SecureWave
Safeguarding Tomorrow

# Installing Sanctuary Application Control Terminal Services Edition on Citrix Environments

www.securewave.com

## Liability Notice

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

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

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

SecureWave claims copyright in this program and documentation as an unpublished work, revisions of which were first licensed on the date indicated in the foregoing notice.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

## Trademarks

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

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

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

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 on: June 2007

# Contents

# Introducing Sanctuary Application Control Terminal Services Edition

Sanctuary Application Control Terminal Services Edition is a proactive software security solution that gives you the ability to exercise total control over applications' execution on your Citrix MetaFrame Presentation Servers. Sanctuary Application Control Terminal Services Edition works on the basis that unless an executable is explicitly authorized, its execution is denied.

Using Sanctuary Application Control Terminal Services Edition ensures that:

- Your users cannot execute programs such as hacking tools, games, or unlicensed software.
- You eliminate the threats posed by Trojans, Worms, and executable viruses, both known and unknown.

Sanctuary Application Control Terminal Services Edition works exactly the opposite way to most security and anti-virus products on the market: Rather than creating a ‘black list' of files that are not allowed to run, Sanctuary Application Control Terminal Services Edition uses a ‘white list' of executable files that are allowed to run. This is done by identifying these allowed files and creating their digital digest (hash) which is then stored in the central database. These hashes are associated with File Groups that are, in turn, associated with users/user groups that are allowed to run them.

This innovative approach offers several significant benefits:

- Greater protection. It does not matter that new Trojans and viruses are written since you purchased Sanctuary Application Control Terminal Services Edition. Any unknown or unauthorized executable, regardless of its origin, simply will not run.
- There is no requirement for regular updates for every new virus, as there is no ‘black list' to maintain.
- Requests for execution are intercepted before an executable file is allowed to run, preventing execution altogether.
- You do not need to know precisely which software is installed on every MetaFrame Presentation Server on your LAN or WAN.

It does not matter how the unauthorized application entered the MetaFrame Presentation Server, (through email, Internet, or network share) Sanctuary Application Control Terminal Services Edition will stop it from being executed.

# Sanctuary Application Control Terminal Services Edition components

A Sanctuary Application Control Terminal Services Edition solution includes three main components and a number of Administration tools. These are the *SecureWave Sanctuary Database* (SX), *SecureWave Application Server (SXS)* and the *Sanctuary Client Driver (SK)*. These components are introduced below. For a full description, see the *Sanctuary's Architecture Guide* located in your installation CD.

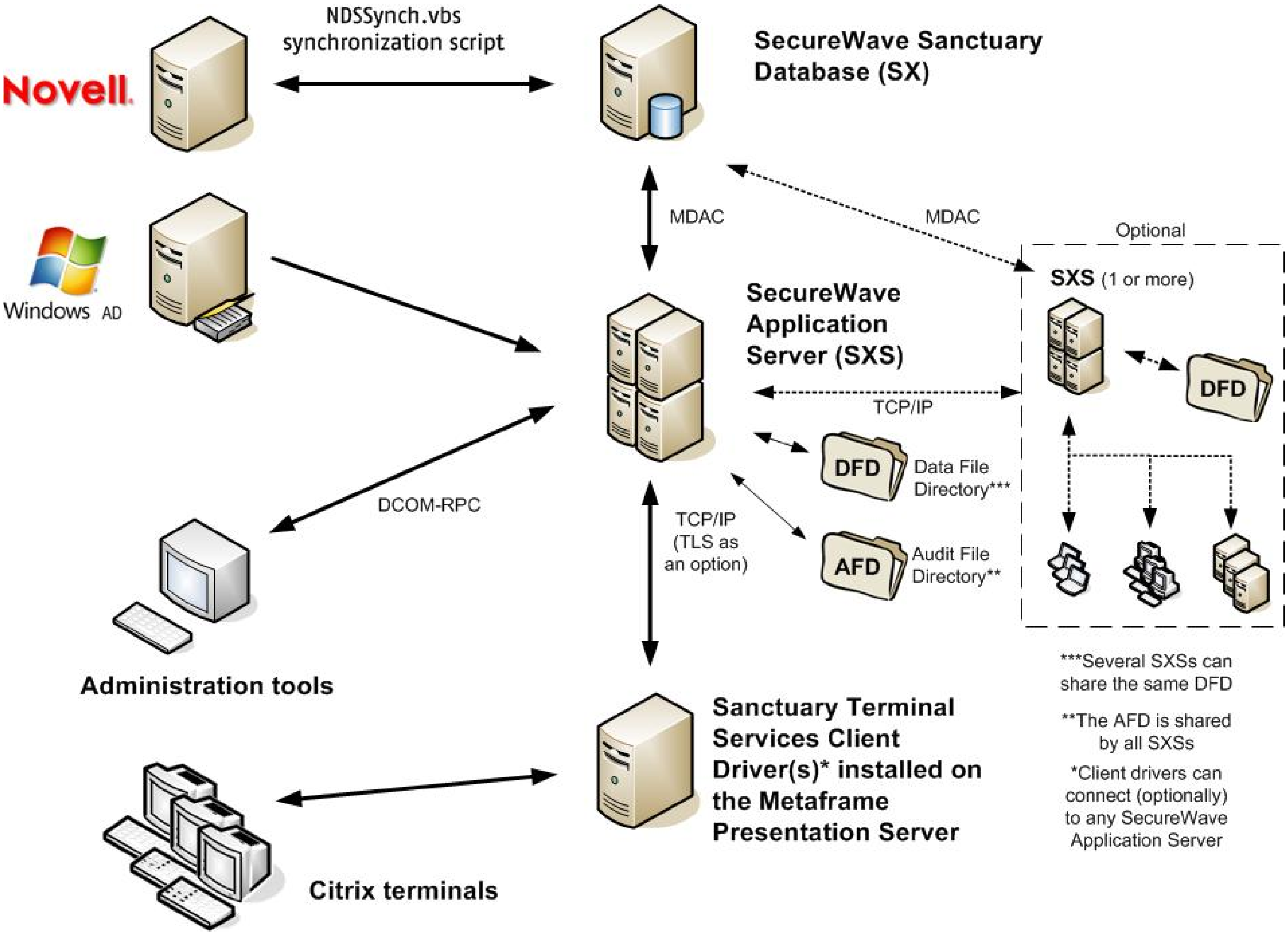

NDSSynch.vbs
synchronization script
Novell
SecureWave Sanctuary Database (SX)
Windows AD
MDAC
MDAC
Optional
SXS (1 or more)
SecureWave Application Server (SXS)
DFD
TCP/IP
DCOM-RPC
DFD
Data File Directory***
TCP/IP (TLS as an option)
AFD
Audit File Directory**
Administration tools
***Several SXSs can share the same DFD
**The AFD is shared by all SXSs
*Client drivers can connect (optionally) to any SecureWave Application Server
Sanctuary Terminal Services Client Driver(s)* installed on the Metaframe Presentation Server
Citrix terminals

Figure 1: Sanctuary components in a Citrix environment

## SecureWave Sanctuary Database (SX)

Each Sanctuary installation must have one SecureWave Sanctuary Database. This is the main storage point for the authorization information. The database uses Microsoft SQL Server 2000/2005, 2005 Express Edition, or Microsoft Database Engine (MSDE) 2000. The Sanctuary Application Control Terminal Services Edition CD-ROM comes with Microsoft SQL 2005 Express Edition that is a royalty-free database engine built and based on core SQL Server technology.

# SecureWave Application Server (SXS)

Your Sanctuary installation will also need one or more SecureWave Application Server. The purpose of the SecureWave Application Server is to communicate with the MetaFrame Presentation Servers and obtain from the Database the lists of files that clients can run.

The SecureWave Application Server component runs as a Windows Service under any domain user account capable of reading Domain users/groups/computers accounts from the Domain Controller. It performs the following functions:

- Gets the latest information about access privileges from the database and stores it in its cache
- Signs or encrypts this information, compress, and passes a differential update of this access data to servers & computers, where it is also stored locally
- Saves a log if an application access is denied

You can control if SXS-Sanctuary Client Driver (SK — explained in the next section) and intra SXS-SXS communications are fully encrypted or not. If you choose the unencrypted protocol, your environment is still safe since it is protected by signing messages using you private-public key pair (generated during the installation process — see details in the *Sanctuary's Setup Guide*).

# Sanctuary Client Driver (SK)

The Sanctuary Client Driver must be installed on each MetaFrame Presentation Server you want to control.

SK ensures that only those executable files that the user has been authorized to use can be run on the MetaFrame Presentation Server. Any attempt to run an unauthorized file is barred and logged. The logs can be viewed using the Sanctuary Management Console (SMC). SK has no user interface and therefore the user cannot interact with it, except to receive notifications that access to a file has been denied. The client has the following features.

- It is a kernel driver.
- It has a built-in TCP client and server.
- It processes all binary files loaded for execution.
- It checks the signature of each file with the authorization list. This communication is encrypted If using TLS protocol
- It generates an access log.
- All communication between the client and the application server is or fully encrypted (TLS protocol) or signed with your private-public key pair

# Administration Tools

The Administration tools available, among others, are the Sanctuary Management Console (SMC) and the Authorization Wizard.

## Sanctuary Management Console (SMC)

The SMC provides the interface to the SecureWave Sanctuary Database through the SecureWave Application Server (SXS). It is used to configure your Sanctuary installation and carry out a range of day-to-day administrative tasks. These include:

- Creating groups of files that are authorized to run.

- Assigning executable files to appropriate File Groups.
- Granting permission to users to run files listed in the different File Groups.
- Setting options in the way the MetaFrame Presentation Servers operate using Sanctuary Application Control Terminal Services Edition.
- Viewing Execution logs.
- Viewing Administrative audit logs and all kind of useful reports

If required, the SMC may be installed on several computers.

## Authorization Wizard

Since the first step in authorizing a file to run is identifying its digest (hash) and comparing it to what is stored in the central database, you can use the Authorization Wizard to spot those files copied to computers by installation routines, and to incorporate their hashes to the SecureWave Sanctuary Database. The source can be either the original CD-ROM or the files held on the target system hard drive.

# Server side components

Given Sanctuary Application Control Terminal Services Edition three-tier architecture, you need first to install Sanctuary's server side components. The exact procedure is described in *Sanctuary's Setup Guide*.

The server and administrative components should be installed onto *another* server — not the one you wish to control. For evaluation purposes, any workstation or server will do as long as the Terminal Services or MetaFrame Presentation Server is not installed.

Once installed, you can take advantage of the Standard File Definitions (SFD) to populate the SecureWave Sanctuary Database with file signatures for your operating system. If not done during the installation, you can proceed to the Sanctuary Management Console, and select *Tools* ➔ *Import Standard File Definitions* from the menu. In the dialog that is displayed, begin by selecting the lists to be imported (click the *Add* button); you will find them in the \SFD folder on the Sanctuary Application Control Terminal Services Edition CD-ROM. Click the Import button to start the process.

Once the file definitions importation finishes, you should select the *User Explorer* module (from the same console) and assign the newly created File Groups to users as follows:

> Everyone: Windows Common, Logon Files

> LocalSystem : Boot Files

> LOCAL SERVICE: Boot Files

> NETWORK SERVICE: Boot Files

> Administrators: all

These assignments represent the minimum that we recommend. Additionally, you may want to assign Entertainment, Communication, Accessories, Control Panel, DOS Applications, and 16bit Applications to users or groups as required.

All other files can be authorized either by means of the execution logs (*Log Explorer* module) or by scanning the target computer (*Scan Explorer* module). Please refer to the *Sanctuary Application Control Suite Administrator's Guide* for further details.

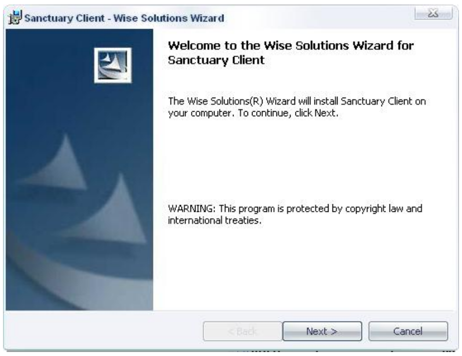
# Installing the Sanctuary Client Driver

## The Installation Procedure

To install the Sanctuary Client Driver on your MetaFrame Presentation Servers, follow the steps below:

1. Log on to the MetaFrame Presentation Server with administrative rights.
2. Start a command line prompt and type: "**change user /install**", which will change your session from execution to installation mode.
3. Select the "Client" folder on the Sanctuary Application Control Terminal Services Edition CD-ROM or navigate to the network share where the Sanctuary Client Driver setup files are located. Run Setup.exe. The Setup program launches the MSI installer.

   When this is complete, the Welcome dialog is displayed. Click on NEXT to continue.



Sanctuary Client - Wise Solutions Wizard

**Welcome to the Wise Solutions Wizard for Sanctuary Client**

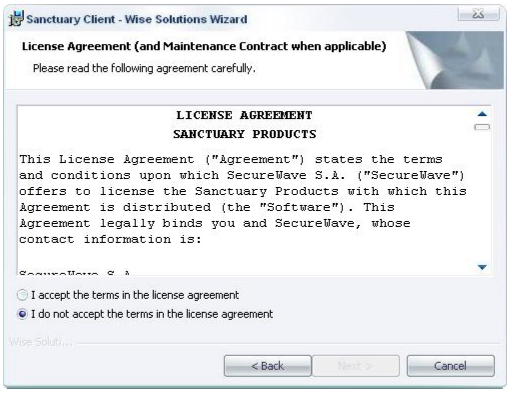
The Wise Solutions(R) Wizard will install Sanctuary Client on your computer. To continue, click Next.

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

Figure 2: Welcome screen

4. The License Agreement is displayed in the next dialog. Copyright and international treaties protect the Sanctuary Application Control Terminal Services Edition software. Read the license agreement carefully and, providing you agree with its conditions, click on I accept the terms in the license agreement and then on the Next button to continue.

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



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:
```

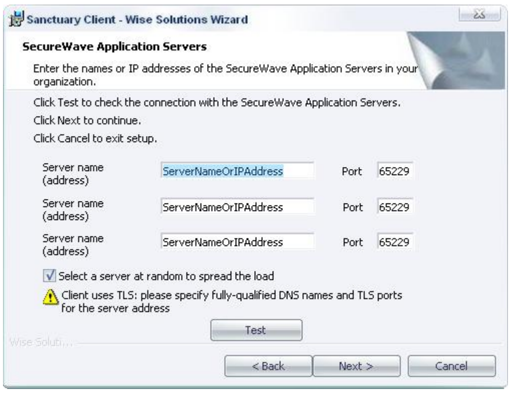
○ I accept the terms in the license agreement

● I do not accept the terms in the license agreement

Figure 3: License agreement

5. In the next step, you must decide if the Sanctuary Client Driver use or not TLS protocol to communicate with SecureWave Application Server (SXS). We recommend selecting TLS protocol (encrypted) — you must already have a valid certificate for the machine. You can use the fist option (non-encrypted communication but still signed with the private key) for testing purposes. Click NEXT.

6. Enter the Server name of at least one SecureWave Application Server on your network. You can enter up to three server names. The dialog accepts fully qualified domain names (FQDN) or IP addresses. You can also proceed without providing a server address. Do not use IP addresses if you are going to use TLS protocol for communication encryption.



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 4: Sanctuary Components

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

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

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

10. Click on NEXT to confirm your settings. The server address is verified but you can still continue if it is invalid or unspecified. See details in the *Sanctuary's Setup Guide*.

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

12. You can now proceed to select the way the uninstall process is controlled in Windows' *Add or Remove Programs* dialog.

After the final screen, where the actual installation process begins, the Sanctuary Client Driver setup prompts you to reboot one final time.

Once installation is complete, if you do not want to reboot, run "**change user /execute**" in the command prompt window you used at the beginning of the installation.

# Uninstalling the Sanctuary Client Driver

At any time after installing Sanctuary Client Driver you can uninstall it from your MetaFrame server. To do this you must log onto the computer using an account with administrative rights.

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.

To uninstall the client you should either:

> Deactivate the “Hardening” option using the management console

- Generate an “Endpoint Maintenance Ticket” that overrules the “hardening option”

Please consult the *Sanctuary Application Control Suite Administrator's Guide* or the help file for a complete description on how to create an Endpoint Maintenance Ticket.

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. On completion of the uninstall process, you must reboot the server.

.

# Glossary

### ACL

Acronym for ***A****ccess* ***C****ontrol* ***L****ist*. A list that keeps the permissions that each user or group has to a specific system object. Each object has a unique security attribute that identifies which users have access to it.

### ADSI

Acronym for ***A****ctive* ***D****irectory* ***S****ervice* ***I****nterface*. Previously known as OLE Directory Services, ADSI makes it easy to create directory management applications using high-level tools such as Basic, Java, or C/C++ without having to worry about the underlying differences between the dissimilar namespaces.

### AES

***A****dvanced* ***E****ncryption* ***S****tandard*. A symmetric key encryption technique that is replacing the commonly used DES standard. It is the result of a worldwide call for submissions of encryption algorithms issued by NIST in 1997 and completed in 2000.

### CAB

File extension for ***cab****inet* files, which are multiple files compressed into one and extractable with the extract.exe utility. Such files are frequently found on Microsoft software distribution disks.

### Client Computer

The computers on your network that Sanctuary Application Control Terminal Services Edition controls.

### CSV

The CSV, ***C****omma* ***S****eparated* ***V****alue*, file format allows easy data table retrieval into a variety of applications. It is often used to exchange data between disparate applications. The file format has become a pseudo standard throughout the industry, even among non-Microsoft platforms. Common examples of applications that use this format are spreadsheets and databases. You can also see and edit these files using an ASCII text editor (Notepad, Word, WordPad, Excel, etc.).

### Delegation

The act of assign responsibilities for management and administration of a portion of the resources or items used in a shared computing environment to another user, group, or organization.

### Dependencies

Additional executable files (.exe, .dll, or others) required by executable files to run properly.

Dependencies are split into two categories: *static dependencies* which are files declared explicitly in the executable file as being required, and *dynamic dependencies* which are additional files an executable may require at runtime.

### DN

***D****istinguish* ***N****ame*. A name that uniquely identifies an object in the Directory Information Tree.

### 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.

### Exploit

A piece of software that takes advantage of a bug, glitch or vulnerability, leading to privilege escalation (exploit a bug) or denial of service (loss of user's services) on a computer system.

### File Group

Organizational groups used to cluster authorized executable files. Files must be assigned to 'File Groups' before users can be granted permission to use them. You can choose to assign files to 'File Groups' from various modules throughout the Sanctuary Management Console, e.g. by double-clicking on a file in the *Database Explorer*, *EXE Explorer*, *Log Explorer* or *Scan Explorer.*

### GUID

A *__G__lobal __U__nique __I__dentifier* number generated when the NDS object is created. It is simply an object's NDS attribute. In order to ensure data consistency, Novell eDirectory implements a globally unique ID (GUID) for all objects within the directory. The total number of unique keys (2128 or 3.4028 x 1038) is so large that the possibility of using the same number twice is nearly zero.

### Hash

A complex digital signature calculated by Sanctuary to uniquely identify each executable file that can be run. The hash is calculated using the SHA-1 algorithm that takes into account the entire contents of the file.

### iFolder

A Novell client that runs on Windows-based computers. It allows a user to work on his files anywhere —online or offline. iFolder integrates encryption and file synchronization services.

### LDAP

*__L__ightweight __D__irectory __A__ccess __P__rotocol*. An LDAP directory entry consists of a collection of attributes and is referenced unambiguously with a name, called a distinguished name (DN). For example, "cn=Bill Dove: ou=marketing: o=SecureWave" — "cn" for common name, "ou" for organizational units, "o" for organization. LDAP directory entries feature a hierarchical structure that reflects political, geographic, and/or organizational boundaries.

### MAPI

*__M__essaging __A__pplication __P__rogramming __I__nterface* enables Windows applications to access a variety of messaging systems.

### MDAC

*__M__icrosoft __D__ata __A__ccess __C__omponents*. Required by Windows computers to connect to SQL Server or MSDE databases.

### MSDE

*__M__icrosoft __D__ata __E__ngine* (also known as Microsoft SQL Server Desktop Engine), is a SQL Server compatible database server, suitable for small and medium size organizations. MSDE databases can subsequently be migrated to SQL Server 2000/2005. SQL Server 2005 Express Edition now supersedes MSDE.

### NDAP

*__N__ovell __D__irectory __A__ccess __P__rotocol*. The NDAP component gives Windows applications full access to the Novell eDirectory and administration capabilities for NetWare servers, and volumes.

### NDS

Novell's eDirectory previously called *__N__ovell __D__irectory __S__ervices*. eDirectory is a hierarchical, object oriented database that represents all the assets in an organization in a logical tree. Assets can include users, positions, servers, workstations, applications, printers, services, groups, etc.

### NICI

***N**ovell **I**nternational **C**ryptographic **I**nfrastructure*. NICI is a base set of cryptographic services available for Novell. NICI provides an API set that offers a consistent interface for application developers to use and deploy cryptography within their applications.

### OU

***O**rganizational **U**nits*. A part of the Active Directory (AD) structure inherited from Novell's NDS structure. Within Novell's NDS/eDirectory there are three classes of objects in the NDS batabase: Roots, Containers, and Leafs. There are three supported types of container objects: Country (C=), Organizations (O=), and Organizational Units (OU=).

### Private Key

One of two keys used in public key encryption. The sender uses the private key to create a unique electronic number that can be read by anyone possessing the corresponding public key. This verifies that the message is truly from the sender.

### 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.

### RPC

A ***R**emote **P**rocedure **C**all* is a protocol that allows a computer program running on one host to run a subroutine on another host. RPC is used to implement the client-server model of distributed computing.

### RSA Encryption

In 1977, Ron Rivest, Adi Shamir, and Len Adleman developed the public key encryption scheme that is now known as RSA, after their initials. The method uses modular exponentiation, which can be performed efficiently by a computer, even when the module and exponent are hundreds of digits long.

### SFD

SecureWave provides a number of pre-computed file hashes for most versions of suites and Windows Operating Systems, in several languages, and for all the available Service Packs. The file hashes are referred to as *Standard File Definitions* or SFD. They are installed during the setup, but you can import them as soon as SecureWave releases new ones. You can find the latest ones on our Web site.

### SHA-1

***S**ecure **H**ash **A**lgorithm 1*, as defined in the Federal Information Processing Standards Publication 180-1. This algorithm produces a one-way 160-bit hash that can be used for a variety of applications including authentication and cryptography.

### SID

Acronym for ***s**ecurity **id**entifier*, a security feature of Windows NT and 2000 operating systems. The SID is a unique name (alphanumeric character string) used to identify an object, such as a user or a group of users in a network.

Windows grants or denies access and privileges to resources based on an ACL (***A**ccess **C**ontrol **L**ist*), which uses a SID to uniquely identify users and their group memberships. When a user requests access to a resource, the user's SID is verified by the ACL to determine if the user, or the group he belongs to, is allowed to perform that action.

### SQL

***S**tructured, **Q**uery **L**anguage*, a language used to construct database queries.

### 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.

### SXS

SecureWave Application Server. The main component of all Sanctuary's products. Beside calculating hashes, authorizing applications and devices, it serves as a bridge between the database and the client.

### TCP/IP

Acronym for ***T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol*. The protocol used by the client computers to communicate with the SecureWave Application Server.

### VBScript

A scripting language created by Microsoft embedded in many applications used in Windows. Although it allows for powerful interoperability and functionality, it also creates a great deal of security risks unless it is tightly controlled.

### Vulnerability

A weakness or other kind of opening in a system, usually caused by a bug or other design flow.

### Well-Known Security Identifiers

A security identifier (SID) is a unique value used to identify a security principal or security group. The values of certain SIDs remain constant across all installations of Windows systems and for this reason are termed well-known SIDs. Everybody, Local, Guest, Domain Guest, etc. are some examples of SIDs.

### WMI

Acronym for ***W**indows **M**anagement **I**nstrumentation*. WMI is a standard technology to access management information in an enterprise environment. WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components. You can use WMI to automate administrative tasks in an enterprise environment. WMI improves administrative control by allowing administrators to correlate data and events from multiple sources and vendors on a local or enterprise basis. It is used as a complement to ADSI.

### 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