SAFEND PROTECTOR™
Security Target

VERSION 1.98

21 JULY 2008

REF: CC-ST

PREPARED FOR:

Safend Ltd.
2 Penn Center
Suite 300
Philadelphia, PA 19102

DOCUMENT CONTROL

DOCUMENT HISTORY

Version	Date	Description
1.0	25 May 2006	initial version
1.1	5 July 2006	modified in response to VID10177-MR-0001 (29 May 2006)
1.2	3 August 2006	modified in response to VID10177-MR-0002 (17 July 2006)
1.3	10 September 2006	modified in response to VID10177-MR-0003 (10 August 2006)
1.4	6 October 2006	modified in response to VID10177-MR-0004 (12 September 2006)
1.5	11 October 2006	modified in response to VID10177-MR-0004 (11 October 2006)
1.6	25 January 2007	modified in response to ASE-ETR Version 1.0 (28 December 2006)
1.7	16 April 2007	modified in response to ADV-ETR Version 1.0 (21 March 2007)
1.8	28 August 2007	modified in response to ADV-ETR Version 2.0 (26 June 2007)
1.9	14 October 2007	modified in response to ADV-ETR Version 3.0 (24 September 2007)
1.91	30 November 2007	further modifications to address ASE-ETR 3.0 (24 September 2007)
1.92	30 January 2008	modified in conjunction with FSP update
1.93	7 March 2008	modified in response to ADV-FSP-ETR v3.0 (27 February 2008)
1.95	22 April 2008	modified to correct document references and supported configurations
1.96	12 June 2008	modified to address issues from result of Final Validation Oversight Review
1.97	17 June 2008	added some descriptions regarding tamper protection and protection against bogus clients
1.98	21 July 2008	final changes to address validator comments

All product and company names are used for identification purposes only and may be trademarks of their respective owners.

NOTES ON THE DOCUMENT

In this document, the pronouns “his” and “him” are meant to be understood in their non-gender specific sense, in conformance with the traditional rules of English grammar. In other words, “his” means “his or hers” and “him” means “him or her”.

TABLE OF CONTENTS

1.1 Overview 10
1.2 ST Identification 10
1.3 Conformance Claims 10
1.4 Document Organization 10
1.5 Conventions and Terminology 11
1.6 Abbreviations 12
2 TOE Description 13
2.1 Section Overview 13
2.2 TOE Description 13
2.2.1 TOE Overview 13
2.2.2 Safend Protector Features 13
2.2.3 Digital Membrane Technology 14
2.2.4 Kernel-Layer Approach 14
2.2.5 Granular Control 15
2.2.6 Positive Security Approach 15
2.2.7 Overlapping Protection Policies 15
2.2.8 Endpoint User Interaction 16
2.2.9 Protection Policy Updates 16
2.2.10 Auditing (Logging and Alerting) 16
2.2.11 Continuous Monitoring 17
2.2.12 Anti-Tampering 17
2.2.13 Protection Policy Suspension 17
2.2.14 TOE Client Uninstall 17
2.3 TOE Architecture 17
2.4 Evaluated Configuration 18
2.5 TOE Environment 19
2.5.1 Physical Boundary 19
2.5.2 Logical Boundary 19
2.6 Inter-Component Communication 20

2.6.1 TOE Client Software Distribution 21

2.6.2 TOE Client Protection Policy Distribution 22

2.6.3 TOE Client Audit Records 22

2.6.4 TOE Client Alerts 22

2.7 TOE System Requirements 22

2.7.1 Deliverables 23

2.8 TOE-Specific Terminology 23

3 Security Environment 25

3.1 Threats 25

3.1.1 Assets 25

3.1.2 Threat Agents 25

3.1.3 Threats Countered by the TOE 25

3.2 Organizational Security Policies 26

3.3 Assumptions 26

4 Security Objectives 27

4.1 Security Objectives for the TOE 27

4.2 Security Objectives for the IT Environment 27

4.3 Security Objectives for the non-IT Environment 28

5 IT Security Requirements 29

5.1 TOE Security Functional Requirements 29

5.1.1 FAU_ARP_EXP.1 – Security Alerts 30

5.1.2 FAU_GEN.1 – Audit Data Generation 30

5.1.3 FAU_SAR.1 – Audit Review 31

5.1.4 FAU_SAR.2 – Restricted Audit Review 31

5.1.5 FAU_SAR.3 – Selectable Audit Review 31

5.1.6 FAU_SEL.1 – Selective Audit 31

5.1.7 FAU_STG.1A – Protected Audit Trail Storage 31

5.1.8 FDP_ACC.1A – Subset Access Control (Ports) 31

5.1.9 FDP_ACC.1B – Subset Access Control (Storage Devices) 31

5.1.10 FDP_ACF.1A –Security Attribute Based Access Control (Ports) 31

5.1.11 FDP_ACF.1b –Security Attribute Based Access Control (Storage Devices) 32

5.1.12 FIA_UID.2A – User Identification Before Any Action 33
5.1.13 FMT_MOF.1 – Management of Security Function Behaviour 33
5.1.14 FMT_MTD.1A – Management of TSF Data (Selected Audit Events) 33
5.1.15 FMT_MTD.1B – Management of TSF Data (Protection Policies) 33
5.1.16 FMT_MTD.1C – Management of TSF Data (Device Groups) 33
5.1.17 FMT_MTD.1D – Management of TSF Data (Roles) 34
5.1.18 FMT_MTD.1E – Management of TSF Data (Security Alerts) 34
5.1.19 FMT_MTD.1F – Management of TSF Data (Alert Destinations) 34
5.1.20 FMT_SMF.1 – Specification of Management Functions 34
5.1.21 FMT_SMR.1 – Security Roles 34
5.1.22 FPT_RVM.1 – Non-bypassability of the TSP 34
5.2 Security Requirements for the IT Environment 35
5.2.1 FAU_STG.1B – Protected Audit Trail Storage 35
5.2.2 FIA_ATD.1 – User Attribute Definition 35
5.2.3 FIA_UAU.2 – User Authentication Before Any Action 35
5.2.4 FIA_UID.2B – User Identification Before Any Action 35
5.2.5 FCS_CKM.1 – Cryptographic Key Generation 36
5.2.6 FCS_CKM.4 – Cryptographic Key Destruction 36
5.2.7 FCS_COP.1 – Cryptographic Operation 36
5.2.8 FPT_STM.1 – Reliable Time Stamps 36
5.2.9 FPT_ITT.1 – Basic Internal TSF Data Protection 36
5.2.10 FPT_SEP.1 – TSF domain separation 37
5.3 TOE Security Assurance Requirements 38
5.3.1 ACM_CAP.2 – Configuration Items 38
5.3.2 ADO_DEL.1 – Delivery Procedures 39
5.3.3 ADO_IGS.1 – Installation, Generation, and Start-up Procedures 39
5.3.4 ADV_FSP.1 – Informal Functional Specification 39
5.3.5 ADV_HLD.1 – Descriptive High-Level Design 39
5.3.6 ADV_RCR.1 – Informal Correspondence Demonstration 40
5.3.7 AGD_ADM.1 – Administrator Guidance 40
5.3.8 AGD_USR.1 – User Guidance 41

5.3.9 ATE_COV.1 – Evidence of Coverage ... 41
5.3.10 ATE_FUN.1 – Functional Testing ... 41
5.3.11 ATE_IND.2 – Independent Testing – Sample ... 42
5.3.12 AVA_SOF.1 – Strength of the TOE Security Function Evaluation ... 42
5.3.13 AVA_VLA.1 – Developer Vulnerability Analysis ... 42
5.4 Strength of Function Claim ... 43
6 TOE Summary Specification ... 44
6.1 TOE Security Functions ... 44
6.1.1 Security Audit ... 44
6.1.2 Identification and Authentication (I&A) ... 46
6.1.3 Security Management ... 46
6.1.4 Policy Enforcement ... 50
6.1.5 Protection of the TSF ... 52
6.2 TOE Security Assurance Measures ... 58
6.2.1 Configuration Management ... 58
6.2.2 Delivery and Operation ... 58
6.2.3 Development ... 59
6.2.4 Guidance Documents ... 59
6.2.5 Tests ... 59
6.2.6 Vulnerability Analysis ... 60
7 Protection Profile Claims ... 61
8 Rationale ... 62
8.1 Introduction ... 62
8.2 Security Objectives Rationale ... 62
8.2.1 T.UA-ACCESS ... 62
8.2.2 T.UA-ACTION ... 63
8.2.3 T.DISABLE ... 63
8.2.4 T.ATTACK ... 63
8.2.5 T.DISCLOSURE ... 64
8.2.6 P.MANAGE ... 64
8.2.7 A.ADMIN ... 64

8.2.8 A.LOCATE 64
8.2.9 A.PROTECT 65
8.3 Security Requirements Rationale 65
8.3.1 O.MANAGE 67
8.3.2 O.AUTH 68
8.3.3 O.AUDIT-MGM 68
8.3.4 O.AUDIT-RVW 68
8.3.5 O.ACCESS 68
8.3.6 O.AUDIT-ATK 69
8.3.7 O.ALERT 69
8.3.8 O.CLIENT 69
8.3.9 O.E.TIME 69
8.3.10 O.E.TOE-PRT 69
8.3.11 O.E.TRANSMIT 70
8.4 Security Functional Requirements Dependencies Rationale 71
8.5 Explicitly Stated Requirements Rationale 72
8.6 Security Assurance Requirements Rationale 73
8.7 Strength of Functions Rationale 74
8.7.1 TOE 74
8.7.2 IT Environment 74
8.8 TOE Summary Specification Rationale 75

FIGURES

Figure 1 Digital Membrane – Kernel-Layer Security 14
Figure 2 Evaluated Configuration 18
Figure 3 Inter-Component Communication 21
Figure 4 Digital Membrane – TOE Client Kernel-Layer Security 51

TABLES

Table 1 TOE Security Functional Requirement Components 29
Table 2 FAU_GEN Auditable Events 30
Table 3 IT Environment Security Functional Requirement Components 35
Table 4 TOE Security Assurance Requirement Components 38
Table 5 TOE Inter-Component Communication 53
Table 6 Mapping of Security Environment to Security Objectives 62
Table 7 Mapping of Security Functional Requirements to Security Objectives 66
Table 8 Functional Requirements Dependencies 71
Table 9 Mapping of Security Assurance Requirements to Documents and Rationale 73
Table 10 Mapping of TOE Security Functional Requirements to TOE Security Functions 75

REFERENCES

Evaluation Documentation

CC-AGD	Safend Protector Administrator and User Guidance
CC-ATE	Safend Protector Test Plan
CC-ATE-RES	Safend Protector Test Results
CC-CFM	Safend Protector Configuration Management
CC-CIL	Safend Protector Configuration Item List
CC-DEL-IGS	Safend Protector Secure Delivery, Installation, Generation and Startup
CC-FSP	Safend Protector Functional Specification
CC-HLD	Safend Protector High Level Design
CC-ST	Safend Protector Security Target
CC-AVA	Safend Protector Vulnerability Analysis

TOE Documentation

SP-IG	Safend Protector Installation Guide
SP-UG	Safend Protector User Guide
SP-RN	Safend Protector Release Notes

Third-Party Documentation

SVN-UG	Version Control with Subversion, by Ben Collins-Sussman, Brian W. Fitzpatrick, and C. Michael Pilato

Common Criteria Documentation

CC-PART-2	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, CCMB 2005-08-002, August 2005.
CC-PART-3	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, CCMB 2005-08-003, August 2005.
CEM	Common Methodology for Information Technology Security Evaluation—Evaluation Methodology, Version 2.3, CCMB 2005-08-004, August 2005.

SECURITY TARGET INTRODUCTION

1.1 OVERVIEW

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization.

The TOE is Safend Protector™ Version 3.0, a software product that complements enterprise data security and network/server-based security products by controlling access to external physical, wireless and storage device interfaces on network endpoints (e.g., workstations, laptops). Safend Protector enables security administrators to define and enforce enterprise security policies on access to the endpoint's physical and wireless interfaces, thus protecting both the endpoint and enterprise network from data leakage, theft and the introduction of malware.

1.2 ST IDENTIFICATION

Title:	Safend Protector™ Security Target
ST Version:	1.98
ST Date:	21 July 2008
ST Author:	Safend Ltd.
TOE:	Safend Protector™ Version 3.0
Common Criteria Version:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005, CCMB 2005-08-002.
EAL:	Assurance claims conform to EAL2 from Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005, CCMB 2005-08-003.
Protection Profile:	No Protection Profile compliance is claimed.
Keywords:	Network, interface, port, device, attack

1.3 CONFORMANCE CLAIMS

The TOE is conformant with the following Common Criteria specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, CCMB 2005-08-002, August 2005
    - Part 2 extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, CCMB 2005-08-003, August 2005
    - Part 3 conformant
    - EAL2.

1.4 DOCUMENT ORGANIZATION

Section 1	Security Target Introduction	This section presents an introduction and overview of the Security Target.

Section 2	TOE description	This section presents 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 of the IT and non-IT environments and the threats that are countered by the TOE and its environment.
Section 4	TOE Security Objectives	This section details the security objectives of the TOE and its environment.
Section 5	IT Security Requirements	This section presents the Security Functional Requirements (SFRs) for the TOE and IT environment that supports the TOE, and details the Security Assurance Requirements (SARs) for EAL 2.
Section 6	TOE Summary Specification	This section describes the TOE Security Functions that satisfy the Security Functional Requirements and the Assurance Measures that satisfy the Security Assurance Requirements.
Section 7	Protection Profile Claims	This section states the conformance of this ST to any specific Protection Profiles.
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.

1.5 CONVENTIONS AND TERMINOLOGY

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 placed at the end of the component. For example FDP_ACC.1A and FDP_ACC.1B 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** text and are surrounded by brackets (e.g., [**assigned text ...**]).
- 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., [***selected text ...***]).
- 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 …").

Explicitly stated Security Functional Requirements – Explicit security functional requirements are identified using '_EXP' as a suffix to the label of the requirement.

Other sections of the Security Target – Other sections of the Security Target use bolding to highlight text of special interest, such as captions.

1.6 ABBREVIATIONS

The following Common Criteria-related abbreviations are used in this document:

CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TSS	TOE Summary Specification

2 TOE DESCRIPTION

2.1 SECTION OVERVIEW

This section provides information regarding the TOE, its functionality, its boundaries and the evaluated configuration.

2.2 TOE DESCRIPTION

2.2.1 TOE OVERVIEW

The TOE is Safend Protector™ Version 3.0 (hereafter also referred to either as the TOE or Protector), a software product that complements enterprise data security and network/server-based security products by controlling access to external physical, wireless and storage device interfaces on network endpoints (e.g., workstations, laptops).

Most current security solutions protect only enterprise network communication that flows through the main gateway and through critical servers, while endpoint (personal computer) interfaces to devices and other networks are exposed and vulnerable. IT security administrators are unable to control and monitor much of the communication to and from these endpoints, leaving their enterprise with a significant security blind spot. True protection can only be obtained by establishing a wall around each computer and by protecting its interfaces, while allowing access though required interfaces by required devices.

Safend Protector enables IT security administrators to design and implement an enterprise-wide security policy (Protection Policy) regulating the peripheral devices and storage media to which enterprise endpoints can connect and communicate with. Safend Protector controls access to physical ports (USB, FireWire, PCMCIA, SecureDigital (SD), serial, parallel, modem), wireless ports (Bluetooth, WiFi, IrDA), and storage media (CD/DVD Drives, flash drives, floppy drives, tape drives). Safend Protector can also identify and restrict USB, FireWire, and PCMCIA devices by their class, vendor, model, or unique serial number, and can identify and restrict storage devices based on their storage capacity, type, model, or unique serial number. It can also identify and restrict WiFi network connections based on the network identity (MAC address or SSID), authentication mode and encryption mode.

Multiple customized Protection Policies, specifying different access rights for different user groups, can be created and automatically distributed according to the organizational units (computers and users) already defined in the enterprise Active Directory.

By controlling access to these endpoint interfaces, Safend Protector prevents:

- data leakage and theft
- enterprise penetration
- introduction of malware.

Safend Protector provides central control over enterprise interfaces, devices and storage devices and ensures that users will only be able to use permitted devices through permitted interfaces.

2.2.2 SAFEND PROTECTOR FEATURES

Safend Protector assists administrators strike a balance between strong information security controls and productivity gains from new technologies. Safend Protector:

- resides at the kernel-level and controls access to ports and storage devices;
- provides tools that enable administrators to deploy security policies to all enterprise endpoints;

- enforces policies based on a “positive security” approach (once a Protection Policy has been installed on the TOE Client machine) whereby all interfaces are blocked until the administrator specifically authorizes exceptions (see “Initial Protection Policy” on page 22 for further information);
- detects attempts to tamper with the endpoint Protection Policy and enforces a restricted Protection Policy if unable to undo the tampering (see “Anti-Tampering” on page 17 for more information);
- enables administrators to define a Protection Policy at the granularity of user and device:
    - administrators can provide more connectivity for some users (e.g., senior management) than for others (e.g., contractors);
    - administrators can specify policies based on device type and device serial number;
- covers a wide variety of devices (USB, Bluetooth, FireWire, PCMCIA, serial, parallel, SD, IrDA and WiFi
- maintains a detailed log of endpoint activity, enabling administrators to analyze endpoint activity and alert administrators of exceptions.

2.2.3 DIGITAL MEMBRANE TECHNOLOGY

The key to Safend Protector is its underlying Digital Membrane™ technology, which enforces the Protection Policy on the TOE Client machine.

With the understanding that every endpoint has a different set of external interfaces, based on differing standards but all employing similar architectures – Safend has created a protocol-level, generic, semi-permeable barrier – a “Digital Membrane” – that can be wrapped around any device to protect communication on all its interfaces.

At the heart of the Digital Membrane is a unique kernel-level protocol inspection engine on the TOE Client machine that analyses in real time all inbound and outbound communication for a given port or interface. The Digital Membrane monitors and controls all incoming and outgoing traffic for each device, blocking or allowing access or data based on the Protection Policy defined in the Safend Protector Management Console.

2.2.4 KERNEL-LAYER APPROACH

Safend Protector operates at the lowest level of the kernel, just above the TOE Client machine’s hardware. For example, Figure 1 shows how Safend Protector’s kernel module monitors all data transfer between a Disk-On-Key device’s native driver and the device itself.

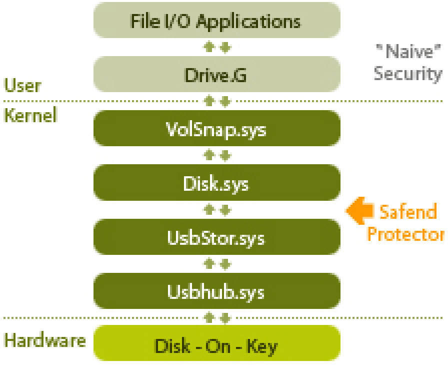

Figure 1 Digital Membrane – Kernel-Layer Security

2.2.5 GRANULAR CONTROL

Safend Protector provides multiple complementary options to secure enterprise endpoints:

- **Port Control** – Safend Protector can fully block access to any local-access desktop or laptop port, including physical ports (USB, FireWire, PCMCIA, SecureDigital, serial, parallel, modem) and wireless ports (WiFi, Bluetooth and IrDA). When a port is blocked, it is as if the wires to the port have been cut – no communication is allowed to or from the port.
- **Device Control** – On USB, FireWire and PCMCIA ports, Safend Protector can identify devices by their class, vendor, model, and serial number (for those devices with a serial number). Safend Protector can customize port restrictions based on this more detailed information. For example, an organization might block access to USB ports, while selectively allowing either printers (e.g., permitted by type), HP 6510 Printers (by model), or the CEO's personal HP 6510 (by serial number) to connect on those ports.
- **Storage Control** – Safend Protector controls on/off access to CD/DVD, floppy, flash, and tape drives. Storage devices can be identified by their type, model and serial number (if available), and also based on their capacity (e.g. allow devices up to 128MB). The TOE Administrator can also set any storage device connected to those ports to "read-only" mode, where files can be accessed, but no new information can be written to that media.
- **WiFi Networks Control** - Safend Protector controls the use of WiFi networks. Networks can be identified based on the MAC address of the access point or the network name (SSID). The Protection Policy can also specify the authentication scheme and the encryption scheme the network must use to connect. Additionally, Safend Protector controls the use of Ad-Hoc networks. Endpoint users can use authorized WiFi networks considered safe by the TOE administrator, while other non-secure or unmonitored networks will not be available to them.

2.2.6 POSITIVE SECURITY APPROACH

Once a Protection Policy has been installed on the TOE Client machine, Safend Protector implements a "positive security" approach, where all ports, devices and networks are blocked until the administrator grants specific access rights. In other words, every endpoint device and WiFi network within the enterprise is disabled unless the Protection Policy specifies otherwise. See "Initial Protection Policy" on page 22 for further information.

Positive security provides several benefits:

- **simplified initial Protection Policy deployment** – The administrator need only identify those devices and WiFi networks to be authorized.
- **simplified on-going Protection Policy management** – The burden of keeping track of proliferating new products and technologies is reduced.
- **immediate Protection Policy effectiveness** – All devices that do not meet policy standards after deployment are immediately denied further access.

2.2.7 OVERLAPPING PROTECTION POLICIES

The Safend Protector Client can enforce one of two Protection Policies, either a user policy or an endpoint policy. If there is a Protection Policy defined for the currently logged-in user, it is enforced. Otherwise the endpoint Protection Policy is enforced. In this manner the endpoint is always secured, whoever is logged in, while at the same time specific users enjoy their customized access rights, wherever they are logged in.

2.2.8 ENDPOINT USER INTERACTION

To minimize interaction with the endpoint user, Safend Protector can optionally display a Safend tray icon on the endpoint only when the user tries to connect an unauthorized device. The administrator can also customize the message that is displayed upon any attempted breach of the Protection Policy. Alternatively, enforcement of the Protection Policy can be configured to be silent and invisible from the user's point of view.

2.2.9 PROTECTION POLICY UPDATES

Protection Policy updates can be deployed either manually or automatically. Automatic deployment of Protection Policy updates is through Active Directory as Group Policy Objects (GPOs) linked to Active Directory Organizational Units (OUs). The frequency of these updates is defined by the GPO update interval set within Active Directory. If the client is not connected to the network and an update is thus not available, the current Protection Policy remains effective until a new Protection Policy is obtained.

The install / update process is unobtrusive from the end-user perspective.

After decrypting the new Protection Policy and validating its signature, the TOE Client starts enforcing the new Protection Policy. Devices that are currently in use but violate the new Protection Policy can either be disabled "gracefully" or "forcefully." A "forcefully" disabled device is immediately shut down, regardless of its activities. A "gracefully" disabled device is allowed to continue until the next system reboot before being disallowed. In this manner, administrators can revise Protection Policies without unduly inconveniencing endpoint users.

2.2.10 AUDITING (LOGGING AND ALERTING)

Safend Protector can log a variety of activities, including:

- **Port Initialization** – each time a Safend Protector client boots or whenever new adaptors are plugged in, for each blocked or approved port
- **Port Activity** – each time an attempt is made to use a port
- **Device Activity** – each time an attempt is made to use a device
- **WiFi Network Activity –** each time an attempt is made to connect to a WiFi link
- **Administrative Events** – Protection Policy updates, *etc*.
- **Malicious Attempts** – tampering attempts, uninstall attempts, *etc*.

Safend Protector TOE Client audit files (logs) are encrypted and stored locally on the TOE Client. The TOE Client uploads these logs to a central repository (on the TOE Management Server) at administrator-defined intervals, when the local audit file fills up, and when a client first logs on to the network. Audit records are sequentially numbered throughout all sessions. Deletion of audit records on the endpoint is detected by the Management Server when it receives the first out-of-sequence audit record.

Logs from across the network, as well as logs generated by the Management Server, are stored in a central repository (the TOE database) and are accessible only to authorized administrators using Safend Management Console, which displays the information contained in the individual endpoint logs in one administrator interface. All logs can be searched and sorted by authorized administrators.

The Management Console provides the administrator with the capability to select the auditable events that are to be audited and to specify which audited events will also generate security alerts.

Safend Protector's alert system enables administrators to be notified of urgent events using any of the following mechanisms:

- Email to one or more addresses
- SNMP trap to third-party network monitoring systems (e.g., IBM Tivoli or HP OpenView)
- Insertion of an entry in the Windows Event Log on a specific host
- Running a custom executable.

In addition, alerts are written to the appropriate Safend Protector log.

In large environments managed by several administrators, logs originating from different policies can be sent to different destinations, so each administrator can keep track of the data relevant to his area of responsibility.

2.2.11 CONTINUOUS MONITORING

TOE administrators are able to monitor in real-time, on the Management Server, the Protection Policy each endpoint is currently enforcing, which endpoints are currently enforcing no Protection Policy, and related information indicating the TOE Client's enforcement. Together with the alert feature, the monitoring tool enables administrators to identify problem Clients and restore protection if it has been interrupted.

In addition, the starting and stopping of Protection Policy enforcement are logged.

2.2.12 ANTI-TAMPERING

Safend Protector detects tampering attempts and alerts administrators of the attempt.

In the event that the Protection Policy becomes unusable, an alert is sent to the Management Server, which initiates a re-install of the Protection Policy. Until a new Protection Policy is received and installed, a built-in policy that blocks all communications on all interfaces except Human Interface Devices (keyboard, mouse, *etc*.) is enforced.

2.2.13 PROTECTION POLICY SUSPENSION

Temporary suspension of the Protection Policy by the endpoint user requires a one-time password that is generated by the TOE Management Server on request from an authorized TOE administrator, who then transmits it off-line (for example, by telephone or by hand delivery) to the endpoint user. At the end of the suspension period, Protection Policy enforcement automatically resumes.

The TOE Client also provides a limited administrator interface that allows the administrator to suspend protection. This requires the administrator to enter a Client Administration Password, which the administrator defines on the TOE Management Server for all Protection Policies or on a per-Policy basis.

2.2.14 TOE CLIENT UNINSTALL

A password, defined by the administrator on the TOE Management Server for all Protection Policies or on a per-Policy basis, is required in order to uninstall the TOE Client. Unauthorized attempts to uninstall generate alerts.

Note - The vendor recommends that the TOE Client (endpoint) machines be configured so that installation and uninstallation of programs be restricted to administrators, and that endpoint users not be defined as administrators on their own machines.

2.3 TOE ARCHITECTURE

The TOE consists of the following components:

- **Protector Management Server** (TOE Management Server), the repository for the TOE database (Protection Policies, integrated logs, *etc*.), downloads Protection Policies to the Protector Clients (via Active Directory), receives logs from the Protector Clients, and manages and displays the centralized log file.

- **Protector Management Console** (TOE Management Console), the graphic interface by which TOE administrators maintain the TOE.
- **Protector Client** (TOE Client), installed on the protected machine (the endpoint), enforces the policy downloaded to it by Protector Management Server (via Active Directory), writes logs (audit records) locally, and periodically uploads those logs to Protector Management Server.

2.4 EVALUATED CONFIGURATION

The evaluated configuration is illustrated in Figure 2.

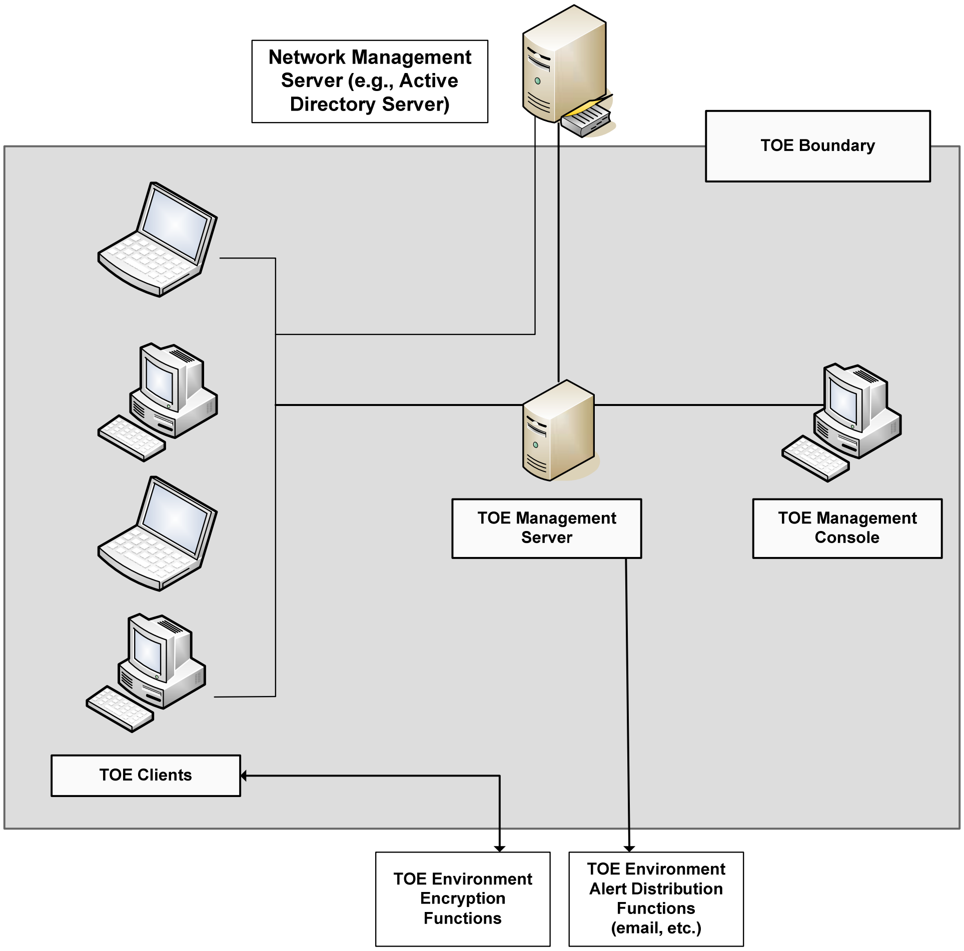
Network Management Server (e.g., Active Directory Server)
TOE Boundary
TOE Management Server
TOE Management Console
TOE Clients
TOE Environment Encryption Functions
TOE Environment Alert Distribution Functions (email, etc.)

Figure 2 Evaluated Configuration

The evaluated configuration consists of the following:

TOE Components

- The Protector Management Server software (TOE Management Server)

- The Protector Management Console software (TOE Management Console)
- The Protector Client software (TOE Client)

IT Environment Components

- The hardware server and operating system supporting the TOE Management Server software, depicted as "TOE Management Server" in Figure 2
- The hardware server and operating system supporting the TOE Management Console software, depicted as "TOE Management Console" in Figure 2. Note that the TOE Management Console software can be installed on the same machine as the TOE Management Server software
- The hardware and operating system of the endpoint client machines on which the TOE Client software is installed, depicted as "TOE Clients" in Figure 2
- An Active Directory Server, which provides and verifies TOE administrator credentials, and optionally distributes the TOE Client software and Protection Policies to TOE Client machines. Alternatively, software and Protection Policies can be distributed manually (see "TOE Client Software Distribution" on page 21 and "TOE Client Protection Policy Distribution" on page 22).
- SSL, which secures some communications between the TOE components (see Figure 3 on page 21)
- MS CAPI, which implements the encryption functions
- Alert distribution functions (e.g., email).

2.5 TOE ENVIRONMENT

The TOE Management Server and TOE Management Console run on machines which are inside the protected network (*i.e.*, behind the firewall).

2.5.1 PHYSICAL BOUNDARY

The physical boundary of the TOE comprises the three software components of TOE Management Server, TOE Management Console and TOE Client.

The hardware and operating systems that these components run on are outside the TOE boundary.

The cryptographic software and messaging and alert systems that support the TOE (listed in Section 2.2.10) are outside the TOE boundary.

2.5.2 LOGICAL BOUNDARY

The logical boundary of the TOE is defined by the external interfaces at which the Security Functions are implemented. The Security Functions are:

- **Security Audit** – The TOE generates audit information for security-relevant events, transmits audit information from the TOE Clients to the TOE Management Server and enables TOE administrators to view the audit records. The TOE provides mechanisms to detect unauthorized modification or deletion of TOE Client audit records and also relies on the IT environment to protect audit records from unauthorized modification or deletion.
- **Identification and Authentication** – The TOE allows only TOE administrators who have been successfully identified (by the TOE) and authenticated (by the IT Environment) to maintain the TOE and its data, including defining Protection Policies and viewing audit records.

- **Security Management** – The TOE enables TOE administrators to define policies specifying the access granted to the physical interfaces of the TOE Client, as well as to define other administrators and system-wide parameters.
- **Policy Enforcement** – The TOE protects TOE Client machines by enforcing, on their physical interfaces (ports) and storage media, the policies defined by TOE administrators.
- **Protection of the TSF** – The TOE and IT Environment protect TSF data stored in the TOE and in transit between TOE components from disclosure and modification.

See “TOE Security Functions” on page 44 for a detailed description of the Security Functions.

The following capabilities of the TOE that are described in the TOE guidance documentation are not included in the scope of the evaluation: no claims have been made about them and they have not been subject to Common Criteria evaluation or testing:

- U3 and autorun control
- Protection against hardware key loggers, including disabling the keyboard if a hardware keyboard logger is detected.

2.6 INTER-COMPONENT COMMUNICATION

If they are installed on separate machines, TOE Management Server and TOE Management Console communicate via SSL.

TOE Management Server and TOE Clients communicate via SSL.

Inter-component communication is illustrated in Figure 3.

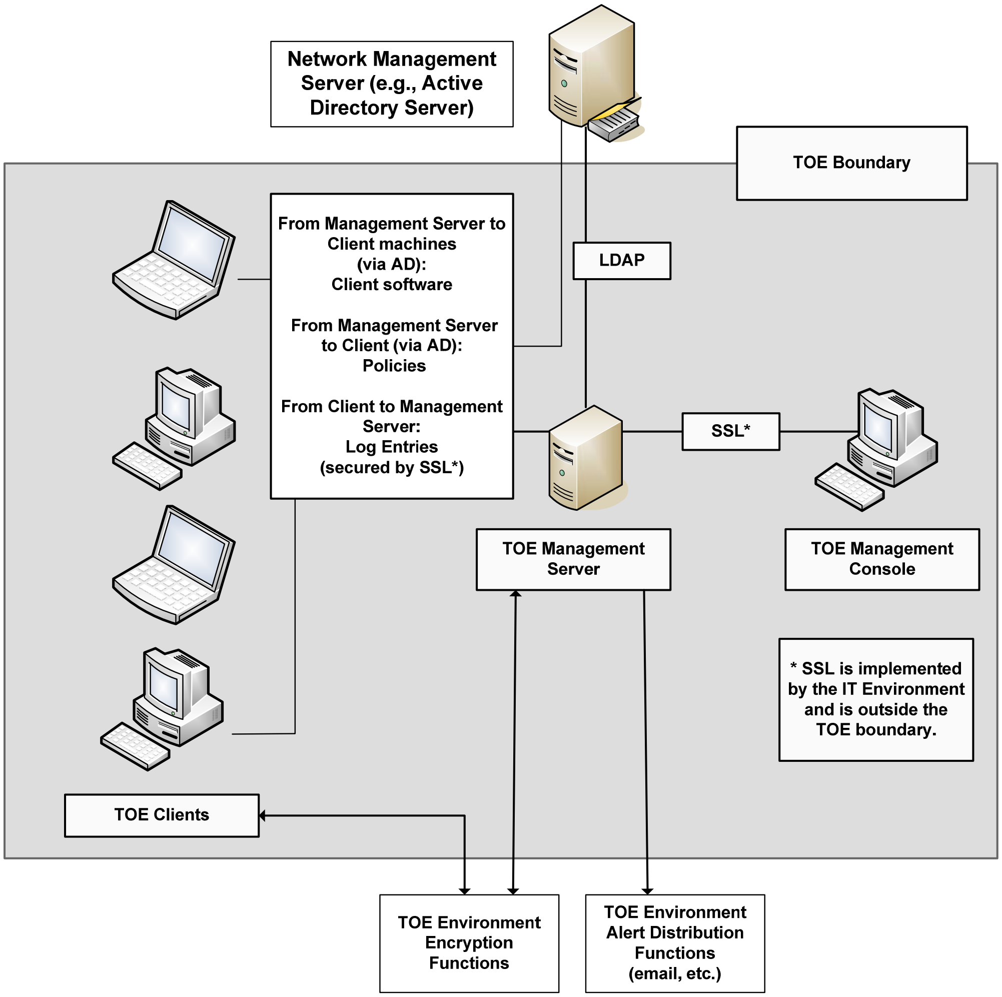
Network Management Server (e.g., Active Directory Server)
TOE Boundary
From Management Server to Client machines (via AD): Client software
From Management Server to Client (via AD): Policies
From Client to Management Server: Log Entries (secured by SSL*)
LDAP
SSL*
TOE Management Server
TOE Management Console
* SSL is implemented by the IT Environment and is outside the TOE boundary.
TOE Clients
TOE Environment Encryption Functions
TOE Environment Alert Distribution Functions (email, etc.)

Figure 3 Inter-Component Communication

The TOE transmits the following data between its components:

- TOE Client software is distributed from the TOE Management Server to the TOE Client machines
- Protection Policies are distributed from the TOE Management Server to the TOE Clients
- Audit data generated by the TOE Clients are transmitted from the TOE Clients to the TOE Management Server.

These processes are described in the following sections.

2.6.1 TOE CLIENT SOFTWARE DISTRIBUTION

Although it is possible to manually install the TOE Client software individually on each of the endpoints using standard OS installation procedures, it is not practical to do so except in very small organizations.

In organizations where manual distribution and installation of software is not feasible, Safend Protector seamlessly integrates with network management software (for example, Active Directory) to deploy the TOE Client software from the TOE Management Server to the enterprise endpoints. Administrators can export the TOE Client software directly to Active Directory as Group Policy Objects (GPOs), which can be assigned to Organizational Units (OUs). The TOE Client software can be applied to the entire company or to a specific domain, department, computer or user – any OU defined in Active Directory. The TOE Client software is then deployed to the endpoints through GPO on a "silent install" basis.

2.6.1.1 INITIAL PROTECTION POLICY

The initial Protection Policy, which takes effect immediately upon the installation of the TOE Client software, allows all access to the protected ports and storage devices. This ensures that there is no change in the behavior of endpoint machines until TOE administrators define and install a Protection Policy.

Once a Protection Policy has been defined on the Management Server and installed on the Client, only access requests explicitly permitted by the Protection Policy are allowed; access requests not explicitly permitted by the Protection Policy are blocked.

2.6.2 TOE CLIENT PROTECTION POLICY DISTRIBUTION

Safend Protector seamlessly integrates with network management software (for example, Active Directory) to deploy Protection Policies to the enterprise endpoints. Administrators can export Protection Policies directly from the TOE Management Server to Active Directory as Group Policy Objects (GPOs), which can be assigned to Organizational Units (OUs). Protection Policies can be applied to the entire company or to a specific domain, department, computer or user – any OU that is defined in Active Directory. Protection Policies are then deployed to the endpoints through GPO.

Alternatively, the TOE Management Server can export Protection Policies to a shared folder, which can then be imported into network management software and distributed to clients.

2.6.3 TOE CLIENT AUDIT RECORDS

TOE Client audit records (log records) are generated in accordance with the Protection Policy and are stored locally (on the TOE Client machine) in encrypted form. Periodically, these audit records are uploaded to the Management Server, where they are decrypted and stored in a central repository for administrator review and analysis.

2.6.4 TOE CLIENT ALERTS

The TOE client generates alerts, based on auditable events as selected by the administrator, to notify administrators of urgent issues requiring their attention. Alerts are sent to the Management Server and are distributed to administrators using the configured alert mechanisms (any of email, SNMP trap, Windows Event Log entry, and custom executables).

2.7 TOE SYSTEM REQUIREMENTS

	Safend Protector Client	Safend Protector Console	Safend Protector Server
Operating System	• Windows 2000 Professional (SP 3-4) • Windows 2000 Server (SP 3-4) • Windows 2000 Advanced Server (SP	• Windows XP Professional (SP 0-2) • Windows 2003 Server (SP 0-2)	• Windows XP Professional (SP 0-2) • Windows 2003 Server (SP 0-2)

	3-4) • Windows XP Professional (SP 0-2) • Windows 2003 Server (SP 0-2)		
Hardware	• Pentium 300 MHz • 128 MB RAM • 10 MB HDD space	• Pentium 300 MHz • 128 MB of RAM • 20 MB HDD space	The server hardware requirements depend on the number of installed Safend Protector clients. To obtain the specifications suitable for your organization, please contact your local Safend partner or Safend support.
Software		• Microsoft .NET Framework 1.1	• Microsoft .NET Framework 1.1 • Microsoft IIS

2.7.1 Deliverables

The deliverable package of the TOE consists of files downloaded from an SSL-protected section of the developer's web site.

Customers can confirm the integrity of the downloaded files by locally calculating their MD5 values and comparing them to the values listed on the developer web site.

Note - The developer web site is protected from tampering by appropriate security mechanisms (firewalls, etc.). In addition, the downloaded files are signed and the installation process validates the signature.

2.8 TOE-Specific Terminology

This section defines some of the TOE-specific terminology used in this document.

term	definition
administrator	A user with the required privileges to configure the TOE. The term "administrator" is used interchangeably with the term "authorized administrator," since no administrator can perform any TOE-related action until he or she has been successfully authenticated.
endpoint	A machine on which the TOE Client is installed and the interfaces of which are monitored by the Protection Policy.
endpoint group	A group of endpoints protected by the same Protection Policy. The members of the group are specified outside the TOE, for example, as an Organizational Unit (OU) in Active Directory.
endpoint user	An endpoint user is the user who is logged in to the endpoint machine. See "user" below.

term	definition
user	In the context of the TOE, there are two types of users: • Authorized TOE administrators (that is, users who have been successfully identified and authenticated) who are able to interact with the TOE. • Users of the endpoints on which the Protection Policy is enforced (“end-users” or “endpoint users”), who have no direct interaction with the TOE except when the TOE is configured in such a way that informative messages are displayed on the protected endpoint. These messages do not call for the end-user to take any action except to close the message window. The end-user cannot influence the operation of the TOE. In fact, the TOE is designed to thwart end-user attempts to do so. There is one case in which the end-user can interact with the TOE: to temporarily suspend policy enforcement. However, this can only be done when the end-user is in off-line contact with an authorized administrator who provides the one-time password required for such temporary enforcement suspension. An end-user is unable to suspend enforcement without the active cooperation of an authorized administrator. In any case, the administrator specifies the duration of the suspension, and enforcement is automatically resumed when the specified time period expires. It is possible to a define a Protection Policy for a specific endpoint user, which is enforced on whatever machine the endpoint user is logged into, instead of the Protection Policy associated with that machine. The endpoint user has no interaction with the TOE when this happens. The TOE enforces the endpoint user Protection Policy based on information received from the IT environment (the user name).

3 SECURITY ENVIRONMENT

This section describes the security aspects of the environment in which the TOE should be used and the manner in which it is expected that the TOE will be used. These include:

- threats that the TOE is designed to counter
- organizational security policies with which the TOE is designed to comply
- assumptions about the operational environment and the TOE's intended method of use

3.1 THREATS

3.1.1 ASSETS

The assets protected by the TOE are:

- TOE data stored on the TOE component machines, or in transit between TOE components
- user data stored on the endpoint and in the protected network

3.1.2 THREAT AGENTS

The threat agents which may compromise the protected assets are:

- attackers who attempt to gain unauthorized access to and/or modify TOE or user data
- malware (*e.g.*, viruses) which may gain control of resources on endpoint machines or in the protected network
- endpoint users who accidentally or deliberately expose user data, or who attempt to undermine the enforcement of the Protection Policy, thus exposing the endpoint and the network to attack by other threat agents

3.1.3 THREATS COUNTERED BY THE TOE

This section describes the threats to the assets that the TOE and its environment are required to counter.

T.UA-ACCESS An unauthorized user may gain access to or modify TOE data, whether stored in the TOE components or in transit between distributed parts of the TOE, in order to acquire knowledge of and/or circumvent the protection afforded by the TOE.

T.UA-ACTION An authorized user may exceed his or her privileges and gain access to or perform unauthorized modifications of TOE data which go undetected, in order to acquire knowledge of and/or circumvent the protection afforded by the TOE.

T.DISABLE An attacker may disable or delete the TOE Client or modify its behavior and thus expose the protected machine (and through the compromised machine, the network as well) to attack. Note that the attacker described here may well be the authorized user of the TOE Client machine.

T.ATTACK An attacker may gain access to the protected machine (the TOE Client) via the machine's physical interfaces, using any of a variety of well-known attack methods, and thereby gain access to and/or modify user data, or install malware on the endpoint machine or in the protected network.

T.DISCLOSURE An endpoint user accidentally or deliberately exposes user data by writing it to a removable storage device or media, or sending it to an insecure device or network.

3.2 ORGANIZATIONAL SECURITY POLICIES

P.MANAGE IT Systems are protected from unauthorized access and modification.

3.3 ASSUMPTIONS

A.ADMIN The administrators assigned to manage the TOE:

- are competent and properly trained;
- are neither careless, willfully negligent, nor hostile;
- follow the guidance and instruction provided in the TOE documentation;
- install and administer the TOE in a manner consistent with organizational policies.

A.LOCATE The TOE Management Server and TOE Management Console and other components on which they rely (for example, the Active Directory Server) are located in a physically secured area, protected from unauthorized physical access.

A.PROTECT The endpoint devices that host the TOE Client are physically protected to the degree necessary to ensure that the TOE Client cannot be uninstalled or otherwise disabled by direct physical interaction with the endpoint device.

4 SECURITY OBJECTIVES

This section describes the security objectives, which – taken together – counter the threats, while complying with the organizational security policies and remaining consistent with the assumptions, as listed in the previous section.

4.1 SECURITY OBJECTIVES FOR THE TOE

O.MANAGE The TOE must provide the functionality that enables an authorized administrator to configure the TOE, define TOE security policies (for example, the Protection Policy), and monitor the TOE's activities.

O.AUTH The TOE must ensure that only authorized administrators are able to access the TOE and its data.

O.AUDIT-MGM The TOE must provide the capability to generate audit records of all security-related actions of TOE users to ensure that these actions can be traced to the users who performed them.

O.AUDIT-RVW The TOE must provide authorized administrators with the capability to review audit records.

O.ACCESS The TOE must control access to endpoint ports and storage devices based on centrally managed Protection Policies.

O.AUDIT-ATK The TOE must provide the capability to generate audit records of detected violation attempts.

O.ALERT The TOE must have the capability to respond to specified events by alerting administrators.

O.CLIENT The TOE must have the ability to protect the TOE Client and its data, including Protection Policies and audit data, from unauthorized disabling, uninstallation, deletion, and modification, either by preventing these events or by detecting them and alerting the TOE administrators.

4.2 SECURITY OBJECTIVES FOR THE IT ENVIRONMENT

O.E.TIME The IT environment must provide a reliable time-stamp for the TOE to be used for audit records.

O.E.TOE-PRT The IT environment must protect the TOE data from unauthorized deletion or modification.

O.E.TRANSMIT The IT environment must have the ability to protect TSF data in transit between distributed parts of the TOE.

4.3 SECURITY OBJECTIVES FOR THE NON-IT ENVIRONMENT

O.E.ADMIN Authorized TOE administrators must be properly trained in all aspects of TOE and TOE resource administration, and must be neither negligent nor hostile.

O.E.BACKUP The TOE, its data and the systems on which it runs will be restored to a secure state after failure by following the relevant backup and restore procedures.

O.E.LOCATE The TOE Management Server, TOE Management Console and other components on which they rely (for example, the Active Directory machine) must be located in a physically secured area, protected from unauthorized physical access.

O.E.INSTALL The TOE and its associated hardware and software environment must be installed, maintained and managed in a manner that complies with the TOE security objectives.

O.E.PROTECT Endpoint devices that host the TOE Client must be physically protected to the degree necessary to ensure that the TOE Client cannot be uninstalled or otherwise disabled by direct physical interaction with the endpoint device.

5 IT SECURITY REQUIREMENTS

This section contains the security requirements that are provided by the TOE and the IT environment. These requirements consist of security functional and assurance components for the TOE derived from Part 2 and 3 of the Common Criteria and an explicitly-stated security functional requirement (FAU_ARP_EXP.1).

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

This section describes the Security Functional Requirements which are satisfied by the TOE.

Table 1 TOE Security Functional Requirement Components

Security Functional Class	Security Functional Requirement	Description
Security Audit	FAU_ARP_EXP.1	Security alerts
	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selectable audit review
	FAU_SEL.1	Selective audit
	FAU_STG.1A	Protected audit trail storage
User Data Protection	FDP_ACC.1A	Subset access control (Ports)
	FDP_ACC.1B	Subset access control (Storage Devices)
	FDP_ACF.1A	Security attribute based access control (Ports)
	FDP_ACF.1B	Security attribute based access control (Storage Devices)
Identification and Authentication	FIA_UID.2A	User identification before any action
Security Management	FMT_MOF.1	Management of security function behavior
	FMT_MTD.1A	Management of TSF data (Selected audit events)
	FMT_MTD.1B	Management of TSF data (Protection policies)
	FMT_MTD.1C	Management of TSF data (Device groups)
	FMT_MTD.1D	Management of TSF data (Roles)
	FMT_MTD.1E	Management of TSF data (Security alerts)
	FMT_MTD.1F	Management of TSF data (Alert destinations)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_RVM.1	Non-bypassability of the TSP

5.1.1 FAU_ARP_EXP.1 – Security Alerts

FAU_ARP_EXP.1.1 The TSF shall be able to generate an alert for each auditable event.

FAU_ARP_EXP.1.2 The TSF shall send generated alerts to an administrator configurable destination.

5.1.2 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) [**auditable events described in Table 2 below**].

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, [**additional information as specified in Table 2 below**].

Table 2 FAU_GEN Auditable Events

Component	Client	Server	Event	Notes
FDP_ACF.1A	X		Port initialization, port activity, device activity, WiFi network activity	These audit records also include the following information: interface, device, operation.
FDP_ACF.1B	X		Device activity	
FIA_UID.2A		X	Login and logout attempts at the Management Console	Includes the user identity.
FMT_MOF.1	X		Protection suspension, protection resumption	
FMT_MTD.1B		X	Protection Policy updates	Includes the user identity.
FMT_MTD.1D		X	Role changes	Includes the user identity.
FPT_RVM.1	X		Tampering attempts	
FPT_RVM.1	X		Uninstall attempts	Both unsuccessful and successful attempts to uninstall the TOE client are audited.

5.1.3 FAU_SAR.1 – AUDIT REVIEW

FAU_SAR.1.1 The TSF shall provide [**Administrator, User with 'Read Logs' role permission**] with the capability to read [**all auditable events**] 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.

5.1.4 FAU_SAR.2 – RESTRICTED AUDIT REVIEW

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.5 FAU_SAR.3 – SELECTABLE AUDIT REVIEW

FAU_SAR.3.1 The TSF shall provide the ability to perform [***searches, sorting***] of audit data based on [**date/time, type of event, subject identity**].

5.1.6 FAU_SEL.1 – SELECTIVE AUDIT

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) [***object identity, event type***]

b) [**no additional attributes**].

5.1.7 FAU_STG.1A - PROTECTED AUDIT TRAIL STORAGE

FAU_STG.1A.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1A.2 The TSF shall be able to [***detect***] unauthorized modifications to the audit records in the audit trail.

5.1.8 FDP_ACC.1A – SUBSET ACCESS CONTROL (PORTS)

FDP_ACC.1A.1 The TSF shall enforce the [**Port Access Control SFP**] on [
Subjects: Users, Client Hosts;
Objects: Ports;
Operations: Port Operations].

5.1.9 FDP_ACC.1B – SUBSET ACCESS CONTROL (STORAGE DEVICES)

FDP_ACC.1B.1 The TSF shall enforce the [**Storage Device Access Control SFP**] on [
Subjects: Users, Client Hosts;
Objects: Storage Devices;
Operations: Storage Device Operations].

5.1.10 FDP_ACF.1A –SECURITY ATTRIBUTE BASED ACCESS CONTROL (PORTS)

FDP_ACF.1A.1 The TSF shall enforce the [**Port Access Control SFP**] to objects based on the following: [
Subject Security Attributes: Policy;
Object Security Attributes: Port Type (USB, Firewire, PCMCIA, SecureDigital, Serial, Parallel, Modem, WiFi, IrDA, Bluetooth), Device Type, Device Model, Device Id, Connection Type, Network Id, Authentication Mode, Encryption Mode].

FDP_ACF.1A.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
Policy Selection

If User is logged in to the Client Host and has a Policy assigned, the User Policy is enforced, otherwise the Client Host Policy is enforced.

Rules For Port Operations

If the Policy allows access to the Port Type of the Port, then the operation is allowed.

If the Policy blocks access to the Port Type of the Port, then the operation is denied.

If the Policy restricts access to the Port Type of the Port, then:

For Port Type == USB or Firewire or PCMCIA:

If the Policy allows access to the Device Type of the Port, then the operation is allowed.

If the Policy restricts access to the Device Type of the Port, then the operation is denied unless:

- **The Device Model is included in a Device Model Group specified in the Policy White List, or**
- **The Device Id is included in a Distinct Device Group specified in the Policy White List.**

For Port Type == WiFi:

If the Policy allows access to the Connection Type of the Port, then the operation is allowed.

If the Policy blocks access to the Connection Type of the Port, then the operation is denied.

If the Policy restricts access to the Connection Type of the Port, then the operation is denied unless:

- **An entry matching the Network Id, Authentication Mode and Encryption Mode on the Port is included in an Approved WiFi Network Group specified in the Policy White List.**].

FDP_ACF.1A.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**All operations are allowed until a Policy is installed**].

FDP_ACF.1A.4 The TSF shall explicitly deny access of subjects to objects based on the [**following additional rules: all operations are denied if the Policy has been corrupted or deleted**].

5.1.11 FDP_ACF.1B –Security Attribute Based Access Control (Storage Devices)

FDP_ACF.1B.1 The TSF shall enforce the [**Storage Device Access Control SFP**] to objects based on the following: [
Subject Security Attributes: Policy;
Object Security Attributes: Device Type, Device Model, Device Id, Capacity].

FDP_ACF.1B.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

Policy Selection

If User is logged in to the Client Host and has a Policy assigned, the User Policy is enforced, otherwise the Client Host Policy is enforced.

Rules For Storage Device Operations

If the Policy allows access to all Storage Devices, then the operation is allowed.

If the Policy blocks access to all Storage Devices, then the operation is denied.

If the Policy restricts access to all Storage Devices, then:

> **If the Device Type is Removable Media and Capacity Control is set, then the following rules apply based on: the access granted to devices with capacity below the specified cut-off mark; the access granted to devices with capacity above the specified cut-off mark; and the Capacity of the Storage Device.**
>
> **If the Policy allows access to the Device Type of the Storage Device, then the operation is allowed.**
>
> **If the Policy restricts access to the Device Type of the Storage Device, then the operation is denied unless:**
>
> - **The Device Model is included in a Storage Model Group specified in the Policy White List, or**
> - **The Device Id is included in a Distinct Storage Group specified in the Policy White List.**

If the Policy allows read-only access to the Device Type of the Storage Device and the Storage Device is not included in the Policy White List (either by Device Model or Device Id), then the operation is allowed only if it is a read operation.].

FDP_ACF.1B.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**All operations are allowed until a Policy is installed**].

FDP_ACF.1B.4 The TSF shall explicitly deny access of subjects to objects based on the [**following additional rules: all operations are denied if the Policy has been corrupted or deleted**].

5.1.12 FIA_UID.2A – User Identification Before Any Action

FIA_UID.2A.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.13 FMT_MOF.1 – Management of Security Function Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [***enable, disable***] the functions [**access control**] to [**Administrator, User with 'Grant Suspend Password' role permission**].

5.1.14 FMT_MTD.1A – Management of TSF Data (Selected Audit Events)

FMT_MTD.1A.1 The TSF shall restrict the ability to [***modify***] the [**set of audited events**] to the [**Administrator, User with 'Write Policies' role permission, User with 'Write Administration' role permission, User with 'Write Global Policy Settings' role permission**].

5.1.15 FMT_MTD.1B – Management of TSF Data (Protection Policies)

FMT_MTD.1B.1 The TSF shall restrict the ability to [***modify, delete, [*****create*****]***] the [**Policies**] to the [**Administrator, User with 'Write Policies' role permission**].

5.1.16 FMT_MTD.1C – Management of TSF Data (Device Groups)

FMT_MTD.1C.1 The TSF shall restrict the ability to [***modify, delete, [*****create*****]***] the [**Device Model Groups, Distinct Device Groups, Approved WiFi Network Groups,**

Storage Model Groups, and Distinct Storage Groups] to the [**Administrator, User with 'Write Policies' role permission**].

5.1.17 FMT_MTD.1D – MANAGEMENT OF TSF DATA (ROLES)

FMT_MTD.1D.1 The TSF shall restrict the ability to [***modify, delete, [*create*]***] the [**Roles**] to the [**Administrator**].

5.1.18 FMT_MTD.1E – MANAGEMENT OF TSF DATA (SECURITY ALERTS)

FMT_MTD.1E.1 The TSF shall restrict the ability to [***modify***] the [**set of generated security alerts**] to the [**Administrator, User with 'Write Policies' role permission, User with 'Write Administration' role permission, User with 'Write Global Policy Settings' role permission**].

5.1.19 FMT_MTD.1F – MANAGEMENT OF TSF DATA (ALERT DESTINATIONS)

FMT_MTD.1F.1 The TSF shall restrict the ability to [***modify***] the [**list of security alert destinations**] to the [**Administrator, User with 'Write Administration' role permission, User with 'Write Global Policy Settings' role permission**].

5.1.20 FMT_SMF.1 – SPECIFICATION OF MANAGEMENT FUNCTIONS

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

a) enable and disable the access control function;

b) modify the set of audited events;

c) create, modify, and delete Policies;

d) create, modify and delete Device Model Groups, Distinct Device Groups, Approved WiFi Network Groups, Storage Model Groups, and Distinct Storage Groups;

e) create, modify and delete Roles (groupings of role permissions)

f) modify set of generated security alerts

g) modify list of security alert destinations].

5.1.21 FMT_SMR.1 – SECURITY ROLES

FMT_SMR.1.1 The TSF shall maintain the roles [**Administrator; Users with any of the following role permissions:**

- **Grant Suspend Password;**
- **Write Policies;**
- **Write Global Policy Settings;**
- **Write Administration;**
- **Read Logs**].

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

5.1.22 FPT_RVM.1 – NON-BYPASSABILITY OF THE TSP

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

5.2 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT

This section lists the Security Functional Requirements that are satisfied by the IT Environment.

Table 3 IT Environment Security Functional Requirement Components

Security Functional Class	Security Functional Requirement	Description
Security Audit	FAU_STG.1B	Protected audit trail storage
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2B	User identification before any action
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Security Management	FMT_MSA.2	Secure security attributes
Protection of the TSF	FPT_STM.1	Reliable time stamps
	FPT_ITT.1	Basic internal TSF data protection
	FPT_SEP.1	Domain Separation

5.2.1 FAU_STG.1B - PROTECTED AUDIT TRAIL STORAGE

FAU_STG.1B.1 The ~~TSF~~ **IT environment** shall protect the stored audit records from unauthorized deletion.

FAU_STG.1B.2 The ~~TSF~~ **IT environment** shall be able to [***prevent***] unauthorized modifications to the audit records in the audit trail.

5.2.2 FIA_ATD.1 – USER ATTRIBUTE DEFINITION

FIA_ATD.1.1 The ~~TSF~~ **IT environment** shall maintain the following list of security attributes belonging to individual users: [**identity, group membership, password**].

5.2.3 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 behalf of that user.

5.2.4 FIA_UID.2B – USER IDENTIFICATION BEFORE ANY ACTION

FIA_UID.2.1b The ~~TSF~~ **IT environment** shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.2.5 FCS_CKM.1 – Cryptographic Key Generation

FCS_CKM.1.1 The ~~TSF~~ **IT environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**Random Number Generation**] and specified cryptographic key sizes [

- **112 bits (3DES)**
- **1024 bit modulus (RSA)**]

that meet the following: [**none**].

5.2.6 FCS_CKM.4 – Cryptographic Key Destruction

FCS_CKM.4.1 The ~~TSF~~ **IT environment** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroization**] that meets the following: [**none**]

5.2.7 FCS_COP.1 – Cryptographic Operation

FCS_COP.1.1 The ~~TSF~~ **IT environment** shall perform [

- **data encryption and decryption,**
- **digital signature generation and verification,**
- **cryptographic checksum generation and verification**]

in accordance with a specified cryptographic algorithm [

- **3DES-mode CBC (data encryption and decryption)**
- **RSA-SHA1 (digital signature generation and verification)**
- **SHA1 (cryptographic checksum generation and verification)**]

and cryptographic key sizes [

- **112 bits (3DES)**
- **1024 bit modulus (RSA)**
- **none (SHA-1)**]

that meet the following: [

- **FIPS 46-3 (3DES)**
- **FIPS 186-2 (RSA)**
- **FIPS 180-1 (SHA-1)**].

Application Note: The specific uses of these methods, algorithms and keys are described in detail in “Protection of the TSF” on page 52.

5.2.8 FPT_STM.1 - Reliable Time Stamps

FPT_STM.1.1 The ~~TSF~~ **IT environment** shall be able to provide reliable time stamps for use by the TSF.

5.2.9 FPT_ITT.1 – Basic Internal TSF Data Protection

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

5.2.10 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.

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.

Table 4 TOE Security Assurance Requirement Components

Assurance Class	Assurance Components
Configuration Management (ACM)	ACM_CAP.2 Configuration Items
Delivery and Operation (ADO)	ADO_IGS.1 Installation, Generation, and Start-up Procedures
	ADO_DEL.1 Delivery Procedures
Development (ADV)	ADV_FSP.1 Informal Functional Specification
	ADV_HLD.1 Descriptive High Level Design
	ADV_RCR.1 Informal Correspondence Demonstration
Guidance Documents (CC-AGD)	AGD_ADM.1 Administrator Guidance
	AGD_USR.1 User Guidance
Tests (ATE)	ATE_IND.2 Independent Testing - Sample
	ATE_COV.1 Evidence of Coverage
	ATE_FUN.1 Functional Testing
Vulnerability assessment (AVA)	AVA_SOF.1 Strength of the TOE Security Function Evaluation
	AVA_VLA.1 Developer Vulnerability Analysis

5.3.1 ACM_CAP.2 - CONFIGURATION ITEMS

ACM_CAP.2.1d The developer shall provide a reference for the TOE.

ACM_CAP.2.2d The developer shall use a CM system.

ACM_CAP.2.3d The developer shall provide CM documentation.

ACM_CAP.2.1c The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2c The TOE shall be labeled with its reference.

ACM_CAP.2.3c The CM documentation shall include a configuration list.

ACM_CAP.2.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.5c The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.6c The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.

ACM_CAP.2.7c The CM system shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 ADO_DEL.1 - DELIVERY PROCEDURES

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2d The developer shall use the delivery procedures.

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.

ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3 ADO_IGS.1 - INSTALLATION, GENERATION, AND START-UP PROCEDURES

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

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.

ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.4 ADV_FSP.1 - INFORMAL FUNCTIONAL SPECIFICATION

ADV_FSP.1.1d The developer shall provide a functional specification.

ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2c The functional specification shall be internally consistent.

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.

ADV_FSP.1.4c The functional specification shall completely represent the TSF.

ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.5 ADV_HLD.1 - DESCRIPTIVE HIGH-LEVEL DESIGN

ADV_HLD.1.1d The developer shall provide the high-level design of the TSF.

ADV_HLD.1.1c The presentation of the high-level design shall be informal.

ADV_HLD.1.2c The high-level design shall be internally consistent.

ADV_HLD.1.3c The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.

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.

ADV_HLD.1.6c The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

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.

5.3.6 ADV_RCR.1 - Informal Correspondence Demonstration

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

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.

ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.7 AGD_ADM.1 - Administrator Guidance

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

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.

AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.8 AGD_USR.1 - USER GUIDANCE

AGD_USR.1.1d The developer shall provide user guidance.

AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.

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.

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 the TOE security environment.

AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

AGD_USR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.9 ATE_COV.1 - EVIDENCE OF COVERAGE

ATE_COV.1.1d The developer shall provide evidence of the test coverage.

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.

ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.10 ATE_FUN.1 - FUNCTIONAL TESTING

ATE_FUN.1.1d The developer shall test the TSF and document the results.

ATE_FUN.1.2d The developer shall provide test documentation.

ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

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.

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.

ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.11 ATE_IND.2 - INDEPENDENT TESTING - SAMPLE

ATE_IND.2.1d The developer shall provide the TOE for testing.

ATE_IND.2.1c The TOE shall be suitable for testing.

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.

ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.12 AVA_SOF.1 - STRENGTH OF THE TOE SECURITY FUNCTION EVALUATION

AVA_SOF.1.1d The developer shall perform a strength of the TOE security function analysis for each mechanism identified in the ST as having a strength of the TOE security function claim.

AVA_SOF.1.1c For each mechanism with a strength of the TOE security function claim the strength of the TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2c For each mechanism with a specific strength of the TOE security function claim the strength of the TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.13 AVA_VLA.1 - DEVELOPER VULNERABILITY ANALYSIS

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.

AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.

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.

AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

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.

AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.4 STRENGTH OF FUNCTION CLAIM

In addition to these requirements, the TOE satisfies a minimum strength of function “SOF-basic.”

See “Strength of Functions Rationale” on page 74 for further information.

6 TOE SUMMARY SPECIFICATION

This chapter describes the Security Functions implemented by the TOE to address the Security Functional Requirements claimed by the TOE (see "TOE Security Functional Requirements" on page 29).

The mapping of the TOE Security Functions to the Security Functional Requirements is summarized in TOE Security Functions on page 44.

6.1 TOE SECURITY FUNCTIONS

The TOE Security Functions are:

- **Security Audit** – The TOE generates audit information for security-relevant events, transmits audit information from the TOE Clients to the TOE Management Server and enables TOE administrators to view the audit records.
- **Identification and Authentication** – The TOE allows only TOE administrators who have been successfully identified (by the TOE) and authenticated (by the IT Environment) to maintain the TOE and its data, including defining Protection Policies and viewing audit records.
- **Security Management** – The TOE enables TOE administrators to define and manage Protection Policies that specify access controls to the physical ports and storage devices of the TOE Client. The TOE also enables the administrator to define other administrators and manage the access control and audit functions.
- **Policy Enforcement** – The TOE protects TOE Client machines by enforcing, on their physical interfaces (ports) and storage media, the policies defined by TOE administrators.
- **Protection of the TSF** – The TOE and IT Environment protect TSF data stored in the TOE and in transit between TOE components from disclosure and modification. The TOE and IT environment work together to ensure the TSP enforcement functions are not bypassed and that the TOE is protected from interference and tampering.

Note - In the detailed descriptions of the Security Function in the following sections, a text box to the left of a paragraph indicates the Security Functional Requirements the implementation of which is described in that paragraph.

6.1.1 SECURITY AUDIT

6.1.1.1 SECURITY FUNCTIONAL REQUIREMENTS

The Security Audit function satisfies the following Security Functional Requirements:

FAU_ARP_EXP.1	The TOE provides the capability to generate an alert for each auditable event. The TOE administrator is able to select the audited events that will also generate an alert and is able to configure where the alert will be sent.
FAU_GEN.1	Audit records are generated for the appropriate security relevant events and include the date and time of the event, type of event, subject identity, and outcome of the event.
FAU_SAR.1	The TOE provides authorized administrators with the ability to read and interpret audit data.
FAU_SAR.2	Access to audit records is restricted to the authorized administrators.

FAU_SAR.3 The TOE provides authorized administrators with the capability to search and sort the audit records based on various criteria.

FAU_SEL.1 The TOE provides the capability to select which auditable events will be audited, based on object identity and event type.

FAU_STG.1A The TOE protects stored audit records from deletion and detects modifications to the audit data.

FAU_STG.1B The IT environment protects stored audit records from unauthorized modification or deletion.

FPT_STM.1 The IT environment provides reliable time stamps for use by the TOE.

6.1.1.2 SECURITY FUNCTION DESCRIPTION

FAU_GEN.1

The TOE Client generates audit events and stores then in the Client Log. The TOE Client is able to generate audit records of the following auditable events:

- Port initialization
- Port activity
- Port device activity
- WiFi network activity
- Storage device activity
- Protection suspension
- Protection resumption
- Unsuccessful and successful attempts to uninstall the TOE Client
- Attempts to tamper with the TOE Client.

The TOE Management Server also generates audit events and stores them in the Server Log. The TOE Management Server is able to generate audit records of the following auditable events:

- Login and logout attempts at the Management Console
- Protection policy updates
- Role changes.

FPT_STM.1

Each audit record, whether generated by the TOE Client or the TOE Management Server, includes the date and time as obtained from the IT environment (OS), subject identity, type of event, and its outcome (success or failure).

FAU_SEL.1

The authorized administrator specifies in the Protection Policy the auditable events that will be audited by the TOE Client. Events related to activity on ports, port devices, WiFi networks and storage devices can be selected based on the port type, device type, WiFi connection type, or device group. Events related to protection suspension, tampering attempts, and uninstall attempts can be selected based on the event type. The authorized administrator also selects the auditable events that will be audited by the TOE Management Server based on event type.

FAU_ARP_
FXP.1

In addition, the authorized administrator can specify any auditable event as an event that will generate an alert, which will be sent to a destination configured by the authorized administrator for immediate attention. See “Policy Enforcement” on page 50 for more information on these events.

FAU_STG.1A
FAU_STG.1B

The Client Logs are stored on the TOE Client machine in encrypted form, using a symmetric key generated by the IT Environment on behalf of the TOE Client for each session, and stored by the

TOE Client in encrypted form. The encrypted audit files are transmitted from the TOE Client to the TOE Management Server over an SSL channel. Audit records are sequentially numbered (throughout all sessions) so that deletion of the local audit file before transmission to the TOE Management Server leaves gaps in the sequence which are detected by the TOE Management Server. If the last audit records in the local file are deleted before transmission, the gap will be detected by the TOE Management Server upon the next transmission. The underlying operating systems of both the TOE Client and the TOE Management Server are also relied on to provide protection of stored audit records from unauthorized modification or deletion, through use of file system access controls.

The Client can be configured so that audit records are uploaded to the Management Server immediately after they are generated on the Client, further reducing the possibility of tampering on the Client.

FAU_SAR.1
FAU_SAR.2
FAU_SAR.3

All audit records (Client Logs and Server Logs) are stored in the TOE database on the Management Server and can be viewed only by authorized administrators (i.e., the Administrator role and users who have the 'Read Logs' role permission), using the TOE Management Console. The authorized administrator can search and sort audit records based on various parameters (including date/time, subject identity, and event type).

6.1.2 IDENTIFICATION AND AUTHENTICATION (I&A)

6.1.2.1 SECURITY FUNCTIONAL REQUIREMENTS

The Identification and Authentication (I&A) function satisfies the following Security Functional Requirement:

FIA_UID.2A	The TOE requires each user to be successfully identified before granting access to the TOE and any of its functions.
FIA_UID.2B	The IT environment requires each user to be successfully identified before granting access to the TOE and any of its functions.
FIA_UAU.2	The IT environment requires each user to be successfully authenticated before granting access to the TOE and any of its functions.

6.1.2.2 SECURITY FUNCTION DESCRIPTION

FIA_UID.2A
FIA_UID.2B
FIA_UAU.2

In order to log on as an administrator, a user must provide their user name, password and domain to the TOE Management Console. The TOE queries Active Directory to confirm the user's credentials and the groups to which the user belongs. If the login is successful, the user is granted access to TOE Management Console with the role permissions associated by the TOE with the user groups to which the user belongs—the user has the union of all role permissions assigned to all user groups of which the user is a member. Administrator access is denied to anyone who is not a member of an administrator group, even if the correct credentials are provided at login.

If the login is unsuccessful, the user is not granted any administrative privileges. Unsuccessful login attempts are logged.

6.1.3 SECURITY MANAGEMENT

6.1.3.1 SECURITY FUNCTIONAL REQUIREMENTS

The Security Management function satisfies the following Security Functional Requirements:

FIA_ATD.1	The IT environment maintains the user identity, password, and group membership security attribute for individual users, thus enabling the TOE to identify users and determine the role permissions for authorized administrators.

FMT_MOF.1 The TOE restricts the ability to enable and disable the access control function to appropriately authorized administrators.

FMT_MTD.1A The TOE restricts the ability to modify the set of audited events to appropriately authorized administrators.

FMT_MTD.1B The TOE restricts the ability to manage Protection Policies to appropriately authorized administrators.

FMT_MTD.1C The TOE restricts the ability to manage Device Model Groups, Distinct Device Groups, Approved WiFi Network Groups, Storage Model Groups, and Distinct Storage Groups to appropriately authorized administrators.

FMT_MTD.1D The TOE restricts the ability to manage administrative roles to the Super Administrator.

FMT_MTD.1E The TOE restricts the ability to modify the set of generated security alerts to appropriately authorized administrators.

FMT_MTD.1F The TOE restricts the ability to modify the list of security alert destinations to appropriately authorized administrators.

FMT_SMF.1 The TOE performs the following security management functions: enable and disable the access control function; modify the set of audited events; manage Protection Policies; manage Device Model Groups, Distinct Device Groups, Approved WiFi Network Groups, Storage Model Groups, and Distinct Storage Groups; manage administrative roles; modify the set of generated security alerts; and modify the list of security alert destinations.

FMT_SMR.1 The TOE maintains the role of Super Administrator (which implements the Administrator role in the SFR) and administrative roles defined by associating role permissions with user groups, and is able to associate users with roles.

6.1.3.2 SECURITY FUNCTION DESCRIPTION

FMT_SMR.1

Access to the TOE Management Server is controlled using existing groups in Active Directory. By default, access is granted to users who have Local Administrator privileges on the computer hosting the TOE Management Server.

FIA_ATD.1

Administrators must provide user name, password and domain in order to log in at the TOE Management Console and assume the administrative role defined by their privileges. User credentials are verified by Active Directory. In addition, the TOE verifies that the administrator is a member of one the administrator groups.

FMT_MTD.1D

At installation, the TOE defines a built-in administrator role called ‘Super Administrator’, which has all administrative privileges. This role cannot be modified or deleted. The Super Administrator can create, modify and delete additional administrator groups with different privileges using role permissions. The TOE defines the following role permissions, which are grouped according to functional area of the TOE Management Console—each permission in each functional group can be individually assigned:

- For Policies
  - Read, Write, Publish
- For Logs
  - Read, Write Queries
- For Clients

    - Read, Grant Suspend Passwords
- For Global Policy Settings
    - Read, Write
- For Administration
    - Read, Write.

An administrator is granted the privileges assigned to the group to which he belongs. If the administrator is a member of multiple groups, the administrator is granted the union of all privileges associated with those groups. Administrator access is denied to anyone who is not a member of an administrator group, even if the correct credentials are provided at login.

TOE data is stored in a MySQL database on the TOE Management Server. Only authorized administrators can access the TOE data through the TOE Management Console interface. TOE data include:

- Protection Policies
- Protection Policy templates
- TOE Client software
- Safend and Management Server certificates
- administrative privileges associated with each user group
- system-wide parameters
- audit data (including alert destinations, level of detail, upload triggers (disk space, *etc.*), frequency of uploads, *etc.*)

FMT_SMF.1

The TOE Management Console provides the following security management functions:

- Enable and disable the access control function
- Modify the set of audited events
- Create, modify, and delete Protection Policies
- Create, modify and delete the Device Model Groups, Distinct Device Groups, Approved WiFi Network Groups, Storage Model Groups, and Distinct Storage Groups, which are used to grant access to specified device models or individually identified devices
- Create, modify and delete groupings of role permissions, which are associated with user groups in the IT environment to define administrative roles
- Modify the set of generated security alerts
- Modify the list of security alert destinations.

FMT_MOF.1

The administrator is able to disable and enable the access control function on a TOE Client by generating a suspension password and providing this to the TOE Client user. The suspension password, when entered on the TOE Client, causes the enforcement of the Protection Policy to be suspended for a period of time specified by the administrator. The ability to generate a suspension password is restricted to the Super Administrator and to an administrator with the 'Grant Suspend Password' role privilege.

FMT_MTD.1A
FMT_MTD.1E
FMT_MTD.1F

Authorized administrators define the set of auditable events to be audited, alert messages (those audit events that are also alerts), alert destinations, and frequency of audit record uploads to the Management Server. The ability to specify the auditable events to be audited and the audit events that will generate a security alert is restricted based on the source of the audit event. Only the Super Administrator and an administrator with the 'Write Policies' role permission can specify the audit events and security alerts for policy-specific audit events generated by the TOE Client (i.e., events related to ports and storage devices), since these are specified within the Protection Policy. Only the Super Administrator and an administrator with the 'Write Global Policy Settings' role permission can specify logging and security alerts for TOE Client events that are not policy-specific (e.g., tampering attempts, policy updates, protection suspension on the client), since these are specified via Global Policy Settings. Only the Super Administrator and an administrator with the 'Write Administration' role permission can specify the audit events and security alerts for audit events generated by the TOE Management Server.

Only the Super Administrator and an administrator with the 'Write Administration' role permission can modify the list of alert destinations for audit events generated by the TOE Management Server, while only the Super Administrator and an administrator with the 'Write Global Policy Settings' role permission can modify the list of alert destinations for audit events generated by the TOE Client. The administrator can specify the following alert destinations:

- Email to one or more addresses
- SNMP trap to third-party network monitoring systems (e.g., IBM Tivoli or HP OpenView)
- Insertion of an entry in the Windows Event Log on a specific host
- Running a custom executable.

FMT_MTD.1B
FMT_MTD.1C

The enforcement of access control on the TOE Clients is based on the Protection Policy associated with the user logged on to the endpoint hosting the TOE Client, or to the Protection Policy associated with the endpoint if the user does not have their own Protection Policy. The TOE restricts the ability to create, modify, and delete Protection Policies to the Super Administrator and to administrators with the 'Write Policies' role permission. Within the Protection Policy, it is possible to grant access to specific device types or models, or individually identified devices or WiFi networks, based on membership of specially defined groups. The TOE restricts the ability to create, modify and delete these groups to the Super Administrator and to administrators with the 'Write Policies' role permission.

Templates can be used to define default parameters for Protection Policies, and new Protection Policies based on those templates can be defined.

Administrators export the TOE Client software directly to Active Directory as Group Policy Objects (GPOs), where it is assigned to Organizational Units (OUs). The TOE Client software is then deployed to the endpoints through GPO on a "silent install" basis.

Administrators export Protection Policies directly from the TOE Management Server to Active Directory as Group Policy Objects (GPOs), where they are assigned to Organizational Units (OUs) and then deployed to the Safend Protector client at endpoints through GPO.

Alternatively, administrators can export the Protection Policies to a shared folder, which can then be imported into network management software and distributed to clients.

The TOE Management Server continuously monitors and displays the status of TOE Clients in real time (for example, which Protection Policy a Client is enforcing, date and time of last update, version of Client software, *etc.*) in the Management Console, enabling administrators to identify and diagnose problems with Clients (regarding which Clients alerts may have also been received) and to take corrective action, for example, to re-install software or Protection Policies.

6.1.4 POLICY ENFORCEMENT

6.1.4.1 SECURITY FUNCTIONAL REQUIREMENTS

The Policy Enforcement function satisfies the following Security Functional Requirements:

FDP_ACC.1A The TOE enforces the Port Access Control SFP on all ports monitored by the TOE.

FDP_ACF.1A The TOE enforces the Port Access Control SFP based on the settings defined in the subject Protection Policy and the attributes associated with ports.

FDP_ACC.1B The TOE enforces the Storage Device Access Control SFP on all removable storage devices and media.

FDP_ACF.1B The TOE enforces the Storage Device Access Control SFP based on the settings defined in the subject Protection Policy and the attributes associated with storage devices.

FPT_RVM.1 The TOE ensures that its security functions cannot be bypassed by restricting access to TOE data to authorized administrators and by monitoring the endpoints and ensuring, for each endpoint, that the TOE Client has been properly installed, that its files (including drivers) and registry values have not been tampered with and that is enforcing a Protection Policy.

6.1.4.2 SECURITY FUNCTION DESCRIPTION

FDP_ACC.1A
FDP_ACF.1A
FDP_ACC.1B
FDP_ACF.1B

The initial behavior of the Policy Enforcement function, which takes effect immediately upon the installation of the TOE Client software, allows all communication through the protected ports. This ensures that there is no change in the behavior of endpoint machines until TOE administrators define and install a Protection Policy. Once a Protection Policy has been defined on the Management Server and installed on the Client, only communications explicitly permitted by the Protection Policy are allowed; communications not explicitly permitted by the Protection Policy are blocked.

The TOE Client enforces the Protection Policy by imposing a protocol-level, generic, semi-permeable barrier – a "Digital Membrane"– that is "wrapped around" controlled interfaces. At the heart of the digital membrane is a kernel-level protocol inspection engine that analyses in real time all inbound and outbound communication for the interface. The Digital Membrane monitors and controls all incoming and outgoing traffic for each interface, blocking or allowing access based on the Protection Policy.

Figure 4 shows how the TOE Client components are imposed just above the hardware and are thus able to control all access requests to the interface. The TOE Client obtains information on the logged-in user from the Client machine OS, as well as information about the device attached to the interface (for example, device type and serial number).

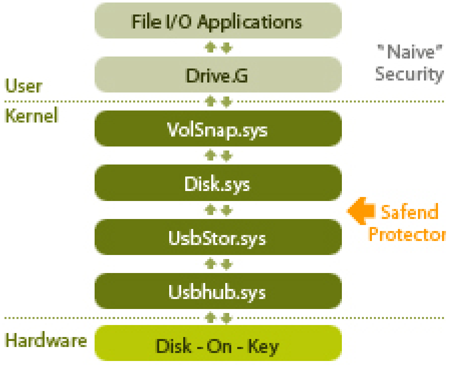

Figure 4 Digital Membrane – TOE Client Kernel-Layer Security

Because the kernel-level driver has complete access to information about the port (for example, the type: USB, FireWire, wireless, etc.), its parameters (for example, in the case of a wireless network port, the SSID; or for storage devices, their capacity), and the unique identifiers of the attached device (for example, in the case of a storage device, its model number and serial number) the TOE Client is able to enforce a fine-grained Protection Policy based on a wide variety of information about the port and the device attached to it.

Each TOE Client enforces one of two Protection Policies: either the one associated with the endpoint machine (i.e., client host) or the one associated with the user logged in at the endpoint machine.

When a user logs into the endpoint machine, the TOE determines whether a Protection Policy is defined for that user. If so, then that Protection Policy is enforced. Otherwise, the endpoint Protection Policy is enforced. At any given time only one of these Protection Policies is enforced, based on whether a Protection Policy is defined for the user logged into the machine.

The TOE examines each access request to a port or storage device and allows it to proceed or blocks it, as specified by the Protection Policy. If the access is explicitly allowed by the Protection Policy, the TOE allows it to proceed. If the access is not explicitly allowed, the TOE blocks the access and the event is regarded as an attempt to violate the Protection Policy.

When the TOE Client detects an attempt to violate the Protection Policy, it can generate an audit record (and optionally an alert) if specified in the Protection Policy. TOE Client audit events are recorded locally (on the TOE Client machine) in encrypted form and periodically transferred for storage to the TOE Management Server over an SSL channel. Management Server audit events are stored in files on the Management Server.

FPT_RVM.1

In addition to monitoring access attempts to the endpoint ports and storage devices, the TOE monitors the state of the Protection Policy and generates alerts when tampering attempts are detected (for example, deleting TOE files or drivers, terminating Client processes, *etc.*).

Enforcement of the Protection Policy can be temporarily suspended at the endpoint by the user requesting a one-time password from a TOE administrator. The administrator generates the password on the TOE Management Server and transmits it off-line (for example, by telephone or by hand delivery) to the endpoint user. The endpoint user enters the password on the TOE Client, which validates it. At the end of the suspension period, Protection Policy enforcement automatically resumes. This suspension password mechanism has a strength of function of SOF-Basic.

The TOE Client also provides a limited administrator interface that allows the administrator to suspend protection. This requires the administrator to enter a Client Administration Password, which the administrator defines on the TOE Management Server for all Protection Policies or on a per-Policy basis. This Client Administration Password mechanism has a strength of function of SOF-Basic.

A password, defined by the administrator on the TOE Management Server for all Protection Policies or on a per-Policy basis, is also required to uninstall the TOE Client. If the TOE Client is uninstalled, the event is logged. In addition, the Management Server displays the status of all Client machines and indicates those where the TOE Client has been uninstalled. The uninstall password mechanism has a strength of function of SOF-Basic.

Note that if the TOE Client is configured according to vendor recommendations, only TOE Client machine users with administrative privileges can uninstall the TOE Client. This check is performed by the IT Environment. The TOE's uninstall password mechanism provides additional protection against unauthorized uninstallation.

6.1.5 PROTECTION OF THE TSF

6.1.5.1 SECURITY FUNCTIONAL REQUIREMENTS

The Protection of the TSF Security Function satisfies the following Security Functional Requirements:

FCS_COP.1 The TOE uses the IT Environment MSFT CAPI for cryptographic operations such as hashing, signature generation, signature verification, encryption and decryption.

FPT_ITT.1 The TOE uses IT Environment provided SSL to protect the TOE data from disclosure and modification when it is transmitted between separate parts of the TOE.

FPT_RVM.1 The TOE ensures that its security functions cannot be bypassed by restricting access to TOE data to authorized administrators and by monitoring the endpoints and ensuring, for each endpoint, that the TOE Client has been properly installed, that its files (including drivers) and registry values have not been tampered with and that is enforcing a Protection Policy.

FPT_SEP.1 The IT environment maintains a separate domain for its execution that protects it from interference and tampering by untrusted subjects, and enforces separation between the security domains of subjects in the TSC.

6.1.5.2 IT ENVIRONMENT

Of the four Security Functional Requirements which satisfy the Protection of the TSF Security Function, three (FCS_COP.1, FPT_ITT.1 and FPT_SEP.1) are fulfilled by the IT Environment, specifically by SSL and MSFT CAPI (encryption and decryption functionality). FPT_RVM.1 is fulfilled by the TOE.

6.1.5.3 SECURITY FUNCTION DESCRIPTION

Protecting Data in Storage on the Client (endpoint)

FCS_COP.1

Audit records generated on the TOE Client are encrypted on the TOE Client, transmitted to the TOE Management Server, where they are decrypted and consolidated with other audit records generated by other TOE Clients.

FPT_SEP.1

The IT Environment on the TOE Client protects TOE processes from tampering by unauthorized users. TOE processes run in OS modes to which unauthorized users have no access.

Protecting Data in Transit

FCS_COP.1
FPT_ITT.1

The IT Environment utilizes a combination of physical configuration, encryption and authentication in order to protect the confidentiality and integrity of TSF data.

Two X.509 certificates are used to ensure the integrity of data transmitted between the TOE Management Server and the TOE Clients.

a. A third-party (Verisign) certificate is used to ensure the integrity of the TOE Client software package.

b. A Safend-generated Management Server certificate, included in the TOE Client software package, is used to ensure the integrity of Protection Policies delivered to the TOE Client.

Table 5 below lists the TSF data transmitted between the TOE components, how the data integrity is assured and when the data is encrypted.

Table 5 TOE Inter-Component Communication

transmitted entity	**between**		**and**	**via**	**protection mechanism**
TSF data	TOE Management Server	⇔	TOE Management Console	directly	SSL, using the keys in the Management Server's Safend-generated certificate.
TOE Client software	TOE Management Server	⇨	TOE Client machines	network management software	The TOE Client software is signed with Safend's Verisign certificate. Both certificates are included in the TOE Client software package.
Protection Policy	TOE Management Server	⇨	TOE Clients	network management software	The Protection Policy is encrypted (see notes below) and signed with the Management Server's Safend-generated certificate.
Audit data (log entries)	TOE Clients	⇨	TOE Management Server	directly	SSL

Notes to Table 5

1. Only the TOE Management Server authenticates itself in SSL sessions. Neither the TOE Client nor the TOE Management Console authenticates itself.
2. The TOE Client software is not encrypted.
3. The TOE Client software installation MSI file is signed with the Safend Verisign-generated X.509 certificate. In addition, each binary component is signed with the same certificate. Authentication is performed by the IT Environment.

4. The TOE Client can be installed over an insecure network (for example, the Internet). It is not impossible for an attacker to install a bogus TOE Client, but the TOE Management Server will become aware of this and alert the TOE administrators.
5. The Protection Policy is encrypted in transit from the TOE Management Server to the TOE Client using the Protection Policy Symmetric Key, which is generated on the Management Server when it is installed and transmitted (in the clear) to the endpoint as part of the TOE Client software package. This is not considered a security risk because knowledge of this key enables only the ability to read the endpoint's Protection Policy (which can in any case be deduced by successively attaching devices and seeing if they are allowed or not) but not to modify or circumvent the Protection Policy. In order to change the Protection Policy, both the symmetric key and the Management Server's private key are required, since the policy is encrypted by the symmetric key and digitally signed using an RSA 1024 bit modulus, with SHA-1 as the hashing algorithm. Without the Management Server's private key, a malicious user on the client machine cannot successfully tamper with the policy.
6. The TOE Client receives the Management Server certificate as part of the TOE Client software package and also as part of the Protection Policy. Before installing the Protection Policy, the TOE Client verifies that the Management Server certificate attached to the Protection Policy is the same as the one it received when it (the TOE Client) was installed.
7. Audit data are stored on the TOE Client machine in encrypted form, using a symmetric key generated by the TOE Client for each session, and stored by the TOE Client in encrypted form.
8. If an integrity violation is detected, the IT Environment aborts the transaction.

Note - All alerts are also logged.

Cryptographic Keys

Both asymmetric and symmetric encryption mechanisms are generated by the IT Environment.

- Asymmetric key pairs are generated when the TOE is installed and are not changed. The public key is included in the Management Server's Safend-generated certificate. These key pairs are used for SSL communications, to sign and validate Protection Policies, and to encrypt and decrypt the symmetrical key used for encrypting TOE Client audit data.
- Symmetric keys are generated on the Management Server (for the encryption of Protection Policies) and on the TOE Client (for encryption of audit data).

  The first key (for the encryption of Protection Policies) never changes.

  The second key (for encryption of audit data) changes for each session (the interval between sending audit data to the Management Server). The key is encrypted (using a public key generated on the Management Server) before it is stored in the Client audit file, and obfuscated before being stored in memory. It is zeroized in memory when it is no longer needed, just before the generation of a new key.

6.1.5.4 TOE DATA PROTECTION

This section describes the mechanisms used to protect TOE data.

TOE Management Server to TOE Management Console

Communication between the TOE Management Server and the TOE Management Console is over an SSL channel (see "SSL" on page 56). The TOE Management Server authenticates itself to the TOE Management Console with its self-signed Safend certificate (X.509).

TOE Client Software in Storage on the Management Server

Only authorized administrators have access to the TOE Client software stored on the Management Server.

TOE Client Software in Transit From the Management Server to the TOE Client

The TOE Client software installation MSI file is signed with a Safend certificate (X.509), provided by Verisign. In addition, each binary component is signed with the same certificate. The parameters are:

- Signature algorithm: SHA-1-RSA
- Public Key: RSA (1024 bit modulus)
- Thumb Print algorithm: SHA-1

The mechanisms used to prevent and detect the installation of a "bogus" TOE Client are described in "Bogus Client" on page 57.

TOE Client Software in Storage on the TOE Client

Upon initialization, the TOE Client validates the signatures of each of its binary components. If the validation is unsuccessful, the TOE Client generates an alert and the component is not used. Validated components are "locked" using a kernel level driver, thus preventing modification or deletion by the user.

Since the TOE Client can be installed over an insecure network (for example, the Internet), it is not impossible for an attacker to install a bogus TOE Client. However, the TOE Management Server will become aware of this and alert the TOE administrators (see "Bogus Client" on page 57 for details).

Note - All alerts are also logged.

Protection Policies in Transit From the Management Server to the TOE Client

Protection Policies are encrypted (3DES CBC, 112 bits) and signed (RSA-SHA-1, 1024 bit modulus) by the TOE Management Server. The TOE Client decrypts the Protection Policy and validates its signature using keys the TOE Client receives as part of the TOE Client software package. These keys, stored on the TOE Client, are protected from disclosure by a variety of tamper-resistant obfuscation mechanisms.

Before loading a Protection Policy, the TOE Client decrypts it and validates its signature. If the validation is unsuccessful, the TOE Client generates an alert and reverts to the previous Protection Policy.

Note - All alerts are also logged.

Protection Policies in Storage in the TOE Client

See "TOE Client Enforcement Protection" on page 57 for a description of how the Protection Policy on the TOE Client is protected from tampering.

Audit Data in Storage on the TOE Client

Audit data are stored on the TOE Client machine in encrypted form (3DES CBC, 112 bits), using a symmetric key generated by the TOE Client for each session, and stored by the TOE Client in encrypted form, using a public key (RSA, 1024 bit modulus) generated by the TOE Management Server.

Audit records are sequentially numbered so that deletion of the local audit file before transmission to the Management Server leaves gaps in the sequence which are detected by the Management Server and indicated to the administrator. The Client can be configured so that audit records are uploaded to the Management Server immediately after they are generated on the Client, further reducing the possibility of tampering on the Client.

The TOE provides no interface for modifying audit records stored on the TOE Client machine.

Audit Data in Transit From the TOE Client to the Management Server

Audit data is sent from the TOE Client to the TOE Management Server over an SSL channel (see "SSL" below). The TOE Management Server authenticates itself to the TOE Client with its self-signed Safend certificate (X.509).

The Protection Policy package includes the Management Server's self-signed Safend certificate and the Management Server's IP address. With this information, the TOE Client knows where to send audit data and is able to authenticate the TOE Management Server.

The Management Server decrypts the symmetric key used by the TOE Client to encrypt the audit records (using the private key) and then decrypts the audit records using the symmetric key.

SSL

SSL is implemented by the IT Environment, and is based on the Microsoft RSA SChannel Cryptographic Provider implementation (IIS on the server side).

- Signature algorithm: SHA-1
- Public Key: RSA (1024 bit modulus)
- Thumb Print algorithm: SHA-1
- Symmetric encryption: 3DES.

The TOE Management Server authenticates itself to the TOE Management Console and TOE Client with its self-signed Safend certificate (X.509). Neither the TOE Client nor the TOE Management Console authenticates itself.

TOE Data Stored on the Management Server

FPT_SEP.1

Access to TOE processes and TOE data on the Management Server (Protection Policies, TOE Client software, audit data generated by both the TOE Clients and the TOE Management Server, *etc.*) is restricted to authorized administrators of the TOE and of the IT Environment (the OS). In addition, these data are inside the enterprise network and are protected from tampering by appropriate security mechanisms (firewalls, OS level protections, *etc.*).

The TOE provides no interface for modifying audit records stored on the TOE Management Server.

The IT Environment protects TOE processes from tampering by unauthorized users.

Third Party Network Management Software

TOE Client software is signed by the TOE Management Server before it is routed to the network management software (for example, Active Directory).

Protection Policies are encrypted and signed by the TOE Management Server before they are routed to the network management software (for example, Active Directory). The third party network management software does not have access to the keys required to decrypt the TOE components stored on them.

6.1.5.5 TOE CLIENT ENFORCEMENT PROTECTION

This section describes the mechanisms used to prevent TOE users from tampering with their endpoint machines in order to circumvent the enforcement of the Protection Policy.

Endpoint Machine Configuration

The vendor strongly recommends that endpoint machines be configured as follows:

- Users are not defined as administrators of their machines, restricting the ability of non-administrator users to access privileged processes.
- The boot sequence is set to start with the local hard-drive, and then to lock down the BIOS configuration with a password, ensuring that non-administrator users are unable to boot from a CD or another drive.
- Administrators should delete the SCC file on the Client (which contains the symmetric key required to encrypt log data in transit from Client to Server and asymmetric key required to decrypt Protection Policies) immediately after installation of the Client. The file can be safely deleted because the key has already been read and stored by the Client.

These recommendations are contained in the documentation provided by the vendor: [SP-IG] and [SP-UG].

Anti-Tampering

FPT_RVM.1

A variety of mechanisms (automatic restart, multiple copies, etc.) prevent the end-user from circumventing the TOE by uninstalling or deleting the TOE Client and the Protection Policy. These mechanisms are implemented by Client kernel-level components which are inaccessible to non-administrator users.

An alert and an audit record are generated when a tampering attempt is detected.

- TOE Client processes continuously confirm each others' presence. If a process is missing, it restarted by another process.
- TOE Client process binaries are locked down at the kernel level so that they cannot be deleted by non-administrator users.
- Kernel components (e.g, drivers) are validated during boot. If the signatures are incorrect, an alert is sent to the Management Server, which initiates a re-install of the TOE Client.
- The TOE Client service continuously monitors registry settings and restores them if they have been corrupted.
- Multiple encrypted copies of the Protection Policy are stored in the registry, monitored and restored if they are corrupted or deleted.
- In the event that the Protection Policy becomes unusable, an alert is sent to the Management Server, which initiates a re-install of the Protection Policy. Until a new Protection Policy is received and installed, a built-in policy that blocks all communications on all interfaces except all except Human Interface Devices (keyboard, mouse, etc.) is enforced.

Bogus Client

FPT_RVM.1

An attempt by the endpoint user to circumvent the enforcement of the Protection Policy by substituting a bogus client for the TOE Client is addressed as follows:

- If the TOE Client machine is configured in accordance with vendor recommendations, the user will not have administrative privileges and will be unable to install and uninstall software on the machine. Remote installation of a bogus client (e.g., via Active Directory) requires the cooperation of an administrator and would in any case be ineffective for the reasons given in the following paragraphs.

- Once a legitimate TOE Client and Protection Policy have been installed, the TOE Client's anti-tampering mechanisms do not allow the non-administrator user to terminate the kernel level processes or delete the drivers and files upon which the enforcement of the Protection Policy depend. If these mechanisms fail, a block-all Policy is enforced.
- The bogus client will not have access to all the keys required for modifying Protection Policies. In addition, the Protection Policy is re-enforced automatically by Active Directory when the Management Server receives an alert that the Protection Policy is unusable
- Since audit records are sequentially numbered throughout all sessions, any interruption in the number sequence is detected by the Management Server.

6.2 TOE SECURITY ASSURANCE MEASURES

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

- Configuration Management
- Delivery and Operation
- Development
- Guidance Documents
- Tests
- Strength of Function Analysis and Vulnerability Assessment

6.2.1 CONFIGURATION MANAGEMENT

The configuration management measures applied by the developer ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. The developer thus ensures changes to the implementation representation are controlled. The developer performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, vulnerability analysis documentation, and configuration management documentation and all of these items are identified in the Configuration Management document [CC-CFM] as configuration items.

These activities are documented in:

- [CC-CFM] Safend Protector Configuration Management

The Configuration management assurance measure satisfies the following EAL 2 Assurance Requirements:

- ACM_CAP.2

6.2.2 DELIVERY AND OPERATION

The developer provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. TOE delivery procedures describe all applicable procedures to be used to prevent inappropriate access to the TOE. The developer also provides documentation that describes the steps necessary to install the TOE in accordance with the evaluated configuration.

These activities are documented in:

- [CC-DEL-IGS] Safend Protector Secure Delivery, Installation, Generation and Startup
- [SP-IG] Safend Protector Installation Guide

The Delivery and Operation assurance measure satisfies the following EAL 2 Assurance Requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 DEVELOPMENT

The developer has documents describing all facets of the design of the TOE. 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).

These activities are documented in:

- [CC-FSP] Safend Protector Functional Specification
- [CC-HLD] Safend Protector High-Level Design

The Development assurance measure satisfies the following EAL 2 Assurance Requirements:

- ADV_FSP.1
- ADV_HLD.1
- ADV_RCR.1

6.2.4 GUIDANCE DOCUMENTS

The developer provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- [SP-UG] Safend Protector User Guide

The Guidance documents assurance measure satisfies the following EAL 2 Assurance Requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 TESTS

The test 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.

These activities are documented in:

- [CC-ATE] Safend Protector Test Plan
- [CC-ATE-RES] Safend Protector Test Results

The Tests assurance measure satisfies the following EAL 2 Assurance Requirements:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.2.6 VULNERABILITY ANALYSIS

The developer has conducted a strength of function analysis wherein all permutational or probabilistic security mechanisms have been identified and analyzed, resulting in a demonstration that all of the relevant mechanisms fulfill the minimum strength of function claim, SOF-Basic.

The developer performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

The strength of function analysis and vulnerability analysis activities are documented in:

- [CC-AVA] Safend Protector Vulnerability Analysis.

The Vulnerability assessment assurance measure satisfies the following EAL 2 assurance requirements:

- AVA_SOF.1
- AVA_VLA.1.

7 PROTECTION PROFILE CLAIMS

This Security Target does not claim conformance to any registered Protection Profile.

8 RATIONALE

8.1 INTRODUCTION

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

- Security Objectives
- Security Requirements
- TOE Summary Specification
- SFR dependencies
- Internal consistency

8.2 SECURITY OBJECTIVES RATIONALE

This section shows that:

- each threat, organizational security policy and assumption is addressed by at least one security objective, and
- each security objective addresses at least one threat, organizational security policy or assumption.

Table 6 Mapping of Security Environment to Security Objectives

	O.MANAGE	O.AUTH	O.AUDIT-MGM	O.AUDIT-RVW	O.ACCESS	O.AUDIT-ATK	O.ALERT	O.CLIENT	O.E.ADMIN	O.E.BACKUP	O.E.LOCATE	O.E.INSTALL	O.E.PROTECT	O.E.TIME	O.E.TOE-PRT	O.E.TRANSMIT
T.UA-ACCESS		X						X							X	X
T.UA-ACTION			X	X										X		
T.ATTACK	X					X	X									
T.DISABLE								X							X	
T.DISCLOSURE	X				X											
P.MANAGE								X	X			X				
A.ADMIN									X	X		X				
A.LOCATE											X					
A.PROTECT													X			

8.2.1 T.UA-ACCESS

An unauthorized user may gain access to or modify TOE data, whether stored in the TOE components or in transit between distributed parts of the TOE, in order to acquire knowledge of and/or circumvent the protection afforded by the TOE.

This threat is addressed as follows:

- O.AUTH ensures that only authorized administrators are able to access the TOE and its data.
- O.E.TOE-PRT ensures the IT environment protects TOE data from unauthorized deletion or modification.
- O.E.TRANSMIT ensures that that the IT Environment protects TSF data in transit between TOE components.
- O.CLIENT ensures that the TOE Client and its data are protected from unauthorized disabling, uninstallation, deletion, and modification, either by preventing these events or by detecting them and alerting the TOE administrators.

8.2.2 T.UA-ACTION

An authorized user may exceed his or her privileges and gain access to or perform unauthorized modifications of TOE data which go undetected, in order to acquire knowledge of and/or circumvent the protection afforded by the TOE.

This threat is addressed as follows:

- O.AUDIT-MGM ensures that the TOE can generate audit records of all security-related actions of TOE users to ensure that these actions can be traced to the users who performed them.
- O.AUDIT-RVW ensures that the TOE provides authorized administrators with the capability to review audit records.
- O.E.TIME ensures the IT environment can supply the TOE with a reliable time stamp for use in audit records.

8.2.3 T.DISABLE

An attacker may disable or delete the TOE Client or modify its behavior and thus expose the protected machine (and through the compromised machine, the network as well) to attack. Note that the attacker described here may well be the authorized user of the TOE Client machine.

This threat is addressed as follows:

- O.E.TOE-PRT ensures that the IT Environment protects the TOE data from unauthorized deletion or modification.
- O.CLIENT ensures that the TOE Client and its data are protected from unauthorized disabling, uninstallation, deletion, and modification, either by preventing these events or by detecting them and alerting the TOE administrators.

8.2.4 T.ATTACK

An attacker may gain access to the protected machine (the TOE Client) via the machine's physical interfaces, using any of a variety of well-known attack methods, and thereby gain access to and/or modify user data, or install malware on the endpoint machine or in the protected network.

This threat is addressed as follows:

- O.MANAGE ensures that the TOE provides the functionality that enables an authorized administrator to configure the TOE, define and enforce TOE security policies, and monitor the TOE's activities.
- O.AUDIT-ATK ensures that the TOE is able to generate audit records of detected attempted violations of the Protection Policy.

- O.ALERT ensures that the TOE responds to specified events by sending alerts to administrators.

8.2.5 T.DISCLOSURE

An endpoint user accidentally or deliberately exposes user data by writing it to a removable storage device or media, or sending it to an insecure device or network.

This threat is addressed as follows:

- O.ACCESS ensures that the TOE controls access to endpoint ports and storage devices based on centrally managed Protection Policies.
- O.MANAGE ensures that the TOE provides the functionality that enables an authorized administrator to define the Protection Policies to be enforced by the TOE.

8.2.6 P.MANAGE

IT Systems are protected from unauthorized access and modification.

This organizational policy is addressed as follows:

- O.CLIENT ensures that the TOE Client and its data are protected from unauthorized disabling, uninstallation, deletion, and modification, either by preventing these events or by detecting them and alerting the TOE administrators.
- O.E.TOE-PRT ensures that the IT Environment protects the TOE data from unauthorized deletion or modification.
- O.E.ADMIN ensures that authorized TOE administrators are properly trained in all aspects of TOE and TOE resource administration, and are neither negligent nor hostile.
- O.E.INSTALL ensures that the TOE and its associated hardware and software environment are installed, maintained and managed in a manner that complies with the TOE security objectives.

8.2.7 A.ADMIN

The administrators assigned to manage the TOE are competent, properly trained, not careless, not willfully negligent, not hostile, follow the guidance and instruction provided in the TOE documentation, and install and administer the TOE in a manner consistent with organizational policies.

This assumption is addressed as follows:

- O.E.ADMIN ensures that authorized TOE administrators are properly trained in all aspects of TOE and TOE resource administration, and are neither negligent nor hostile.
- O.E.BACKUP ensures that the TOE, its data and the systems on which it runs are restored to a secure state after failure by following the relevant backup and restore procedures.
- O.E.INSTALL ensures that the TOE and its associated hardware and software environment are installed, maintained and managed in a manner that complies with the TOE security objectives.

8.2.8 A.LOCATE

The TOE Management Server and TOE Management Console and other components on which they rely (for example, the Active Directory Server) are located in a physically secured area, protected from unauthorized physical access.

This assumption is addressed as follows:

- O.E.LOCATE ensures that TOE Management Server, TOE Management Console and other components on which they rely (for example, the Active Directory machine) must be located in a physically secured area, protected from unauthorized physical access.

8.2.9 A.PROTECT

The endpoint devices that host the TOE Client are physically protected to the degree necessary to ensure that the TOE Client cannot be uninstalled or otherwise disabled by direct physical interaction with the endpoint device.

This assumption is addressed as follows:

- O.E.PROTECT ensures that the endpoint devices that host the TOE Client are physically protected to the degree necessary to ensure that the TOE Client cannot be uninstalled or otherwise disabled by direct physical interaction with the endpoint device.

8.3 SECURITY REQUIREMENTS RATIONALE

This section provides a rationale for the completeness and internal consistency of the claimed Security Functional Requirements in meeting the identified security objectives (see "Security Objectives" on page 27) by showing that each Security Functional Requirement addresses at least one security objective.

Table 7 Mapping of Security Functional Requirements to Security Objectives

	O.MANAGE	O.AUTH	O.AUDIT-MGM	O.AUDIT-RVW	O.ACCESS	O.AUDIT-ATK	O.ALERT	O.CLIENT	O.E.TIME	O.E.TOE-PRT	O.E.TRANSMIT
FAU_ARP_EXP.1						X	X	X			
FAU_GEN.1			X			X		X			
FAU_SAR.1				X							
FAU_SAR.2				X							
FAU_SAR.3				X							
FAU_SEL.1	X										
FAU_STG.1A			X								
FAU_STG.1B										X	
FCS_COP.1											X
FDP_ACC.1A					X						
FDP_ACC.1B					X						
FDP_ACF.1A					X						
FDP_ACF.1B					X						
FIA_ATD.1										X	
FIA_UAU.2										X	
FIA_UID.2A		X									
FIA_UID.2B										X	
FMT_MOF.1	X										
FMT_MTD.1A	X										
FMT_MTD.1B	X										
FMT_MTD.1C	X										
FMT_MTD.1D	X										
FMT_MTD.1E	X										
FMT_MTD.1F	X										
FMT_SMF.1	X										
FMT_SMR.1	X										
FPT_ITT.1											X
FPT_RVM. 1					X			X			
FPT_SEP.1										X	

	O.MANAGE	O.AUTH	O.AUDIT-MGM	O.AUDIT-RVW	O.ACCESS	O.AUDIT-ATK	O.ALERT	O.CLIENT	O.E.TIME	O.E.TOE-PRT	O.E.TRANSMIT
FPT_STM.1									X		

8.3.1 O.MANAGE

The TOE must provide the functionality that enables an authorized administrator to configure the TOE, define TOE security policies (for example, the Protection Policy), and monitor the TOE's activities.

FAU_SEL.1 The TOE provides the ability to select which auditable events will be audited, based on the object identity for auditable events associated with ports and storage devices, and on the event type for all other auditable events. This enables the authorized administrator to monitor the TOE's activities that are of most interest.

FMT_MOF.1 The TOE restricts the ability to enable and disable the access control security function to authorized administrators, by providing authorized administrators with the capability to generate a suspension password that an endpoint user can use to temporarily disable the Port Access Control SFP and the Storage Device Access Control SFP.

FMT_MTD.1A Only authorized administrators can modify the set of audited events. This supports FAU_SEL.1 by ensuring only the authorized administrator can determine what events will or will not be audited.

FMT_MTD.1B Only authorized administrators have the ability to create, modify, or delete the Protection Policies used to enforce the Port Access Control SFP and the Storage Device Access Control SFP.

FMT_MTD.1C Only authorized administrators have the ability to create, modify and delete the various groups used to grant specific "white list" access to devices and networks within the scope of the access control SFPs.

FMT_MTD.1D Only authorized administrators have the ability to create administrative roles, by associating role permissions with user groups defined in the IT environment.

FMT_MTD.1E Only authorized administrators have the ability to specify which auditable events will result in the generation of a security alert.

FMT_MTD.1F Only authorized administrators have the ability to configure the destinations to which generated security alerts will be sent.

FMT_SMF.1 The TOE performs the following security management functions: enable and disable the access control function; modify the set of audited events; manage Protection Policies; manage device groups; manage administrative roles; manage the set of security alerts; and manage the security alert destinations.

FMT_SMR.1 The TOE maintains the role of Administrator, which has full administrative control of the TOE, and allows the creation and management of other administrative roles based on groupings of role permissions. The TOE is able to associate users with roles, based on group membership.

8.3.2 O.AUTH

The TOE must ensure that only authorized administrators are able to access the TOE and its data.

FIA_UID.2A The TOE requires each user to identify himself before granting access to the TOE and any of its functions.

8.3.3 O.AUDIT-MGM

The TOE must provide the capability to generate audit records of all security-related actions of TOE users to ensure that these actions can be traced to the users who performed them.

FAU_GEN.1 Audit records are generated for the appropriate security relevant events and include the date and time of the event, type of event, user identity, and outcome of the event.

FAU_STG.1A The TOE protects stored audit data from deletion and detects modifications to the audit data.

8.3.4 O.AUDIT-RVW

The TOE must provide authorized administrators with the capability to review audit records.

FAU_SAR.1 The TOE provides authorized administrators with the ability to read and interpret audit data.

FAU_SAR.2 Access to audit records is restricted to the authorized administrators.

FAU_SAR.3 The TOE provides authorized administrators the capability to search the audit trail based on various criteria and to sort the results returned based on various criteria.

8.3.5 O.ACCESS

The TOE must control access to endpoint ports and storage devices based on centrally managed Protection Policies.

FDP_ACC.1A The TOE enforces the Port Access Control SFP on users and client hosts and all ports of the client host (endpoint).

FDP_ACC.1B The TOE enforces the Storage Device Access Control SFP on users and client hosts and all storage devices of the client host (endpoint)

FDP_ACF.1A The TOE enforces the Port Access Control SFP based on port attributes and the Protection Policy associated with the logged in user, or with the client host if the logged in user does not have an associated Protection Policy.

FDP_ACF.1B The TOE enforces the Storage Device Access Control SFP based on storage device attributes and the Protection Policy associated with the logged in user, or with the client host if the logged in user does not have an associated Protection Policy.

FPT_RVM.1 The TOE ensures that its security functions cannot be bypassed by restricting access to TOE data to authorized administrators and by monitoring the endpoints and ensuring, for each endpoint, that the TOE Client has been properly installed, that its files and registry values have not been tampered with and that is enforcing a Protection Policy.

8.3.6 O.AUDIT-ATK

The TOE must provide the capability to generate audit records of detected violation attempts.

FAU_GEN.1 Audit records are generated for the appropriate security relevant events and include the date and time of the event, type of event, subject identity, and outcome of the event.

FAU_ARP_EXP.1 In the event of an auditable event for which alert generation is configured, the TOE sends an alert to a configured alert destination and generates an audit record.

8.3.7 O.ALERT

The TOE must have the capability to respond to specified events by alerting administrators.

FAU_ARP_EXP.1 In the event of an auditable event for which alert generation is configured, the TOE sends an alert to a configured alert destination and generates an audit record.

8.3.8 O.CLIENT

The TOE must have the ability to protect the TOE Client and its data, including Protection Policies and audit data, from unauthorized disabling, uninstallation, deletion, and modification, either by preventing these events or by detecting them and alerting the TOE administrators.

FAU_GEN.1 The TOE is able to generate audit records of attempts to tamper with the TOE client.

FAU_ARP_EXP.1 The TOE is able to generate alerts of attempts to tamper with the TOE client.

FPT_RVM.1 The TOE ensures that its security functions cannot be bypassed by restricting access to TOE data to authorized administrators and by monitoring the endpoints and ensuring, for each endpoint, that the TOE Client has been properly installed, that its files and registry values have not been tampered with and that is enforcing a Protection Policy.

8.3.9 O.E.TIME

The IT environment must provide a reliable time-stamp for the TOE to be used for audit records.

FPT_STM.1 The IT environment provides reliable time stamps for use by the TOE.

8.3.10 O.E.TOE-PRT

The IT environment must protect the TOE data from unauthorized deletion or modification.

FAU_STG.1B The IT environment protects the TOE audit records stored on the TOE Client and the TOE audit records stored on the Management Server from unauthorized modification or deletion.

FIA_ATD.1 The IT environment maintains the user security attributes of user identity, group membership, and password, in order to support identification and authentication of users within the IT environment, including users of the TOE. The TOE administrators also obtain their role permissions to perform security management functions through membership of groups defined in the IT environment.

FIA_UAU.2 The IT environment requires authentication before any TOE TSF action.

FIA_UID.2B The IT environment requires identification before any TOE TSF action.

FPT_SEP.1 The IT Environment enforces domain separation and protects the TOE from unauthorized access by untrusted subjects.

8.3.11 O.E.TRANSMIT

The IT Environment must have the ability to protect TSF data in transit between distributed parts of the TOE.

FCS_COP.1	The IT Environment encrypts TOE data to prevent its disclosure and employs digital signature and checksum mechanisms to prevent its modification.
FPT_ITT.1	The IT Environment protects TOE data from modification when it is in transit between separate parts of the TOE.

8.4 SECURITY FUNCTIONAL REQUIREMENTS DEPENDENCIES RATIONALE

Table 8 Functional Requirements Dependencies

Requirement	Dependencies	Included ?
TOE SFRs		
FAU_ARP_EXP.1	FAU_GEN.1 FMT_MTD.1	Yes, TOE SFR Yes, TOE SFR (FMT_MTD.1F)
FAU_GEN.1	FPT_STM.1	Yes, IT environment SFR
FAU_SAR.1	FAU_GEN.1	Yes, TOE SFR
FAU_SAR.2	FAU_SAR.1	Yes, TOE SFR
FAU_SAR.3	FAU_SAR.1	Yes, TOE SFR
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	Yes, TOE SFR Yes, TOE SFR (FMT_MTD.1A)
FAU_STG.1A	FAU_GEN.1	Yes, TOE SFR
FAU_STG.1B	FAU_GEN.1	Yes, TOE SFR
FDP_ACC.1A	FDP_ACF.1	Yes, TOE SFR (FDP_ACF.1A)
FDP_ACC.1B	FDP_ACF.1	Yes, TOE SFR (FDP_ACF.1B)
FDP_ACF.1A	FDP_ACC.1 FMT_MSA.3	Yes, TOE SFR (FDP_ACC.1A) No, see rationale below
FDP_ACF.1B	FDP_ACC.1 FMT_MSA.3	Yes, TOE SFR (FDP_ACC.1B) No, see rationale below
FIA_UID.2	none	
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	Yes, TOE SFR Yes, TOE SFR
FMT_MTD.1A	FMT_SMF.1 FMT_SMR.1	Yes, TOE SFR Yes, TOE SFR
FMT_MTD.1B	FMT_SMF.1 FMT_SMR.1	Yes, TOE SFR Yes, TOE SFR
FMT_MTD.1C	FMT_SMF.1 FMT_SMR.1	Yes, TOE SFR Yes, TOE SFR
FMT_MTD.1D	FMT_SMF.1 FMT_SMR.1	Yes, TOE SFR Yes, TOE SFR
FMT_MTD.1E	FMT_SMF.1 FMT_SMR.1	Yes, TOE SFR Yes, TOE SFR

Requirement	Dependencies	Included ?
FMT_MTD.1F	FMT_SMF.1 FMT_SMR.1	Yes, TOE SFR Yes, TOE SFR
FMT_SMF.1	none	
FMT_SMR.1	FIA_UID.1	Yes, hierarchical to the TOE SFR FIA_UID.2
FPT_RVM.1.	none	
IT Environment SFRs		
FCS_COP.1	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	Yes, IT environment SFR Yes, IT environment SFR Yes, IT environment SFR
FIA_ATD.1	none	
FIA_UAU.2	FIA_UID.1	The Security Functional Requirement FIA_UAU.2 is satisfied by the IT Environment. The TOE plays no role in the authentication of users.
FIA_UID.2	none	
FPT_ITT.1	none	
FPT_SEP.1	none	
FPT_STM.1	none	

FDP_ACF.1 has a dependency on FMT_MSA.3, which requires that the TSF provide default values for relevant object security attributes (which can potentially be overridden by an initial value). However, in the Port Access Control SFP and the Storage Device Access Control SFP, the controlled objects are Ports and Storage Devices respectively. Both of these object types are physical entities that are outside the TOE and already exist when the TOE is installed and started. Furthermore, the object security attributes on which access control decisions are made are attributes of these physical entities and likewise exist outside the scope of the TOE. The TOE can detect the attributes and make access control decisions based on those attributes and the settings in the applicable Protection Policy, but the TOE has no control over the initial values of those attributes. It is therefore not necessary to require the TOE to provide default values for the object security attributes, and hence the dependencies of FDP_ACF.1A and FDP_ACF.1B on FMT_MSA.3 do not need to be satisfied.

8.5 EXPLICITLY STATED REQUIREMENTS RATIONALE

This Security Target defines the explicit functional requirement FAU_ARP_EXP.1. It is modeled on FAU_ARP.1 defined in Part 2 of the CC, but differs from that SFR by specifying that the TSF be able to generate an alert for any auditable event, not just on the detection of a potential security violation. The approach to security alerts implemented by the TOE is to allow the TOE administrator to directly specify the auditable events that are of sufficient interest to warrant generation of an alert, rather than to monitor audited events and to make a decision on a potential security violation based on some analysis of those events (as represented by the FAU_SAA family of requirements). The TOE also provides the administrator the ability configure the destinations to which alerts will be sent.

8.6 SECURITY ASSURANCE REQUIREMENTS RATIONALE

EAL2 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. The security objectives defined for the TOE are consistent with an EAL2 assurance level and EAL2 is sufficient to satisfy the security objectives of the TOE.

EAL2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behavior. The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain). EAL2 also provides assurance through a configuration list for the TOE and evidence of secure delivery procedures. The TOE and related documentation have all of the characteristics required for EAL2.

Table 9 provides a mapping of the EAL2 Security Assurance Components to the documentation demonstrating how the TOE and the TOE developer satisfy the requirements. The detailed justification for the mapping is given in "TOE Security Assurance Measures" on page 54.

Table 9 Mapping of Security Assurance Requirements to Documents and Rationale

Assurance Components	Documents Satisfying the Assurance Component	Rationale
ACM_CAP.2	[CC-CFM] Safend Protector Configuration Management [CC-CIL] Safend Protector Configuration Item List	Shows the CM system is being used, and includes a Configuration Item List which comprises the following: • list of the source code files and version numbers • list of design documents with version numbers • test documents with version numbers • user and administrator documentation with version numbers
ADO_IGS.1	[SP-IG] Safend Protector Installation Guide [CC-AGD] Safend Protector Administrator and User Guidance [CC-DEL-IGS] Safend Protector Delivery and Installation	Provides detailed instructions for installation of the product.
ADO_DEL.1		Provides a description of all procedures that are necessary to maintain security when distributing the product to the distributor. Applicable across all phases of delivery from packaging, storage, distribution.
ADV_FSP.1	[CC-FSP] – Safend Protector Functional Specification	Describes the TSF interfaces and TOE functionality.
ADV_HLD.1	[CC-HLD] – Safend Protector High-Level Design	Describes the TOE subsystems and their associated security functionality
ADV_RCR.1	[CC-RCR] – Safend Protector Representation Correspondence	Provides the following two dimensional mappings: • TSS and functional specification; • functional specification and high-level design.
AGD_ADM.1	[SP-UG] Safend Protector User	Describes how to securely administer the TOE.

Assurance Components	Documents Satisfying the Assurance Component	Rationale
AGD_USR.1	Guide	Describes the secure use of the TOE.
ATE_IND.2	[CC-ATE] – Safend Protector Test Plan [CC-ATE-RES] – Safend Protector Test Results Test documentation	Not applicable
ATE_COV.1		Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_FUN.1		Test documentation includes test plans and procedures and expected and actual results.
AVA_SOF.1	[CC-SOF] – Safend Protector Strength of Functions Analysis	Provides a rationale that each mechanism identified in the ST as having an SOF meets or exceeds the minimum strength level specified there.
AVA_VLA.1	[CC-VLA] – Safend Protector Vulnerability Assessment	Provides an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

8.7 STRENGTH OF FUNCTIONS RATIONALE

The claimed TOE minimum strength of function is SOF-basic. This strength of function level was selected because it generally corresponds with the claimed assurance level of EAL 2.

8.7.1 TOE

The TOE implements one applicable (*i.e.*, probabilistic or permutational) Security Functional Requirement:

- FPT_RVM.1.1

The TOE allows temporary suspension of Client Protection Policy enforcement by the endpoint user. To accomplish this temporary suspension, the endpoint user must enter a password communicated to him by a TOE administrator. This password mechanism is of a probabilistic or permutational nature.

The TOE also allows temporary suspension of Client Protection Policy enforcement by an administrator, who must first enter a Client Administration Password. The Client Administration Password is defined by the administrator on the TOE Management Server for all Protection Policies or on a per-Policy basis. This password mechanism is of a probabilistic or permutational nature.

The TOE also requires entry of a password in order to uninstall the TOE Client. As with the Client Administration Password, the Client Uninstall Password is defined by the administrator on the TOE Management Server for all Protection Policies or on a per-Policy basis. This password mechanism is of a probabilistic or permutational nature.

The intent is that these password mechanisms meet or exceed SOF-basic and the evidence can be found in the strength of function analysis included in [CC-SOF].

8.7.2 IT ENVIRONMENT

The IT Environment implements one applicable Security Functional Requirement:

- FIA_UAU.2

It is assumed that the IT Environment would provide mechanisms of the appropriate strength; that is, meeting or exceeding SOF-basic.

8.8 TOE SUMMARY SPECIFICATION RATIONALE

The following table represents a mapping between the TOE Security Functions in this Security Target to their related TOE Security Functional Requirements; the rationale for how each security function meets the corresponding Security Functional Requirement is provided in "TOE Security Functions" on 44, which lists each SFR and describes how the SFR is met by the TOE Security Function.

Table 10 Mapping of TOE Security Functional Requirements to TOE Security Functions

Security Functional Requirements	**TOE Security Functions**				
	Security Audit	Identification and Authentication	Security Management	Policy Enforcement	Protection of the TSF
TOE Security Functional Requirements					
FAU_ARP_EXP.1	X				
FAU_GEN.1	X				
FAU_SAR.1	X				
FAU_SAR.2	X				
FAU_SAR.3	X				
FAU_SEL.1	X				
FAU_STG.1A	X				
FDP_ACC.1A				X	
FDP_ACC.1B				X	
FDP_ACF.1A				X	
FDP_ACF.1B				X	
FIA_UID.2A		X			
FMT_MOF.1			X		
FMT_MTD.1A			X		
FMT_MTD.1B			X		
FMT_MTD.1C			X		
FMT_MTD.1D			X		
FMT_MTD.1E			X		
FMT_MTD.1F			X		
FMT_SMF.1			X		
FMT_SMR.1			X		
FPT_RVM.1				X	X
IT Environment Security Functional Requirements					
FAU_STG.1B	X				X
FCS_COP.1					X

Security Functional Requirements	**TOE Security Functions**				
	Security Audit	Identification and Authentication	Security Management	Policy Enforcement	Protection of the TSF
FIA_ATD.1			X		
FIA_UAU.2		X			
FIA_UID.2B		X			
FPT_ITT.1					X
FPT_SEP.1					X
FPT_STM.1	X				