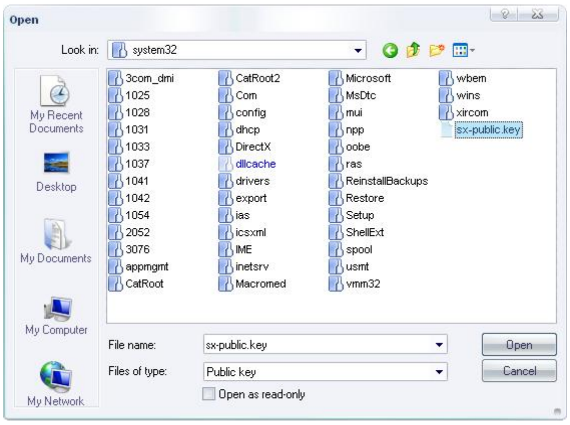
Sanctuary Client Deployment menus

Packages Menu

The *Packages* menu has the following items:

Item	***Description***
New	Allows the user to create a new deployment package, using the process in *To install packages* on page *66.*
Delete	Deletes the selected deployment package.
Rename	Renames the selected deployment package.
Import public key	Allows the user to choose a public key to be included in the selected deployment package. The dialog shown in *Figure 107* is displayed, allowing you to select the public key to be added.
Set Licenses	Opens a dialog where you can import a license to include in the package when it is installed in *Standalone mode*. This is done so that the correct options are installed with the client.
Set Policies	Opens a dialog where you can specify a server from where to retrieve the policies. Policies are exported from this server and placed in a special file — policies.dat. This file is included in the package. See *Figure 108*.
Test Connection	Allows you to verify that the SecureWave Application Server, defined in the package, are up and running before proceeding to the deployment on the client computers. It is not available if you choose the *Serverless Mode* option.
Install	Installs the selected package on all computers in the list. (This performs the same function as the INSTALL button as described in step 7 of *Using the Sanctuary Client Deployment tool to install the Sanctuary* Client on page *71*).
Uninstall	Uninstalls the selected package from all machines in the list.
Open last report	Displays a report describing the last install or uninstall, indicating which machines were modified and status (e.g. whether the install was successful or not).
Options	Allows you to change the root directory where the packages and the SecureWave Application Server are stored.

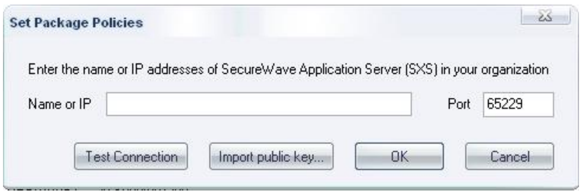
Table 9: Sanctuary Client Deployment menu: Packages menu



File name: sx-public.key

Files of type: Public key

Figure 107: Sanctuary Client Deployment menus: Import public key



Enter the name or IP addresses of SecureWave Application Server (SXS) in your organization

Name or IP

Port 65229

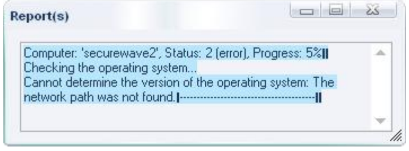
Figure 108: Sanctuary Client Deployment menus: Set policies

Computers menu

The *Computers* menu has the following items.

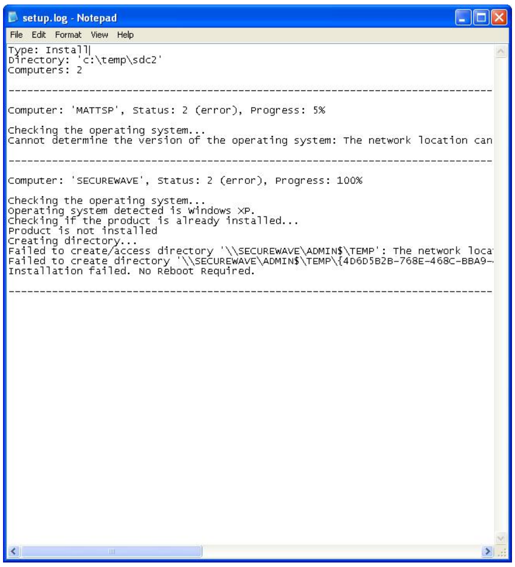
Item	***Description***
Add	Displays a dialog allowing you to add one or more computers to the list of computers. This is the same dialog as appears when you click on the ADD COMPUTER button.
Remove	Removes the selected computer from the list.
Import	Allows you to import a list of computers from an external ASCII or Unicode text file. The file must be a flat text file with one machine per line. The machine name is optionally followed by the domain name and separated from it only by a '|' sign. Every line looks like this: 'ComputerName|DomainName'.
Export	Allows you to export a list of computers selected in the computer list to a text file. The file produced is a flat text file with one machine per line. The machine name is followed by the domain name and separated from it only by a '|' sign. Every line looks like this: 'ComputerName|DomainName'.
Change TLS mode	When using this menu item, you can control some options governing client installation. See the description of *Figure 90* on page *73*.
Reboot	Forces a reboot of the selected computers in the list of computers. You can also select here the server from where the 'Endpoint Maintenance Ticket' will be retrieved.
Query	Performs the same function as clicking on QUERY (see *Querying the client status* on page *80*). The program queries the client versions and drivers status for every machine in the list. It also reports the operating system version and service pack.
Progress details	Displays an additional window providing details of the install / uninstall / query operation on the selected computers. An example of the progress window is shown in *Figure 109*.
Open last log	Opens the log of the last installation. An example log file is shown in *Figure 110*.

Table 10: Sanctuary Client Deployment menu: Computers menu



```
Computer: 'securewave2', Status: 2 (error), Progress: 5%||
Checking the operating system...
Cannot determine the version of the operating system: The
network path was not found.|------------------------------------||
```

Figure 109: Sanctuary Client Deployment menus: Progress detail



```
Type: Install|
Directory: 'c:\temp\sdc2'
Computers: 2

------------------------------------------------------------------------------

Computer: 'MATTSP', Status: 2 (error), Progress: 5%

Checking the operating system...
Cannot determine the version of the operating system: The network location can

------------------------------------------------------------------------------

Computer: 'SECUREWAVE', Status: 2 (error), Progress: 100%

Checking the operating system...
Operating system detected is Windows XP.
Checking if the product is already installed...
Product is not installed
Creating directory...
Failed to create/access directory '\\SECUREWAVE\ADMIN$\TEMP': The network loca
Failed to create directory '\\SECUREWAVE\ADMIN$\TEMP\{4D6D5B2B-768E-468C-BBA9-
Installation failed. No Reboot Required.

------------------------------------------------------------------------------
```

Figure 110: Sanctuary Client Deployment menus: Log example

Help menu

The *Help* menu has the following items.

Item	*Description*
Help	Displays the online help.
About Deploy…	Displays a dialog giving copyright and version information about the Sanctuary Client Deployment tool.

Table 11: Sanctuary Client Deployment menu: Help menu

Context menus

You have two context menus displayed, depending on which panel you right click:

> In the *Packages* panel the available options are those of the *Packages* menu.

> In the *Computers* panel the available options are those found in the *Computers* menu.

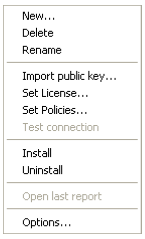


Figure 111: Package panel context menu

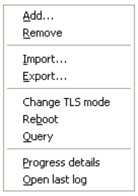
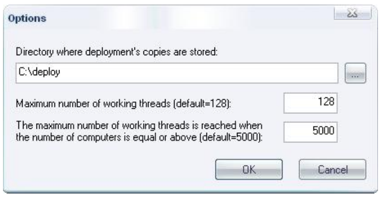


Figure 112: Computers panel context menu

The Options Screen

If you select the *Options* item in the *Packages* menu, the following dialog appears, allowing you to modify the Sanctuary Client Deployment options.


Options

Directory where deployment's copies are stored: C:\deploy

Maximum number of working threads (default=128): 128

The maximum number of working threads is reached when the number of computers is equal or above (default=5000): 5000

Figure 113: Sanctuary Client Deployment menus: Options screen

The first field lets you choose the folder where you would like to store all the deployment packages.

Do not specify the root directory of the system drive or any other directory where existing files 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.

The value of the maximum number of working threads defines the highest number of deployment tasks that the program can perform in parallel. Choosing a lower value reduces the impact on the computer and network performance. Choosing a higher value allows faster deployments — if there are enough computer and network resources available.

The third parameter defines the number of computers threshold for which the maximum number of threads will be used. Both parameters are combined to allow you to fine-tune the application performances. The relation that links both parameters is explained in *Figure 114*.

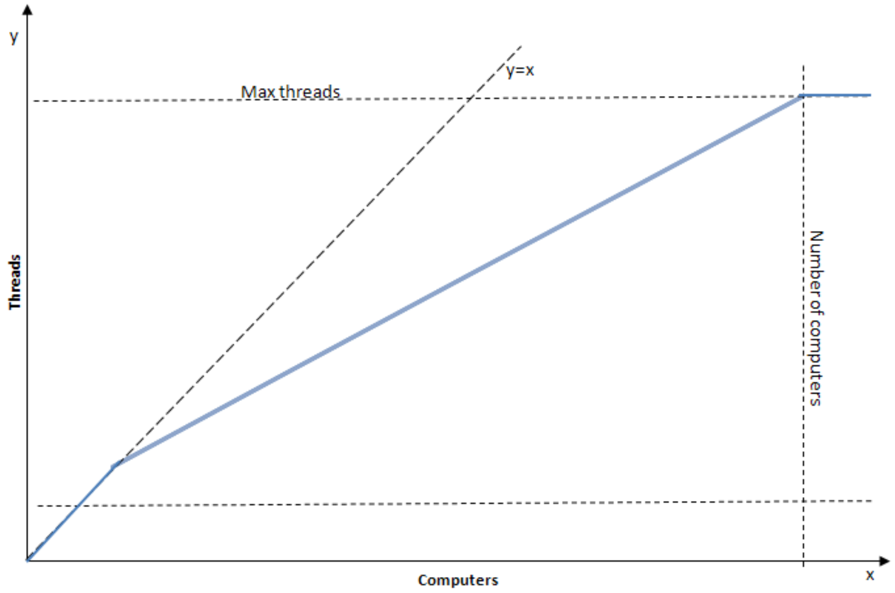


Figure 114: Sanctuary Client Deployment menus: Number of threads vs. number of computers

Chapter 9: Using the SXDomain Command line tool

This chapter explains how you can synchronize domain information with that contained in the SecureWave Sanctuary Database.The information in this chapter is relevant to all Sanctuary products.

Introduction

The SXDomain command-line tool is an alternative to the Add Domain / Synchronize Domain items in the *Tools* menu on the Sanctuary Management Console. You can use it to:

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

SXDomain.exe can be found within the C:\Program Files\SecureWave\Sanctuary\SXTools directory (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***
`-s servername`	The fully qualified domain name or IP address of the computer on which SecureWave Application Server is running.
`-i`	Instructs the utility to read domain names to add or synchronize from a standard input stream (interactive mode).
`-e`	Instructs the utility to write the domain names that could be neither added nor synchronized to a standard error stream.
`-u username`	The user name used to authenticate on the remote computer.
`-p password`	Password. SXDomain prompts you for one, if not supplied.
`-q`	Do not prompt for user name or password if cannot authenticate.
`domain`	The name of the domain(s) or computer(s) that you want to add or refresh.

Table 12: SXDomain parameters

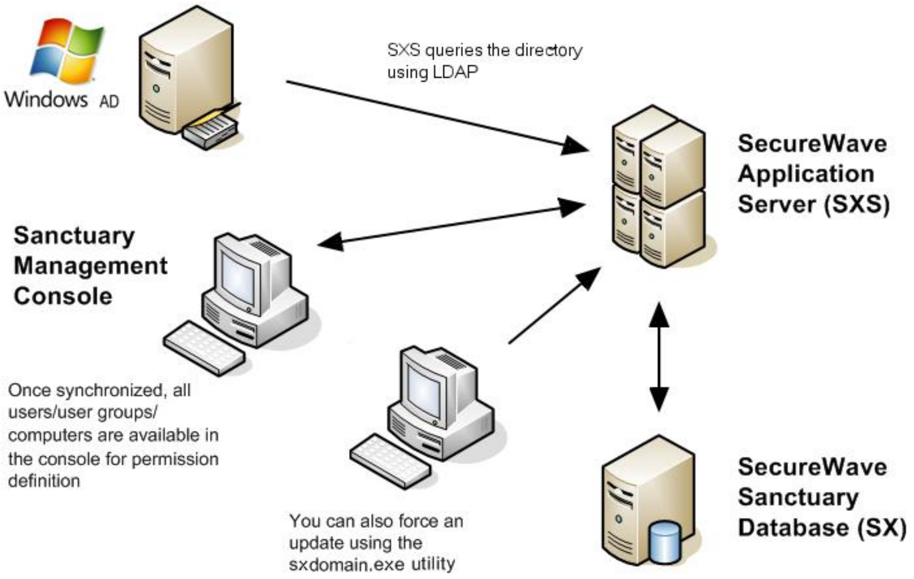

Windows AD
SXS queries the directory using LDAP
SecureWave Application Server (SXS)
Sanctuary Management Console
Once synchronized, all users/user groups/ computers are available in the console for permission definition
You can also force an update using the sxdomain.exe utility
SecureWave Sanctuary Database (SX)

Figure 115: Active Directory objects' synchronization

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 following 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 SecureWave Application Server from retrieving 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
```

If you prefer, you can synchronize domains interactively:

```
SXDOMAIN –i
```

Type in the name of each domain followed by the ENTER key. Once you are finished, use Ctrl+C to end the interactive mode and exit to the operating system.

Scheduling domain synchronizations

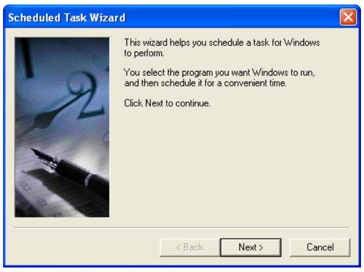
You can schedule domain synchronizations with your favorite task scheduler. Here is a procedure using the Windows Tasks Scheduler.

In the C:\Program Files\SecureWave\Sanctuary\SXTools 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.



This wizard helps you schedule a task for Windows to perform.

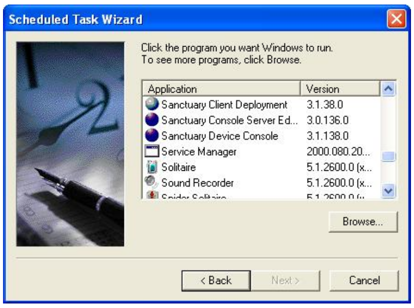
You select the program you want Windows to run, and then schedule it for a convenient time.

Click Next to continue.

Figure 116: Scheduled task: First step

2. Click on NEXT.

3. In the following screen, click on BROWSE and select the sxsynch.bat file:

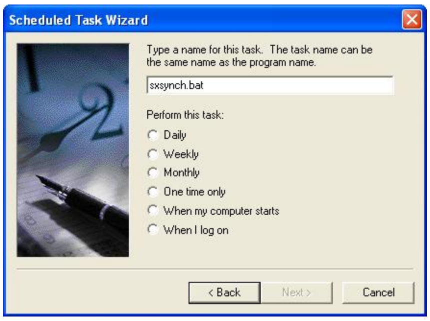


Click the program you want Windows to run.
To see more programs, click Browse.

Application	Version
Sanctuary Client Deployment	3.1.38.0
Sanctuary Console Server Ed...	3.0.136.0
Sanctuary Device Console	3.1.138.0
Service Manager	2000.080.20...
Solitaire	5.1.2600.0 (x...
Sound Recorder	5.1.2600.0 (x...

Figure 117: Scheduled task: Select program

4. In the next two screens, choose how often you want the task to be performed:



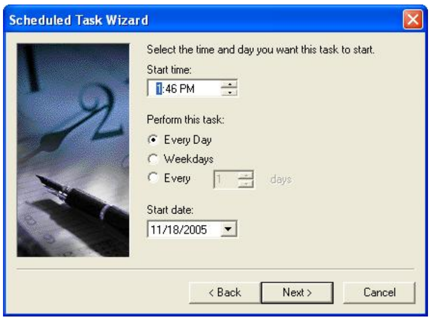
Type a name for this task. The task name can be the same name as the program name.

sxsynch.bat

Perform this task:

○ Daily
○ Weekly
○ Monthly
○ One time only
○ When my computer starts
○ When I log on

Figure 118: Scheduled task: Select period (1/2)



Select the time and day you want this task to start.

Start time: 1:46 PM

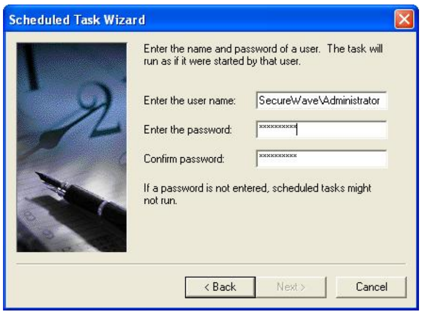
Perform this task:

● Every Day
○ Weekdays
○ Every 1 days

Start date: 11/18/2005

Figure 119: Scheduled task: Select period (2/2)

5. Specify an account that has rights to use the Sanctuary Management Console. This is the account that runs the sxdomain command:



Enter the name and password of a user. The task will run as if it were started by that user.

Enter the user name: SecureWave\Administrator

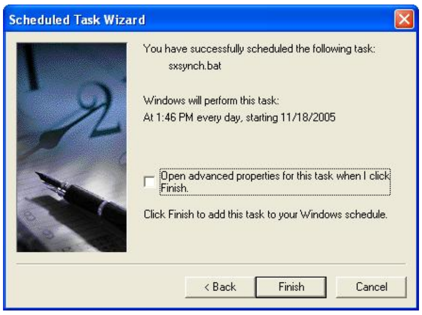
Enter the password: **********

Confirm password: **********

If a password is not entered, scheduled tasks might not run.

Figure 120: Scheduled task: Select account

6. Click on FINISH to end the Wizard:



You have successfully scheduled the following task:
sxsynch.bat

Windows will perform this task:
At 1:46 PM every day, starting 11/18/2005

□ Open advanced properties for this task when I click Finish.

Click Finish to add this task to your Windows schedule.

Figure 121: 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 10: Registering your Sanctuary product

This chapter explains what happens when you register your Sanctuary product. It provides examples of information contained in a typical license file. The information in this chapter is relevant to all Sanctuary products.

Licensing

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

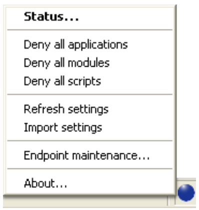


Figure 122: Client's options when several Sanctuary products are installed

If the license information changes, for example when it expires, or a new Sanctuary product is added, the client is informed and its options changed accordingly.

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 functionality of Sanctuary software, but with the following limitations:

- It only lasts 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 is sent to you by e-mail. This license key is specifically configured for the license you have purchased. You do not need to uninstall the software when switching from an evaluation license to a full license. The SecureWave Application Server uses the new license file within an hour. If you want SecureWave Application Server to use the new license file immediately, restart the SecureWave Application Server service on every SecureWave 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 runs SecureWave Application Server. It is *not* required to be present on client machines.

If you are using more than one SecureWave Application Server the same license file must be used on all the servers.

License file format

A Sanctuary license file comprises a series of name and value pairs, one per line. It includes the following important information:

Key	***Description of value***
ProjectName	Identifies the software product for which the license is valid.
ExpiryDate	Validity of the license file.
LicensedClients	Number of clients that can be registered in the SecureWave Sanctuary Database. This corresponds to the sum of the number of computers where Sanctuary Client Driver is used.
LicensedSessions	This limits the number of sessions that SecureWave Application Server allows. 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 circumstances by some server programs (mail, web, FTP servers, and so on).
LicensedServers	Number of instances of SecureWave Application Server that may be run at the same time. SecureWave Application Server refuses to start if it detects a number of already running SecureWave Application Server instances exceeding this limit.
ProductName	The full name of the product for which the license was created.
ClientName	The name of the customer to whom the product was licensed.
GeneratedOn	The date on which the license was created. This is useful if you are unsure when to renew your maintenance contract.
Serial#	The serial number of this license.
LicensedTo	The name and/or email address of the person to whom the license was issued.

Table 13: 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 using secondary logon services ('runas' command in Windows 2000/XP/2003).

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

License-related SecureWave Application Server actions at start-up

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

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

No other license related conditions cause SecureWave Application Server to refuse to start.

License-related SecureWave Application Server actions while running

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

SecureWave Application Server 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, SecureWave Application Server 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 Application Control Server 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 applies 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 ceases to apply Sanctuary policies if not licensed. This only affects customers violating the license, but this can also be a result of incorrect license management and can represent a security risk for your organization.

Appendix A: 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 components used in a Sanctuary implementation and details the limitations of installing the Sanctuary Client on Terminal Servers and Citrix environments for some products of our suite.

System requirements

	SecureWave Application Server	***SecureWave Sanctuary Database***	***Administration Tools***	***Sanctuary Client***	
Operating System	Windows 2000 Server (SP4 or later) or Windows Server 2003 SP1 or SR2 (32-bit).	Windows 2000 Server (SP4 or later) or Professional, Windows XP Professional (SP2 or later), Windows Server 2003 SP1 or SR2 (32-bit) or Vista (32-bit).	Windows 2000 Server (SP4 or later) or Professional, Windows XP Professional (SP2 or later), Windows Server 2003 SP1 or SR2 (32-bit) or Vista (32-bit).	Sanctuary Device Control, Sanctuary Custom Edition	Windows 2000 Professional (SP4 or later), Windows XP Professional (SP2 or later), Windows XPe SP2, Windows Embedded for Point of Service (WEPOS) SP2, Windows XP Tablet PC Edition SP2 and Vista (32- and 64-bit versions).
				Sanctuary Server Edition, Sanctuary Terminal Services Edition	Windows 2000 Server (SP 4 or later) Windows Server 2003 SP1 or SR2 (32-bit).
Hard Disk Space	40 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 (depending on the number of users).	140 Mb free disk space for program files and 15 Mb for the installation.	6 Mb free disk space for program files and 15 Mb for the installation. The local data requirements depend on whether you chose to do 'Shadow' or not and goes from 10 MB to several GB.	
Memory	128 MB (256 MB recommended)				
Display	Not applicable		1024x768	Not applicable	
File System	NTFS				
Other	MDAC v2.6 SP1 or later if you are using Windows 2000. A Certificate Authority installed and configured if TLS protocol is chosen for intra Application Server communication.	Microsoft SQL Server 2000/2005, SQL Server 2005 Express Edition (needs MS .Net Framework 2.0), or MSDE 2000, MDAC V2.6 SP1 or later if using Windows 2000.	Adobe PDF Reader v5.0 or later to consult the on-line manuals.	Novell client v4.91 SP2/SP3 or later if connected to a Novell environment. A Certificate Authority installed and configured if TLS protocol is chosen for Client-Application Server communication. Daemon Tools and Alcohol cd burning software are not compatible with Sanctuary Device Control.	

Using central encryption or TLS communication protocol	You need a valid Certificate Authority installed to issue and manage certificates if you want encrypted client SecureWave Application Server and intra-SecureWave Application Server TLS communications. This authority is also needed if you plan to centrally encrypt removable devices (if using Sanctuary Device Control). If no Certificate Authority is found, you can still encrypt devices (with some limitations) and the communication channel is assured by signing messages with a private key.
Using Novell	You will need the following elements installed on the computer used to synchronize Novell's objects: Novell (and optionally ZENworks) client v4.91 SP2/SP3 or later, NDAP (for workstation object synchronization), the synchronization script, an access to Sanctuary's database. We recommend installing all these components on the same machine as the one used to host the database. Synchronizing environments running versions of NetWare earlier than 6.5 is not supported. At time of printing of this document, there is currently no Vista-compatible Novell platform therefore we do not support Novell environments on Vista.

Table 14: System requirements

✍ *If you are using Sanctuary Device Control and plan to use encrypted devices, you must have Active Directory and DNS installed and properly configured. The Microsoft Certificate Authority must be installed, properly configured, and published. See Appendix H: Installing a Certificate Authority for encryption and TLS Communication.*

✍ *You can find the NDAP component required for Novell synchronization in the installation CD or on 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.*

✍ *SecureWave Application Server cannot be installed on Windows XP or Windows 2000 Pro.*

💣 *You should resolve all hardware conflicts before installing Sanctuary solutions. You can use Windows' Device Manager to troubleshoot and fix software-configurable devices. All hardware devices that use jumper pins or dip switches must be configured manually.*

Sanctuary Device Control

Terminal services limitations

The Terminal Services administration mode and the remote desktop functionality allow access to computers 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 Driver 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 denies all proxy access. This means for example that the users cannot 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 cannot 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. The user cannot be determined when there are active RunAs logon sessions.

When the Sanctuary Client Driver 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 **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 *cannot* create new CDs. Bill has to log off and log on as John to create new DVDs/CDs. Since writing a DVD/CD requires a proxy, it is subject to the limitation described in this section.

✍ *Writing a DVD/CD 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 disk drive, whereas John has Read/Write access to it. If Bill uses a RunAs command to run the Windows File Explorer under the credentials of John, he can read and write to Floppy disks. Indeed, access to the Floppy disk drive is done without a proxy. The limitation described in this section does not apply to this device.

Appendix B: 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. All 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
```

*Keys whose names are marked with an asterisk * should not be modified except under the supervision of SecureWave Support personnel.*

Database connection loss registry keys

The SecureWave Application Server continues to run even if it has an intermittent database connection. It ignores database connection problems for a certain period of time, retrying connections to the SecureWave Sanctuary Database until it succeeds. If the problems persist, the SecureWave Application Server stops accepting client and console connections until it detects database connectivity has been restored.

You can configure the following parameters to determine the exact behavior of the SecureWave Application Servers if they lose connection to the SecureWave Sanctuary Database:

Key Name	***Description***	***Default***
DbConnectionCount	The number of database connections in the connection pool.	20
DbConnectionMaxCount	The maximum number of DB connections (if it is less than DbConnectionCount, it will be assumed equal to it)	40
DbConnectionPoolTimeout	The timeout, in seconds, for connection acquisition from the DB pool. If no connection can be acquired within the timeout, an attempt to grow the pool will be made. Note that if the pool has reached the maximum number of connections, no new connections will be created and the wait will be repeated.	15
DbConnectionString	Driver, server, database, and either a trusted connection, or username and password. The default value is ‘Provider=sqloledb;Data Source=;Initial Catalog=sx;Trusted_Connection=yes;’	See description
DbInitializationDelay*	Number of seconds that SecureWave Application Server waits before contacting the SQL Server	300
DbLossLatency	The graceful DB loss period, in seconds, during which the server accepts client and console connections after DB loss has been detected (3600 is one hour).	3600
DbPingPeriod	The periodicity, in seconds, of DB pinging when the server has stopped accepting client and console connections (60 is one minute).	60

Table 15: SecureWave Application Server registry keys (Database related)

Log insertion process registry keys

The following table shows all registries that can be modified to fine-tune the endpoint data reception facility that controls logs and shadow files received from the Sanctuary Client Driver. The endpoint data reception facility places all incoming data in a staging queue, from which endpoint data batches are generated and dispatched in a regular fashion, without stressing the database. Advanced configuration parameters are available to fine-tune batching and dispatching of endpoint data; statistical information is available in the Windows Application Event Log to help examine and fine-tune the configuration:

Key Name	***Description***	***Default***
edrBatMaxDuration	Max batching time per batch, in seconds. If a batch has not reached the minimal number of entries, but exceeded this duration being batched, it will be put into the	30

Key Name	Description	Default
	queue.	
edrBatMinEntries	Minimum entries per batch. A batch will be put into the queue as soon as it has at least this number of entries, or it has been being batched longer than the max batch duration (see next).	10000
edrBatThreads	The number of batching threads.	2
edrDspPause	Successful dispatch mean sleep time, in seconds. Zero by default. Once a dispatcher submits a batch to the DB successfully, it will sleep that long.	0
edrDspPauseFail	Initial unsuccessful dispatch mean sleep time, in seconds.	60
edrDspRetryCount	Max number of retries for unsuccessful dispatches.	5
edrDspThreads	The number of dispatching threads.	1
edrQueLength	The length of batch queue.	3
edrStaPeriod	The periodicity of statistical output, in seconds. Zero disables statistical output (43200 is 12 hours).	43200
edrTmpTimeout	Max file slot allocation time, in seconds. When clients upload data, temporary files are allocated. The temporary directory can contain a limited number of files. If the directory becomes congested and no more temp files are available, the server will wait up to this duration for a free temp file slot.	30

Table 16: SecureWave Application Server registry keys (Log insertion process)

Debugging registry keys

The following registry keys are used to debug SecureWave Application Server:

Key Name	Description	Default
Debug*	If ‘yes’ or ‘1’ and if SecureWave Application Server runs as a service, it attempts 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
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 Sanctuary Device Control. Key used by *Spread Check*. If configured, it would also monitor the spread of DLLs that have been authorized implicitly in the *DLL don't care* mode. If not configured, only applications and explicitly authorized DLLs are monitored. See the *Sanctuary Application Control Suite Administrator's Guide* for more details.	no
LogMonitorPeriod	Not used for Sanctuary Device Control. Period, in seconds, between two checks.	300
LogMonitorResetOptions	Not used for Sanctuary Device Control. Controls whether the global user option is set to blocking mode when the alert is generated, if ‘no’, SecureWave Application Server 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
LogMonitorThreshold	Not used for Sanctuary Device Control. Number of distinct users that must execute the same locally authorized executable for an alert to be issued.	10
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 SecureWave Application Server 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 SecureWave Application Server service to take the VerboseSyncLogging Value into account. You should not set this option to ‘yes’ permanently for performance reasons.	no

Table 17: SecureWave Application Server registry keys (Debugging purpose)

General registry keys

This registry keys are general ones:

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
DataFileDirectory	The base directory under which the SecureWave Application Server stores data files (log files, for instance). If multiple SecureWave Application Servers are in use, their DataFileDirectory entries may all resolve to the same directory on disk. This is the directory created during the Database setup process. All servers can optionally write to the same, shared, directory or you can opt for having different ones for each server (see *Figure 1*).	.
Products	Internal use. Do not modify.	3

Table 18: SecureWave Application Server registry keys (general keys)

Security registry keys

These registry keys are related to security configuration and parameters:

Key Name	***Description***	***Default***
CertificateQueryPeriod	(optional) Controls the periodicity the SecureWave Application Server checks user’s certificates published in AD.	180
CommVer	The SecureWave Application Server 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 3.2. A value of ‘2’ indicates a client version 4.0, and ‘3’ is used for version 4.1 or greater.	3
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 SecureWave Application Server is momentarily busy or because it has reached the limit imposed by MaxSockets. SecureWave Application Server 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 SecureWave Application Server, see ‘MaxRpcCalls’ for that. Minimum: 1, maximum: 50000 (arbitrary). See ‘Port’, ‘TLSPort’, and ’TLSMaxSockets’. See also *Table 20* & *Table 21*.	5000
Port	The TCP port on which the socket-based SecureWave Application 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. Transmissions that do not use the TLS protocol are always signed. See ‘TLSPort’, ‘TLSMaxSockets’, and ’MaxSockets’.	65129
RpcProtectionLevel	Determines whether the RPC (Remote Procedure Call) server will require RPC clients to identify (authenticate). Valid levels are: ‘0’: Instructs the OS to pick a protection level. At the time of this writing, this is equivalent to ‘2’. ‘1’: No protection. Should not be used except for testing. ‘2’: The client's identity is verified when connecting to SecureWave Application Server. RPC messages are vulnerable to tampering and man-in-the-middle attacks. ‘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. ‘4’: Examines client credentials not only once per request (like ‘3’) but with every single packet. ‘5’: Like ‘4’, with added cryptographic signing of every packet to defend against tampering. ‘6’: Like ‘5’, but also encrypts data in both directions. The recommended setting is ‘5’ or more. Note that any setting except ‘0’ requires the client to be in the same domain as the server, or in a domain that is trusted by the server's domain.	6

Key Name	***Description***	***Default***
SecureInterSxs	If set to 'yes', all inter-SecureWave Application Server traffic is done using the TLS protocol. Note that SecureWave Application Servers register the fully qualified DNS name in the servers table (for compatibility with older versions) and, depending on the communication mode selected, the TLS or the non-TLS port. Servers with different Inter-SecureWave Application Server modes will not be able to communicate between them - they should either all have the 'yes' or 'no' value set for this parameter. When this value is set to 'no', communication is done using non-TLS ports. When setting this value to 'yes', you should also set the number of non-TLS sockets ('MaxSockets', see *Table 20* & *Table 21*) to zero and 'CommVer' to '3' (client drivers v4.1 or later) to obtain the maximum level of security.	no
SndPort	The TCP port on which the Sanctuary Client Driver is expected to listen. If absent or zero, 33115 is used. Minimum: 1, maximum: 65534.	33115
SxdConnectTimeoutMSec	The time, in milliseconds, that SecureWave Application Server waits for the Sanctuary Client Driver 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 Driver built-in server is expected to listen. If absent or zero, 33115 is used. Minimum: 1, maximum: 65,534.	33115
TLSMaxSockets*	The maximum number of TCP connections that are allowed at any one time when using TLS protocol. See description on MaxSockets. Minimum: 1, maximum: 50000 (arbitrary). See 'Port', 'TLSPort', and 'MaxSockets'. See also *Table 20* & *Table 21*.	64
TLSPort	The TLS port on which the socket-based SecureWave Application Server machine listens for new connections. Minimum: 1, maximum: 65534. This affects only client drivers. Minimum: 1, maximum: 65534. Transmissions using TLS protocol are always encrypted. See 'Port', 'TLSMaxSockets', and 'MaxSockets'.	65229
** See note on next section.		

Table 19: SecureWave Application Server registry keys (general registry keys)

The next table describes the configuration rules that follow the TLSMaxSockets and MaxSockets parameters (as described in the previous table) — see also *Table 21*:

TLSMaxSockets and MaxSockets values	***Description***
TLSMaxSockets > 0 AND MaxSockets = 0	Only TLS connections are available for SecureWave Application Server-Sanctuary Client Driver communication using the port specified on 'TLSPort'
TLSMaxSockets = 0 AND MaxSockets > 0	Only non-TLS connections are available for SecureWave Application Server-Sanctuary Client Driver communication using the port specified on 'Port'
TLSMaxSockets > 0 AND MaxSockets > 0	Both TLS and non-TLS connections are available for SecureWave Application Server-Sanctuary Client Driver communication using the ports specified on 'Port' and 'TLSPort'

Table 20: Configuring MaxSockets and TLSMaxSockets

Several registry keys (SecureInterSxs, CommVer, TLSMaxSockets, MaxSockets. Port, and TLSPort) interact together and some combinations are not valid as shown in the following table:

SecureInterSxs	***CommVer***	***TLSMaxSockets***	***MaxSockets***	***Result***	***Notes***
no	<3	0	0	✗	You must set the Non TLS Clients *Max Concurrence* field to a value >0 when selecting an older client protocol.
		0	>0	✓	SecureWave Application Server -Client and intra-SecureWave Application Server communication will be done using a non-TLS channel, This is only recommended when you already have an older installation and you are updating it.
		>0	0	✗	You must set the Non TLS client *Max Concurrence* field to a value >0 since you did not select the *Secure Inter-*SecureWave Application Server option.
		>0	>0	✓	You should already have a valid computer certificate. Only used for migration purposes (updates) and not recommended for a new installation.
	3	0	0	✗	The selected protocol is 3: TLS is a requirement.
		0	>0	✗	The selected protocol is 3: TLS is a requirement.
		>0	0	✗	You must first select the *Secure Inter-*SecureWave Application Server option.
		>0	>0	✓	You should already have a valid computer certificate. Only used for migration purposes (updates) and not recommended for a new installation.
yes	<3	0	0	✗	You cannot select the *Secure Inter-*SecureWave Application Server option when the TLS Clients *Max Concurrence* field is set to a value = 0.
		0	>0	✗	You cannot select the *Secure Inter-*SecureWave Application Server option when the TLS Clients *Max Concurrence* field is set to a value = 0.
		>0	0	✓	You should already have a valid computer certificate.
		>0	>0	✓	You should already have a valid computer certificate. Only used for migration purposes (updates) and not recommended for a new installation.
	3	0	0	✗	The selected protocol is 3: TLS is a requirement.
		0	>0	✗	The selected protocol is 3: TLS is a requirement.
		>0	0	✓	You should already have a valid computer certificate.
		>0	>0	✓	You should already have a valid computer certificate. Only used for migration purposes (updates) and not recommended for a new installation.

Table 21: Configuring SecureInterSxs, CommVer, TLSMaxSockets, MaxSockets. Port, and TLSPort

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.	
ReportMaxRecords	Maximum number of records a report will contain.	10000
ReportGenerationTimeout	Cancel the report generation of a report, if it is not possible to generate it within a specific time. The timeout is in milliseconds.	120000
ReportThreads	Number of threads to use. A default of 0 implies two threads per processor.	0
ReportStoragePath	A path SecureWave Application Server will use for temporary storage.	sxsdata
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. Other values are: 0x00 Success 0x01 Error 0x02 Warning 0x04 Information 0x08 Success 0x10 Failure	0x1F

Table 22: SecureWave Application Server registry keys

Sanctuary Client registry keys

The changes to the registry values are only effective after a reboot of the client computer. Sanctuary Command Control, SCC, is in charge of all communication between server and client(s). Its keys are located in `HKLM\system\CurrentControlSet\Services\scomc\parameters`.

The following table contains details of each registry key entry for SCC (all these entries are of type REG_SZ; string value):

Key Name	***Description***	***Default***
CertGeneration	'yes' means that the client is in 'automatic' mode and request the needed certificate. 'no' means that the client in 'manual' mode, the certificate has to be generated manually.	Defined during client installation.
Debug (optional)	Use for debugging purposes.	3 (you must reboot in order to make it work).
FirstServer (optional)	If this is greater than or equal to the number of IP addresses in the list located on the Servers key, Sanctuary Client Driver will use 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 fashion. If the key is missing or has a -1 value, existing servers are randomly chosen.	
HardeningMode	Defines the level of permissibility allowed to modify, repair, or remove the client driver, registry keys, or special directories (disabled, basic, or extended).	disabled
HardeningStatus	Defines if the Hardening Mode is taken or not into consideration.	inactive
HID*	Internal use. Do not modify.	
HistoryPeriodSecs (optional)	Internal use. Do not modify.	
ImportDir	The directory used to import the policies file.	C:\Program Files \SecureWave \Sanctuary\Import
LastSeenComputerName	Internal use. Do not modify.	
LastShadowUploadTime	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	Indicates the last time logs were transmitted.	
Log file name	Gives the name of the log file written if 'Log to file' is 'yes'.	'scomc.log'
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 below).	'no'
Salt	An internally generated 15-byte random value used for protection purposes. It is calculated when the client driver starts.	N/A

Key Name	Description	Default
Servers	A list of SecureWave Application Server names (FQDN) 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.
ServersOverride	Internal use. Do not modify.	
ShadowDirHistory (optional)	Internal use. Do not modify.	
TicketDir	Directory where the endpoint maintenance ticket has to be copied in order to relax 'client hardening'.	
UseTLS	'yes' when TLS is used (all communication is encrypted) 'no' when TLS is not used (all communication is signed).	Defined during client installation.

Table 23: Client registry keys (1/2)

- The Parameters subentry is used to save different program options. Its keys are located in: `HKLM\system\CurrentControlSet\services\sk\parameters`

The following table contains details of the major registry key entries for Sanctuary Client Driver.

Key Name	Type	Description	Default value
Enum	Subkey	Contains device list.	
Limits	Subkey	Copy limit settings (UpdateTime, CachedSize, and so on).	
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 24: Client registry keys (2/2)

Appendix C: Upgrading from old versions

The information in this appendix is product specific.

If you are upgrading from a previous version of Sanctuary, you should be aware that the upgrade process should always be done in the following order:

1. If you are using any of the programs that form our Sanctuary Application Control Suite, 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 setup cannot proceed, as it would be classified as an unknown executable that needs authorization.

2. Stop the SecureWave Application Server service. This service can be started and stopped through the Windows Services Panel or using the command line (net stop sxs and net start sxs). The setup Wizard stops, updates, and starts the service automatically without your intervention only if the SecureWave Application Server resides on the same machine as the SecureWave Sanctuary Database. If you are using several SecureWave Application Servers please stop their respective services manually before proceeding.

✍ *We strongly recommend backing up your database before updating Sanctuary.*

3. Update the SecureWave Sanctuary Database in your SQL server (SQL Server 2000/2005, SQL Server 2005 Express Edition, or MSDE 2000).

4. Update all existing SecureWave Application Server.

5. Update the Sanctuary Management Console.

6. Finally, update the Sanctuary Client(s).

💣 *Old Sanctuary Management Console simply refuses to communicate with a more recent SecureWave Application Server.*

💣 *A Sanctuary Client update requires a reboot.*

💣 *Never change the key pair during a Sanctuary upgrade where client hardening is switched on, otherwise your upgrade will fail.*

✍ *If you update from older versions of Sanctuary, but you keep the old clients, device/application permissions are **NOT** sent to them. You must consider updating these older clients **as soon as possible**. You also lose the added security that new Sanctuary Client offers against deleting, modifying, or altering its components.*

✍ *You must stop SecureWave Application Server(s) — using ‘net stop SXS’ from the command-line prompt — BEFORE updating the database.*

✍ *If you are planning to keep old clients versions, do not forget to choose the correct communication protocol supported by your Sanctuary Client when updating your SecureWave Application Server(s).*

✍ *You must have a Certificate Authority if you want to take advantage of an encrypted channel for Sanctuary Client Driver -SecureWave Application Server and intra-SecureWave Application Server communications.*

To summarize, the upgrade is done in two broad stages:

- First, upgrade all server-side components – during this first stage, the new server-side components have to work with the old client versions.
- Second, deploy the new client upgrade packages – the client deployment stage 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 Application Control Custom Edition v2.8. You should change them back to the correct value after installing this new version. See the Sanctuary Application Control Suite Administrator's Guide for more information about how to change these options.

Since permission’s structure has changed radically from previous versions, your risk not transmitting them properly to older clients. You should consider an immediate client update in these cases.

You may have to manually re-classify some devices in other classes. This is specially true if the class they belong to has been reclassified or disappear. Please check the Sanctuary Device Control Administrator's Guide and the readme file for more info.

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 Application Control Server Edition doing one of the following actions:

- Running the setup.exe file from the Client folder of the Sanctuary CD-ROM.

  If you are installing the Sanctuary Client on a Vista machine with Vista’s UAC functionality turned on, you must use setup.exe (not Control Panel ➔ Add/Remove Programs) otherwise the operation will fail.

- Deploying the Sanctuary Client.msi and a Sanctuary Client.mst files as described in *Chapter 8: Unattended Client installation* on page *63*.
- After upgrading to a new version of the Sanctuary Client using this method it is important that you reboot the client machine as network cards may otherwise be disabled.
- Running the Setup in command-line mode. Refer to *Chapter 8: Unattended Client installation* on page *63* for more information about how to create a transform file (.mst extension):

```
Msiexec /i "SanctuaryClient.msi" /qn TRANSFORMS="SanctuaryClient.mst" /L*v
%TMP%\setupcltsu.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 SecureWave Application Server service on that computer before upgrading:

   ```
   net stop sxs
   ```

2. Run the setup.exe file located in the \SERVER\db folder on the computer where you installed the SecureWave Sanctuary Database.

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

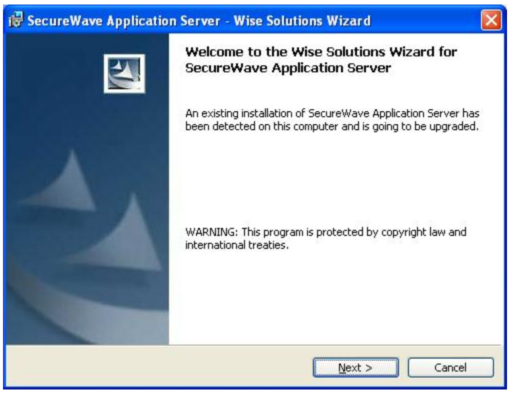
3. Run the setup.exe file located in the \SERVER\SXS folder on the computer(s) where you installed the SecureWave Application Server.
4. Run the setup.exe file located in the \SERVER\SMC folder on the computer(s) where you installed the Sanctuary Management Console.

It is very important that you upgrade first the database, then the SecureWave Application Server(s), and finally the Management tools. Furthermore, always upgrade server-side components before upgrading the clients.

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 SecureWave Application Server installation 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 SecureWave Application Server service (c>Net Stop SXS).
3. Insert the Sanctuary CD in your DVD/CD drive and run setup.exe located in the \SERVER\sxs folder.
4. The *Welcome* dialog is displayed informing you that a previous version of the server is already installed and there is an upgrade.



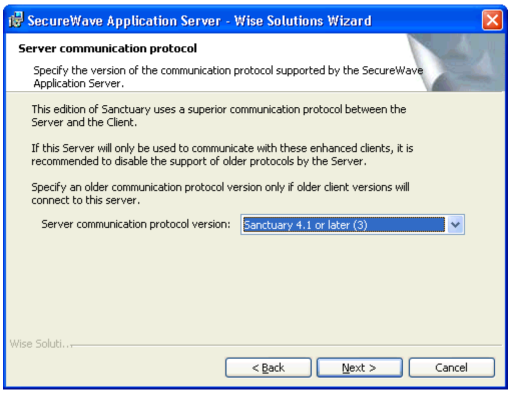
SecureWave Application Server - Wise Solutions Wizard

Welcome to the Wise Solutions Wizard for SecureWave Application Server

An existing installation of SecureWave Application Server has been detected on this computer and is going to be upgraded.

WARNING: This program is protected by copyright law and international treaties.

5. Figure 123: SecureWave Application Server upgrade: First step
6. Click on the NEXT button to continue. You are now asked what kind of communication protocol the SecureWave Application Server should use. You can choose among four: v3.0 or older, v3.1, v4.0, v4.1 or newer. Choose your option from the list. You can always change this setting later by modifying the CommVer registry key — see *Table 19* on page *100* for more information.



SecureWave Application Server - Wise Solutions Wizard

Server communication protocol

Specify the version of the communication protocol supported by the SecureWave Application Server.

This edition of Sanctuary uses a superior communication protocol between the Server and the Client.

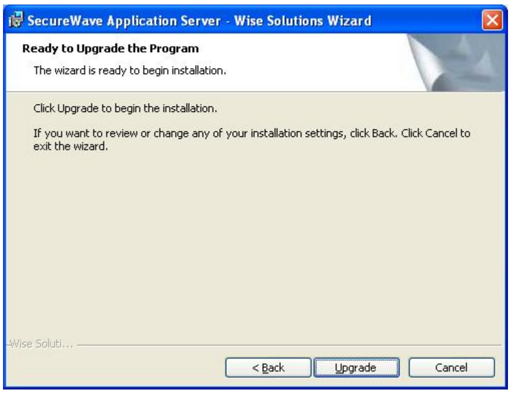
If this Server will only be used to communicate with these enhanced clients, it is recommended to disable the support of older protocols by the Server.

Specify an older communication protocol version only if older client versions will connect to this server.

Server communication protocol version: Sanctuary 4.1 or later (3)

Figure 124: SecureWave Application Server upgrade: Protocol selection dialog

7. The setup program has now all the necessary elements to begin the installation or upgrade process.



SecureWave Application Server - Wise Solutions Wizard

Ready to Upgrade the Program

The wizard is ready to begin installation.

Click Upgrade to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Figure 125: SecureWave Application Server upgrade: Protocol selection dialog

8. Click on UPGRADE to begin the process.

9. The program verifies you license and RPC protocol.

✍ *Beware that the Sanctuary Client Driver v2.8x communicate with the SecureWave Application Server through ports 33114 & 33115 while the updated SecureWave Application Server only uses port 33115. If you do not update all your old client drivers, you should modify the SxdPort registry key accordingly. See Sanctuary Client registry keys on page* 102 *for more information.*

Appendix D: Installing Sanctuary components on Windows XP SP2/2003 SP1

The information in this appendix is relevant 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, 65129, and 65229 (if using TLS protocol) that are used by Sanctuary Client Driver and SecureWave Application Server to communicate over TCP. Sanctuary Client Drivers 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 reduces the attack surface of Windows XP/2003. Sanctuary Management Console 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.

💣 *Although you can use Windows XP for the database or/and console, you should not use it for the SecureWave Application Server (or Sanctuary Client in the case of Sanctuary Application Control Server Edition).*

Connection between SecureWave Application Server and the SecureWave Sanctuary 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 SecureWave Application Server, relies on a protocol called Tabular Data Stream (TDS). By default, TDS uses port 1433 for incoming database traffic.

When the SecureWave 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 *112* for information about 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 ADD. 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 OK to close the dialog and accept the new Alias.

During the setup process, you must then 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 2000’, available at Microsoft’s Web site.

Connection between the Sanctuary Management Console and the SecureWave 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 Management Console uses the RPC protocol to connect to the SecureWave Application Server.

Please note that there have been several important changes concerning the TCP/IP communication protocol, RPC, firewall, and other points on Windows XP SP2. Please refer to Microsoft’s Web site for more information.

Stage 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 SecureWave 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 SecureWave 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]’

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

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

Stage 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, see *Configuring the firewall* on page *112* for more details.

Connecting to the Server using the fixed port

In the *Connect* dialog of the Sanctuary Management 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 Management 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 first queries 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 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 uses NTLM to authenticate to the Endpoint Mapper.

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

You may also experience some authentication problems when running the Sanctuary Management 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 Management 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

See http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx for more information about these settings.

✍ *The Sanctuary Management Console setup prompts you 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 Management 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 Management Console and the SecureWave Application Server.		

Table 25: Communication ports in Windows XP

Connection between the Sanctuary Client Driver 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 may 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 (65229 if using TLS protocol).
- The Sanctuary Client Driver listens on port TCP 33115.

See the next section, *Configuring the firewall*, for information about 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 97 and Sanctuary Client registry keys on page 102.*

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 on START, and then click on RUN.
2. In the *Run* dialog box, type Firewall.cpl, and then click on OK.
3. On the *Exceptions* tab, click on ADD PORT.
4. In the *Port number* box, type the number of the port to open (33115, 65129, and 65229 — if using TLS protocol), and then click on the TCP button.
5. In the *Name* box, type a name for the port, and then click on 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 on 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 on START, and then click on RUN.
2. In the *Run* dialog box, type 'netsh firewall set portopening TCP 33115 SecureWave_33115 ENABLE', and then click on OK. In this example, we use port 33115. You will also need to open port 65129 and 65229 (if using TLS protocol).

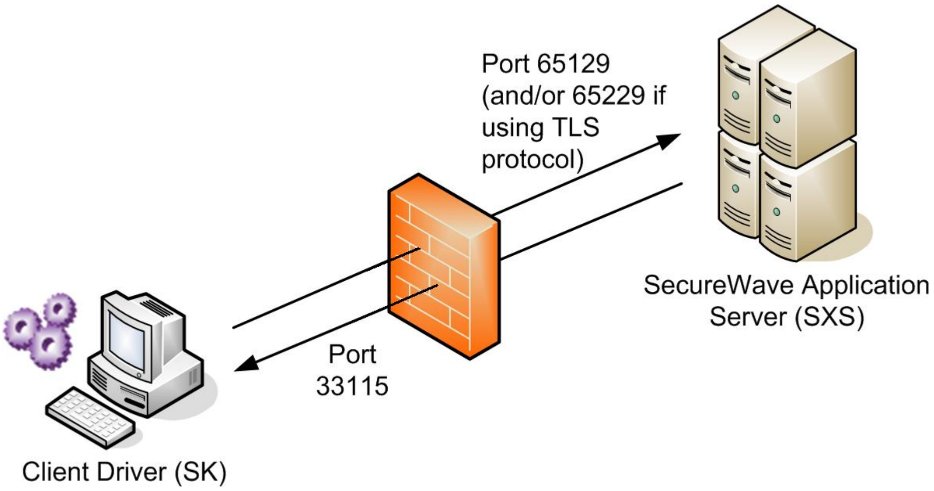


Figure 126: Communication ports between SecureWave Application Server and the client driver

Appendix E: Opening firewall ports for client deployment

The information in this appendix is relevant to all Sanctuary software suite except for Sanctuary Application Control Server Edition (as the client cannot be installed on Windows XP, Windows 2000 Pro computers).

Microsoft Windows XP SP2 and Vista 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 and Vista 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 appendix, 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.

✍ *You should activate the 'File and Print Sharing to Microsoft Networks' & 'Client for Microsoft Networks' services in all your machines. These services are used for the Sanctuary Client deployment, eDirectory synchronization, and if you are planning to install SQL Server 2005 Express Edition.*

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

1. *Start* → *Settings* → *Control Panel* → *Windows Firewall* (or click on 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 on OK to close the Windows Firewall control panel.

3. Restart the computer to enable these choices.

To open the ports on 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/Vista 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 centrally manage Windows Firewall settings.

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

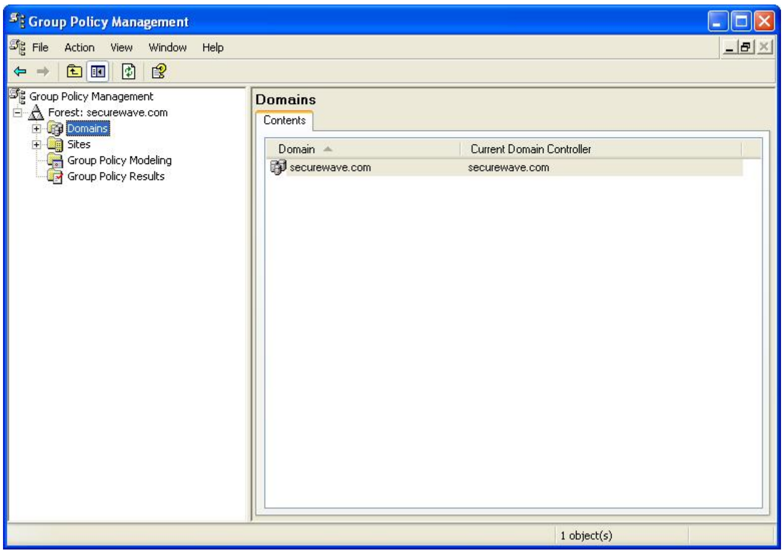
✍ *To avoid compatibility problems ensure that the machine has the latest patches and service packs.*

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*)



Group Policy Management

- Group Policy Management
  - Forest: securewave.com
    - Domains
    - Sites
    - Group Policy Modeling
    - Group Policy Results

Domains

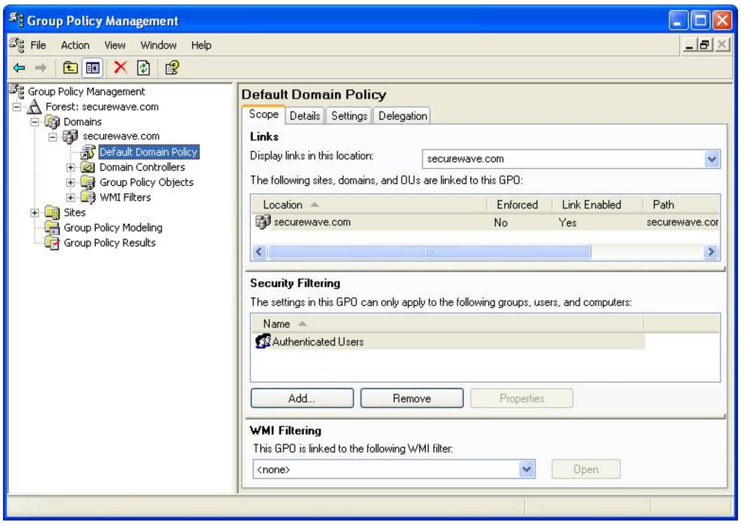
Contents

Domain	Current Domain Controller
securewave.com	securewave.com

1 object(s)

Figure 127. Open firewall ports: Select domain and forest

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



Group Policy Management

File Action View Window Help

- Group Policy Management
  - Forest: securewave.com
    - Domains
      - securewave.com
        - Default Domain Policy
        - Domain Controllers
        - Group Policy Objects
        - WMI Filters
    - Sites
    - Group Policy Modeling
    - Group Policy Results

Default Domain Policy

Scope Details Settings Delegation

Links

Display links in this location: securewave.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
securewave.com	No	Yes	securewave.cor

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

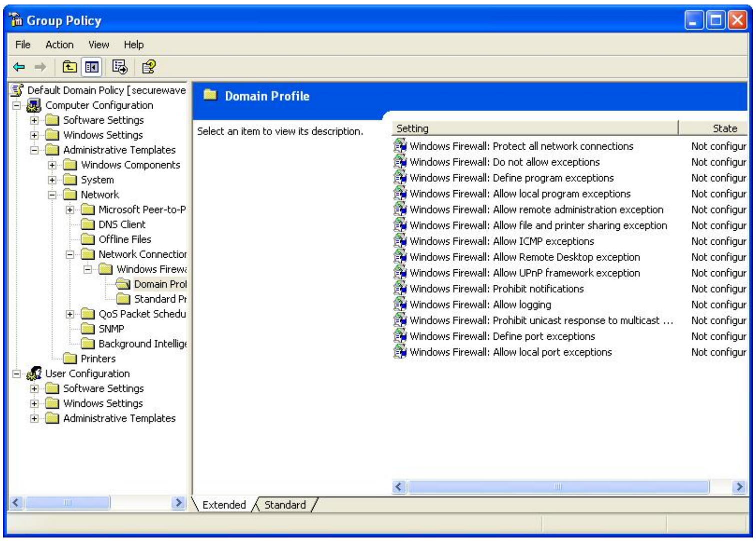
WMI Filtering

This GPO is linked to the following WMI filter:

<none>

Figure 128. Open firewall ports: Edit the Default Domain Policy

This opens a *Group Policy* window for the selected domain:



Select an item to view its description.

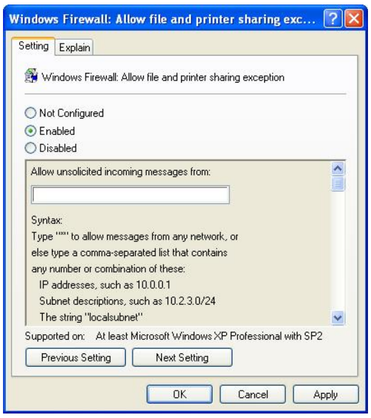
Setting	State
Windows Firewall: Protect all network connections	Not configur
Windows Firewall: Do not allow exceptions	Not configur
Windows Firewall: Define program exceptions	Not configur
Windows Firewall: Allow local program exceptions	Not configur
Windows Firewall: Allow remote administration exception	Not configur
Windows Firewall: Allow file and printer sharing exception	Not configur
Windows Firewall: Allow ICMP exceptions	Not configur
Windows Firewall: Allow Remote Desktop exception	Not configur
Windows Firewall: Allow UPnP framework exception	Not configur
Windows Firewall: Prohibit notifications	Not configur
Windows Firewall: Allow logging	Not configur
Windows Firewall: Prohibit unicast response to multicast ...	Not configur
Windows Firewall: Define port exceptions	Not configur
Windows Firewall: Allow local port exceptions	Not configur

Figure 129. Open firewall ports: Modify file and printer sharing exceptions

4. 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*.

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



Windows Firewall: Allow file and printer sharing exception

○ Not Configured
● Enabled
○ Disabled

Allow unsolicited incoming messages from:

Syntax:
Type "*" to allow messages from any network, or
else type a comma-separated list that contains
any number or combination of these:
IP addresses, such as 10.0.0.1
Subnet descriptions, such as 10.2.3.0/24
The string "localsubnet"

Supported on: At least Microsoft Windows XP Professional with SP2

Figure 130. Open firewall ports: Enable the required ports

6. Choose *Enabled* and then enter *Localsubnet* in the *Allow unsolicited incoming messages from* field.

7. To save these settings click on APPLY and then on OK.

Enabling File and Printer Sharing access opens 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 appear completely blocked for 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 F: Using the synchronization script for Novell

The information in this appendix is relevant to all Sanctuary products. When using Sanctuary Application Control Server Edition, be aware that the client cannot be installed on Windows XP or Windows 2000 Pro computers, you will be limited to an installation in a Windows Server 2003.

Introduction

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

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

> ✍ *You should activate the ‘File and Print Sharing to Microsoft Networks’ service & ‘Client for Microsoft Networks’ in all your machines. These services are used for the endpoint driver deployment, eDirectory synchronization, and if you are planning to install SQL Server 2005 Express Edition.*

What components are required?

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

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

How does the Novell interface works?

Once Sanctuary is installed and configured completely — including the SecureWave Application Server, SecureWave Sanctuary Database, and Sanctuary Client — Novell’s eDirectory trees are synchronized using an external script and appear on the Sanctuary Management Console structure so that permissions and rules can be assigned to explicit objects. This VBScript translates and synchronizes the Globally Unique Identifiers (GUIDs) of eDirectory objects into the Security Identifiers (SID) used internally by Sanctuary.

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

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

- In the manual execution, the administrator starts the VBScript by running it directly from the Windows' Run menu or command window.
- For a scheduled execution, the administrator uses the Windows Task Scheduler Service (AT or WINAT). Please see *Scheduling domain synchronizations* on page *87* for an example.

Synchronization script parameters

The script asks for four parameters, only one of which is mandatory:

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

Table 26: Novell script's parameters

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

✍ *If you are using Microsoft SQL 2005 you should specify the SQL server (optionally the user name and password), even if it is local to the machine, as (local)\SQLExpress: c:\>cscript.exe \path_to_folder\NDSSync.vbs Novell_Server_Tree (local)\SQLExpress*.

How to use Novell's synchronization script

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

1. Configure initial policies using the well-known accounts (Everyone, LocalSystem, etc).
2. Deploy Sanctuary Client. The Sanctuary Clients must be able to communicate with the SecureWave Application Server and they must adhere to the policies that apply to the well-known accounts.
3. Run the synchronization script, either manually or automatically.
4. Once the script finishes, the account selection dialogs in the console should display the user accounts, groups, and OUs.
5. Make the changes you want to the Sanctuary policies.
6. Update the clients and check whether they follow the new policies.

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

✍ *Only user, group, OU, and Organization objects are synchronized. If ZENworks is installed, Workstation objects are also synchronized.*

Script examples

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

1. cscript.exe NDSSync.vbs Novell_server_tree
   In this example, we are trying to synchronize objects from the Novell tree called 'Novell_server_tree' and place them on the local database SQL server. You will need to run it directly from the SQL server machine so you need Novell's client, synchronization script, NDAP and the database on the same physical machine. You can find these components on Novell's Web site or on your Sanctuary CD.

2. In the next example, the script is not run locally from the SQL server machine. You need to specify, besides the Novell server, the emplacement of the database server:
   cscript.exe NDSSync.vbs Novell_Server_tree DB_server

3. The next example explicitly sets the user and password to access the table in the database since they are not the same as the logged user who runs the script:
   cscript.exe NDSSync.vbs Novell_Server_tree DB_server Authorized_user User's_Password

4. If you want to save the results in a log file, you can use redirection characters:
   cscript.exe NDSSync.vbs Novell_Server_tree > log.txt

✍ *Remember that you require Novell's client, the synchronization script, and NDAP on a Windows machine.*

What can go wrong and how do I fix it?

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

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

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

I get the message 'DB connect failed'

Check you are specifying the correct SQL server address, user's name and password. Ensure the SQL server is up and running. Check there is a valid connection between your machine and the SQL server (try troubleshooting using the PING command). Check that the database table (sx) has been correctly installed.

I get the message 'DBStart failed'

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

I get the message 'DBFeedDomain failed'

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

I get the message 'DBComplete failed'

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

There is no synchronization when running NDSSync.vbs script

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

I get the message “ActiveX component can’t create object: ‘NWDirLink.NWDDirCtrl.1’”

Check NDAP is installed on the machine from where you are running the script.

Installing your synchronization script

Please follow these steps to quickly get your synchronization script installation up and running (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 store diverse information. The database is stored in a SQL server (full-blown version or MSDE 2000, depending on your company’s size). To install the database, see *Chapter 2: Installing the SecureWave Sanctuary* Database on page *17*.

2. Install the SecureWave Application Server. This provides 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 SecureWave Application Server. This can be on the same computer as the database. To install the SecureWave Application Server, see *Chapter 3: Installing the SecureWave Application* Server on page *25*.

3. Install the Sanctuary Management Console, 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 SecureWave Application Server or in a different one. To install the console, see *Chapter 4: Installing the Sanctuary Management* Console on page *37*.

4. Install a Novell client and our synchronization script on one of your Windows client machines. This machine must already have Novell’s NDAP ActiveX objects installed (available on Novell’s Web site or 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, LocalSystem, etc.) using the Console installed in step 3. See *Sanctuary's Quick Setup and Configuration Guide*.

6. Install or deploy the clients through your network to start the protection process. To install a single client, run setup.exe located in the \CLIENT folder of your installation CD: to deploy several, consult *Chapter 8: Unattended Client installation* and *Chapter 5: Installing the Sanctuary Client on* your endpoint computers.

✍ *If you are installing/uninstalling the Sanctuary Client Driver on a Vista machine with Vista’s UAC functionality turned on, you must use setup.exe (not Control Panel → Add/Remove Programs) otherwise the operation will fail.*

7. Ensure that the clients are communicating with the SecureWave Application Server and the policies defined in step 5 are enforced.

8. Run the script (c:\>cscript.exe \path_to_folder\NDSSync.vbs Novell_Server_Tree) as an Administrator on the client machine installed in step 6. 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 application. 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 Sanctuary Management Console. You can now select the user accounts, groups, workstations, and OUs when defining permissions. Create a simple permissions rule for a device/application. 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 SecureWave Sanctuary 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 SQL 2005 Server Express Edition 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.	*Chapter 2: Installing the SecureWave Sanctuary* Database.
2	Install the SecureWave Application Server.	Interface between database and clients/console.	*Chapter 3: Installing the SecureWave Application Server*.
3	Install the console.	Manage permissions, options, and rules.	*Chapter 4: Installing the Sanctuary Management Console*.
4	Install Sanctuary Synchronization script, a Novell client, and NDAP on a Windows machine.	Setup required to run Sanctuary Synchronization script.	Help file, Administrator's Guides, *Script examples*, and Novell's guides.
5	Define basic permissions.	Be sure that everything is working correctly by defining some permissions for well-know groups.	Help file, Sanctuary's Quick Setup and Configuration Guide, and the Administrator's Guides.
6	Install clients.	Begin the protection process.	*Chapter 5: Installing the Sanctuary Client on* your endpoint computers and *Chapter 8: Unattended Client installation*.
7	Run Sanctuary Synchronization script .	Convey all eDirectory information to the database.	See *Script examples* on page *121.*
8	Define new permissions for a Novell user in the console.	Test.	Help file and Administrator's Guides.
9	Proceed to define all of your company's policies.	Protect and enforce company's policies.	

Table 27: Novell quick guide installation steps

Appendix G: Using Novell shares for your DataFileDirectory

The information in this appendix is relevant to all Sanctuary products. If you are using Sanctuary Application Control Server Edition, be aware that Novell's client cannot be installed on Windows XP or Windows 2000 Pro, you will be limited to an installation on Windows Server 2003.

DataFileDirectory access to a Novell share

When installing the SecureWave Application Server, the setup asks for a data file directory where all logs files are stored. All servers can optionally write to the same, shared, directory or you can opt for having different ones for each server (see *Figure 1*). 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/They must be able to have create/read/write/erase access on the Novell share.

> It/They should have a transparent authentication access to the Novell server.

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

Transparent SecureWave Application Server 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 SecureWave Application Server.

Window's user credentials (name and password) are, by default, passed to Novell. 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 SecureWave Application Server 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 information about 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.

Using Novell v5.0 or later, follow these steps to enable this transparent authentication:

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

Now search the user account (sxs) in the root of the context TEST. This account is used to access the Novell share by SecureWave Application Server, as shown below:

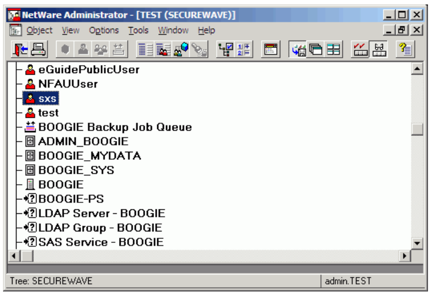
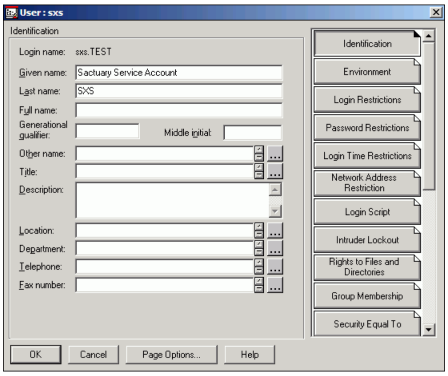


Figure 131: Searching the account that SecureWave Application Server is going to use

2. Open the properties window for user ‘sxs’. To do this, right click on the user and select *Details*.


User : sxs

Identification

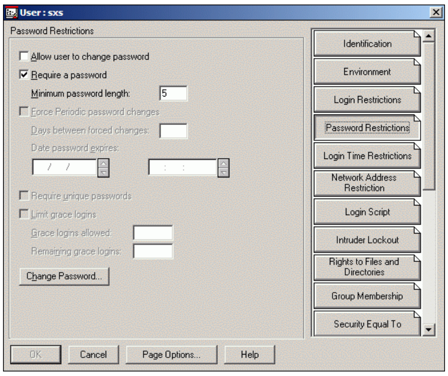
Login name: sxs.TEST

Given name: Sactuary Service Account

Last name: SXS

Figure 132: Properties of the Novell account used for the SecureWave Application Server service

3. Click on PASSWORD RESTRICTIONS (located at the right panel of this window) and activate the *Require a password* option.


User : sxs

Password Restrictions

☐ Allow user to change password

☑ Require a password

Minimum password length: 5

☐ Force Periodic password changes

Days between forced changes:

Date password expires:

☐ Require unique passwords

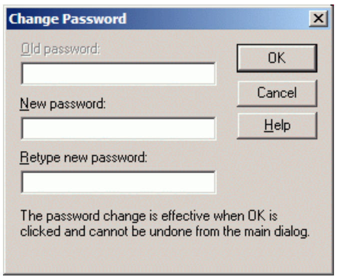
☐ Limit grace logins

Grace logins allowed:

Remaining grace logins:

Figure 133: Password restrictions windows for the Novell user

4. Click on CHANGE PASSWORD and enter the *same* password and name as for its Windows counterpart.



Change Password

Old password:

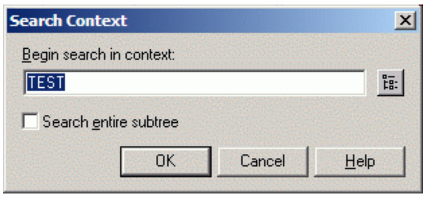
New password:

Retype new password:

The password change is effective when OK is clicked and cannot be undone from the main dialog.

Figure 134: Change the password for the Novell user

5. Click on Rights to Files and Directories (located on the right panel of the properties window), click on Find, and select the TEST context:



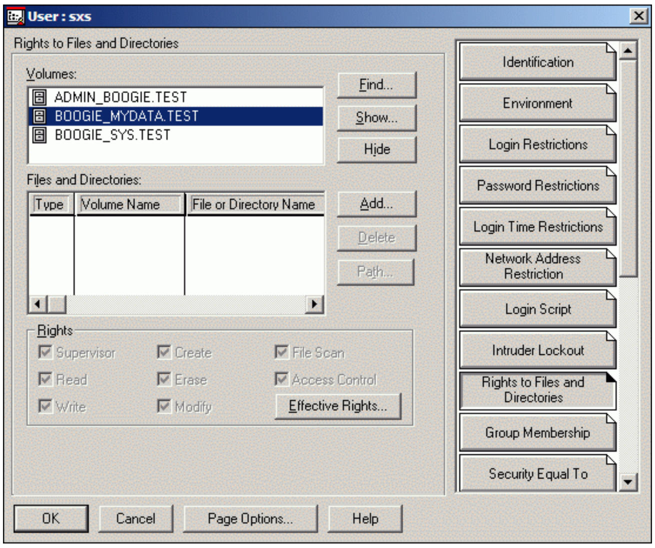
Search Context

Begin search in context: TEST

☐ Search entire subtree

Figure 135: Selecting the context for the user's rights

You should now see a window similar to the following one:



User : sxs

Rights to Files and Directories

Volumes:
ADMIN_BOOGIE.TEST
BOOGIE_MYDATA.TEST
BOOGIE_SYS.TEST

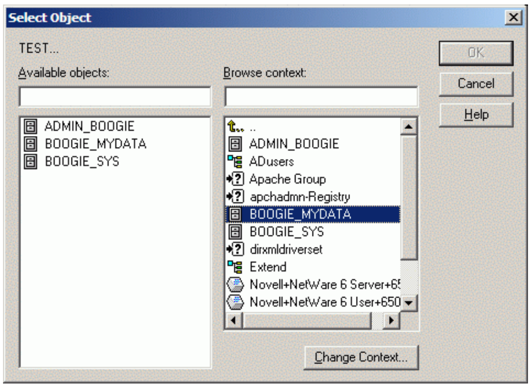
Files and Directories:

Type	Volume Name	File or Directory Name

Rights
☑ Supervisor ☑ Create ☑ File Scan
☑ Read ☑ Erase ☑ Access Control
☑ Write ☑ Modify

Figure 136: User rights for DataFileDirectory

6. 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.



Select Object

TEST...

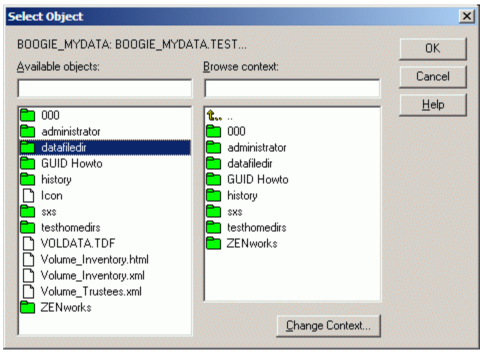
Available objects:

ADMIN_BOOGIE
BOOGIE_MYDATA
BOOGIE_SYS

Browse context:

..
ADMIN_BOOGIE
ADusers
Apache Group
apchadmn-Registry
BOOGIE_MYDATA
BOOGIE_SYS
dirxmldriverset
Extend
Novell+NetWare 6 Server+65
Novell+NetWare 6 User+650

Figure 137: Selecting the data file directory location on the Novell file server (1/2)



Select Object

BOOGIE_MYDATA: BOOGIE_MYDATA.TEST...

Available objects:

000
administrator
datafiledir
GUID Howto
history
Icon
sxs
testhomedirs
VOLDATA.TDF
Volume_Inventory.html
Volume_Inventory.xml
Volume_Trustees.xml
ZENworks

Browse context:

..
000
administrator
datafiledir
GUID Howto
history
sxs
testhomedirs
ZENworks

Figure 138: 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 SecureWave Application Server for opening shadow files and logs.
WRITE	Required by SecureWave Application Server to write to log files.
CREATE	Needed by SecureWave Application Server to save fetched shadow files and create new logs.
ERASE	Required by SecureWave Application Server when performing database maintenance.
MODIFY	Needed by SecureWave Application Server when temporary SecureWave Application Server files are converted into log files.
FILE SCAN	Required at startup of SecureWave Application Server to enumerate the present shadow files and logs.

Table 28: Novell user's rights

Appendix H: Installing a Certificate Authority for encryption and TLS Communication

This appendix explains how to install and set up a Windows Certificate Authority (CA). You need a Certificate Authority to grant certificates for your client drivers and SecureWave Application Server if you are going to use TLS protocol for encrypted message communication. You will also need a CA if you are planning to centrally encrypt removable devices.

Requirements

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

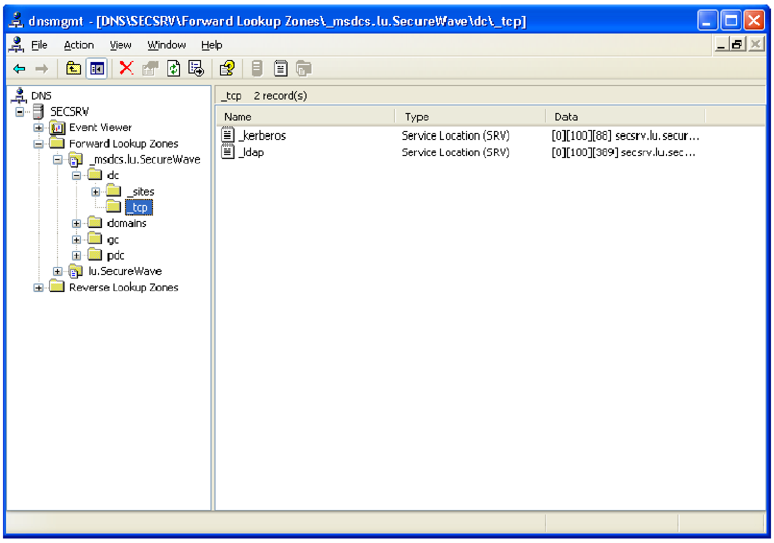
✍ *If you are planning to install a Certificate Authority on a stand-alone server that is going to be integrated to your network later, you need to be connected to at least one computer so that Windows can recognize your network interface connector (NIC).*

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

Integrating DNS with Active Directory

Although it is not a requirement to have the DNS integrated with Active Directory, it is important that the DNS server be properly configured.

To check if your Microsoft DNS is properly configured and integrated with Active Directory, open the DNS Management Console and check that the DNS zone contains the '_msdcs' records. The following screenshot shows how to check the DNS zone:



Name	Type	Data
_kerberos	Service Location (SRV)	[0][100][88] secsrv.lu.secur...
_ldap	Service Location (SRV)	[0][100][389] secsrv.lu.sec...

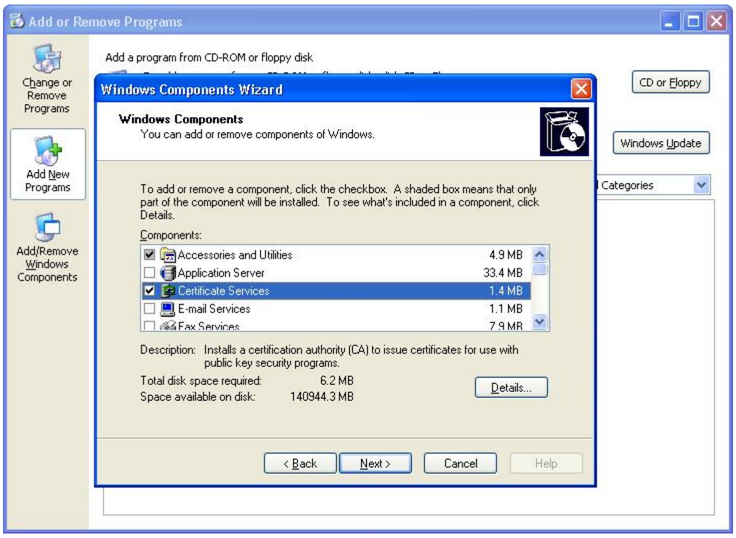
Figure 139: Verifying the DNS zone

Please refer to the Microsoft's Web site to get more information about how to check the configuration of your DNS servers.

Installing the Certificate Services

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

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


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Add a program from CD-ROM or floppy disk
CD or Floppy
Windows Update
Categories
Windows Components Wizard
< Back
Next >
Cancel
Help
Details...

Windows Components
You can add or remove components of Windows.

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

Components:

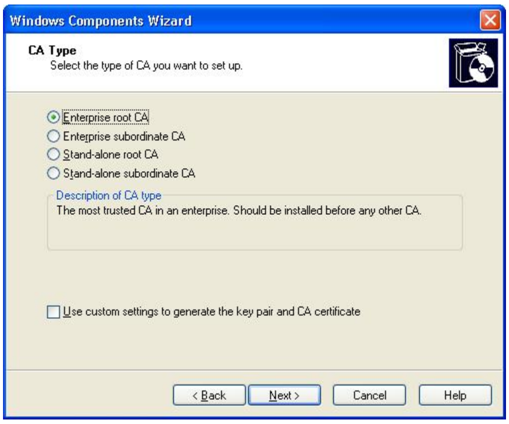
☑ Accessories and Utilities	4.9 MB
□ Application Server	33.4 MB
☑ Certificate Services	1.4 MB
□ E-mail Services	1.1 MB
□ Fax Services	7.9 MB

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

Total disk space required: 6.2 MB
Space available on disk: 140944.3 MB

Figure 140: Adding certificate services

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



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

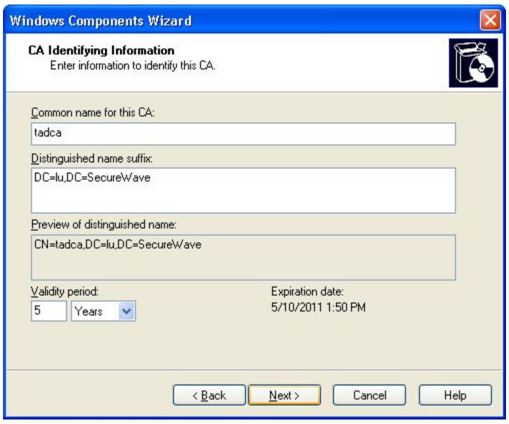
● Enterprise root CA
○ Enterprise subordinate CA
○ Stand-alone root CA
○ Stand-alone subordinate CA

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

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

Figure 141: The Windows components wizard (1st page)

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



Windows Components Wizard

CA Identifying Information

Enter information to identify this CA.

Common name for this CA: tadca

Distinguished name suffix: DC=lu,DC=SecureWave

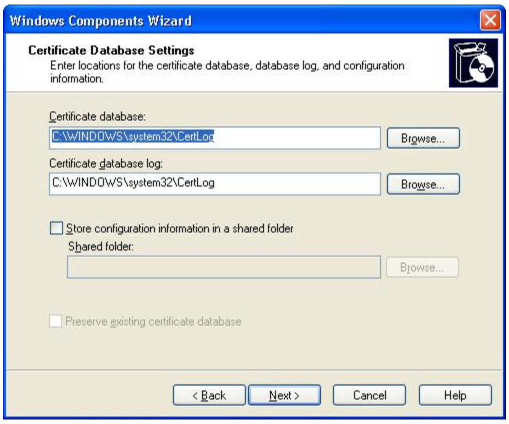
Preview of distinguished name: CN=tadca,DC=lu,DC=SecureWave

Validity period: 5 Years

Expiration date: 5/10/2011 1:50 PM

Figure 142: The Windows components wizard (2nd page)

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



Windows Components Wizard

Certificate Database Settings

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

Certificate database: C:\WINDOWS\system32\CertLog

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

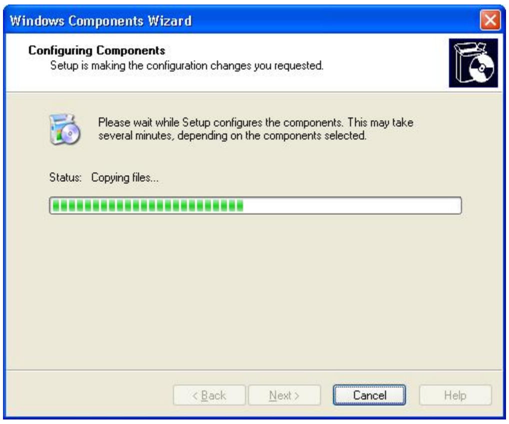
□ Store configuration information in a shared folder

Shared folder:

□ Preserve existing certificate database

Figure 143: The Windows components wizard (3rd page)

Windows proceeds with the certificate services installation.



Windows Components Wizard

Configuring Components

Setup is making the configuration changes you requested.

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

Status: Copying files...

Figure 144: The Windows components wizard (final page)

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

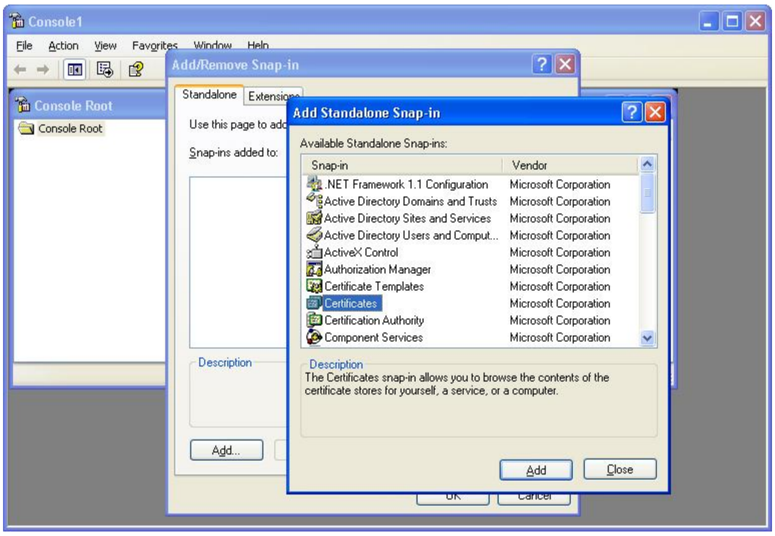
✍ *Depending on your Active Directory configuration and replication between domain controllers setting, it may take some time to issue a certificate during the first user logon and publish it to the Active Directory. During that period, the user is not authorized to access the media.*

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

Checking certificates are correctly issued to the users

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

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

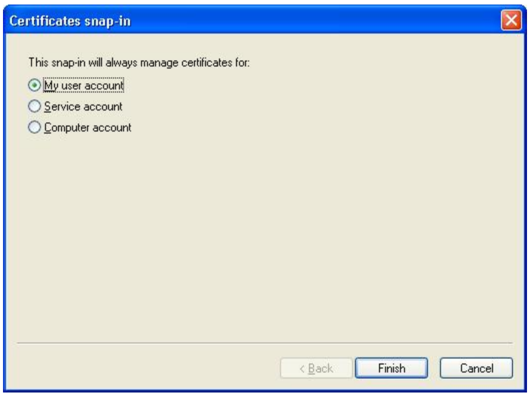


Snap-in	Vendor
.NET Framework 1.1 Configuration	Microsoft Corporation
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Comput...	Microsoft Corporation
ActiveX Control	Microsoft Corporation
Authorization Manager	Microsoft Corporation
Certificate Templates	Microsoft Corporation
Certificates	Microsoft Corporation
Certification Authority	Microsoft Corporation
Component Services	Microsoft Corporation

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

Figure 145: The certificate snap-in

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

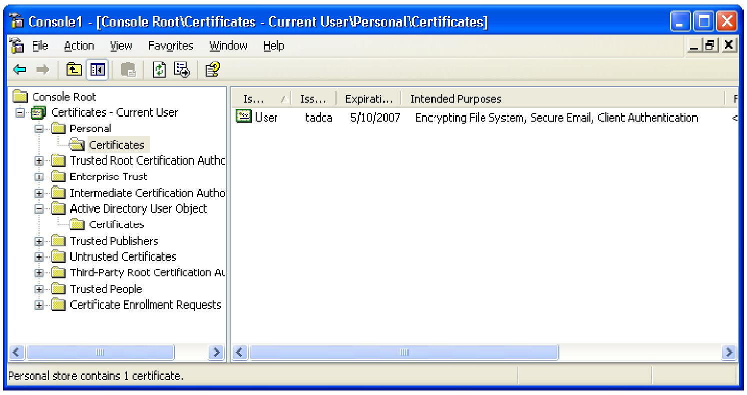


This snap-in will always manage certificates for:

● My user account
○ Service account
○ Computer account

Figure 146: The certificate snap-in: User account

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

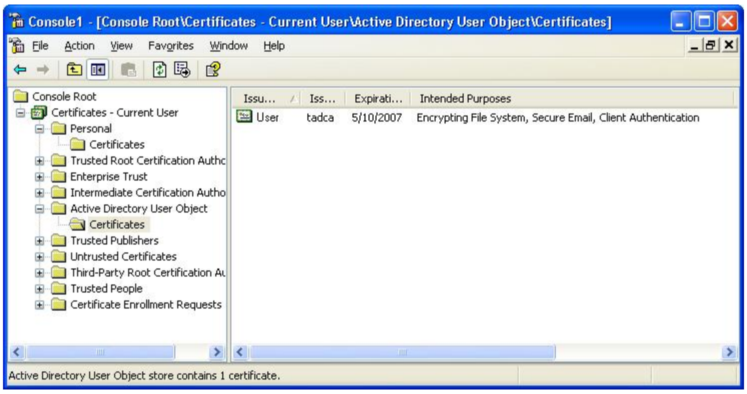

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authc
Enterprise Trust
Intermediate Certification Autho
Active Directory User Object
Certificates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

Is...	Iss...	Expirati...	Intended Purposes
User	tadca	5/10/2007	Encrypting File System, Secure Email, Client Authentication

Personal store contains 1 certificate.

Figure 147: The console: Certificate intended purposes

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


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

Issu...	Iss...	Expirati...	Intended Purposes
User	tadca	5/10/2007	Encrypting File System, Secure Email, Client Authentication

Active Directory User Object store contains 1 certificate.

Figure 148: Verifying the user's certificate

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

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

> *The user inserts and accesses an encrypted media.*

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

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

Checking certificates are correctly issued to endpoint machines

If you choose to use TLS for Sanctuary Client Driver-SecureWave Application Server or intra-SecureWave Application Server communications, there should exist issued certificates for each machine that uses this mode. You can verify if they were correctly emitted by using the procedure described in the *Checking certificates are correctly issued to the users* section on page *132*. Note that you should select *Computer Account* instead of *My user account* in step 7.

Appendix I: Importing file definitions during setup

The information in this appendix applies only to Sanctuary Application Control Suite.

During the installation of SecureWave Application Server, you are offered the opportunity of importing Standard File Definitions (SFD). These definitions are sets of all the hashes of various operating systems files supported by Sanctuary. We recommend installing 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 of File Groups 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 is automatically be suggested in the *Assign Files to File Group* dialog.

> If you use Standard 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 Standard 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 29: Created file groups and assigned users and groups

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

✍ *Importing Standard File Definitions (SFD) can be a time-consuming task. To save yourself time, only import the 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: Controlling administrative rights for Sanctuary’s administrators

When installing your SecureWave solution, several Visual Basic Script file tools are provided. These include Ctrlacx.vbs, which narrows the administrative rights to control organizational units/users/computers/groups for special users designated as Sanctuary’s administrators.

Ctrlacx.vbs

Ctrlacx.vbs is a Visual Basic Script file that can be used to set, view, or modify the *Manage Sanctuary Settings* control rights in the Active Directory. It allows Active Directory administrators to delegate Sanctuary management for computers, users, groups, and organizational units without entrusting any other tasks (which is required by default) to them. This script may also be use to show the other control/rights defined in the Active Directory forest.

You can find Ctrlacx.vbs in the installation folder, usually under the SCRIPTS directory. You can also locate it on your installation CD.

When Ctrlacx.vbs runs, it creates a special entry in the permissions list of the organization unit called *Manage Sanctuary Settings*. This entry only affects Sanctuary Device Control software administrator users and the devices they control. If you assign this setting to a specific user, who is also a Sanctuary Administrator (as defined on the *User Access Manager* dialog of the console), he would only be able to manage the designated users/groups/computers for which he has rights directly from the Sanctuary Management Console.

You must synchronize with the domain after running Ctlacx.vbs before these rights are activated. To do this, use the *Synchronize Domain Members* item of the *Tools* menu (or from the *Control Panel*).

✍ *You can only use this tool to create authorizations per forest, not per domain and only those users assigned as Enterprise Administrators are allowed to create, set or view control rights.*

Requirements

You must have the *Windows Script Host* (WSH, which includes wscript.exe and cscript.exe) interpreter installed on your system before you can run any VBScript. Some antivirus programs reject the execution of these types of scripts.

Usage

To use ctrlacx.vbs:

1. Open a command screen (*Start → Run → Command*) to run the script or execute it directly from the *Run* dialog using the following syntax:

```
cscript Ctrlacx.vbs [-parameter list]>file.txt
```

where the parameters are explained in the following table.

The previous syntax sends the output directly to a text file specified, in this case, by *file.txt*. If you want to use it interactively, utilize the following syntax:

```
ctrlacx.vbs [-parameter list]
```

- or -

```
wscript Ctrlacx.vbs [-parameter list]
```

Parameter	***Description***
-?	Displays a brief description of each possible parameter. You must run this script in interactive mode or from the command line in order to see the text.
-e	Enumerate all control access rights. Condensed output.
-v	Enumerate all control access rights. Detailed output (verbose).
-q cn	Displays a control right by its canonical name (cn).
-s	Display SecureWave's Manage Sanctuary Settings rights.
-create	Creates or updates SecureWave's Manage Sanctuary Settings rights.
-delete	Deletes SecureWave's Manage Sanctuary Settings rights.

Table 30: Ctrlacx script options

Examples

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

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

To show the *Manage Sanctuary Settings* rights interactively.

```
ctrlacx.vbs -s
```

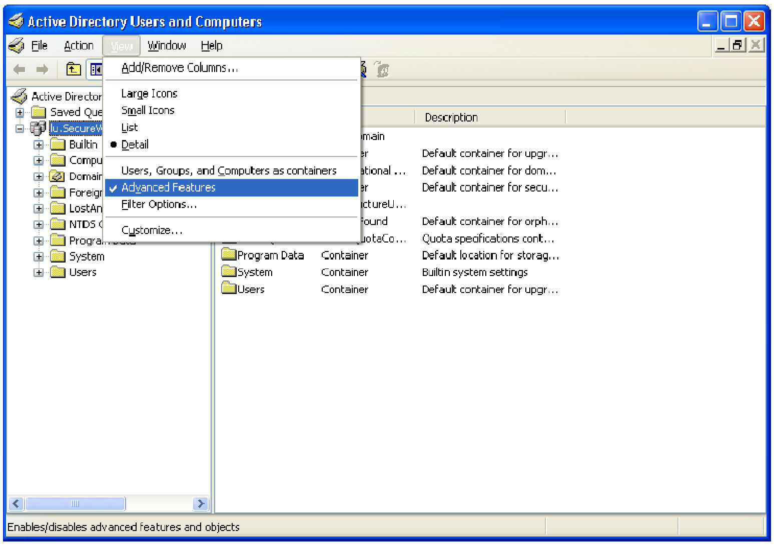
What to do after running the script

Once you run the script on a domain machine, you have to assign the delegation rights you just created for Sanctuary. To do this, follow these steps:

1. Run the script with the *-create* parameter to generate or update SecureWave's rights on the active directory.

2. Open the Microsoft Management Console (MMC) window.

3. Activate the *Advanced Features* option from the *View* menu:



		Description
	main	
	er	Default container for upgr...
	ational ...	Default container for dom...
	er	Default container for secu...
	ctureU...	
	Found	Default container for orph...
	uotaCo...	Quota specifications cont...
Program Data	Container	Default location for storag...
System	Container	Builtin system settings
Users	Container	Default container for upgr...

Enables/disables advanced features and objects

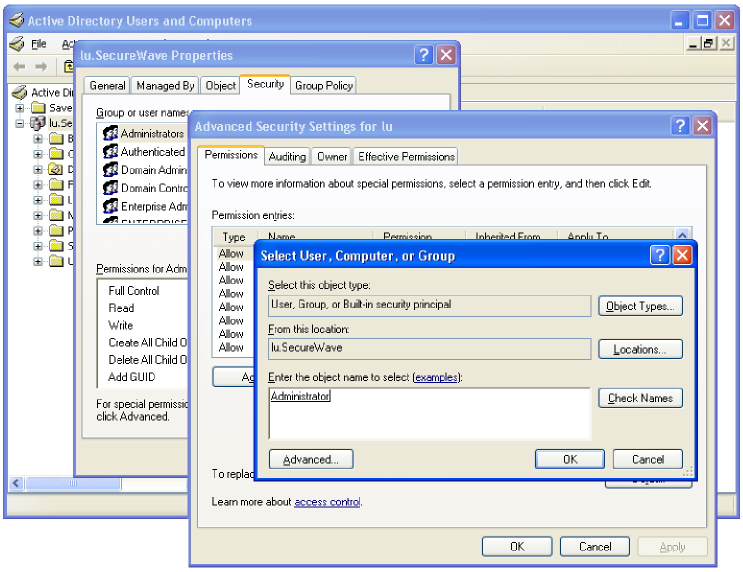
Figure 149: Advanced feature option of the MMC

4. Right click on the desired Organizational Unit (OU) and select *Properties* from the pop-up menu.

5. Go to the *Security* tab and click on ADVANCED to open the *Advanced Security Settings* dialog.

6. Go to the *Permissions* tab and click on ADD or EDIT.

7. Select the user or group to which you want to delegate rights, as shown in the following image.



Select User, Computer, or Group

Select this object type:
User, Group, or Built-in security principal [Object Types...]

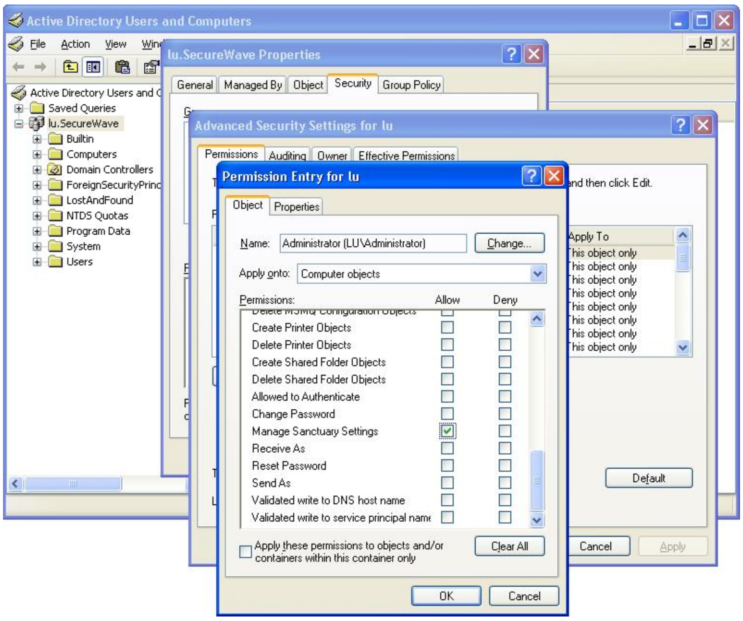
From this location:
lu.SecureWave [Locations...]

Enter the object name to select (examples):
Administrator [Check Names]

[Advanced...] [OK] [Cancel]

Figure 150: Select user, computer, or group to which delegate.

8. Click on Object Types, select *Computers* and click on OK to close the dialog
9. Click on the OK button to open the *Permissions entry* dialog:



Permission Entry for lu

Object | Properties

Name: Administrator (LU\Administrator) [Change...]

Apply onto: Computer objects

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

□ Apply these permissions to objects and/or containers within this container only [Clear All]

[OK] [Cancel]

Figure 151: Manage Sanctuary Settings object

Three important objects exist in the *Apply onto* field of this dialog that are relevant to the Sanctuary settings: *Computer objects*, *Group objects*, and *User objects*. Figure 3 shows only one of them: *Computer objects*.

The script narrows the Active Directory rights by creating a special entry in each of the above-mentioned objects: *Manage Sanctuary Settings*. If you assign this permission to a user, he/she can only manage the designated users/groups/computers in the Sanctuary Management Console.
Note the special check box option in the permissions entry: *Apply these permissions to objects and/or containers within this container only*. If activated, you will see only the real objects — users or computers from this OU — in the console and nothing from the child OUs beneath.

The 'new' delegated administrator can now manage the objects (users/computers/groups) explicitly assigned to him.

Appendix K: Installation checklist

Requirements

Before starting to install any Sanctuary products make sure to have the following:

If you are using Windows…

- Active Directory installed and configured within a domain.
- Configure DNS as AD integrated and create a reverse lookup zone.

– or –

- A workgroup network properly configured.

If you are using Novell…

- NDAP installed on the machine you are going to use to synchronize your eDirectory structure. We recommend installing it on the same machine as the database server.
- ZENworks client optionally installed on the client computer.

The SecureWave Sanctuary Database

The database is used to hold permissions, logs, available in-line machines, users, devices, etc. There is only one database per organization but you can use SQL clustering for disaster recovery purposes.

Software

The Database component requires a Microsoft SQL Server database. This can either be Microsoft SQL Server 2000/2005 or Microsoft SQL Server 2005 Express Edition. If you do not have an SQL server, you can install Microsoft SQL Server 2005 Express Edition directly from the Sanctuary's CD.

Hardware

The hardware specifications of the database server should be the following, as a minimum (depending on your enterprise size and number of clients):

- Memory: 256 MB.
- CPU: Pentium 3 or 4 processor or equivalent AMD processor.
- HD: 3 GB SCSI or IDE.
- NIC 100 MBits/s.

Network configuration

- Configure your DNS server.
- DHCP server started.

Additional settings

- Change the Event Viewer settings to 1024 KB in size and choose to overwrite events as needed.
- Change the Performance settings to prioritize for background applications.

Firewall configuration

If you are using Windows XP SP2 or Windows 2003 server SP1 for the database, the firewall may be active and blocking certain ports needed to communicate with the SecureWave Application Server.

The SecureWave Application Server

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

Software

- Windows 2000/2003 Server with latest service packs.
- Install Microsoft Enterprise Certificate Authority (root) for central encryption.
- Adobe PDF Viewer to read the documents.

Hardware

The hardware specifications of the SecureWave Application Server should be the following, as a minimum (depending on your enterprise size and number of clients):

- Memory: 256 MB.
- CPU: Pentium 3 or 4 processor or equivalent AMD processor.
- HD: 3 GB SCSI or IDE (bigger if you plan to use shadow when installing Sanctuary Device Control and if the Data File Directory (see *Data file directory* on page *143*) is defined on this machine.
- NIC 100 MBits/s.

The Sanctuary Management Console

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

✍ *You must install the client driver in the Sanctuary Management Console machine if you are planning to encrypt and/or authorize removable media.*

Firewall configuration

If you are using Windows XP SP2 or Windows 2003 server SP1 or later for the console the firewall may be active and blocking certain ports needed to communicate with the SecureWave Application Server.

Sanctuary Client

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 or — in large organizations, or when you cannot visit each client computer (server) individually — using our unattended client installation software. You can also use any other software that supports MSI packages to install Sanctuary Clients.

Software

The client requires a Windows XP SP1/SP2,Windows 2000 SP3, or Windows Vista machine. We recommend defining Windows updates from Windows Server Update Services (WSUS) if you are installing Sanctuary Application Control Suite.

Hardware

The hardware specifications of the client should at least meet the following ones:

- Memory: 256 MB.
- CPU: Pentium 3 or 4 processor or equivalent AMD processor.
- HD (SCSI or IDE): 10 Mb to install the client and up to 3 GB of free space if you are planning to activate or not the ‘full shadow’ feature when installing Sanctuary Device Control.
- NIC 100 MBits/s.

Network configuration

- Select the corresponding DNS server.
- Configure the NIC for receiving IP by the DHCP service.

Additional settings

- If you are using Sanctuary Client in a Novell eDirectory: Install the Novell, and optionally the ZENworks, client.
- Change the Event viewer settings to 1024 KB in size and choose to overwrite events as needed.

Firewall configuration

Unblock firewall ports as needed to communicate with the SecureWave Application Server. This is particularly important if you are using Windows XP SP2 or Windows Vista.

License

Each SecureWave Application Server has a license file that specifies whether you have a valid copy of one or several of our Sanctuary programs, for example, Sanctuary Application Control Server Edition, Sanctuary Device Control, and so on.

There are two types of license available:

- Evaluation license.
- Full license.

When you receive the license file, copy it to the %SYSTEMROOT%\SYSTEM32 folder of each computer that runs the SecureWave Application Server. It is *not* required on client machines.

Private and public keys

Sanctuary provides a utility that you can use to create a key pair that is used to assure communication integrity between the SecureWave Application Server and the client driver.

In a production environment, you must create your own key pair **BEFORE** deploying the Sanctuary Client Driver on the first client computer and after installing your SecureWave Application Server.

Data file directory

When installing the SecureWave Application Server, the setup asks for at least one data file directory where all shadow and log information is stored. We call it DataFileDirectory or DFD.

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 (several ones can be defined). On the other hand, for evaluation purposes a local directory is better.

It is possible to define such directory if you are using a Novell server in the same way as it is done for a Windows server. If your DFD is defined on a Novell server, you should use an account with the same name and password to access this shared directory.

You should take into consideration the hard disk drive size when defining log options.

SXS account

The SecureWave Application Server service 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 administer computers in a workgroup.

Certificate Authority

You must have a Certificate Authority installed and configured if you plan to use the TLS protocol when installing the client drivers and/or central encryption if installing Sanctuary Device Control. Microsoft’s

Certificate Authority installation is described in *Appendix H: Installing a Certificate Authority for encryption and TLS Communication* on page *129*.

Implementation actions

To help you to implement Sanctuary, the following table explains the actions required:

#	*Action*	*Description*
1	Create devices, media, and software inventory. We provide a special software tool for you device inventory, Sanctuary Device Scanner Tool, in our Web site.	The inventory lists all devices and media that you want to control (depending on which Sanctuary products you bought).
2	Write a company policy that defines the permissions, shadowing options, encrypted devices, Sanctuary administrators/roles, and Add Domain Global Groups for Sanctuary permissions and Sanctuary administrators (optional).	The document of the company's policies lists all the settings that are used to control Sanctuary's installation. It includes permissions and to whom they will be assigned, users that will become Sanctuary Administrators, etc.
3	Plan the architecture of the installation, based on the sizing considerations.	The resulting document can be a network diagram that reflects the architecture together with server's hostnames and IP addresses.
4	Create a SecureWave Application Server service account in your Domain.	The SecureWave Application Server is a standard Windows service that runs under a regular account. It is a good practice to create a new dedicated, domain account, for this purpose and set its options to 'User cannot change password' and 'Password never expires'. This account MUST have local administration rights if you plan to use TLS for client-SecureWave Application Server or intra-SecureWave Application Server communications.
5	(Sanctuary Device Control only!) Install a Microsoft Enterprise Certificate Authority for Encryption or TLS protocol for client – SecureWave Application Server or intra-SecureWave Application Server communications.	In case you want to encrypt removable devices such as pen drives, memory sticks, and so on, we recommend you install a Microsoft Enterprise Certificate Authority. You also need this component if you plan to use TLS protocol for Sanctuary Client Driver–SecureWave Application Server or intra–SecureWave Application Server communications (all messages are encrypted). If you do not use TLS protocol, all messages are signed using the private key.
6	Install DBMS: MSSQL 2000/2005 or MSSQL 2005 Express Edition.	The Database Management System used by Sanctuary is either a Microsoft SQL Server 2000/2005 or Microsoft SQL 2005 Express Edition — depending on the number of clients to be controlled.
7	Install SecureWave Sanctuary Database and grant owner rights to the SecureWave Application Server service account.	The SecureWave Sanctuary Database is installed and you grant owner rights to the SecureWave Application Server Service account, before starting the installation of the first SecureWave Application Server.
8	Create a Share (DataFileDirectory) for the SecureWave Application Server on a fileserver (required in configurations with multiple SecureWave Application Servers).	If the sizing analysis has determined that more than one SecureWave Application Server should be used, you must create a network share (DataFileDirectory - a common repository to all SecureWave Application Servers) before installing the first SecureWave Application Server. If you are going to use only one SecureWave Application Server, this can be local to the machine where the SecureWave Application Server is going to be installed.
9	Install the first SecureWave Application Server.	Install the first SecureWave Application Server, taking into account the following: • Use the SecureWave Application Server service account. • Connect to the DBMS that hosts the SecureWave Sanctuary Database. • Use the defined Network Share for the DataFileDirectory.
10	Generate a new key-pair to secure the communication between the SecureWave Application Server and the clients.	Once the first SecureWave Application Server is installed, create your own key-pair and implement this key-pair on the first SecureWave Application Server (copy both keys to the '%SystemRoot%\SxsData' folder and restart the SecureWave Application Server service).
11	Install additional SecureWave Application Server and licenses.	If more SecureWave Application Servers are needed, you can proceed to install them following the same steps as for the first SecureWave Application Server. You need a license for each installation. After each installation, copy your own key-pair, so that all SecureWave Application Server are using the same ones.
12	Install the Sanctuary Management Console.	Install the console on the selected machines. Also, install the client on the same machine(s) if you are using Sanctuary Device Control and you are planning to centrally encrypt devices and authorize media.
13	Schedule Domain (and Novell's objects) synchronization.	Schedule a task with the command-line tool 'sxdomain.exe' that will synchronize all relevant objects from your domain into SecureWave Sanctuary Database. Create another task if you are working on a Novell environment (NDSSync.vbs).

14	Add devices, media from your inventory into the SecureWave Sanctuary Database (if needed/ wanted) in order to assign permissions.	If you have planned to assign permissions for specific models or uniquely identified media (CD/DVD or Removable devices), add them to the database.
15	Assign permissions and options based on the company policy and Devices/Applications inventory and define the Sanctuary Administrators.	Assign the permissions for the devices, media, and software to the domain groups. Also, define the Sanctuary Administrators.
16	Install a Sanctuary Client on a test workstation.	Install the client software on a test workstation and connect it to the server components.
17	Validate the test client installation and permissions.	Test your installation on functionality, validate the permissions defined in the previous step. If necessary, adapt the permissions and update the Company Policy.
18	Prepare and test the Sanctuary Client Deployment package.	Prepare the deploy package of the Sanctuary Client software based on the instructions of this Setup Guide and your existing, internal procedures. Check the public key file, policies exportation data, and MST Installer Transform file.
19	Deploy the client software.	Deploy Sanctuary Client Driver to all client computers. Read the notes regarding policy exportation.

Table 31: Implementation actions

Installation checklist

#	***Description***	***Done/ Resolved***	***Comments***	***Reference***
1	Verify the minimum requirements for each component.	□		See *Appendix A: Detailed system requirements and limitations* on page *93.*
2	Are you using a firewall or are you installing the Console on Windows XP SP2 with the firewall activated?	□	Open needed ports.	See *Appendix E: Opening firewall ports for client deployment* on page *115.*
3	Do all basic protection steps for all your computers?	□	Seal/chassis intrusion protector, Password protected BIOS, NTFS Partition, etc.	See the printed *Sanctuary's Quick Setup and Configuration Guide*.
4	Decide between using a full-blown SQL Server or the 'light' version.	□		See *Choosing a SQL engine* on page *17.*
5	Are you installing the SecureWave Sanctuary Database, SecureWave Application Server, and Sanctuary Management Console in the same physical machine?	□	Only recommended when testing the product.	
6	Install the SecureWave Sanctuary Database.	□	Install the SQL Server 2005 Express Edition or use your SQL Server.	See *Stage 1: To install the SQL database* engine on page *18*.
		□	Create the 'sx' database.	See *Stage 2: To install the SecureWave Sanctuary* Database on page *19*.
7	Install SecureWave Application Server. (Are you going to have a single SecureWave Application Server?)	□	Install MDAC.	Microsoft's Web site.
		□	If doing central encryption or using TLS for your clients, install a Certification Authority.	See Sanctuary Device Control Administrator's Guide.
		□	Define a fixed IP for his machine.	Configure DHCP / DNS correctly. Windows' manuals or help file, see *Before you install* on page *25*.
		□	If installing on a different machine from that of the database, check that the SecureWave Application Server has the proper rights to use the database.	See *Before you install* on page *25.*
		□	Check license file.	See *Before you install* on page *25.*
		□	Generate key pair to encrypt communication between server(s) and clients (only once).	See *Chapter 7: Using the Key Pair Generator* on page *59.*
8	Are you going to have a single Sanctuary Management Console?	□	Install the Sanctuary Management Console	See *Chapter 4: Installing the Sanctuary Management Console* on page *37*.
		□	Synchronize domain members to fill-up the database.	See *Chapter 9: Using the SXDomain Command line* tool on page *85*.
9	Are you planning to centrally encrypt media? (if using Sanctuary Device Control)	□	Install client on Console machine.	See *Chapter 5: Installing the Sanctuary Client on* your endpoint computers on page *41*.

#	Description	Done/ Resolved	Comments	Reference
		□	Install Microsoft Enterprise Certificate Authority (optionally) on a Domain Controller.	See Sanctuary Device Control Administrator's Guide. Microsoft's Web site.
10	Are you using TLS for your clients or intra-SecureWave Application Server communications?	□	Install Microsoft Enterprise Certificate Authority on a Domain Controller.	See Sanctuary Device Control Administrator's Guide. Microsoft's Web site.
11	Install a single client machine for testing purposes.	□	Better to do this on a test machine that you can fully control.	See Sanctuary's Quick Setup and Configuration Guide (printed manual).
12	Test your installation.	□	Test device/application denial when accessing a device (e.g. CD drive).	Consult the Sanctuary's Quick Setup and Configuration Guide (printed manual).
		□	Define simple permissions for a device/application (e.g. CD drive or Calculator).	
		□	Re-test for the permission defined in previous step.	
		□	Check different permissions and options to understand how the program works.	
13	Deploy clients.	□	Create MSI installation packages using public key generated on step 7.	See *To install* packages on page *66*.
		□	Do you already have permission definitions from a subsidiary/previous Sanctuary installation? Optionally create policies.dat	Consult the Administrators' Guides.
		□	Assign computers to the installation package(s).	See *Chapter 8: Unattended Client installation* on page *63*.
		Deploy	□ Automatically.	See *Chapter 8: Unattended Client installation* on page *63*.
			□ Command line.	See *Using the command line* to install clients on page *77.*
			□ Windows' group policy.	See *Using Windows Group Policy* to install clients on page *77*.
14	Schedule the domain synchronization process.	□		See *Scheduling domain synchronizations* on page *87*.
15	Are you using Novell machines?	□	Synchronize eDirectory objects	See *Appendix F: Using the synchronization script for Novell* on page *119*.
16	Define permissions, rules, and options according to corporate policies.	□		Consult the Administrators' Guides. See also next table.

Table 32: Installation checklist

Defining permissions in Sanctuary Device Control

Permission type	***Description***	Biometric devices	COM/Serial ports	DVD/CD drives	Floppy disk drives	Imaging devices	LPT/Parallel ports	Modems/Secondary network access devices	Palm handheld devices	Printers (USB)	PS/2 Ports	Removable storage devices	RIM BlackBerry handhelds	Smart Card readers	Tape drives	User-defined devices	Windows CE handheld devices	Wireless NICs (network interface controllers)
Root level	Event notification																	
	Permissions (R, R/W, or None)																	
Device Class level	Permissions (R, R/W, or None)	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Online permissions	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Offline permissions	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Scheduled permissions		□	□	□	□	□	□	□	□		□	□		□	□	□	
	Temporary permissions																	
	Shadow		□	□	□		□	□				□						
	Copy Limit				□							□						
	Event notification	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Decentralized encryption											□						
	File type filtering			□	□							□						
Device Group level	Permissions (R, R/W, or None)	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Online permissions	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Offline permissions	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Scheduled permissions		□	□	□	□	□	□	□	□		□	□		□	□	□	
	Temporary permissions																	
	Shadow		□	□	□		□	□				□						
	Copy Limit				□							□						
	Event notification	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Decentralized encryption											□						
	File type filtering			□	□							□						
Device level	Permissions (R, R/W, or None)	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Online permissions	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Offline permissions	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Scheduled permissions		□	□	□	□	□	□	□	□		□	□		□	□	□	
	Temporary permissions																	
	Shadow		□	□	□		□	□				□						
	Copy Limit				□							□						
	Event notification	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Decentralized encryption											□						
	File type filtering			□	□							□						
Computer level	Permissions (R, R/W, or None)	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Online permissions	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Offline permissions	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Scheduled permissions		□	□	□	□	□	□	□	□		□	□		□	□	□	
	Temporary permissions		□	□	□	□	□	□	□	□		□	□		□	□	□	
	Shadow		□	□	□		□	□				□						
	Copy Limit				□							□						
	Event notification	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Decentralized encryption											□						
	File type filtering			□	□							□						
Computer Group level	Permissions (R, R/W, or None)	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Online permissions	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Offline permissions	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Scheduled permissions		□	□	□	□	□	□	□	□		□	□		□	□	□	
	Temporary permissions		□	□	□	□	□	□	□	□		□						
	Shadow		□	□	□		□	□				□						
	Copy Limit				□							□						
	Event notification	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Decentralized encryption											□						
	File type filtering			□	□							□						

User Group Settings	Permissions (R, R/W, or None)	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Online permissions	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Offline permissions	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Scheduled permissions		□	□	□	□	□	□	□	□		□	□		□	□	□	
	Temporary permissions		□	□	□	□	□	□	□	□		□	□		□	□	□	
	Shadow		□	□	□		□	□				□						
	Copy Limit				□							□						
	Event notification	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
User Specific Settings	Permissions (R, R/W, or None)	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Online permissions	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Offline permissions	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	Scheduled permissions		□	□	□	□	□	□	□	□		□	□		□	□	□	
	Temporary permissions		□	□	□	□	□	□	□	□		□	□		□	□	□	
	Shadow		□	□	□		□	□				□						
	Copy Limit				□							□						
	Event notification	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Table 33: Defining permissions

Glossary

ACE

***A**ccess **C**ontrol **E**ntries*. An entry in the Access Control List (ACL) that contains a set of access rights and a security identifier (SID) identifying a trustee.

ACL

***A**ccess **C**ontrol **L**ist*. A list of security protections that apply to an object (file, process, event, or anything else having a security descriptor).

ADC

Advanced **D**ata **C**onnector. 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 in Microsoft software distribution packages.

Certificate Authority (CA)

Authority charged of issuing user or computer certificates (among other tasks).

Certificate store

The storage location where Windows locally saves certificates requested by a computer or device. This store can have several certificates possibly issued by various CAs. If you have the user rights to do so, you can import or export certificates from any folder or file to the certificate store.

Certificate revocation list (CRL)

A list containing the compromised, revoked, or superseded certificates. The CRL is used during the digital signature verification process to certificate’s validity using the public key extracted from the same certificate.

Client Computer

The computers on your network that Sanctuary Application Control Suite and 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

***D**omain **N**ame **S**ystem* (also *Service* or *Server*). A service that translates computer names 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

***F**ile **A**llocation **T**able*. This 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 using several Sanctuary Management Console modules (*Database Explorer*, *Exe Explorer*, *Log Explorer* and *Scan Explorer).*

Hash

A complex digital signature calculated by the Sanctuary Application Control Suite components to uniquely identify each executable file, script or macro 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 **P**ort.

MDAC

***M**icrosoft **D**ata **A**ccess **C**omponents*. This is required by Windows computers to connect to SQL Server and MSDE databases.

MSDE

***M**icrosoft **S**QL Server **D**esktop **E**ngine*. You can use MSDE 2000 with Sanctuary.

MSI

Microsoft's Windows Installer engine (Sanctuary supports MSI from version 2.0 up to v3.1). It is also the extension of the file used by this component.

NTFS

***N**ew **T**echnology **F**ile **S**ystem* offers several enhancements and advantages over older FAT systems. These include an improved architecture, support for larger files, enhanced reliability, automatic encryption/decryption, 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

***R**emote **A**ccess **S**ervices* is a Windows program that allows most of the available network facilities to be accessed over a modem link.

RDC

***R**emote **D**ata **C**onnector*. 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

***R**emote **P**rocedure **C**all*. 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 C**ommand **C**ontrol*. The Sanctuary component that is in charge of all communication between server and client(s).

SFD

Standard File Definitions. SecureWave provides a number of pre-computed file hashes for most versions of Windows Operating Systems, in several languages, and for all the available Service Packs. These are typically installed during setup, but you can also import new ones.

SID

***S**ecurity **Id**entifier*. This is a unique alphanumeric character string. It identifies each operating system and user in a network.

SQL Server

The industry standard database server, supported by Sanctuary. Either MSSQL 2000, MSSQL 2005, or SQL Server 2005 Express Edition, can be used with Sanctuary.

SK

The Sanctuary Kernel Driver, the client component that runs as a kernel driver.

Sanctuary Management Console

The console used to define the device permissions and default options. Its functions are described in your corresponding *Administrator's Guide*.

SUS

***S**oftware **U**pdate **S**ervices* is a tool provided by Microsoft to assist Windows administrators with the distribution of security fixes and critical update releases.

SecureWave Application Servers

The Sanctuary component that serves as a link between Sanctuary Client and the SecureWave Sanctuary Database

TCP/IP

The protocol used by the client computers to communicate with the SecureWave Application Server.

TLS

***T**ransport **L**ayer **S**ecurity*. The protocol (based on SSL — Secure Socket Layers) that addresses security issues related to message interception during communication between hosts.

UAC

***U**ser **A**ccount **C**ontrol*. A new security component used in Windows Vista that enables users to permform common tasks as non-administrators, called standard users, and as administrators without having to switch users, log off, or use the Run As command.

UPC

***U**niversal/**U**niform **N**aming **C**onvention*. A path convention that uses a \\server\volume\directory\file convention instead of arbitrary mapped letters to describe the actual location of a file or directory.

WINS

***W**indows **I**nternet **N**aming **S**ervice* (formerly known as WBEM). 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 IP addresses assigned to them.

WMI

***W**indows **M**anagement **I**nstrumentation*. WMI is a set of extensions that provide an operating system management technology allowing scripts to monitor and control managed resources throughout the network.

WSUS

***W**indows **S**erver **U**pdate **S**ervices* (previously SUS v2.0) is a new version of Software Update Services (SUS).

Index of figures

Index of tables

Index