SecureWave Sanctuary Device Control v3.2
Security Target

Version 1.0

15 March 2007

Prepared for:
SecureWave
43869 Cowgill Court
Ashburn, VA 20147

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

Table of Content

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. SecureWave provides the TOE, which is Sanctuary Device Control v3.2. Sanctuary Device Control v3.2 is a powerful desktop security enhancer that allows system administrators to implement strict security policies by controlling end-user access to, and use of, I/O devices such as USB memory sticks, CD and DVD R/W devices, PDA's, as well as other devices.

The Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description
  This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Section 3 – TOE Security Environment
  This section details the expectations (assumptions) of the environment and the threats that are countered by Sanctuary Device Control v3.2 and IT environment.
- Section 4 – TOE Security Objectives
  This section details the security objectives of the Sanctuary Device Control v3.2 and its environment.
- Section 5 – IT Security Requirements
  The section presents the security functional requirements (SFR) for Sanctuary Device Control v3.2 and IT Environment that supports the TOE, and details the assurance requirements for EAL2.
- Section 6 – TOE Summary Specification
  The section describes the security functions represented in the Sanctuary Device Control v3.2 that satisfy the security requirements.
- Section 7 – Protection Profile Claims
  This section presents any protection profile claims.
- Section 8 – Rationale
  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability.
- Section 9 – Terminology and Acronyms
  This section includes a list of terms and acronyms that is used throughout the ST.

1.1 Security Target, TOE and CC Identification

ST Title – SecureWave Sanctuary Device Control v3.2 Security Target

ST Version – Version 1.0

ST Date – 15 March 2007

TOE Identification – Sanctuary Device Control v3.2

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.1, August 1999, ISO/IEC 15408-2.
  - Part 2 Conformant

- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999, ISO/IEC 15408-3.
    - Part 3 Conformant
    - Evaluation Assurance Level 2 (EAL2)

1.3 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target. Refer to Terminology and Acronyms section, for a complete list of acronyms and terms used throughout the ST

1.3.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1(a) and FDP_ACC.1(b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

2. TOE Description

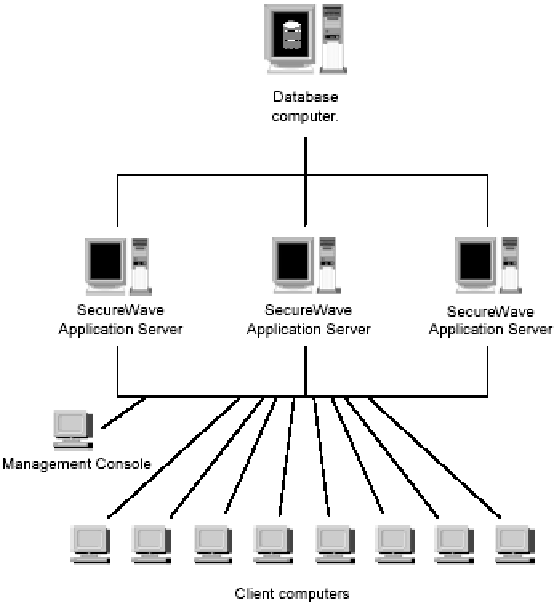
The Target of Evaluation (TOE) is the Sanctuary Device Control v3.2. The remainder of this section summarizes the Sanctuary Device Control v3.2 architecture. The TOE is a subset of the product. The Product includes the MSDE 2000 database. The MSDE 2000 database is in the IT environment and not considered part of the TOE. Refer to 2.2.1.1 Sanctuary Device Control v3.2 components.

2.1 Product Type

Sanctuary Device Control v3.2 is a powerful desktop security enhancer that allows system administrators to implement strict security policies by controlling end-user access to I/O devices such as the floppy drive, CD-ROM, serial and parallel ports, as well as other devices. Sanctuary Device Control v3.2 hinders the introduction of malicious code, unlicensed software, and other counterproductive applications that promote inappropriate use of corporate resources.

2.2 Product Description

Sanctuary Device Control v3.2 is a three-tiered client/server system designed to allow system administrators to implement strict security policies by controlling end-user access to I/O Devices. The three tiers are: A backend database (SQL Server); a middle tier of SecureWave Application Servers; and a client tier. The clients fall into administrative clients, software used to control and direct the operation of the system, and client drivers, residing on the computers that Sanctuary Device Control v3.2 protects. The administrative client software resides in a main program Management Console (Administrative Tools) and some smaller utility programs; the client drivers for Sanctuary Device Control v3.2 Client, consist of one driver each for Microsoft Windows NT 4.0, Microsoft Windows 2000, and Microsoft Windows XP.



2.2.1.1 Sanctuary Device Control v3.2 components

A Sanctuary Device Control v3.2 solution includes four components. These are the Database, SecureWave Application Server, Sanctuary Device Control v3.2 Client Driver, and the Administrative Tools. These components are described below:

- **Database:** This is the main storage point for the information. Each Sanctuary Device Control v3.2 site must have at least one database. This is the master storage point for the user policies and permissions. The database is hosted by Microsoft SQL Server 7/2000, MSDE or MSDE 2000 and the underlying operating system. The Sanctuary Device Control v3.2 relies on the environment to provide Microsoft SQL Server 7/2000, MSDE or MSDE 2000 database for its use.

- **SecureWave Application Server:** Each Sanctuary Device Control v3.2 installation can also have one or more SecureWave Application Servers. The purpose of SecureWave Application Server is to communicate with the Sanctuary Device Control v3.2 Client computers and obtain from the Database, the lists of devices and permissions.

- **Sanctuary Device Control v3.2 Client Driver**: The purpose of the Sanctuary Device Control v3.2 Client is to enforce the policies and permissions for each user. The client is installed on each computer that is to be included in the Sanctuary Device Control v3.2 solution. Each Sanctuary Device Control client system contains a client component that runs as a kernel driver (sk.sys (SK)). The SK driver enforces the policy management (and permissions) for each user, provides device shadowing capability that tracks the data written to any Sanctuary Device Control protected device, and enforces a device white list that blocks access to unknown (i.e., not managed by the SK driver) devices. When the client is first installed, the SK places a default ACL (access control list) on all of the devices (block all devices by default, as SDC applies the "least privilege principle" which requires deny access to any device that is not expressly permitted). Following placement of the default ACL, it hooks each of the device entry points to their respective drivers. When a user logs on to the client, the SK send a message to the SecureWave Application Server to retrieve the list of the permissions for known devices for the user. The Sanctuary Client, installed on the client machines, ensures that only those I/O devices that the user has been authorized to use can be access on the client computer. Any attempt to access an unauthorized device is denied, regardless of the computer from which a users attempts access. The setup also installs an application (RTNotify) that provides to the end user information about the status of each device (denied, changed/updated and permitted).

- **Administrative Tools**
  - **Sanctuary Device Console (a.k.a. Management Console)**: The Sanctuary Device Console is used to configure Sanctuary Device Control v3.2 and to perform day-to-day administrative functions. If required, the Sanctuary Device Console may be installed on several computers.
  - **Key Pair Generator** - The Key Pair Generator is used to create an encryption key pair. The SecureWave Application Server uses an asymmetric encryption system to communicate with the Sanctuary Device Control v3.2 Client Driver.
  - **SXDomain command-line tool** - The SXDomain command-line tool is used to inform the Database of changes to the users, user groups, and client workstations within the network.

2.3 Product Features

The TOE implements the following features:

- Centralized Device Access Control: Sanctuary Device Control v3.2's core functionality is the ability to centrally control user and/or user group access to I/O Devices on the client workstations and/or domain level.

- Intuitive User Interface: I/O Device access is controlled by means of native Access Control Lists similar to Access Control List for files and folders.

- Native support for Plug and Play devices: All types of buses, such as PCMCIA, FireWire, and USB are supported and all Plug and Play devices are detected and access control policies are enforced.

- Read-only Access: Sanctuary Device Control v3.2 makes it possible to set the access to a particular I/O Device to be read-only. This option is valid for all file-system based I/O Devices such as the floppy drive or PCMCIA hard drives.
- Copy limit: The authorized administrator can set permissions that limit the quantity of data a user can write to each device on a per-day basis.
- Scheduled Access: Scheduled I/O Device access gives the option of granting or denying device access for a specific period of time. This feature allows for the development of sophisticated security policies where certain devices can only be used from 9 to 5, Monday to Friday, for example.
- Per-device encryption: Access can be restricted for a specific device to a particular user or group of users that incorporates an encryption process to ensure that sensitive data is not inadvertently exposed to those without authorized access.
- File Shadowing: Sanctuary Device Control v3.2's Shadow technology enables full auditing of all data written to file-system based devices such as Recordable DVD/CD, floppy, Zip and PCMCIA drives, as well as to serial and parallel ports. This feature is available on a per user basis. All shadowing files are automatically transferred to the server at regular intervals.
- Media Authorization: Access to a known set of DVD/CD/removable media can be granted to individual users and groups.
- Offline updates: It is possible to update the permissions of remote machines that cannot establish a network connection to the company. New permissions can be exported to a file that is later imported onto the client computer.

In addition, Sanctuary Device Control v3.2 supports a wide range of device types that represent key sources of security breaches. Device types currently managed by Sanctuary Device Control v3.2 include: Biometric devices, Bluetooth radio devices, COM/Serial ports and LPT/Parallel ports, DVD/CD drives, Floppy disk drives, Imaging devices, Infrared ports (IrDA), Modems/Secondary network access devices, Palm handheld devices (USB), Removable storage devices, RIM Blackberry RIM handhelds (USB), Scanners, Smart Card readers, Tape drives, Unauthorized encrypted media, USB printers, User-defined devices, Windows CE handheld devices (USB), Wireless NICs (network interface controllers), Plug and Play devices, USB, FireWire, and PCMCIA.

2.4 Security Environment TOE Boundary

The TOE includes both physical and logical boundaries.

2.4.1 Physical Boundaries

The physical boundary for each component of the TOE is the environment that each component requires for effective operation. Each of the TOE components is a software application designed to execute within an operating system context provided by the environment. The Database is installed on the computer that is to hold the Sanctuary Device Control authorization information. The SecureWave Application Server is installed on the computers that are going to be the SecureWave Application Servers. The Sanctuary Device Console is installed on the computers that are will be used to configure Sanctuary Device Control, and subsequently carry out the day-to-day administrative tasks and procedures. The Sanctuary Device Control v3.2 Client is installed on the client workstations within the network that will be controlled.

Refer to 3.2.3 System Assumptions for detailed information on the supported operating systems. The underlying operating system and supporting hardware are not considered part of the TOE.

2.4.2 Logical Boundaries

The logical boundaries are the security functions provided by the TOE. The TOE supports the following security functions:

- Security audit

- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- Resource utilization

2.4.2.1 Security Audit

Sanctuary Device Control v3.2 audits the actions that occur at the SecureWave Application Servers and the Sanctuary Device Control v3.2 Client workstation. All administrative actions performed on the Sanctuary Device Console are audited and stored by the TOE. The Sanctuary Device Control v3.2 Client logs the actions of the client on the client workstation. These logs are stored and protected by the operating system of the client computer. See Security Audit section for more information.

2.4.2.2 Cryptographic Support

The TOE implements cryptographic functionality to protect communication between its client and server components. The TOE also implements cryptographic functionality to protect removable media.. See Cryptographic Support section for more information.

2.4.2.3 User Data Protection

The Sanctuary Device Control v3.2 stores the user identity, user groups, and I/O Device access control list (ACL), and the associated access rights. When a user logs onto a client computer, the access control list of the permissions and I/O Devices are transmitted, first to SecureWave Application Server, and then the Sanctuary Device Control v3.2 Client workstation. When a user attempts to access an I/O Device, the access permission will be verified to determine if access is allowed as well as the access right that was granted. See User Data Protection section for more information.

2.4.2.4 Identification and authentication

The Database stores the user identity, user groups, and I/O Device access control list (ACL). See Identification and Authentication section for more information.

2.4.2.5 Security Management

The Sanctuary Device Console provides the administrator with graphical user interfaces that can be used to configure and modify the options of the TOE. There are several modules available to the authorized administrator, such as the Device Explorer, which is used to grant access rights to I/O Devices for specific user and user groups and the audit viewers that are used to view the audit records of administrative activities. See Security Management section for more information.

2.4.2.6 Protection of the TSF

Sanctuary Device Control v3.2 controls access to devices by applying an Access Control List (ACL) to each device type. Based on the Least Privilege Principle, device access for all users is not allowed by default. Therefore, to grant access, the administrator only needs to associate those users or user groups to the devices to which they should have access. See Protection of the TSF section for more information.

2.4.2.7 Resource Utilization

When the Sanctuary Device Control v3.2 Client workstation cannot communicate with the SecureWave Application Server, it will be operated in a standalone mode, utilizing the copy of the access control listing that was placed in a secure area on the hard disk of the workstation. The Sanctuary Device Control v3.2 Client workstation will utilize this listing until a new logon is performed. See Resource Utilization section for more information

2.5 TOE Documentation

SecureWave offers a series of documents that describe the installation process for the TOE, as well as guidance for subsequent use and administration of the system security features. Refer to Section 6.2 TOE Security Assurance Measures for information about these and other evidence assurance documents.

3. Security Environment

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed.

The statement of TOE security environment defines the following:

- Threats that the product is designed to counter,
- Assumptions made on the operational environment and the method of use intended for the product.

3.1 Threats to Security

The following are threats identified for the TOE. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides.

T.ACCESS Authorized users may gain unauthorized access to the functions of the TOE.

T.ACCOUNTABILITY The security relevant actions of users may go undetected.

T.DATA_CORRUPT An attacker may be able to inappropriately modify or otherwise tamper with TSF data.

T.FAULT_TOLERANCE The users of the system may attempt to access an I/O Device when the Sanctuary Device Control v3.2 Client loses communications with SecureWave Application Servers

T.PRIVILEGE An authorized user of the TOE may gain unauthorized access to a resource.

T.TRANSIT A user may alter the TSF data as it is transmitted between the distributed parts of the TOE and the modification goes undetected.

3.2 Secure Usage Assumptions

The following usage assumptions are made about the intended environment of the TOE.

3.2.1 Physical Assumptions

A.CONNECT Any network resources used for communication between TOE components will be adequately protected from unauthorized access.

A.PROTECT The components of the TOE critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.

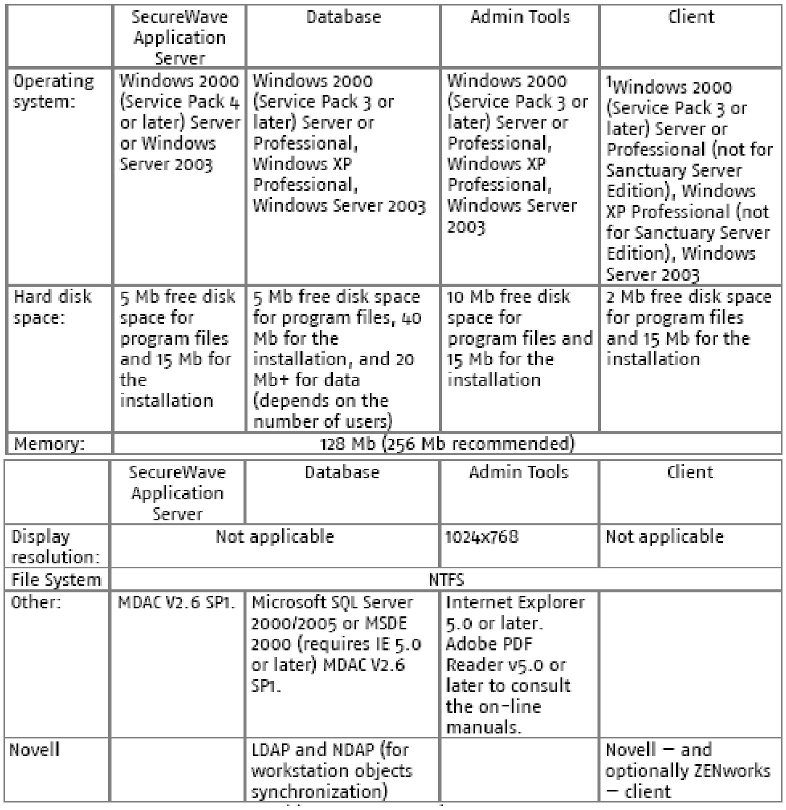
3.2.2 Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The administrative personnel are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the administrative guidance.

3.2.3 System Assumptions

A.HARDWRE The TOE will be installed on a computing environment system that meets or exceeds the following constraints:



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

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

4. Security Objectives

This section defines the security objectives of the TOE and its supporting environment. Security objectives are categorized as either IT Security Objectives for the TOE, IT Security Objectives for the Environment, or Non-IT Security Objectives for the Environment. The security objectives specify the stated intent to counter identified threats and address the identified assumptions. All of the identified threats and assumptions are addressed under one of the categories below.

4.1 IT Security Objectives for the TOE

The following security objectives are intended to be satisfied by the TOE.

O.AUDIT The TSF must record the security relevant actions of users of the TOE and have the ability to associate each action with a unique subject. In addition, the TSF must present this information in a readable format to authorized administrators and ensure that authorized administrators are able to access this information.

O.CONTROL The TSF must control access to resources and I/O Devices based on subject's identification. The TSF must provide the ability to limit each subject's access.

O.DATA_TRANSFER The TSF must have the capability to protect TSF data in transmission between distributed parts of the TOE

O.FAULT_TOLERANCE The TSF must continue to enforce access control policies if communications are lost with the SecureWave Application Servers.

O.MANAGE The TOE must allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

4.2 IT Security Objectives for the Environment

The following security objectives for the IT environment of the TOE must be satisfied in order for the TOE to fulfill its own security objectives.

OE.AUTH_ACCESS The TOE operating environment must ensure that only authorized users gain access to the TOE and to the data contained in the TOE by ensuring all users are identified and authenticated.

OE.ENV_ADMIN The TOE operating environment must assign the administrative user to manage the TOE, until the TOE administrators are specifically assigned to manage the Administrative Tools component of the TOE.

OE.SEP The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and ensure that TOE components cannot be tampered with or bypassed.

OE.TIME_SOURCE The TOE operating environment must provide a reliable time source for the TOE to provide accurate timestamps for audit records.

4.3 Non-IT Security Objectives for the Environment

The following security objectives are intended to be satisfied by the Non-IT environment of the TOE.

OE.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives.

OE.PERSON Authorized users of the TOE shall be properly trained in the configuration and usage of the TOE and will follow the guidance provided. These users are not careless, negligent, or hostile.

OE.PHYCAL Those responsible for the TOE must ensure that the network resources and the parts of the TOE critical to security policy are protected from physical attack that might compromise the TOE security objectives.

5. IT Security Requirements

This section defines the security functional and security assurance requirements for the TOE and associated Information Technology (IT) environment components. The SFRs were drawn from the Part 2 Common Criteria version 2.1. The SARs were drawn from the Part 3 Common Criteria version 2.1.

5.1 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. This section organizes the SFRs by CC class. **Table 1 Security Functional Components** identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

SECURITY FUNCTIONAL CLASS	SECURITY FUNCTIONAL REQUIREMENTS
Security audit (FAU)	FAU_GEN.1 Audit data generation
	FAU_GEN.2 User identity association
	FAU_SAR.1 Audit review
	FAU_SAR.3 Selectable audit review
Cryptographic support (FCS)	FCS_CKM.1(a) Cryptographic key generation
	FCS_CKM.1(b) Cryptographic key generation
	FCS_COP.1 Cryptographic operation
User data protection (FDP)	FDP_ACC.2 Complete access control
	FDP_ACF.1 Security attribute based access control
Identification and authentication (FIA)	FIA_ATD.1 User attribute definition
Security management (FMT)	FMT_MSA.1 Management of security attributes
	FMT_MSA.2 Secure security attributes
	FMT_MSA.3 Static attribute initialization
	FMT_MTD.1(a) Management of TSF data (Audit Data and Shadowing Information)
	FMT_MTD.1(b) Management of TSF data (Administrator)
	FMT_REV.1 Revocation
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1(a) Security roles
Protection of the TSF (FPT)	FPT_ITT.1 Basic internal TSF data transfer protection
	FPT_RVM.1 Non-bypassability of the TSP
Resource utilization (FRU)	FRU_FLT.1 Degraded Fault Tolerance

Table 1 Security Functional Components

5.1.1 FAU - Security audit

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [***not specified***] level of audit; and
c) [**Attempts to access the shadow files, and**
d) **See Table 2 Auditable Events**].

Component	Event	Details
FDP_ACF.1	Enforcement of device access control based upon security attributes	User identity, user group, I/O Device
FMT_MSA.3	Setting of security attributes and their default values	
FMT_MTD.1	All modifications to the values of TSF data	User identity
FMT_REV.1	All attempts to revoke security attributes	

Table 2 Auditable Events

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the ~~PP/~~ST, [**user group, I/O Device**].

FAU_GEN.2 User identity association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [**Enterprise Administrator, Administrator**] with the capability to read [**all audit information**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform [***searches, ordering***] of audit data based on [**date of event**].

5.1.2 FCS - Cryptographic support

FCS_CKM.1(a) Cryptographic key generation

FCS_CKM.1.1(a) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA key generation algorithm]** and specified cryptographic key sizes [**2048 bits (RSA)**] that meet the following: [**ANSI X9.31-1998**].

FCS_CKM.1(b) Cryptographic key generation

FCS_CKM.1.1(b) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**AES key generation algorithm]** and specified cryptographic key sizes [**256 bits**] that meet the following: [**FIPS 197**].

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [**the following cryptographic operations:**

a) hashing

b) digital signature generation/verification

c) **symmetric encryption and decryption**

d) **Asymmetric encryption and decryption**

in accordance with a specified cryptographic algorithm [**listed below**] and cryptographic key sizes [**listed below**] that meet the following:[**listed below**].

a) **hashing**

- **SHA-1 based on standard: FIPS 180-2**
- **key size: N/A**
- **Modes of operation: N/A**

b) **digital signature generation/verification**

- **algorithm: RSA with SHA-1 based on standard: FIPS 186-2**
- **key size: 2048**
- **Modes of operation: RSASSA-PKCS1-v1_5**

c) **Symmetric encryption and decryption**

- **algorithm: AES based on standard: FIPS 197**
- **key size: 256**
- **Modes of operation: ECB**

d) **Asymmetric encryption and decryption**

- **algorithm: RSA based on standard: RSA**
- **key size: 2048**
- **Modes of operation: RSAES-PKCS1-v1_5**

5.1.3 FDP - User data protection

FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the [**Management Access Control SFP**] on [**subject: users, object: I/O Devices**] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

FDP_ACF.1 Security attribute based access control[1]

FDP_ACF.1.1 The TSF shall enforce the [**Management Access Control SFP**] to objects based on [**subject: users**

- **user identity**
- **user group**
- **permissions**

Object: I/O Devices

- **Access control list (ACL)**].

[1] This requirement has been modified to comply with International Interpretation RI# 103.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a) if the I/O Device ACL and the permissions grants the requesting user identity the requested access, the requested access is allowed, or

b) if the I/O Device ACL and the permissions grants a user group access and the user identity is a member of the user group, the requested access is allowed].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**no additional access rules**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [**no additional explicit denial rules**].

5.1.4 FIA - Identification and authentication

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**user identity, user group, permissions**]**.**

5.1.5 FMT - Security management

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [**Management Access Control SFP**] to restrict the ability to [***modify, delete,*** **create**] the security attributes [**permissions, I/O device ACL**] to [**Enterprise Administrator, Administrator**].

FMT_MSA.2 Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [**Management Access Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**no user**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1(a) Management of TSF data (Audit Data and Shadowing Information)

FMT_MTD.1.1(a) The TSF shall restrict the ability to [***query***] the [**audit data and Shadowing Information**] to [**Enterprise Administrator, Administrator**].

FMT_MTD.1(b) Management of TSF data (Administrator)

FMT_MTD.1.1(b) The TSF shall restrict the ability to [***delete,*** **assign**] the [**Administrator role**] to [**Enterprise Administrator**].

FMT_REV.1 Revocation

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the [***subjects, objects***] within the TSC to [**Enterprise Administrator, Administrator**]**.**

FMT_REV.1.2 The TSF shall enforce the rules [**upon the next login**].

FMT_SMF.1 Specification of Management Functions[2]

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

a) Review of Audit
b) Review of Shadowing Information files
c) Management of users, user groups, and permissions (modify, create, delete)
d) Management of I/O Device ACL (modify, create, delete)].

FMT_SMR.1(a) Security roles

FMT_SMR.1.1(a) The TSF shall maintain the roles [**Enterprise Administrator, Administrator**].

FMT_SMR.1.2(a) The TSF shall be able to associate users with roles.

5.1.6 FPT - Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from [***modification***] when it is transmitted between separate parts of the TOE.

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.7 FRU - Resource utilization

FRU_FLT.1 Degraded fault tolerance

FRU_FLT.1.1 The TSF shall ensure the operation of [**Management Access Control SFP**] when the following failures occur: [**Sanctuary Device Control v3.2 Client is unable to communicate with SecureWave Application Servers**].

5.2 IT Environment Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the IT Environment. This section organizes the SFRs by CC class. **Table 3 Security Functional Components for the IT Environment** identifies all SFRs implemented by the IT Environment and indicates the ST operations performed on each requirement.

Security Functional Class	Security Functional Components
Security Audit (FAU)	FAU_STG.1 Protected audit trail storage
Identification and authentication (FIA)	User identification before any action (FIA_UID.2)
	User authentication before any action (FIA_UAU.2)

[2] This requirement has been added to comply with International Interpretation #65

Security Functional Class	Security Functional Components
Security Management (FMT)	Security roles (FMT_SMR.1(b))
Protection of the TSF (FPT)	Reliable time stamps (FPT_STM.1)
	TSF domain separation (FPT_SEP.1)

Table 3 Security Functional Components for the IT Environment

5.2.1 FAU – Security Audit

FAU_STG.1 Protected audit trail storage[3]

FAU_STG.1.1 The ~~TSF~~ **IT Environment** shall protect the stored audit records **in the audit trail** from unauthorized deletion.

FAU_STG.1.2 The ~~TSF~~ **IT Environment** shall be able to [***prevent***] unauthorized modifications to the audit records **in the audit trail**.

5.2.2 FIA - Identification and authentication

FIA_UID.2 User identification before any action

FIA_UID.2.1 The ~~TSF~~ **IT Environment** shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The ~~TSF~~ **IT Environment** shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on the behalf of that user.

5.2.3 FMT - Security Management

FMT_SMR.1(b) Security roles

FMT_SMR.1.1(b) The ~~TSF~~ **IT Environment** shall maintain the roles [**Administrator**].

FMT_SMR.1.2(b) The ~~TSF~~ **IT Environment** shall be able to associate users with roles.

5.2.4 FPT - Protection of the TSF

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The ~~TSF~~ **IT Environment** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The ~~TSF~~ **IT Environment** shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The ~~TSF~~ **IT Environment** shall be able to provide reliable time stamps for its own **and TOE** use.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level (EAL) 2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

[3] This requirement has been added to comply with U.S Interpretations #422 and #423.

Assurance Class	Assurance Components
Configuration Management (ACM)	ACM_CAP.2 Configuration items
Delivery and Operation (ADO)	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Development (ADV)	ADV_FSP.1 Informal Function Specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance Documents (AGD)	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Tests (ATE)	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability Assessment (AVA)	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

Table 4 EAL2 Assurance Components

5.3.1 Configuration Management (ACM)

5.3.1.1 Configuration Items (ACM_CAP.2)

5.3.1.1.1 ACM_CAP.2.1D

The developer shall provide a reference for the TOE.

5.3.1.1.2 ACM_CAP.2.2D

The developer shall use a CM system~~.~~

5.3.1.1.3 ACM_CAP.2.3D

The developer shall provide CM documentation.

5.3.1.1.4 ACM_CAP.2.1C

The reference for the TOE shall be unique to each version of the TOE.

5.3.1.1.5 ACM_CAP.2.2C

The TOE shall be labeled with its reference.

5.3.1.1.6 ACM_CAP.2.3C

The CM documentation shall include a configuration list.

5.3.1.1.7 International Interpretation #3

The configuration list shall uniquely identify all configuration items that comprise the TOE.[4]

[4] This requirement has been added to comply with International Interpretation #3

5.3.1.1.8 ACM_CAP.2.4C

The configuration list shall describe the configuration items that comprise the TOE.

5.3.1.1.9 ACM_CAP.2.5C

The CM documentation shall describe the method used to uniquely identify the configuration items.

5.3.1.1.10 ACM_CAP.2.6C

The CM system shall uniquely identify all configuration items.

5.3.1.1.11 ACM_CAP.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and Operation (ADO)

5.3.2.1 Delivery Procedures (ADO_DEL.1)

5.3.2.1.1 ADO_DEL.1.1D

The developer shall document procedures for delivery of the TOE or parts of it to the user.

5.3.2.1.2 ADO_DEL.1.2D

The developer shall use the delivery procedures.

5.3.2.1.3 ADO_DEL.1.1C

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

5.3.2.1.4 ADO_DEL.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

5.3.2.2.1 ADO_IGS.1.1D

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

5.3.2.2.2 ADO_IGS.1.1C

The **installation, generation and start-up** documentation shall describe **all** the steps necessary for secure installation, generation, and start-up of the TOE.[5]

5.3.2.2.3 ADO_IGS.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

[5] This requirement has been modified to comply with International Interpretation #51.

5.3.2.2.4 ADO_IGS.1.2E

The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal Function Specification (ADV_FSP.1)

5.3.3.1.1 ADV_FSP.1.1D

The developer shall provide a functional specification.

5.3.3.1.2 ADV_FSP.1.1C

The functional specification shall describe the TSF and its external interfaces using an informal style.

5.3.3.1.3 ADV_FSP.1.2C

The functional specification shall be internally consistent.

5.3.3.1.4 ADV_FSP.1.3C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

5.3.3.1.5 ADV_FSP.1.4C

The functional specification shall completely represent the TSF.

5.3.3.1.6 ADV_FSP.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.1.7 ADV_FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security requirements.

5.3.3.2 Descriptive high-level design (ADV_HLD.1)

5.3.3.2.1 ADV_HLD.1.1D

The developer shall provide the high level design of the TSF.

5.3.3.2.2 ADV_HLD.1.1C

The presentation of the high level design shall be informal.

5.3.3.2.3 ADV_HLD.1.2C

The high level design shall be internally consistent.

5.3.3.2.4 ADV_HLD.1.3C

The high level design shall describe the structure of the TSF in terms of subsystems.

5.3.3.2.5 ADV_HLD.1.4C

The high level design shall describe the security functionality provided by each subsystem of the TSF.

5.3.3.2.6 ADV_HLD.1.5C

The high level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

5.3.3.2.7 ADV_HLD.1.6C

The high level design shall identify all interfaces to the subsystems of the TSF.

5.3.3.2.8 ADV_HLD.1.7C

The high level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

5.3.3.2.9 ADV_HLD.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.2.10 ADV_HLD.1.2E

The evaluator shall determine that the high level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

5.3.3.3.1 ADV_RCR.1.1D

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

5.3.3.3.2 ADV_RCR.1.1C

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

5.3.3.3.3 ADV_RCR.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance Documents (AGD)

5.3.4.1 Administrator Guidance (AGD_ADM.1)

5.3.4.1.1 AGD_ADM.1.1D

The developer shall provide administrator guidance addressed to system administrative personnel.

5.3.4.1.2 AGD_ADM.1.1C

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

5.3.4.1.3 AGD_ADM.1.2C

The administrator guidance shall describe how to administer the TOE in a secure manner.

5.3.4.1.4 AGD_ADM.1.3C

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

5.3.4.1.5 AGD_ADM.1.4C

The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

5.3.4.1.6 AGD_ADM.1.5C

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

5.3.4.1.7 AGD_ADM.1.6C

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

5.3.4.1.8 AGD_ADM.1.7C

The administrator guidance shall be consistent with all other documentation supplied for evaluation.

5.3.4.1.9 AGD_ADM.1.8C

The administrator guidance shall describe all security requirements on the IT environment that are relevant to the administrator.

5.3.4.1.10 AGD_ADM.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence

5.3.4.2 User Guidance (AGD_USR.1)

5.3.4.2.1 AGD_USR.1.1D

The developer shall provide user guidance.

5.3.4.2.2 AGD_USR.1.1C

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

5.3.4.2.3 AGD_USR.1.2C

The user guidance shall describe the use of user-accessible security functions provided by the TOE.

5.3.4.2.4 AGD_USR.1.3C

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

5.3.4.2.5 AGD_USR.1.4C

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

5.3.4.2.6 AGD_USR.1.5C

The user guidance shall be consistent with all other documentation supplied for evaluation.

5.3.4.2.7 AGD_USR.1.6C

The user guidance shall describe all security requirements on the IT environment that are relevant to the user.

5.3.4.2.8 AGD_USR.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Security Testing (ATE)

5.3.5.1 Evidence of coverage (ATE_COV.1)

5.3.5.1.1 ATE_COV.1.1D

The developer shall provide evidence of the test coverage.

5.3.5.1.2 ATE_COV.1.1C

The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

5.3.5.1.3 ATE_COV.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.2 Functional testing (ATE_FUN.1)

5.3.5.2.1 ATE_FUN.1.1D

The developer shall test the TSF and document the results.

5.3.5.2.2 ATE_FUN.1.2D

The developer shall provide test documentation.

5.3.5.2.3 ATE_FUN.1.1C

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

5.3.5.2.4 ATE_FUN.1.2C

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

5.3.5.2.5 ATE_FUN.1.3C

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

5.3.5.2.6 ATE_FUN.1.4C

The expected test results shall show the anticipated outputs from a successful execution of the tests.

5.3.5.2.7 ATE_FUN.1.5C

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

5.3.5.2.8 ATE_FUN.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.3 Independent testing – sample (ATE_IND.2)

5.3.5.3.1 ATE_IND.2.1D

The developer shall provide the TOE for testing.

5.3.5.3.2 ATE_IND.2.1C

The TOE shall be suitable for testing.

5.3.5.3.3 ATE_IND.2.2C

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

5.3.5.3.4 ATE_IND.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.3.5 ATE_IND.2.2E

The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

5.3.5.3.6 ATE_IND.2.3E

The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.5.4 Strength of TOE security function evaluation (AVA_SOF.1)

5.3.5.4.1 AVA_SOF.1.1D

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

5.3.5.4.2 AVA_SOF.1.1C

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

5.3.5.4.3 AVA_SOF.1.2C

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

5.3.5.4.4 AVA_SOF.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.4.5 AVA_SOF.1.2E

The evaluator shall confirm that the strength claims are correct.

5.3.5.5 Developer vulnerability analysis (AVA_VLA.1)

5.3.5.5.1 AVA_VLA.1.1D

The developer shall perform **a vulnerability analysis.**[6]

5.3.5.5.2 AVA_VLA.1.2D

The developer shall **provide vulnerability analysis documentation.** [7]

5.3.5.5.3 AVA_VLA.1.1C

The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.[8]

[6] This requirement has been modified to comply with International Interpretation #51.
[7] This requirement has been modified to comply with International Interpretation #51.
[8] This requirement has been modified to comply with International Interpretation #51.

5.3.5.5.4 AVA_VLA.1.2C

The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.[9]

5.3.5.5.5 AVA_VLA.1.3C

The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. [10]

5.3.5.5.6 AVA_VLA.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.5.7 AVA_VLA.1.2E

The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

[9] This requirement has been added to comply with International Interpretation #51.
[10] This requirement has been added to comply with International Interpretation #51.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the necessary requirements.

6.1.1 Security Audit

FAU_GEN.1 Audit Data Generation

The TOE audits all activities performed by the administrator including changes of user and system access rights to specific devices. The following information is recorded:

- Date and time of change
- Domain and user name; author of change
- Domain and user name or group; change applicable to
- Target computer; if applicable
- Devices; changes are applicable to
- Permissions applied to device

I/O Shadowing enables full auditing of all data written to file-system based devices such as Recordable CD/DVD, floppy, Zip and PCMCIA drives, as well as to serial and parallel ports. All audit files are automatically transferred to the server at regular intervals as specified by the administrator.

The data transfer auditing logs the following information:

- File name of file copied to device
- Type of file
- Size of file
- Date and time file copied
- Date audit file transferred to server
- User name; user copying file
- Computer where file copied from
- Device file copied to

In addition to events and action listed above, the following events are also either audited or logged:

- Startup and shutdown of the audit function
- All modification to the behavior of the TSF
- All modifications of the default settings; restrictive values.
- All modifications to TSF data values, which includes the identification of the user who modified the data
- All attempts to revoke the security attributes

Furthermore, each audit and log record contains the following information: date and time the event occurred, the type of event, identity of the user, and the success or failure of the event.

FAU_GEN.2 User identity association

Each audit and log record generated is associated to the user that performed the actions that triggered the generation of an audit or log record.

FAU_SAR.1 Audit Review

The TOE provides the ability for the administrator to view audit data and the log data for the system. The audit and log records are viewable by the Sanctuary Device Console via the Shadow Files Explorer or the Audit Logs Viewer.

FAU_SAR.3 Selectable Audit Review

The Sanctuary Device Console provides the ability for the administrator to search and order the audit records generated by the date of the event. The Shadowing Information file(s) can be searched by filename, by users or user groups, a specific computer, or specific date.

6.1.2 Cryptographic Support

FCS_CKM.1(a)(b) Cryptographic key generation

The TOE uses a random number generator to generate the private-public (RSA asymmetric 2048 bit) key pair. The private-public key pairs are generated during installation of the TOE. The random number generator meets the ANSI X9.31-1998 standard.

The TOE uses a random number generator to generate the AES symmetric 256 bit key. The AES keys are generated when used to encrypt the removable media. The random number generator meets the FIPS 197 standard.

FCS_COP.1 Cryptographic operation

The TOE implements cryptographic functionality to protect communication between its client and server components. The TOE also implements cryptographic functionality to protect removable media.

Communication between the SecureWave Application Server and the Sanctuary Device Control Clients is protected by the use of private keys; though a digest of the message is created, the message itself is not encrypted. A hash of the message is appended and the entire package is signed by the private key of the server.

The protection is achieved through the use of cryptographic signatures combined with timestamps. A SHA-1 digest serves a fingerprint of the message that is to be transmitted; encrypting the fingerprint with an asymmetric encryption algorithm like RSA ensures that the sender can be verified. To tamper-proof its messages, SecureWave Application Server adds unique IDs to them in order to prevent replay attacks, generates a message digest (MAC) by running the message contents through SHA-1, and then encrypts the digest with the Rivest-Shamir-Adelman algorithm, using a 2048 bit key. The resulting encrypted digest is appended to the message. The SHA-1 digest serves as a fingerprint of the message that is to be transmitted. Encrypting the fingerprint with an asymmetric encryption algorithm ensures that the sender can be verified.

Media key (mkey) information is used to validate user requests for media decryption. The mkey is AES 256 compliant and is part of the TCP/IP packet. Keys are stored in BER format, a PKCS-standardized format. Media keys are themselves encrypted by the public key of the user’s certificate.

6.1.3 User Data Protection

FDP_ACC.2 Complete access control

When a new user logs on, the Sanctuary Device Control v3.2 will store a copy of user’s security attributes; user identity, user group, and permissions in its database. The user identity or user group attributes and the permissions are utilized by the Device Explorer as well as the I/O device ACL, to grant user access to I/O Devices.

FDP_ACF.1 Security attribute based access control.

The administrator assigns permission to users or user groups to use the supported I/O Devices. The options within the Device Explorer determine which devices users can use. Users or user groups can gain access to I/O Devices as long as they are identified in the I/O Device ACL and have the appropriate permissions. Permissions further define the functions a user is allowed to perform. Permissions include read-only access, copy limit, scheduled access, offline updates, file shadowing, media authorization, etc.

When a user logs onto a computer equipped with Sanctuary Device Control v3.2 Client, the client computer communicates with a SecureWave Application Server, and requests the list of the permissions for known devices. The SecureWave Application Server in turn communicates with the Database, and downloads a list of the devices the user is authorized to use. The SecureWave Application Server then forwards the list to the client computer. When the user logs on, the Sanctuary Device Control v3.2 Client Drive checks, and downloads if changed, the permissions from the SecureWave Application Server, which are then applied immediately.

In addition to the user identity and user group assigned to the I/O Device ALC, the authorized administrator can also restrict access to I/O Devices using the schedules access function that is based on days (Monday to Friday) and timeframe (from 8 AM to 5 PM). If the schedule access has been defined, when the user attempts to access the I/O Device, the day and time is checked. If access is within the allotted time on the for the current day, then access is granted. Otherwise access is denied.

The media authorizer function allows the authorized administrator to define permissions that recognize specific DVD/CD/removable media which users can be permitted to use, even where they have not been granted access rights to access the DVD/CD/removable media drive, as well as establish specific encrypted removable media which users can be permitted to use. Authorized Administrator scans the DVD/CD/removable media and enters its details into the Database of Authorized DVD/CD/removable media. When this action is finished, the DVD/CD/ removable media are ready to be assigned to a user or group, define its permissions, and be used in the organization. When a DVD/CD/removable media is scanned, the Media Authorizer calculates a checksum. When a DVD/CD/removable media is inserted into a client computer, the driver verifies the checksum. If it coincides with the Authorized DVD/CD/removable media that the user is allowed to access, then the DVD/CD/removable is made available. If the checksum and label do not correspond, access will be denied, thus preventing the use of unauthorized DVD/CD/removable media.

To encrypt removable media the authorized administrator must add the device to the media authorizer much in the same manner as any other DVD/CD/removable media, except an encryption method is chosen; Full & Slow (secure for existing data) to encrypt the media while preserving any file written to the media, Quick Format (insecure for existing data) to quickly encrypt the device, or Easy Exchange (insecure for existing data): to quickly encrypt the device with the added advantage of being able to access the device in computers that do not have the Sanctuary Client installed. Permissions to encrypted removable media can only be assigned to users and not groups. In addition, read-only cannot be assigned as a permission to encrypted media. When a user has received the proper access rights to encrypted media, the Sanctuary Client provides a transparent access to the media. Data copied to the media is encrypted/decrypted transparently upon media access. If the encrypted removable media is to be shared outside the organization, the encryption key is normally exported to the device itself and is password protected. The authorized administrator would then have to communicate the key and the password to the authorized user.

6.1.4 Identification and Authentication

FIA_ATD.1 User Attribute Definition

The Database stores authorization information associated with the user and user groups. The Database associates each user's identification; SID, with the list of I/O Devices, and the permissions granted the user and user group. This information is utilized to determine which I/O Devices authorized users, user group are allowed to access and the functions they can perform.

Accounts on the TOE contain the following attributes: user identity and user group.

6.1.5 Security Management

FMT_MSA.1 Management of security attributes

The Sanctuary Device Console provides the administrator with the ability to manage the permissions assigned to the users and user groups, and the I/O devices to which they have access. Access to the management functions is restricted to the authorized administrators.

FMT_MSA.2 Secure security attributes

When an authorized user or authorized administrator deems removable media needs to be encrypted the authorized user or authorized administrator can export its encryption key, either by creating a password-protected encryption key file that can be sent to another computer or user, or by writing the encryption key to the media, where it will also be password-protected. The Sanctuary Device Console ensures that the password that is used to protect the exported key meets the complexity rules. The password must be at least 8 characters long, contain upper case and lower case letters, contain numbers, and contain at least one non-alphabetical character (!@#$%*...).

FMT_MSA.3 Static attribute initialization

Sanctuary Device Control v3.2 controls access to devices by applying an Access Control List (ACL) to each device type. Based on the Least Privilege Principle, device access for all users is not allowed by default. To grant access, the administrator associates users or user groups to the devices. Access to the management functions is restricted to the authorized administrators.

FMT_MTD.1(a)(b) Management of TSF Data

The Sanctuary Device Console administration interface provides the abilities for authorized administrators to perform the following tasks:

- To query, and subsequently view the audit logs and the Shadowing Information file. Access to the management functions is restricted to the authorized administrators.
- The ability to assign or delete a user to the Administrator role is restricted to the Enterprise Administrator

FMT_REV.1 Revocation

The Sanctuary Device Console provides the administrator with ability to enable or disable the permissions of a user and/or user group access to I/O Devices on the computer and/or domain level I/O Devices. When changes are made that affect access rights, the changes are implemented upon next logon.

FMT_SMF.1 Specification of Management Functions

The Sanctuary Device Console consists of five modules. These modules are used to configure Sanctuary Device Control v3.2 and carry out day-to-day administration. The five modules provide the following management functions:

- Review of Audit
- Review of Shadowing Information files
- Management of users and user groups (modify, create, delete)
- Management of I/O Device ALC (modify, create, delete)

FMT_SMR.1(a) Security Roles

By default all members of the local administrators group of the computer where SecureWave Application Server is installed are also Sanctuary Device Control v3.2 administrators. There must be at least one Enterprise Administrator defined. When the first user is assigned to the Enterprise Administrator role, the other users in the local Administrators group no longer have administrative privileges on the TOE. The Enterprise Administrator can then assign users to the Administrator role as necessary. The Enterprise Administrator and the Administrator are given the privilege to perform all administrative actives that are provided by the Sanctuary Device Console. The difference is that only the Enterprise Administrator is capable of assigning a user to the administrator group.

6.1.6 Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

The TOE ensures that the I/O device permission list is protected from modification by attaching an encrypted message digest to the listing. If the verification of the signature by Sanctuary Device Control v3.2 Client fails, the data is ignored. The Sanctuary Device Control v3.2 Client will use the local I/O device permission list until a valid I/O device permission list is received from the SecureWave Application Server.

FPT_RVM.1 Non-bypassability of the TSP

The TOE restricts all access to the I/O Device to which the user has not been granted access. If the list is somehow deleted, then the user is denied access. This can only be bypassed by deleting the Sanctuary Device Control v3.2's client driver from the computer.

6.1.7 Resource Utilization

FRU_FLT.1 Degraded Fault Tolerance

SecureWave Application Server provides the listings that determine the permissions of the users to the client's computer. When the client's computer cannot communicate with the SecureWave Application Server, it will be operated in a standalone mode and utilizing the copy of the listings that were placed in a secure area on the hard disk of the computer. The Sanctuary Device Control v3.2 Client will utilize this listing until connection is reestablished and a new logon is performed or changes to the permissions were made.

6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL2 assurance requirements:

- Process Assurance;
- Delivery and Guidance;
- Design Documentation;
- Tests; and
- Vulnerability Assessment.

6.2.1 Process Assurance

6.2.1.1 Configuration Management

The configuration management measures applied by SecureWave ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. SecureWave ensures changes to the implementation representation are controlled and that TOE associated configuration item modifications are properly controlled. SecureWave performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, and the CM documentation. These activities are documented in:

- SecureWave Software Configuration Management, 2.0, 4 June 2006

The Configuration Management assurance measure satisfies the ACM_CAP.2 assurance requirements

6.2.2 Delivery and Guidance

6.2.2.1 Delivery and Operations

SecureWave provides delivery documentation that explains how the TOE is delivered and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. SecureWave's delivery procedures describe the steps to be used for the secure installation, generation, and start-up of the TOE along with configuration settings to secure the TOE privileges and functions. These procedures are documented in:

- ADO_DEL.1 SecureWave Delivery Procedures, 20 October 2003

SecureWave provides guidance in the installation and initialization procedures for Sanctuary Device Control v3.2. The installation and generation procedures, included in the installation guidance, describe the steps necessary to install and operate Sanctuary Device Control v3.2 products in accordance with the evaluated configuration, detailing how to establish and maintain the secure configuration.

The installation guidance is documented in:

- Sanctuary Suite Setup Guide, 3.2.0, April 2006

The Delivery and Operations assurance measure satisfies the following Assurance requirements:

- ADO_DEL.1;
- ADO_IGS.1;

6.2.2.2 Administrative and User Guidance

SecureWave provides administrator guidance on how to utilize the TOE security functions, other administrative functions and warnings to authorized administrators about actions that can compromise the security of the TOE. The procedures, included in the administrator guidance, describe the steps necessary to operate Sanctuary Device Control v3.2 in accordance with the evaluated configuration, detailing how to establish and maintain the secure configuration. Since the only users with an interface are administrators, that is the only guidance provided.

The administrator guidance is documented in:

- SecureWave Sanctuary Device Control Administrator’s Guide, 3.2.0, April 2006

The Guidance assurance measure satisfies the following Assurance requirements:

- AGD_ADM.1,
- AGD_USR.1.

6.2.3 Development

The Design Documentation provided for Sanctuary Device Control v3.2 is provided in two documents:

- SecureWave EAl2 Functional Specification Sanctuary Device Control, 1.7, 27 July 2006
- SecureWave High-level Design, 0.92, 27 July 2006

These documents serve to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST). The Design Documentation security assurance measure satisfies the following security assurance requirement:

- ADV_FSP.1;
- ADV_HLD.1; and,
- ADV_RCR.1.

6.2.4 Tests

The Test Documentation is found in the following documents:

- SecureWave QA Test Plan Structure & Strategy, 1.1, 18 January 2006
- SecureWave QA Test Environment Setup, 1.2, 14 March 2006
- SDC Test Plan, 4 July 2006
- Mapping, 5 April 2006

- SecureWave Test Specification

These documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

The Tests assurance measure satisfies the following assurance requirements:

- ATE_COV.1;
- ATE_FUN.1; and,
- ATE_IND.2.

6.2.5 Vulnerability Assessment

There are no probabilistic or permutational mechanisms included in the TOE for which a strength of function claim is appropriate. Therefore, a SOF analysis is not applicable to the TOE.

Sanctuary Device Control v3.2 performed a vulnerability analysis of the TOE to identify weaknesses that can be exploited in the TOE. The vulnerability analysis is documented in:

- SecureWave Vulnerability Analysis, 0.1, 14 September 2005

The Vulnerability Assessment assurance measure satisfies the following assurance requirements:

- AVA_SOF.1; and,
- AVA_VLA.1.

7. Protection Profile Claims

This TOE does not claim conformance to a Protection Profile.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- TOE Summary Specification;
- Security Functional Requirement Dependencies; and
- Internal Consistency.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, security threats and organizational security policies are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption or organizational security policy.

8.1.1 Security Objective for the TOE Rationale

Table 5 Mapping of TOE Security Objectives to Threats or Organizational Security Policies provides a mapping of TOE security objectives to those threats that the security objectives that the TOE is designed to counter and organizational security policies that the TOE must enforce.

TOE Security Objectives	Threats and Organizational Policies
O.AUDIT	T.ACCOUNTABILITY T.DATA_CORRUPT
O.CONTROL	T.ACCESS T.PRIVILEGE
O.DATA_TRANSFER	T.TRANSIT
O.FAULT_TOLERANCE	T.FAULT_TOLERANCE
O.MANAGE	T.ACCESS T.ACCOUNTABILITY T.PRIVILEGE

Table 5 Mapping of TOE Security Objectives to Threats or Organizational Security Policies

The following objectives will address the threats and organizational policies listed in the ST.

O.AUDIT – This objective counters the threat T.ACCOUNTABILITY, by ensuring that all relevant TOE security actions are recorded. This objective also counters the threats T.DATA_CORRUPT by restricting access to all audit records and shadow files to only authorized users.

O.CONTROL - This objective counters the threat T.ACCESS by ensuring access is only granted if the subject is authorized access. Access to the TOE and its protected resources is based on the subject's identification. Further, this objective counters the threat T.PRIVILEGE by ensuring access to resources and I/O Devices is explicitly granted, preventing an unauthorized user from gaining access to a resource or I/O Device.

O.DATA_TRANSFER – This objective counters the threat, T. TRANSIT by ensuring the TOE detects modifications made to the file signatures transmitted between the SecureWave Application Server and the Sanctuary Device Control v3.2 Client.

O.FAULT_TOLERANCE – This objective counters the threat T.FAULT_TOLERANCE by ensuring that the access control functions of the TOE will continue to operate if the Sanctuary Device Control v3.2 Client losses communications with the SecureWave Application Server.

O.MANAGE – This objective ensures that TOE provides the functions and tools necessary to support the authorized administrator in managing TOE. The objective assists in countering T.ACCESS, T.ACCOUNTABILITY, and T.PRIVILEGE by requiring the TOE to provide functionality to support the management of audit, access protection and other administrative functions..

8.1.2 Security Objectives for Environment Rationale

8.1.2.1 Security Objectives for the IT Environment Rationale

Table 6 Security objectives for the IT environment mapped to assumptions identifies security objectives for the IT environment in which the TOE is designed to operate and provides a mapping to assumptions that are made about that environment.

TOE Security Objectives for the IT Environment	Assumptions
OE.AUTH_ACCESS	T.ACCESS
OE.ENV_ADMIN	T.ACCESS T.ACCOUNTABILITY T.PRIVILEGE
OE.SEP	T.ACCESS T.PRIVILEGE
OE.TIME_SOURCE	T.ACCOUNTABILITY

Table 6 Security objectives for the IT environment mapped to assumptions

OE.AUTH_ACCESS - This objective ensures that only authorized administrators have access to the TOE, thus countering T.ACCESS.

OE.ENV_ADMIN - This objective is to ensure that an IT environment administrator is able to manage the TOE until the TOE administrators are specially assigned to manage the Administrative Tools component of the TOE. As a result, this objective assists in mitigating the threat T.ACCESS by ensuring access is only granted if the user is authorized, T.ACCOUNTABILTY by recording all relevant TOE security actions, and T.PRIVILEGE by ensuring that only authorized users gain access to the TOE and its resources..

OE.SEP - This objective provides the support needed by the TOE to counter threats T.ACCESS and T.PRIVILEGE by ensuring that the TOE cannot be tampered with or bypassed.

OE.TIME_SOURCE - The IT environment must provide a reliable time source for the TOE to provide a reliable timestamp for all audit records ensuring T.ACCOUNTABILITY is addressed.

8.1.2.2 Security Objectives for the Non-IT Environment Rationale

Table 7 Security objectives for the non-IT environment mapped to assumptions identifies security objectives for the non-IT environment in which the TOE is designed to operate and provides a mapping to assumptions that are made about that environment.

TOE Security Objectives for the Non-IT Environment	Assumptions
OE.INSTALL	A.HARDWARE A.MANAGE
OE.PERSON	A.NOEVIL A.MANAGE
OE.PHYCAL	A.CONNECT

TOE Security Objectives for the Non-IT Environment	Assumptions
	A.PROTECT

Table 7 Security objectives for the non-IT environment mapped to assumptions

OE.INSTALL – This objective ensures the TOE is delivered, properly installed, managed, and operated in a secure manner to protect both itself and its resources addresses the assumption A.HARDWARE and A.MANAGE.

OE.PERSON - This objective ensures that competent, trained personnel operate the TOE in a secure manner, which addresses A.NOEVIL and A.MANAGE assumptions.

OE.PHYCAL - This objective ensures that the TOE is operated in an environment that will protect it from unauthorized access and physical threats and attacks that can disturb and corrupt the information generated. This objective addresses A.CONNECT and A.PROTECT.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target.

The purpose for the environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of TOE in meeting security needs.

8.2.1 Security Functional Requirements Rationale

Table 8 SFRs mapped to Security Objectives provides the correspondence mapping between security objectives for the TOE and the security functional requirements that satisfy them.

SECURITY FUNCTIONAL REQUIREMENT	O.AUDIT	O.CONTROL	O.DATA_TRANSFER	O.FAULT_TOLERANCE	O.MANAGE	OE.AUTH_ACCESS	OE.ENV_ADMIN	OE.SEP	OE.TIME_SOURCE
FAU_GEN.1	X								
FAU_GEN.2	X								
FAU_SAR.1	X								
FAU_SAR.3	X								
FCS_CKM.1(a)			X						
FCS_CKM.1(b)		X							
FCS_COP.1		X	X						
FDP_ACC.2		X							
FDP_ACF.1		X							
FIA_ATD.1		X							
FIA_UID.2						X			
FIA_UAU.2						X			
FMT_MSA.1					X				
FMT_MSA.2		X			X				

SECURITY FUNCTIONAL REQUIREMENT	O.AUDIT	O.CONTROL	O.DATA_TRANSFER	O.FAULT_TOLERANCE	O.MANAGE	OE.AUTH ACCESS	OE.ENV ADMIN	OE.SEP	OE.TIME SOURCE
FMT_MSA.3					X				
FMT_MTD.1(a)	X				X				
FMT_MTD.1(b)					X				
FMT_REV.1					X				
FMT_SMF.1	X				X				
FMT_SMR.1(a) (b)					X		X		
FPT_ITT.1			X						
FPT_RVM.1		X							
FPT_SEP								X	
FPT_STM									X
FRU_FLT.1				X					

Table 8 SFRs mapped to Security Objectives

O.AUDIT

FAU_GEN.1 and FAU_GEN.2 define the TOE events that will be audited, along with the details that will be recorded along with the event.

FAU_SAR.1 restricts access to the audit trail to authorized administrators, and FAU_SAR.3 provides them a method for viewing the data according to various criteria.

FMT_MTD.1(a) ensures that the ability to query, and subsequently view the audit data and Shadow Information file is restricted to the authorized administrators.

FMT_SMF.1 The TOE also provides a set of tools that are accessible to the administrator to review the audit and the Shadowing Information file(s).

O.CONTROL

FIA_ATD.1 defines the security attributes that are associated with individual users.

FCS_CKM.1(b) and FCS_COP.1 define the symmetric encryption system that is used to establish specific (encrypted) removable media which users can be permitted to use.

FDP_ACC.2 ensures subjects and objects within the TOE are under the enforcement of the Management Access Control policy. All operations between the subjects and objects are controlled by the Management Access Control policy.

FDP_ACF.1 requires subjects and objects under the Management Access Control policy have certain rules that apply to all accesses between them. All access is controlled by decisions based on user identity or user group and the ACL on the objects.

FMT_MSA.2 ensures that only secure values are accepted for the password-protected encryption key file of encrypted removable media. Users must be granted access to the removable media as well as the proper permissions that enable the functions to allow them to perform the functions to encrypt removable media.

FPT_RVM.1 ensures that the TOE allows access to protected objects only after it makes informed access decision.

O.DATA_TRANSFER

FCS_CKM.1(a) and FCS_COP.1 define the generated public-private key pair and the asymmetric encryption system that the SecureWave Application Servers uses to communicate with the Sanctuary Device Control v3.2 Client Driver.

FPT_ITT.1 ensures the TSF is able to detect if the TSF data has been modified when it is transmitted between separate parts of the TOE. The TSF verifies the signature on the transmitted data and if the signature cannot be verified, the TSF data is ignored; hence the TSF protects the TSF data from modification.

O.FAULT_TOLERANCE

FRU_FLT.1 requires that the TOE will continue to enforce the Management Access Control policy in the event of a communication failure with the SecureWave Application Servers.

O.MANAGE

FMT_MSA.2 ensures that only secure values are accepted for the password-protected encryption key file of encrypted removable media. Administrators must grant users access to the removable media as well as the proper permissions that enable the functions to allow them to perform the functions to encrypt removable media.

FMT_MSA.3 requires restrictive default settings for new users, user groups, and I/O Devices.

FMT_MTD.1(a) provides the ability for the administrator to query, and subsequently view the audit and Shadow Information file data.

FMT_MTD.1(b) requires the ability to assign and/or delete a user to the Administrator role is restricted to the Enterprise Administrator.

FMT_REV.1 provides the administrator with the ability to revoke user access on, which will take effect upon the next login.

FMT_SMR.1(a) requires the TOE to provide the ability to set roles for security relevant authority; Enterprise Administrator and Administrators.

FMT_SMF.1 requires that the TOE provide the ability to manage its security functions including the management of access control, management of users and groups, and management of the audit trail and I/O Shadow file.

OE.AUTH_ACCESS

FIA_UID.2 and FIA_UAU.2 require a user be identified and authenticated before any access to the TOE and TOE-protected resources is allowed.

OE.ENV_ADMIN

FMT_SMR.1(b) ensures that TOE operating environment defines the administrator role (Enterprise Administrator), thus providing the authorized administrators who will have access to the TOE and its associated data.

OE.SEP

FPT_SEP.1 ensures that the IT Environment protect the TOE from untrusted process that could attempt to tamper with or bypass the TSF.

OE.TIME_SOURCE

FPT_STM.1 ensures the IT environment provides a reliable time stamp that will be available to the TOE.

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL2 assurance package. EAL 2 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. SecureWave Sanctuary Device Control v3.2 is targeted at an environment with good physical access security (OE.PHYCAL) and competent administrators (A.NOEVIL, A.MANAGE, OE.PERSON, OE.INSTALL), where EAL 2 should provide adequate assurance. Within such environments it is assumed that attackers will have little attack potential. As such, EAL2 is appropriate to provide the assurance necessary to counter the limited potential for attack.

8.4 Requirement Dependency Rationale

The ST satisfies all the requirement dependencies of the Common Criteria, except as noted below. **Table 9 Requirement Dependency Rationale** lists each requirement from TOE Security Functional Requirements with a dependency and indicates which requirement was included to satisfy the dependency, if any.

Functional Requirement	Dependencies	Dependency Met
FAU_GEN.1	FPT_STM.1	✓(Environment)
FAU_GEN.2	FAU_GEN.1	✓
	FIA_UID.1	✓(FIA_UID.2)
FAU_SAR.1	FAU_GEN.1	✓
FAU_SAR.3	FAU_SAR.1	✓
FAU_STG.1 (IT Environment)	FAU_GEN.1	✓
FCS_CKM.1(a)(b)	FCS_CKM.2 or FCS_COP.1	✓(FCS_COP.1)
	FCS_CKM.4	Rationale provided below
	FMT_MSA.2	✓
FCS_COP.1	FDP_ITC.1 or FCS_CKM.1	✓(FCS_CKM.1(a)(b))
	FCS_CKM.4	Rationale provided below
	FMT_MSA.2	✓
FDP_ACC.2	FDP_ACF.1	✓
FDP_ACF.1	FDP_ACC.1	✓
	FMT_MSA.3	✓
FIA_ATD.1	No dependencies	
FIA_UID.2 (IT Environment)	No dependencies	
FIA_UAU.2 (IT Environment)	FIA_UID.1	✓(FIA_UID.2)
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	✓(FDP_ACC.2)
	FMT_SMF.1	✓
	FMT_SMR.1	✓
FMT_MSA.2	FDP_ACC.2	✓
	FMT_MSA.1	✓
	FMT_SMR.1	✓
FMT_MSA.3	FMT_MSA.1	✓
	FMT_SMR.1	✓
FMT_MTD.1(a)(b)	FMT_SMF.1	✓
	FMT_SMR.1	✓
FMT_REV.1	FMT_SMR.1	✓
FMT_SMF.1	No dependencies	
FMT_SMR.1(a)(b)	FIA_UID.1	✓(FIA_UID.2)
FPT_ITT.1	No dependencies	
FPT_RVM.1	No dependencies	
FPT_SEP.1 (IT Environment)	No dependencies	
FPT_STM.1 (IT Environment)	No dependencies	

Functional Requirement	Dependencies	Dependency Met
FRU_FLT.1	FPT_FLS.1	Rationale provided below

Table 9 Requirement Dependency Rationale

For FCS_CKM.1(a)(b) and FCS_COP.1 requirements, the CC identifies the following dependency of FCS_CKM.4. The dependency for this requirement is not applicable for this TOE. Following is the justification for not including this requirement:

> FCS_CKM.4: this requirement is for key destruction that is applicable to cryptographic operations that rely upon the secure management of keys. For this TOE, there is only one key pair that is generated. SecureWave Application Server uses an asymmetric encryption system to communicate with the Sanctuary Device Control Clients. This key pair is only generated once during the installation and is utilized until the TOE is uninstalled from the system, where the process deletes that associated key file. The keys that are used to encrypt removable media are created at the time when the removable media is encrypted. The keys are only destroyed when the data on the encrypted media is no longer needed. Destroying the keys that encrypted the removable media could render the media unaccessible depending on the method used to encrypt the media. Therefore keys are only destroyed (deleting the key file) when the data on the encrypted media is no longer needed.

For FRU_FLS.1, the FPT_FLS.1 dependency was not included in the ST, because the requirement addresses the preservation of a secure state. The SecureWave Application Server component of the TOE enforces the Management Access Control SFP policy regardless of the state of the computer. The removal or corruption of the listing would cause the SFP to be enforced as the TOE without the presence of valid listing will deny all access to the devices, thus the requirement to preserve a secure state is not applicable to this TOE.

8.5 Internal Consistency Rationale

The ST includes no instance of a requirement that contradicts another requirement in the ST. In instances where different requirements apply to the same events or types of data, the requirements and the operations performed within the requirements do not contradict each other, but provide supporting functionality ensuring that the TOE is internally consistent.

The combination of several different supporting security functions and the inclusion of all dependencies as illustrated in **Table 9 Requirement Dependency Rationale** ensures that together the selected requirements form a mutually supportive whole. The following items also support this claim:

- Mapping and suitability of the requirements to security objectives (as justified in **Table 8 SFRs mapped to Security Objectives**);
- Inclusion of audit requirements to detect attacks of other security functional requirements; and
- Inclusion of security management requirements to ensure proper configuration and control of other security functional requirements.

8.6 Strength of Function Rationale

The TOE includes security functional requirements that have a specific strength of function metrics. Of those requirements; FCS_CKM.1(a)(b) and FCS_COP.1 are cryptographic mechanisms, which is outside the scope of the evaluation. The TOE does not identify any other functions that are of a permutational or probabilistic nature. Therefore, a minimum SOF claim is not included for the TOE.

8.7 TOE Summary Specification Rationale

Each subsection in TOE Summary Specification describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security and assurance requirements.

Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section, in conjunction with TOE Summary Specification provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE Summary Specification are all necessary for the required security functionality in the TSF. **Table 10 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

REQUIREMENT	SECURITY AUDIT	CRYPTOGRAPHIC SUPPORT	USER DATA PROTECTION	IDENTIFICATION AND AUTHENTICATION	SECURITY MANAGEMENT	PROTECTION OF THE TSF	RESOURCE UTILIZATION
FAU_GEN.1	X						
FAU_GEN.2	X						
FAU_SAR.1	X						
FAU_SAR.3	X						
FCS_CKM.1(a)		X					
FCS_CKM.1(b)		X					
FCS_COP.1		X					
FDP_ACC.2			X				
FDP_ACF.1			X				
FIA_ATD.1				X			
FMT_MSA.1					X		
FMT_MSA.2					X		
FMT_MSA.3					X		
FMT_MTD.1(a)					X		
FMT_MTD.1(b)					X		
FMT_REV.1					X		
FMT_SMF.1					X		
FMT_SMR.1(a)					X		
FPT_ITT.1						X	
FPT_RVM.1						X	
FRU_FLT.1							X

Table 10 Security Functions vs. Requirements Mapping

9. Terminology and Acronyms

Following is the list of terms and acronyms that is used throughout the ST.

CAB

File extension for cabinet 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.

CD/DVD

Compact Disk - Read Only Memory. Digital Versatile Disc (originally, Digital Video Disc) An optical storage medium that provides greater capacity and bandwidth than CD-ROM; DVDs are frequently used for multimedia as well as data storage.

CD-ROM

Compact Disk - Read Only Memory. A drive that reads CD-ROMs. It may be installed in the computer or removable.

Client Computer

The computers on the network that Sanctuary Device Control v3.2 controls.

DAO

Disc-at-once mode. A CD’s recording mode.

Direct cable connection (DCC)

A RAS networking connection between two computers, or between a computer and a Windows CE–based device, which uses a serial or parallel cable directly connected between the systems instead of a modem and a phone line.

EAL

Evaluation Assurance Level

Executable Program

A program that can be run. The term usually applies to a compiled program translated into machine code in a format that can be loaded in memory and run by a computer's processor.

FIPS

Federal Information Processing Standard

I/O

Input/Output

IOCP

I/O Completion Port

LAN

Local Area Network

MDAC

Microsoft Data Access Components. Required by Windows NT4 computers to connect to SQL Server 7 and MSDE databases.

Mkey

Media key – a key used in SDC to decrypt media.

MSDE

Microsoft SQL Server Desktop Engine. Either MSDE 1.0 or MSDE 2000 can be used with Sanctuary Device Control v3.2.

MSI

Windows Installer Package utilized to install the components for the TOE.

NT 4.0

Microsoft Windows NT 4.0 Operating System

PCMCIA

Personal Computer Memory Card International Association card. A lightweight, removable module about the size of a credit card that adds features to a portable computer. Its official name is the PC Card. A PCMCIA card may add memory, modem and networking capability, a radio transceiver, more hard drive space, or enhanced sound.

PDA

Personal Digital Assistant. Refers to a wide variety of handheld and palm-size PCs, electronic organizers, Smartphones, and pagers. A pocket-sized personal computer. PDAs usually can store phone numbers, appointments, and to-do lists. Some PDAs have a small keyboard, others have only a special pen that is used for input and output. A PDA can also have a wireless fax modem. Files can be created on a PDA, which are later entered into a larger computer.

PP

Protection Profile

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.

RSA

Rivest-Shamir-Adelman. An asymmetric encryption algorithm. In the context of SAC and SDC, its interesting property is that data can be *encrypted* with a secret key and *decrypted* with a public key; the public key need not be kept safe from prying eyes, and successful decryption at a receiver's indicates that the sender was in possession of the secret key.

RTnotify

Displays protection status and permission changes on the end-user's computer.

SAO

Session-At-Once. A CD’s recording mode.

SCC

Sanctuary™ Command Control (scomc.exe), a user-mode component that is in charge of all communication between the server and the client(s); also referred to as Sanctuary™ Command and Control or Sanctuary™ Command & Control.

SDC

Sanctuary™ Device Control

SDC[11]

Sanctuary™ Device Console – the primary administrative interface to → SecureWave Application Server and the client drivers.

SHA-1

Secure Hash Algorithm 1. A method to generate a "digest", of fixed length, corresponding to the original data. The important attribute of this digest is the difficulty of finding a different input text that will give the same digest; therefore, if the digest can be protected against unauthorized alteration, it can be used to check whether the input text was changed.

Shadow File Explorer

The feature used to see which files (shadowing information) have been copied from a PC to an authorized device.

SID

Security ID

SFP

Security Function Policy

SFR

Security Function Requirement

SK

The Sanctuary™ Kernel Driver, the client component that runs as a kernel driver; also referred to as the Sanctuary™ Client Driver and the Sanctuary™ Client Kernel Driver.

SQL Server 7

The industry standard database server; Microsoft SQL Server 7, supported by Sanctuary Device Control v3.2.

ST

Security Target

SXS

SecureWave Application Server

TAO

Track-At-Once. A CD's recording mode.

TCP/IP

The protocol used by the client computers to communicate with the SecureWave Application Servers.

TOE

Target of Evaluation

TSF

TOE Security Functions

TSP

TOE Security Policy

TSC

TSF Scope of Control

[11] Due to the nature of two different concepts sharing the same acronym, SDC will be used to refer to Sanctuary™ Device Control; the console for SDC will be referred to as the Sanctuary Device Console.

Unauthorized User

A user that is not authorized access to the TOE, TOE functions, and TOE data.

USB

Universal Serial Bus. A computer bus which can support up to 127 peripheral devices in a daisy chain configuration including printers, digital cameras, keyboards and mice, and storage devices.

Windows 2000

Microsoft Windows 2000 Operating System

XP

Microsoft Windows XP Operating System

ZIP

Zigzag In-line Package/pin. ZIP Drive - A small, lightweight, portable disk drive from Iomega, which uses 100, 250-megabyte 3.5" removable cartridges. ZIP Disk - A 3.5" removable cartridge used with the Iomega Zip drive. Zip disks can store 25-250MB, and are used to back up data or transfer data from one computer to another.