Security Target

Symantec™ Network Access Control Version 12.1.2

Document Version 0.12

February 14, 2013

Prepared For:

Symantec Corporation

350 Ellis Street

Mountain View, CA 94043

www.symantec.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Network Access Control Version 12.1.2. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	Security Target: Symantec™ Network Access Control Version 12.1.2
ST Revision	0.12
ST Publication Date	February 14, 2013
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	Symantec™ Network Access Control Version 12.1.2.

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets and a change in text color, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *underlined italicized* text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FIA_UAU.1.1 (1) and FIA_UAU.1.1 (2) refer to separate instances of the FIA_UAU.1 security functional requirement component.

Italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table[1] describes the terms and acronyms used in this document:

TERM	DEFINITION
CC	Common Criteria version 3.1 (ISO/IEC 15408)
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
OSP	Organizational Security Policy
SFR	Security Functional Requirement
SFP	Security Function Policy
SOF	Strength Of Function
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target Of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy

Table 2 – Terms and Acronyms Used in Security Target

[1] Derived from the IDSPP

1.6 TOE Overview

The Symantec Network Access Control Version 12.1.2 validates and enforces policy compliance for all types of endpoints on all types of networks. This validation and enforcement process begins prior to an endpoint's connection to the network and continues throughout the duration of the connection, with policy serving as the basis for all evaluations and actions. It blocks or quarantines non-compliant devices from accessing the corporate network and resources. It hosts Integrity tests against pre-defined templates such as patch level, service packs, antivirus, and personal firewall status, as well as custom created checks tailored for the enterprise environment. It provides pervasive endpoint coverage for managed and unmanaged laptops, desktops, and servers existing both on and off the corporate network.

Network Access Control Version 12.1.2 may hereafter also be referred to as the TOE in this document.

1.7 TOE Description

The product type of the Target of Evaluation (TOE) described in this Security Target (ST) is a network access control solution running on clients (e.g., desktops and laptops), an Enforcer to grant the endpoint network access, block network access, or remediate non-compliant computers, and a management component running on a central server to control and monitor execution of the network access control client application.

The primary purpose of Symantec Network Access Control is to ensure that the clients that run the software are compliant with an organization's security policies. Security policy compliance is enabled by using the Host Integrity policies created in the Symantec Endpoint Protection Manager component. Together, Host Integrity policies and hardware enforcement keep non-compliant computers off of the network. This software also can direct the clients that are not compliant to remediation servers, where software, patches, and virus updates can be downloaded.

Symantec Network Access Control is a companion product to Symantec Endpoint Protection, with which it shares the same management console. Symantec Endpoint Protection provides Symantec AntiVirus protection with advanced threat protection that protects endpoints (laptops, desktops, and servers) from both known threats and those threats that have not been seen before.

1.7.1 Physical Boundary

The TOE is a combined hardware/software TOE and is defined as the Network Access Control Version 12.1.2. In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	Network Access Control Version 12.1.2
TOE Hardware	Symantec Network Access Control Enforcer 6100 Series Appliance

TOE COMPONENT	VERSION/MODEL NUMBER
IT Environment	See Section 1.7.2 – Hardware and Software Supplied by the IT Environment

Table 3 – Evaluated Configuration for the TOE

The TOE boundary is shown below:

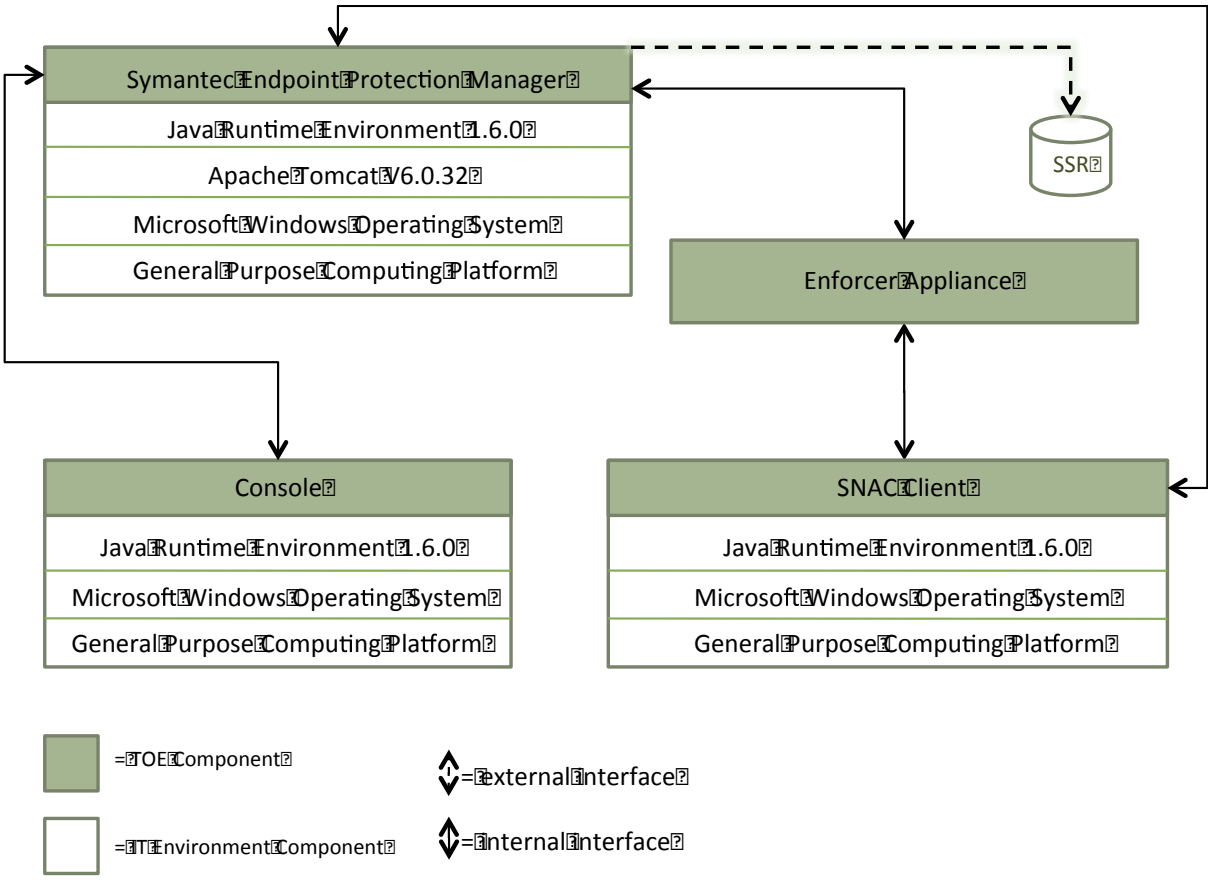

Figure 1 – TOE Boundary

At a high level, the TOE interfaces include the following:

1. Software interfaces for connection to internal TOE components and external IT products.
2. Software interfaces to receive and process traffic from internal TOE components and external IT products.
3. Management interface to handle administrative actions[2].
4. Hardware interfaces for the Enforcer appliance.

The TOE's evaluated configuration requires one or more instances of a SNAC Client, one instance of a SEP Manager, one or more instances of a workstation for management via Console, and one or more

[2] Note that Identification and Authentication functions for the Administrative role using SEPM Console are performed by the IT Environment (i.e., via LDAP).

instances of an Enforcer appliance configured as Gateway Enforcer. Communications between the components are protected via SSL tunnel, provided by the Operational Environment.

1.7.2 Hardware and Software Supplied by the IT Environment

The Symantec Endpoint Protection Manager system requirements are as follows:

- 32-bit processor: 1-GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended)
- 64-bit processor: 2-GHz Pentium 4 with x86-64 support or equivalent minimum Intel Itanium IA-64 is not supported.
- Operating systems: Windows 7 (32-bit and 64-bit SP1), Windows XP (32-bit and 64-bit, SP-3), Windows Server 2003 (32-bit, 64-bit, R2, SP-2), Windows Server 2008 (32-bit, 64-bit SP2), Windows Small Business Server 2008 (64-bit), Windows Small Business Server 2011 (64-bit), or Windows Essential Business Server 2008 (64-bit)
- Other Software: Java Runtime Environment 1.6.0, Apache Tomcat V6.0.32
- Windows Vista (32-bit, 64-bit) is not officially supported.
- RAM memory: 1 GB of RAM minimum (2 GB of RAM recommended)
- Hard disk: 4 GB or more free space
- Hardware and software for Symantec Security Response

The client and console system requirements are as follows:

- 32-bit processor: for Windows operating systems, 1-GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended); for Mac operating systems, Intel Core Solo, Intel Core Duo
- 64-bit processor: for Windows operating systems, 2-GHz Pentium 4 with x86-64 support or equivalent minimum; for Mac operating systems, Intel Core 2 Duo, Intel Quad-Core Xeon
- Intel Itanium IA-64 is not supported.
- PowerPC is not supported (32-bit or 64-bit).
- Operating systems: Windows XP (32-bit and 64-bit, SP-3), Windows XP Embedded (SP-3), Windows Vista (32-bit and 64-bit SP2), Windows 7 (32-bit and 64-bit SP1), Windows Server 2003 (32-bit, 64-bit, R2, SP-2), Windows Server 2008 (32-bit, 64-bit SP2), Windows Small Business Server 2008 (64-bit), or Windows Essential Business Server 2008 (64-bit), Mac OS X 10.4, 10.5 or 10.6
- RAM memory: 512 MB of RAM minimum (1 GB of RAM recommended)
- Hard disk: 400 MB or more free space
- Browser: Internet Explorer 6 or later. Required to install the client by using Remote Push (Windows clients only).

The Symantec Endpoint Protection Manager includes an embedded database (tested configuration). Alternatively, the following version of Microsoft SQL Server can be used:

- SQL Server 2008, SP-2 or later

1.7.3 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

TSF	DESCRIPTION
Audit	The audit services include details on actions taken when a non-compliant endpoint is detected as well as administrative actions performed while accessing the TOE. The TOE generates audits when security-relevant events occur, stores the audit information on the local system, transmits the audit information to a central management system, generates alarms for designated events, and provides a means for audit review. Protection of audit data in the audit trail involves the TOE and the Operating System (OS). The TOE controls the insertion of audit events into the audit log and the deletion of audit events from the audit log. The OS provides basic file protection services for the audit log.
Information Flow Control	The TOE is designed to help prevent unwanted and non-compliant endpoints from gaining access to the local area network. The Client compares endpoint configuration with defined security policies; a non-compliant endpoint is not allowed full access to the network.
Management	The TOE provides administrators with the capabilities to configure, monitor and manage the TOE to fulfill the Security Objectives. Security Management principles relate to Information Flow Control and Audit.

Table 4 – Logical Boundary Descriptions

1.8 TOE Security Functional Policies

The TOE supports the following Security Functional Policy:

1.8.1 NAC Information Flow Control SFP

The TOE implements an information process flow policy named *NAC Information Flow Control SFP*. This SFP determines the procedures utilized to process information entering the TOE and the action taken upon the detection of an endpoint that is not compliant with the TOE's Host Integrity Policies. The actions taken at the occurrence of a violation is configurable by an authorized administrator via the Symantec Endpoint Protection Manager console.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 conformant and Part 3 conformant at Evaluation Assurance Level 2 augmented with ALC_FLR.2.

2.2 Protection Profile Conformance Claim

The TOE does not claim conformance to a Protection Profile.

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organizational security policy statements or rules with which the TOE must comply.
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.AUDIT_COMPROMISE	A user or process may gain unauthorized access to the audit trail and cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a security relevant event.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.UNAUTH_ENDPOINT	An unidentified or unsecure endpoint may attempt to access a network, resulting in malicious or unidentified activity on that network.
TE.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
TE.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of memory used by the TOE to verify compliance or process administrator requests.

Table 5 – Threats Addressed by the TOE and IT Environment

3.2 Organizational Security Policies

The following Organizational Security Policies apply to the TOE:

POLICY	DESCRIPTION

POLICY	DESCRIPTION
P.ACCESS_BANNER	The system shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ROLES	The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

Table 6 – Organizational Security Policies

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.AUDIT_BACKUP	Administrators will back up the audit files and monitor disk usage to ensure audit information is not lost.
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) nor storage repository capabilities on the system on which SEPM executes.
A.NOEVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.PHYSICAL	It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
A.SECURE_COMMS	It is assumed that the IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.

Table 7 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ADMIN_ROLE	The TOE will provide an authorized administrator role to isolate administrative actions.
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security relevant events.
O.AUDIT_PROTECTION	The TOE will provide the capability to protect audit information.
O.AUDIT_REVIEW	The TOE will provide the capability to selectively view audit information.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE.
O.UNAUTH_ENDPOINT	The TOE will detect unauthenticated, unauthorized, or non-compliant endpoints and deny access to the network until the endpoint is authenticated, authorized, and complaint to internal security policies.

Table 8 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.AUDIT_ALARM	The IT Environment will provide the capability to produce an audit alarm before the audit log is full.
OE.AUDIT_BACKUP	Audit log files are backed up and can be restored, and audit log files will not run out of disk space.
OE.AUDIT_STORAGE	The IT environment will provide a means for secure storage of the TOE audit log files.
OE.DISPLAY_BANNER	The IT environment will display an advisory warning regarding use of the system.
OE.DOMAIN_SEPARATION	The IT environment will provide an isolated domain for the execution of the TOE.
OE.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) nor storage repository capabilities on the system on which SEPM executes.
OE.NO_BYPASS	The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.

OBJECTIVE	DESCRIPTION
OE.NO_EVIL	Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.PHYSICAL	Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
OE.RESIDUAL_INFORMATION	The IT environment will ensure that any information contained in a protected resource within the TOE Scope of Control is not released when the resource is reallocated.
OE.SECURE_COMMS	The IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.
OE.TIME_STAMPS	The IT environment will provide reliable time stamps.
OE.TOE_ACCESS	The IT Environment will provide mechanisms that control a user's logical access to the TOE.

Table 9 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies (if applicable). The following table provides a high level mapping of coverage for each threat, assumption, and policy:

THREATS/ ASSUMPTIONS / OBJECTIVES	A. AUDIT_BACKUP	A.GENPUR	A.NO_EVIL	A.PHYSICAL	A.SECURE_COMMS	T._AUDIT_COMPROMISE	TE.MASQUERADE	TE.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNAUTH_ENDPOINT	P.ACCESS_BANNER	P.ACCOUNTABILITY	P.ROLES
O.ADMIN_ROLE													✓
O.AUDIT_ GENERATION												✓	
O.AUDIT_PROTECTION						✓							
O.AUDIT_REVIEW									✓				
O.MANAGE									✓				
O.UNAUTH_ENDPOINT										✓			
OE.AUDIT_ALARM						✓							
OE.AUDIT_BACKUP	✓												
OE.AUDIT_STORAGE						✓							

THREATS/ ASSUMPTIONS / OBJECTIVES	A. AUDIT_BACKUP	A.GENPUR	A.NO_EVIL	A.PHYSICAL	A.SECURE_COMMS	T._AUDIT_COMPROMISE	TE.MASQUERADE	TE.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNAUTH_ENDPOINT	P.ACCESS_BANNER	P.ACCOUNTABILITY	P.ROLES
OE.DISPLAY_BANNER											✓		
OE.DOMAIN_ SEPARATION						✓			✓				
OE.GENPUR		✓											
OE.NO_BYPASS						✓			✓				
OE.NO_EVIL			✓										
OE.PHYSICAL				✓									
OE.RESIDUAL_ INFORMATION						✓		✓	✓				
OE.SECURE_COMMS					✓								
OE.TIME_STAMPS												✓	
OE.TOE_ACCESS							✓					✓	

Table 10 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

The following table provides detailed evidence of coverage for each threat, policy, and assumption:

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
T.AUDIT_ COMPROMISE: A user or process may cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	**O.AUDIT_PROTECTION:** The TOE will provide the capability to protect audit information. **OE.AUDIT_ALARM:** The IT Environment will provide the capability to produce an audit alarm before the audit log is full. **OE.AUDIT_STORAGE:** The IT Environment will contain mechanisms to provide secure storage and management of the audit log. **OE.RESIDUAL_ INFORMATION:**	**O.AUDIT_PROTECTION** contributes to mitigating this threat by controlling access to the individual audit log records. No one is allowed to modify audit records, the System Administrator is the only one allowed to delete audit records, and the TOE has the capability to overwrite the oldest stored audit records if the audit trail is full. **OE.AUDIT_ALARM** helps prevent the loss of audit records by sending an alarm if the available storage space for the audit log meets a certain threshold. **OE.AUDIT_STORAGE** contributes to mitigating this threat by restricting the ability of users in the IT Environment to access the audit log file.

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
	The IT Environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. **OE.DOMAIN_SEPARATION:** The IT Environment will provide an isolated domain for the execution of the TOE. **OE.NO_BYPASS:** The IT Environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	**OE.RESIDUAL_INFORMATION** prevents a user not authorized to read the audit trail from access to audit information that might otherwise be persistent in a resource used by the TOE (e.g., memory). By preventing residual information in a resource, audit information will not become available to any user or process except those explicitly authorized for that data. **OE.DOMAIN_SEPARATION** contributes to countering this threat by ensuring that the TSF is protected from users through mechanisms other than its own interfaces. If the OS could not maintain and control a domain of execution for the TSF separate from other processes, the TSF could not be trusted to control access to the resources under its control, which includes the audit trail which are always invoked is also critical to the migration of this threat. **OE.NO_BYPASS** ensures audit compromise can not occur simply by bypassing the TSF.
TE.MASQUERADE: A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	**OE.TOE_ACCESS:** The IT Environment will provide mechanisms that control a user's logical access to the TOE.	**OE.TOE_ACCESS** mitigates this threat by requiring authorized administrators and workstation users to be identified and authenticated, a necessary step in controlling the logical access to the TOE and its resources by constraining how and when users can access the TOE. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.
TE.RESIDUAL_DATA: A user or process may gain unauthorized access to data through reallocation of memory used by the TOE to scan files or process	**OE.RESIDUAL_INFORMATION:** The IT Environment will ensure that any information contained in a protected resource within the TOE Scope of Control is not released when the resource is reallocated.	**OE.RESIDUAL_INFORMATION** counters this threat by ensuring that memory contents are not persistent when resources are released by the TOE and allocated to another user/process.

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
administrator requests.		
T.TSF_COMPROMISE: A user or process may gain unauthorized access to data through reallocation of memory used by the TOE to verify compliance or process administrator requests.	**OE.RESIDUAL_INFORMATION:** The IT Environment will ensure that any information contained in a protected resource within the TOE Scope of Control is not released when the resource is reallocated. **OE.DOMAIN_SEPARATION:** The IT environment will provide an isolated domain for the execution of the TOE. **O.AUDIT_REVIEW:** The TOE will provide the capability to selectively view audit information. **O.MANAGE:** The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE. **OE.NO_BYPASS:** The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	**OE.RESIDUAL_INFORMATION** is necessary to mitigate this threat, because even if the security mechanisms do not allow a user to explicitly view TSF data, if TSF data were to inappropriately reside in a resource that was made available to a user, that user would be able to inappropriately view the TSF data. **OE.DOMAIN_SEPARATION** is necessary so that the TSF is protected from other processes executing on the workstation. **O.MANAGE** is necessary because an access control policy is not specified to control access to TSF data. This objective is used to dictate who is able to view and modify TSF data, as well as the behavior of TSF functions. **O.AUDIT_REVIEW** helps to mitigate this threat by providing the Security Administrator with a required minimum set of configurable audit events that could indicate a potential security violation. By configuring these auditable events, the TOE monitors the occurrences of these events (e.g. set number of authentication failures, set number of information policy flow failures, etc.). **O.CORRECT_TSF_OPERATION** provides assurance that the TSF continues to operate as expected in the field. **OE.NO_BYPASS** ensures TSF compromise cannot occur simply by bypassing the TSF.
T.UNAUTH_ENDPOINT: An unidentified or unsecure endpoint may attempt access a network, resulting in malicious or identified activity on that network.	**O. UNAUTH_ENDPOINT:** The TOE will detect unauthenticated, unauthorized, or non-compliant endpoints and deny access to the network until the endpoint is authenticated, authorized, and complaint to internal security	**O. UNAUTH_ENDPOINT** mitigates this threat by providing mechanisms to prevent a non-compliant endpoint introduced onto a network.

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
	policies.	
P.ACCESS_BANNER: The system shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.	**OE.DISPLAY_BANNER:** The IT Environment will display an advisory warning regarding use of the system.	**OE.DISPLAY_BANNER** satisfies this policy by ensuring that the system displays a banner that provides all authorized users with a warning about the unauthorized use of the system.
P.ACCOUNTABILITY: The authorized users of the TOE shall be held accountable for their actions within the TOE.	**O.AUDIT_GENERATION:** The TOE will provide the capability to detect and create records of security-relevant events associated with users. **OE.TIME_STAMPS:** The IT environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps. **OE.TOE_ACCESS:** The IT environment will provide mechanisms that control a user's logical access to the TOE.	**O.AUDIT_GENERATION** addresses this policy by recording security-relevant events. The administrator's ID is recorded when any security relevant change is made to the TOE. **OE.TIME_STAMPS** plays a role in supporting this policy by requiring the IT environment to provide a reliable time stamp. The audit mechanism is required to include the current date and time in each audit record. **OE. TOE_ACCESS** supports this policy by requiring the IT environment to identify and authenticate all authorized administrators and workstation users prior to allowing any TOE access.
P.ROLES: The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.	**O.ADMIN_ROLE:** The TOE will provide an authorized administrator role to isolate administrative actions.	**O.ADMIN_ROLE** addresses this policy by requiring the TOE to support an administrator role, and restrict specific actions to that role.
A.AUDIT_BACKUP: Administrators will back up the audit files and monitor disk usage	**OE.AUDIT_BACKUP:** Audit log files are backed up and can be restored, and audit log files will not run out of disk	**OE.AUDIT_BACKUP** addresses the assumption by requiring the audit log files to be backed up, and by requiring monitoring of disk space usage to ensure

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
to ensure audit information is not lost.	space.	space is available.
A.GENPUR: There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) nor storage repository capabilities on the system on which SEPM executes.	OE.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) nor storage repository capabilities on the system on which SEPM executes.	OE.GENPUR addresses the assumption by requiring SEPM to execute on a dedicated system.
A.NO_EVIL: Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	**OE.NO_EVIL:** Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.	**OE.NO_EVIL** restates the assumption.
A.PHYSICAL: It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.	**OE.PHYSICAL:** Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.	**OE.PHYSICAL** restates the assumption.
A.SECURE_COMMS: It is assumed that the IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.	**OE.SECURE_COMMS:** The IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.	**OE.SECURE_COMMS** restates the assumption. The workstation OS will provide a secure line of communication for the TOE.

Table 11 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 Extended Security Functional Components

There are no extended security functional components in this evaluation.

5.2 Extended Security Assurance Components

There are no extended security assurance components in this evaluation.

6 Security Requirements

The security requirements that are levied on the TOE are specified in this section of the ST.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and those that were explicitly stated, all of which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1(1)	Audit Review
	FAU_SAR.1(2)	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG.4	Site-Configurable Prevention of Audit Loss
Information Flow Control	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
Security Management	FMT_MOF.1	Management of Security Functions Behavior
	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_MTD.1(1)	Management of TSF Data
	FMT_MTD.1(2)	Management of TSF Data
	FMT_MTD.1(3)	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles

Table 12 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 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) [The events identified in Table 13 – FAU_GEN.1 Events and Additional Information.

]

FAU_GEN.1.2 The TSF shall record within each audit record at last the following information:

a) Date and time of the event, type of event, subject identity (if applicable), 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, [the additional information identified in Table 13 – FAU_GEN.1 Events and Additional Information].

SFR	AUDITABLE EVENTS
FAU_GEN.1	None
FAU_GEN.2	None
FAU_SAR.1(1)	None
FAU_SAR.1(2)	None
FAU_SAR.2	None
FAU_STG.1	None
FAU_STG.4	Selection of an action
FDP_IFC.1	Action taken in response to detection of a non-compliant endpoint
FDP_IFF.1	Action taken in response to detection of a non-compliant endpoint
FMT_MOF.1	None
FMT_MSA.1	None
FMT_MSA.3	None
FMT_MTD.1	None
FMT_SMF.1	None
FMT_SMR.1	None

Table 13 – FAU_GEN.1 Events and Additional Information

6.1.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1(1) The TSF shall provide [the System Administrator] with the capability to read [all audit information] from the audit records **on the central management system**.

FAU_SAR.1.2(1) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.1.1(2) The TSF shall provide [the System Administrator and Workstation Users] with the capability to read [all audit information] from the audit records **on the workstation being used**.

FAU_SAR.1.2(2) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application Note: The Workstation User is permitted to review all audit records saved on the workstation being used by that user. The System Administrator is permitted to review all logs on a specific workstation (which will only apply to that workstation) or on the central management system (which will apply to all workstations within that domain).

6.1.1.4 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.

Application Note: This SFR applies to read access to the audit records through the TSFIs. The IT Environment (OS) is responsible for prohibiting read access to the audit file via OS interfaces.

6.1.1.5 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion **via the TSFI**.

FAU_STG.1.2 The TSF shall be able to *prevent* unauthorized modifications to the audit records in the audit trail **via the TSFI**.

Application Note: FAU_STG.1 applies to both the central management system and the individual workstations.

Application Note: This instance of FAU_STG.1 applies to protection of the audit records via the TSFI. The IT Environment (OS) is responsible for preventing deletion of the audit file via OS interfaces.

6.1.1.6 FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4.1 The TSF shall **provide the administrator the capability to select one or more of the following actions** *overwrite the oldest stored audit records* and [no other actions] to be taken if the audit trail is full.

6.1.2 User Data Protection

6.1.2.1 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [NAC Information Flow Control SFP] on [

Subjects: External IT entities attempting to send traffic through the TOE

Information: Host Integrity Policy

Operations: Block, Remediate, Allow]

6.1.2.2 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [NAC Information Flow Control SFP] based on the following types of subject and information security attributes: [

Subject Security Attributes: Symantec Network Access Control client is running, the client has a unique identifier (UID), the client has been updated with the latest Host Integrity Policy, the client computer passed the Host Integrity check

Information Security Attributes: Antivirus On; Antivirus Updated; Personal Firewall On; Service Pack Updated; Patch Updated; Custom scripts containing "and/or" logic to allow or deny access based on file, process, or registry parameters]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[Monitoring option is enabled for the service and information structure type and:

1. The endpoint is compliant to the Host Integrity Policy or
2. The endpoint is remediated in an isolated area of the network to attain compliance with the Host Integrity Policy or
3. The endpoint MAC address is contained within an exception list configured in the Enforcer

].

FDP_IFF.1.3 The TSF shall enforce the [no additional information flow control SFP rules].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [no explicit authorization rules].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [no explicit denial rules].

6.1.3 Security Management (FMT)

6.1.3.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behavior of, disable, enable* the functions [Auditing, Configuring Host Integrity Policies] to [System Administrator].

6.1.3.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [NAC Information Flow Control SFP] to restrict the ability to *query, modify, delete* the security attributes [TSF data] to [System Administrator].

6.1.3.3 FMT_MSA.3 Static Attribute Initialization

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

FMT_MSA.3.2 The TSF shall allow the [System Administrator] to specify alternative initial values to override the default values when an object or information is created.

6.1.3.4 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1(1) The TSF shall restrict the ability to *query, modify, delete* the [

a) Actions to be taken on workstations when a non-compliant endpoint is detected,

b) Information security attributes to be scanned automatically on workstations,

c) Processes authorized to transmit data over an internal network,

d) Audit logs on the central management system]

to [the System Administrator].

FMT_MTD.1.1(2) The TSF shall restrict the ability to *modify* the [Host Integrity Policies] to [the System Administrator].

FMT_MTD.1.1(3) The TSF shall restrict the ability to *query, delete* the [audit logs on the workstation being used] to [the System Administrator].

6.1.3.5 FMT_SMF.1 Specification of Management Functions

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

a) Configure operation of the TOE on workstations,

b) Update Host Integrity Policies,

c) Acknowledge alert notifications from the central management system,

d) Review audit logs on the central management system,

e) Acknowledge alert notifications on the workstation being used, and

f) Review audit logs on the workstation being used

].

6.1.3.6 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [System Administrator, Administrator, Limited Administrator, Workstation User].

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

6.2 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	None	FPT_STM.1	Satisfied by the Operational Environment (OE.TIME_STAMPS)
FAU_GEN.2	None	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied by the Operational Environment (OE.TOE_ACCESS)
FAU_SAR.1(1)	None	FAU_GEN.1	Satisfied
FAU_SAR.1(2)	None	FAU_GEN.1	Satisfied
FAU_SAR.2	None	FAU_SAR.1	Satisfied
FAU_STG.1	None	FAU_GEN.1	Satisfied
FAU_STG.4	FAU_STG.1	FAU_STG.1, FMT_MTD.1	Satisfied Satisfied
FDP_IFC.1	None	FDP_IFF.1	Satisfied
FDP_IFF.1	None	FDP_IFC.1 FMT_MSA.3	Satisfied
FMT_MOF.1	None	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MSA.1	None	FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied Satisfied
FMT_MSA.3	None	FMT_MSA.1 FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1(1)	None	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1(2)	None	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1(3)	None	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	None	None	None
FMT_SMR.1	None	FIA_UID.1	Satisfied by the Operational Environment (OE.TOE_ACCESS)

Table 14 - TOE SFR Dependency Rationale

6.3 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2). The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
ASE: Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 15 – Security Assurance Requirements at EAL2

6.3.1 Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 2 augmented with ALC_FLR.2. EAL2 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL2 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface.

6.4 Security Requirements Rationale

6.4.1 Security Functional Requirements for the TOE

The following table provides a high level mapping of coverage for each security objective:

SFR \ OBJECTIVE	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.MANAGE	O.UNAUTH_ENDPOINT
FAU_GEN.1		✓				
FAU_GEN.2		✓				
FAU_SAR.1(1)				✓	✓	

SFR \ OBJECTIVE	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.MANAGE	O.UNAUTH_ENDPOINT
FAU_SAR.1(2)				✓	✓	
FAU_SAR.2			✓			
FAU_STG.1			✓			
FAU_STG.4			✓			
FDP_IFC.1						✓
FDP_IFF.1						✓
FMT_MOF.1	✓				✓	
FMT_MSA.1						✓
FMT_MSA.3						✓
FMT_MTD.1(1)	✓				✓	
FMT_MTD.1(2)	✓				✓	
FMT_MTD.1(3)	✓				✓	
FMT_SMF.1	✓				✓	
FMT_SMR.1	✓				✓	

Table 16 – Mapping of TOE SFRs to Security Objectives

The following table provides detailed evidence of coverage for each security objective:

OBJECTIVE	ADDRESSED BY	SFR AND RATIONALE
O.ADMIN_ROLE: The TOE will provide an authorized administrator role to isolate administrative actions.	FMT_MOF.1 FMT_MTD.1(1) FMT_MTD.1(2) FMT_MTD.1(3) FMT_SMF.1 FMT_SMR.1	**FMT_SMR.1** requires that the TOE establish a System Administrator role and **FMT_SMF.1** provides the administrative actions available in the TOE. **FMT_MOF.1, FMT_MTD.1(1)** and **FMT_MTD.1(2)** specify the privileges that only the System Administrator may perform. **FMT_MTD.1(3)** specifies privileges for the System Administrator and Workstation Users.
O.AUDIT_GENERATION:	FAU_GEN.1	**FAU_GEN.1** defines the set of events that the TOE must be capable of recording. This

OBJECTIVE	ADDRESSED BY	SFR AND RATIONALE
The TOE will provide the capability to detect and create records of security relevant events.	FAU_GEN.2	requirement ensures that the Administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. **FAU_GEN.2** ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the userid. In all other cases, the association is based on the source network identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated.
O.AUDIT_PROTECTION: The TOE will provide the capability to protect audit information.	FAU_SAR.2 FAU_STG.1 FAU_STG.4	**FAU_SAR.2** restricts the ability to read the audit trail to the System Administrator, thus preventing the disclosure of the audit data to any other user. However, the TOE is not expected to prevent the disclosure of audit data if it has been archived or saved in another form (e.g., moved or copied to an ordinary file). The FAU_STG family dictates how the audit trail is protected. **FAU_STG.1** restricts the ability to delete audit records to the System Administrator. **FAU_STG.4** defines the actions that must be available to the administrator, as well as the action to be taken if there is no response. This helps to ensure that audit records are kept until the System Administrator deems they are no longer necessary. This requirement also ensures that no one has the ability to modify audit records (e.g., edit any of the information contained in an audit record). This ensures the integrity of the audit trail is maintained.

OBJECTIVE	ADDRESSED BY	SFR AND RATIONALE
O.AUDIT_REVIEW: The TOE will provide the capability to selectively view audit information.	FAU_SAR.1(1) FAU_SAR.1(2)	**FAU_SAR.1(1)** and **FAUSAR.1(2)** provide the ability to review the audits in a user-friendly manner.
O.MANAGE: The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE.	FMT_MOF.1 FMT_MTD.1(1) FMT_MTD.1(2) FMT_MTD.1(3) FMT_SMF.1 FMT_SMR.1 FAU_SAR.1(1) FAU_SAR.1(2)	Restricted privileges are defined for the System Administrator and Workstation Users. **FMT_MOF.1** defines particular TOE capabilities that may only be used by the System Administrator. **FMT_MTD.1(1)**, **FMT_MTD.1(2)**, and **FMT_MTD.1(3)** defines particular TOE data that may only be altered by users of the TOE. **FMT_SMF.1** and **FMT_SMR.1** define the administrative functions and roles provided by the TOE. **FAU_SAR.1(1)** and **FAUSAR.1(2)** provide the ability to review the audits in a user-friendly manner.
O.UNAUTH_ENDPOINT: The TOE will detect unauthenticated, unauthorized, or non-compliant endpoints and deny access to the network until the endpoint is authenticated, authorized, and complaint to internal security policies	FDP_IFC.1 FDP_IFF.1 FMT_MSA.1 FMT_MSA.3	**FDP_IFC.1** defines the information flow control security function policy. **FDP_IFF.1** defines the parameters by which an endpoint can be allowed access to the network. **FMT_MSA.1** restricts the ability to filter traffic to an authorized administrator. **FMT_MSA.3** ensures that the default values of security attributes are restrictive in nature and enforce specification of initial configuration parameters to the Administrator

Table 17 – Rationale for Mapping of TOE SFRs to Objectives

6.4.2 Security Assurance Requirements

This section identifies the Configuration Management, Delivery/Operation, Development, Test, and Guidance measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Architecture Description: Symantec Network Access Control Version 12.1.2
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: Symantec Network Access Control Version 12.1.2
ADV_TDS.1: Basic Design	Basic Design: Symantec Network Access Control Version 12.1.2
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: Symantec Network Access Control Version 12.1.2
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: Symantec Network Access Control Version 12.1.2
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: Symantec Network Access Control Version 12.1.2
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: Symantec Network Access Control Version 12.1.2
ALC_DEL.1: Delivery Procedures	Delivery Procedures: Symantec Network Access Control Version 12.1.2
ALC_FLR.2: Flaw Reporting Procedures	Flaw Reporting Procedures: Symantec Network Access Control Version 12.1.2
ATE_COV.1: Evidence of Coverage	Security Testing: Symantec Network Access Control Version 12.1.2
ATE_FUN.1: Functional Testing	Security Testing: Symantec Network Access Control Version 12.1.2
ATE_IND.2: Independent Testing – Sample	Security Testing: Symantec Network Access Control Version 12.1.2

Table 18 – Security Assurance Rationale and Measures

7 TOE Summary Specification

7.1 TOE Security Functions

The security functions described in the following subsections fulfill the security requirements that are defined in Section 6 – Security Requirements. The security functions performed by the TOE are as follows:

- Audit
- Information Flow Control
- Management

7.1.1 Audit

The TOE provides robust reporting capabilities to provide the System Administrator with insight on the Server and Workstation Host Integrity Policy compliance activities. Additionally, the TOE supports the provision of log data from each system component.

The reporting functions give the up-to-date information to monitor and make informed decisions about the security of the network. The management console Home page displays the automatically generated charts that contain information about the important events that have happened recently in your network. You can use the filters on the Reports page to generate predefined or custom reports. You can use the Reports page to view graphical representations and statistics about the events that happen in your network. You can use the filters on the Monitors page to view more detailed, real-time information about your network from the logs.

Reporting runs as a Web application within the management console, and TOE reporting features include the following:

- Customizable Home page with your most important reports, overall security status, and links to Symantec Security Response
- Summary views of reports on compliance status and site status
- Predefined quick reports and customizable graphical reports with multiple filter options that you can configure
- The ability to schedule reports to be emailed to recipients at regular intervals
- Support for Microsoft SQL or an embedded database for storing event logs
- Configurable notifications that are based on security or compliance events

The TOE generates audit data for various events, and this audit data is aggregated into a series of pre-defined reports. An authorized administrator can view and filter the following reports:

REPORT TYPE	DESCRIPTION
Audit	Displays information about the policies that clients and locations use currently.
Compliance	Displays information about the compliance status of your network. These reports include information about Enforcer servers, Enforcer clients, Enforcer traffic, and host compliance.
Computer Status	Displays information about the operational status of the computers in your network, such as which computers are infected. These reports include information about versions, clients that have not checked in to the server, client inventory, and online status.
System	Displays information about event times, event types, sites, domains, servers, and severity levels.

Table 19 – Available Reports

Reports are available only to operators that have explicit access to reports, and this privilege is defined by the system administrator (i.e., System Administrator role). Only System Administrators can review reports on the SEPM, while System Administrators and Workstations users can review reports on the workstation.

All system reports and audit logs are stored in an embedded Sybase database on the SEPM. If the database reaches storage capacity, the TOE will overwrite the oldest records.

The Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1
- FAU_GEN.2
- FAU_SAR.1(1)
- FAU_SAR.1(2)
- FAU_SAR.2
- FAU_STG.1
- FAU_STG.4

7.1.2 Information Flow Control

Host Integrity Policies are configured to ensure that the client computers that connect to an enterprise network run the required applications and data files. The client that runs a Host Integrity check implements the Host Integrity Policy settings defined by the administrator.

During the Host Integrity check, the client follows the requirements that are set in the Host Integrity Policy. It examines the registry keys, active applications, date and size of a file, and other possible parameters to determine the existence of the required software.

The client automatically generates an entry in the Security log whenever it finds that the required software is not installed on the computer. If user notification is enabled on the client, a message appears on the user's computer.

If the required software is not installed on the computer, the client can be set to silently connect to a remediation server. From there it can download and install the required software. The software can include a software patch, a hotfix, an update to virus definitions, and so on. The client can give the user a choice to download immediately or postpone a download. The computer cannot connect to the enterprise network until the software is installed.

The client can also detect whether or not an antivirus application is out of date. If an antivirus application is older than what a system administrator has specified, the client can be prevented from connecting to the enterprise network. Before it can connect, the client needs an up-to-date version of the antivirus application.

The Host Integrity Policy includes the settings that determine how often the client runs a Host Integrity check on the client computer. The client computer can connect to the network through a Symantec Enforcer. In this scenario, you can set up the Host Integrity Policy such that the client runs the Host Integrity check only when prompted by the Enforcer. The Enforcer can verify the following: the client is running, the client's policy is up to date, and the Host Integrity check is passed before it allows access to the network.

Every time a client receives a new security policy, it immediately runs a Host Integrity check. The client can be set up to automatically download and install the latest security policy. A security log entry is generated if the policy update fails. If user notification is enabled on the client, a message appears on the user's computer.

The following is an example of the kinds of requirements you need to consider when you set up Host Integrity enforcement. In this example, the Host Integrity Policy has been set up to require the following:

- The client runs up-to-date antivirus software
- The Host Integrity check is done only when the client tries to connect to the network through an Enforcer
- The check triggers the actions that takes place silently on the client

The Enforcer automatically does the following:

- Verifies that a client has been installed on a user's computer
- Prompts a client to retrieve updated security policies, if available

The Enforcer then prompts the client to run the Host Integrity check. The client first verifies that the latest antivirus software is installed and runs. If it has been installed but is not running, the client silently starts the antivirus application. If it is not installed, the client downloads the software from a URL that is specified in the Host Integrity requirement. Then the client installs and starts the software.

Next, the client verifies that the antivirus signature files are current. If the antivirus files are not current, the client silently retrieves and installs the updated antivirus files.

The client runs the Host Integrity check again and passes. The Enforcer receives the results and grants the client access to the enterprise network. In this example, the following requirements must be met:

- The file server that is used for Host Integrity updates has the latest files installed. The client obtains updated applications from the file server. You can set up one or more remediation servers that are connected to the enterprise network. From the remediation servers, users can copy or automatically download the required patches and hotfixes for any required application. If a remediation server fails, then Host Integrity remediation also fails. If the client tries to connect through an Enforcer, the Enforcer blocks the client if Host Integrity fails. You have the option to set up the Host Integrity Policy so that the client notifies the Enforcer that the Host Integrity check passed even though it failed. In this case, the Enforcer does not block the client. Information about the failed Host Integrity check is recorded in the client's Security log.
- The management server must be configured so that updates of the security policy are automatically sent to any computer that runs the client.

If the parameters that are defined for the Host Integrity Policies are not successful, then the Enforcer does not allow the client to connect to the enterprise network.

The following message appears on the client:

```
Symantec Enforcer has blocked all traffic from the client. rule: {name
of requirement} failed.
```

The client tries to recover. If the client's Host Integrity Policy is set up to update files before it allows the client to connect to the enterprise network, then the user is notified that an update needs to be provided. A progress indicator for the update follows the update. If the user disconnects from the enterprise network, the process starts again.

The Information Flow Control function is designed to satisfy the following security functional requirements:

- FDP_IFC.1
- FDP_IFF.1
- FMT_MSA.1
- FMT_MSA.3

7.1.3 Management

The functionality in the TOE requires management to ensure proper configuration control. These pieces of Management functionality are described in the following subsections:

7.1.3.1 Security Roles

The TOE maintains four roles: system administrator, administrator, limited administrator, and workstation user. The table below provides a brief description of each:

SNAC ROLE	DESCRIPTION
System Administrator	Domain management Administrator management Server management
Administrator	Create administrators in their domain Delete and modify the administrators that were created in their domain Change attributes for the administrators that are created in their domain. These attributes include notification, security, and permission settings.
Limited Administrator	Perform the work that is assigned to them by the system administrator or administrator Configure their own attributes including security settings and notification settings
Workstation User	Install patches and other software updates to bring the endpoint to compliance with policies Receive alert notifications for events on the workstation being used Acknowledge alert notifications for events on the workstation being used Review the TOE audit information on the workstation being used

Table 20 – Description of Roles Supported in the TOE

The System Administrator role in the TOE is responsible for all management functions of the TOE, including management of TOE security functions and review of TOE audit data.

7.1.3.2 Security Audit

A TOE Administrator can view system reports and specific component logs. The Administrator can further define lifespans for the storage of reports/logs and can view, print, save, schedule, and delete them as part of the Security Audit capabilities.

7.1.3.3 Access Control

The Administrator manages the creation and enforcement of different levels of access within the TOE, and each level of access has set of services available (as defined in Table 20 – Description of Roles Supported in the TOE). The Administrator can define services available to various privilege levels/roles without granting full System Administrator privileges.

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MSA.1
- FMT_MSA.3
- FMT_MOF.1
- FMT_MTD.1(1)
- FMT_MTD.1(2)
- FMT_MTD.1(3)
- FMT_SMF.1
- FMT_SMR.1