Security Target

Symantec Risk Automation Suite Version 4.0.5

Document Version 1.2

February 9, 2011

Prepared For:

Symantec Corporation

350 Ellis Street

Mountain View, CA 94043-2202

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 Risk Automation Suite Version 4.0.5. 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 Risk Automation Suite Version 4.0.5
ST Revision	1.2
ST Publication Date	February 9, 2011
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	Symantec Risk Automation Suite Version 4.0.5

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.

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
AD	Active Directory
ADV	Assurance Development
AGD	Assurance Guidance Documents
ALC	Assurance Life-Cycle
ASE	Assurance Security Target Evaluation
ATE	Assurance Tests
AVA	Assurance Vulnerability Assessment
C&A	Certification and Accreditation
CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation
CCE	Common Configuration Enumeration
CCEF	Common Criteria Evaluation Facility

[1] Derived from the IDSPP

TERM	DEFINITION
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CEM	Common Evaluation Methodology
CPE	Common Platform Enumeration
CSEC	Communications Security Establishment Canada
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
EAL	Evaluation Assurance Level
EAL 3+	Evaluation Assurance Level 3+
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Over Secure Socket Layer
ICMP	Internet Control Message Protocol
INT	Introduction
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NetBIOS	Network Basic Input/Output System
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OBJ	Security Objectives
OS	Operating System
OSP	Organizational security policies
OVAL	Open Vulnerability and Assessment Language
P2P	Peer to Peer
RPC	Remote Procedure Call
SCAP	Security Content Automation Protocol
SFP	Security Functional Policy
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
ST	Security Target
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
XCCDF	Extensible Configuration Checklist Description Format

Table 2 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

Risk Automation Suite Version 4.0.5 is a highly-scalable, integrated framework of compliance technologies, which enables organizations to measure security and compliance across the enterprise

network. Built as Service Oriented Architecture (SOA), Risk Automation Suite Version 4.0.5 uses agent-less and agent based technologies and scales to any size of enterprise network. Risk Automation Suite Version 4.0.5 discovers and classifies assets connected to the network, scans the appropriate assets for vulnerabilities and compliance with requisite standards and provides a centralized portal for continuous, repeatable measurement and reporting.

Risk Automation Suite Version 4.0.5 automates enterprise-wide asset discovery, vulnerability detection, configuration reporting, and policy compliance measurement in a single, easy to deploy, easy to manage solution. Risk Automation Suite Version 4.0.5 offers asset classification, scheduling and reporting features to provide users with complete command and control over enterprise scans and report generation. Risk Automation Suite Version 4.0.5 provides a centralized portal for continuous, repeatable measurement and reporting. Risk Automation Suite Version 4.0.5 continuously measures IT security and compliance with government policies and standards, including: FISMA, FDCC, C&A criteria, and NIST 800 Series standards and uses a Web Services API allowing for integration with third party applications.

1.6.1 TOE Description

The TOE (Risk Automation Suite Version 4.0.5) is a software suite that helps enterprises continuously visualize all IT assets, prioritize risk accordingly, and measure remediation efforts for a total risk assessment of the IT environment. The TOE is a collection of integrated modules that provides a view of the technology and risks present in large IT networks.

The TOE is a multi-tier application consisting of integrated components that can be installed on one server, or multiple, distributed scanners. They are fully compatible with virtual server environments. In the evaluated configuration the TOE and the database are installed on a single server. Each of the integrated components is described below.

- RAS Portal - the central hub of Risk Automation Suite Version 4.0.5 that provides all data analysis, reporting, scheduling, workflow, and management capabilities. The RAS Portal consists of a web-based user interface, web services API, and a back-end database.
- RAS Asset Discovery - rapidly discovers and inventories all networks and network assets, including managed and unmanaged devices. This component consists of three scanning processes: network discovery, host discovery and OS discovery.
- RAS Vulnerability Management - orchestrates vulnerability scanners to conduct ongoing vulnerability detection and reporting for operating systems, infrastructure, network applications and databases.
- RAS Configuration Management - performs authenticated configuration scans and maintains an accurate inventory of system configurations, including installed software, patches, vulnerabilities, user accounts, and other system information.
- RAS Policy Management - continuously evaluates system configuration and compliance with industry standards and corporate policies.

1.6.2 Physical Boundary

The TOE is a software TOE and is defined as the Risk Automation Suite Version 4.0.5. In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	Risk Automation Suite Version 4.0.5.2506
IT Environment	Workstations meeting the requirements specified in Table 4 – Hardware and Software Requirements for the TOE

Table 3 – Evaluated Configuration for the TOE

The TOE boundary is shown below:

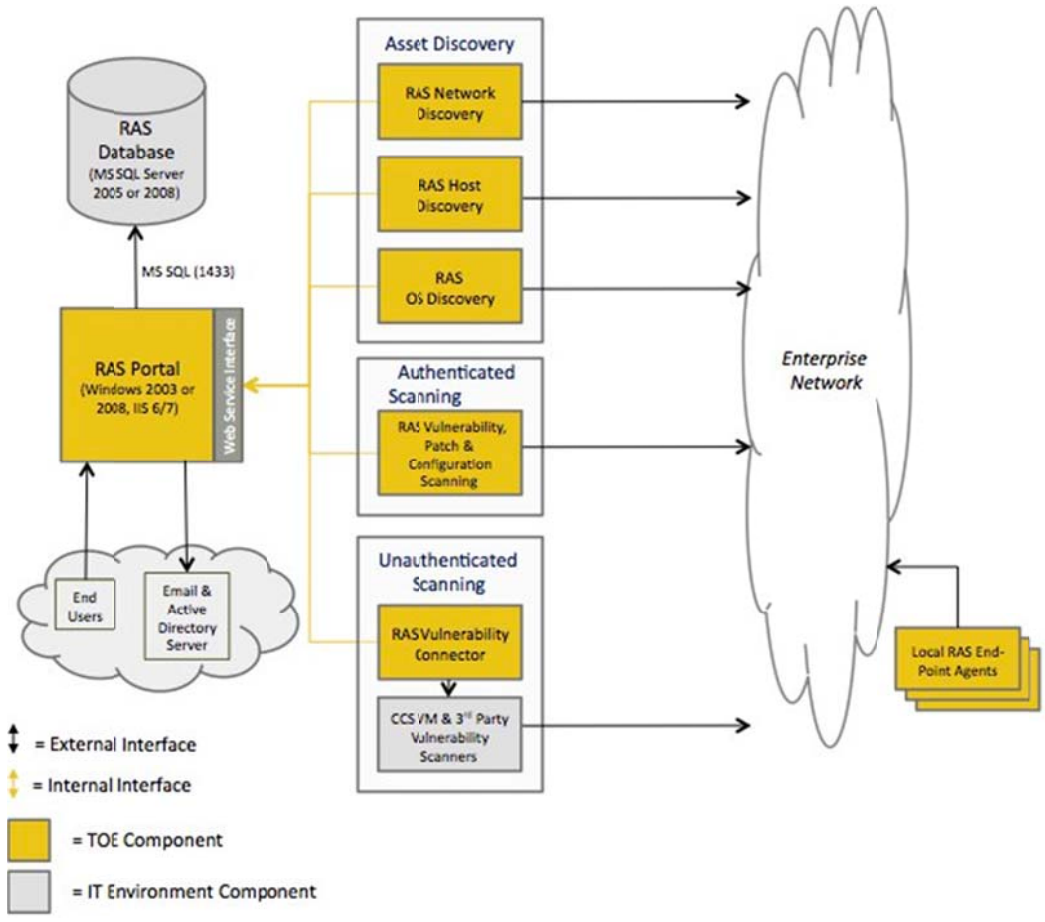

Figure 1 – TOE Boundary

1.6.3 Hardware and Software Supplied by the IT Environment

The TOE is a software-only TOE and is installed on a Microsoft Windows Server operating system with IIS. A Microsoft SQL Server database is also required. In the evaluated configuration, the TOE and the database are installed on a single server. A standard Internet browser is also required for user access to the RAS Portal. An external active directory server and mail server are required if external authentication or email functionality are used.

The following table identifies the minimum hardware and software requirements for components provided by the IT Environment:

Component	Minimum Requirement
Operating System	Microsoft Windows 2003 Server or 2008 Server
Database	Microsoft SQL Server 2005 or 2008
Other software	Microsoft Internet Explorer, Firefox, or Safari

Table 4 – Hardware and Software Requirements for the TOE

1.6.4 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
Security Audit	Audit logs are generated by RAS and stored in the RAS Database. The audit records include the time that the event occurred and the identity of the user performing the event. The time is provided by the IT environment.
Identification and Authentication	The RAS portal is accessed by using a desktop web browser to browse to the RAS portal. Identification and Authentication occur locally or via Active Directory, which is a function of the IT Environment.
Scanning and Security Assessment	RAS is capable of performing discovery, configuration and vulnerability scans. Administration takes place via the RAS web interface where scanning is managed by the administrator(s). The main portal page (also referred to as the Control Panel) provides the management interface for the TOE. All data is encrypted to and from the portal via Secure Sockets Layer (SSL) provided by the IT Environment. All communications between the RAS scanners and the RAS portal occurs over SSL encrypted web services (provided by the IT Environment) with 128 bit encryption keys. In addition, all interaction between end users and the RAS™ portal is forced to occur over an HTTPS session with 128 bit encryption provided by the IT Environment. Agent-less configuration scanning requires the use of credentials. Credential information related to these authorized scans is governed by the Configuration Management module. Credential information at the host or domain level is controlled via the Scan Scheduling child menu option off of

TSF	DESCRIPTION
	the parent Configuration menu branch. The credentials used in the scanning require sufficient privileges to the hosts to gather configuration and security settings. Only the Configuration scanning module requires credentials, Discovery scans and Vulnerability scans don't require credentials. All scans can be controlled and scheduled to run based on user-selected factors. This includes time of day, frequency, type of device to be scanned (e.g. operating system), specific groups of devices (e.g. asset classes, asset categories), locations, or business unit. By combining these options, users have extensive command and control over exactly what gets scanned and when. The schedules are set separately for each scanning process. Each scanner integrated into RAS has options for throttling scans. Throttling limits can be set uniquely per network, so that scans can occur much faster on high capacity networks, while conserving bandwidth on slower or smaller network connections. Throttling limits can also be set uniquely for each scanning process. RAS incorporates blacklisting options giving end users greater control over scanning processes. Blacklisting is a process by which individual devices or entire networks can be eliminated from any or all scans. This feature is useful if target systems need to be excluded during scans, or if there is concern about specific network devices being impacted by scans. Common Vulnerability Enumeration (CVE) is used within RAS to associate any vulnerabilities reported in the RAS portal to a corresponding CVE ID. CVE IDs are displayed in vulnerability reporting. Common Configuration Enumeration (CCE) is used within RAS to associate configuration values reported in the RAS Portal to a corresponding CCE ID. CCE IDs are displayed in compliance reporting. Common Platform Enumeration (CPE) is used by RAS to align SCAP data streams and assessment results with the intended platforms. CPE values are imported from SCAP data streams. The Common Vulnerability Scoring System (CVSS) is used within RAS to prioritize and display risk scores for vulnerabilities reported in the RAS portal. CVSS scores can be viewed in vulnerability reporting. RAS uses Extensible Configuration Checklist Description Format (XCCDF) to import benchmark content. XCCDF data can be viewed under compliance reporting. The Open Vulnerability Assessment Language (OVAL) is used by RAS to define and test system inventory, vulnerabilities, patches and configuration values. OVAL content, consisting of configuration and patch definitions, can be imported into RAS and included in the RAS scanning processes. OVAL data can be viewed in compliance and vulnerability reporting. RAS

TSF	DESCRIPTION
	interprets OVAL definitions, executes scans remotely against target machines, and returns the data to the RAS portal for measurement.
Security Management	RAS has default roles consisting of Global Auditor, Global User, and Global Administrator. The Global Auditor role can be assigned to any user and provides rights to view data within RAS. A user assigned the Global Auditor role is not allowed to change anything within the application. The Global Administrator role can perform all RAS Portal functions. The Global User role has limited change rights. In addition RAS supports user-defined roles. User defined roles can be restricted by organization, host category, OS type, and OS version in conjunction with specific user rights.

Table 5 – Logical Boundary Descriptions

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 extended and Part 3 conformant at Evaluation Assurance Level 3 augmented with ALC_FLR.1 – Basic Flaw Remediation.

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 threats listed below are addressed by the TOE. The threat agents consist of unauthorized persons or external IT entities that are not authorized to use the TOE as well as authorized administrators of the TOE who make errors in configuring the TOE.

The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings/parameters and no physical access to the TOE.

- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE (TOE users are, however, assumed not to be wilfully hostile to the TOE).

Users in both categories are assumed to have a low level of motivation. The IT asset requiring protection is the user data saved on the TOE.

The TOE and IT Environment address the following threats:

THREAT	DESCRIPTION
T.DATA_LOSS	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System which may result in the TOE being affected by unauthorized users.
T.NETWORK	Vulnerabilities or improper security configuration settings may exist in the IT System the TOE monitors, or users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions

THREAT	DESCRIPTION
T.PRIVILEGE	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

Table 6 – Threats Addressed by the TOE

3.2 Organizational Security Policies

There are no Organizational Security Policies with which the TOE must comply.

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.ADMINISTRATOR	The authorized administrators are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance and to periodically check the audit record; however, they are capable of error. Personnel will be trained in the appropriate use of the TOE to ensure security.
A.EXTERNAL_AUTHENTICATION	If external authentication is to be used, external authentication services will be available via Active Directory (AD) authentication credentials.
A.EXTERNAL_EMAIL	If email functionality is to be used, external email services will be available.
A.INTEROPERABILITY	The TOE is interoperable with the IT Systems it monitors.
A.LOCATION	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access such that the TOE can only be accessed by authorized users.
A.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) on the TOE.
A.TIMESTAMP	The operational environment provides the TOE with the necessary reliable time stamp.

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.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.ANALYZE	Using data collected by the scanning the TOE shall apply analytical processes and information to derive conclusions, and display results and generate reports, about system configuration and compliance with industry standards and corporate policies.
O.AUDIT	The TOE will generate audit records which will include the time that the event occurred and the identity of the user performing the event. The TOE will provide the privileged administrators the capability to review audit data and will restrict audit review to users who have been granted explicit read-access. The TOE will also protect audit data.
O.AUTHENTICATE	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.INTEGRITY	The TOE must ensure the integrity of all audit and system data.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.SCAN	The TOE must scan, collect, analyze, and perform actions on static system configuration and compliance information gathered from an IT System.

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.ADMINISTRATOR	The authorized administrators are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance (e.g., procedures to review/manage audit records); however, they are capable of error. Personnel will be trained in the appropriate use of the TOE to ensure security.
OE.COMPATIBLE	IT systems that the TOE monitors support communication with the TOE via standard internet protocols.
OE.EXTERNAL_SERVERS	Active Directory (LDAP) and email (SMTP) servers must be available for external authentication and email services, respectively.
OE.LOCATION	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

OBJECTIVE	DESCRIPTION
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) on the TOE.
OE.TIME	The TOE will have access to a reliable time source from the operational environment.
OE.TRUSTED_PATH/CHANNEL	The IT environment will provide the necessary SSL trusted path/channel interfaces for remote administration, user communication, and connection to 3rd party components.

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:

THREAT/ASSUMPTION / OBJECTIVE	T.DATA_LOSS	T.MISUSE	T.PRIVILEGE	T.NETWORK	A. ADMINISTRATOR	A.EXTERNAL_AUTHENTICATION	A.EXTERNAL_EMAIL	A.INTEROPERABILITY	A.LOCATION	A.NO_GENERAL_PURPOSE	A.TIMESTAMP
O.ACCESS	✓		✓	✓							
O.ANALYZE		✓		✓							
O.AUDIT		✓									
O.AUTHENTICATE	✓		✓	✓							
O.INTEGRITY	✓										
O.MANAGE			✓								
O.SCAN		✓		✓							
OE.ADMINISTRATOR		✓			✓						
OE.COMPATIBLE								✓			
OE.EXTERNAL_SERVERS	✓		✓	✓		✓	✓				
OE.LOCATION									✓		
OE.NO_GENERAL_PURPOSE										✓	
OE.TIME											✓
OE.TRUSTED_PATH/CHANNEL	✓			✓							

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	RATIONALE
T.DATA_LOSS	• O.ACCESS ensures that users can only access appropriate TOE functions and data. • O.AUTHENTICATE requires that users are identified and authenticated prior to accessing the TOE. • O.INTEGRITY requires that the TOE ensure the integrity of all audit and system data. • OE.TRUSTED_PATH/CHANNEL ensures that user and administrator communication is protected. • OE.EXTERNAL_SERVERS provides for the necessary external email services.
T.MISUSE	• The O.AUDIT objective requires that the TOE mitigate this threat by generating audit records. O.AUDIT requires the TOE provide the Authorized administrator with the capability to view Audit data. O.AUDIT requires that the TOE protect audit data. O.AUDIT also requires the TOE to restrict audit review to users who have been granted explicit read-access. • O.ANALYZE ensures that the TOE is able to provide system configuration and compliance information on results of the scanning. • O.SCAN ensures that the TOE can perform scans. • The OE.ADMINISTRATOR objective on the environment assists in covering this threat on the TOE by requiring that the administrator abide by the instructions provided by the TOE documentation, including the administrator guidance to periodically check the audit record.
T.NETWORK	• O.ACCESS allows authorized users to access only appropriate TOE functions and data. • O.AUTHENTICATE requires that users are identified and authenticated prior to accessing TOE functions and data. • O.ANALYZE ensures that the TOE is able to provide system configuration and compliance information on results of the scanning. • O.SCAN ensures that the TOE can perform scans. • OE.TRUSTED_PATH/CHANNEL ensures that user and administrator communication is protected. • OE.EXTERNAL_SERVERS provides for the necessary external email services.
T.PRIVILEGE	• The O.ACCESS only permits authorized users to access TOE functions. • The O.AUTHENTICATE objective provides for authentication of users prior to any TOE function accesses. • O.MANAGE limits the use of the TOE's functions. • OE.EXTERNAL_SERVERS provides for the necessary external email services.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.ADMINISTRATOR	OE.ADMINISTRATOR helps mitigate this assumption by ensuring that TOE administrators are suitable.
A.EXTERNAL_AUTHENTICATION	OE.EXTERNAL_SERVERS provides for the necessary external authentication resources.
A.EXTERNAL_EMAIL	OE.EXTERNAL_SERVERS provides for the necessary external email services.
A.INTEROPERABILITY	OE.COMPATIBLE ensures that the TOE supports the necessary communication protocols.
A.LOCATION	OE.LOCATION provides for the physical protection of the TOE.
A.NO_GENERAL_PURPOSE	OE.NO_GENERAL_PUROSE ensures that the TOE is not used for other purposes.
A.TIMESTAMP	OE.TIME ensures that a time stamp is available.

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

5 Extended Components Definition

5.1 Class SDC: System Data Collection

Data collection and reporting provides for the ability to collect, review, and manage data. These capabilities are not addressed by existing CC components.

5.1.1 Data Collection, Analysis, Display, and Reporting (SDC_ADR_EXT)

5.1.1.1 Family Behavior

This family addresses the data collected and analyzed. The audit class of the CC (FAU) was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of data and provide for requirements about collecting, reviewing and managing the data.

5.1.1.2 Component Leveling

SDC_ADR_EXT.1 System data collection defines the data that the TSF shall be able to collect.

SDC_ADR_EXT.2 System data analysis defines the analysis functions that the TSF shall be able to perform on the collected data.

SDC_ADR_EXT.3 System data display defines the display and reporting that the TSF performs on the collected data.

SDC_ADR_EXT.4 System data actions defines the actions that the TSF performs on the collected data.

5.1.1.3 Management

The following actions could be considered for the management functions in FMT:

Component	Management Function
SDC_ADR_EXT.1	Control of changes to the data that is to be collected.
SDC_ADR_EXT.2	None
SDC_ADR_EXT.3	Maintenance (deletion, modification, addition) of the users with read access to the collected data.
SDC_ADR_EXT.4	Maintenance (deletion, modification, addition) of the users with the ability to perform actions on the collected data.

5.1.1.4 Audit

There are no auditable events foreseen for SDC_ADR_EXT.1, SDC_ADR_EXT.2, SDC_ADR_EXT.3, and SDC_ADR_EXT.4.

5.1.1.5 SDC_ADR_EXT.1 (System data collection)

Hierarchical to: No other components.

Dependencies: None.

SDC_ADR_EXT.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) configuration information consisting of [selection: installed software, patches, vulnerabilities, user accounts, [assignment: other information]]; and

b) discoverable network information;

c) discoverable hosts information; and

d) discoverable application information.

5.1.1.6 SDC_ADR_EXT.2 (System data analysis)

Hierarchical to: No other components.

Dependencies: SDC_ADR_EXT.1.

SDC_ADR_EXT.2.1 The TSF shall perform the following analysis functions(s) on data received:

a) [selection: compliance evaluation, metrics calculation, vulnerability analysis, inventory identification, patch analysis, statistical analysis]; and

b) [assignment: other analytical functions].

5.1.1.7 SDC_ADR_EXT.3 (System data display)

Hierarchical to: No other components.

Dependencies: SDC_ADR_EXT.1.

SDC_ADR_EXT.3.1 The TSF shall provide data collected and analyzed in SDC_ADR_EXT.1 and SDC_ADR_EXT.2 to [assignment: identified users].

5.1.1.8 SDC_ADR_EXT.4 (System data actions)

Hierarchical to: No other components.

Dependencies: SDC_ADR_EXT.1.

SDC_ADR_EXT.4.1 The TSF shall permit [assignment: identified users] to [selection: add, edit, delete] collected data and its associated meta data.

6 Security Requirements

The security functional requirements and assurance 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	Audit review
	FAU_STG.1	Protected audit trail storage
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
System Data Collection	SDC_ADR_EXT.1	System data collection
	SDC_ADR_EXT.2	System data analysis
	SDC_ADR_EXT.3	System data display
	SDC_ADR_EXT.4	System data actions

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) [Both successful and failed authentications;

d) For failed authentication attempts, the connection IP addresses; and

e) Last update of a user's account settings: account status, expiration date, logon environment, last logon, number of logons, date created, date activated, activated by, last update updated by, date suspended, suspended

by, and administrator comments/notes.]

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 (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, [no other 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 The TSF shall provide [Global Administrators, Global Auditors, and authorized user defined roles] with the capability to read [all logged data] 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.

6.1.1.4 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.

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

6.1.2 Identification and Authentication (FIA)

6.1.2.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within the set* [3, 5, 7, 10, 12, 15, 20, 25, 30, 40, 50] unsuccessful authentication attempts occur related to [all authentication].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [prevent the users from performing activities that require authentication until an action is taken by an Global Administrator or a user with sufficient rights].

Note: Enable account lockout must be set to Yes (default value).

6.1.2.2 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) [account status (i.e. lockout, authentication success/failure); and

b) role (Global Administrator, Global User, Global Auditor, user defined roles)].

6.1.2.3 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following:

a) [Administrator configurable minimum password length (3-18);

b) if enabled by the Administrator, passwords contain at least one number and one letter; and

c) if enabled by the Administrator, passwords contain at least one special character].

6.1.2.4 FIA_UAU.2 User Authentication before Any Action

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

6.1.2.5 FIA_UID.2 User Identification before Any Action

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

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 *modify the behavior of* the functions [identified in the table below] to [the roles as identified in the table below].

	GLOBAL ADMINISTRATOR	GLOBAL AUDITOR	GLOBAL USER	USER DEFINED ROLE[2]
User management	✓			✓
Application settings	✓			✓

6.1.3.1 FMT_MTD.1 – Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [control] the [data described in the table below] to [the roles as identified in the table below]:

	GLOBAL ADMINISTRATOR	GLOBAL AUDITOR	GLOBAL USER	USER DEFINED ROLE[3]

[2] By default a user defined role does not have any user rights but can be assigned any user rights
[3] By default a user defined role does not have any user rights but can be assigned any user rights

	GLOBAL ADMINISTRATOR	GLOBAL AUDITOR	GLOBAL USER	USER DEFINED ROLE[3]
Data collection parameters and scheduling	✓		✓	✓
Data analysis	✓		✓	✓
Data display	✓	✓	✓	✓
Data actions	✓		✓	✓

6.1.3.2 FMT_SMF.1 Specification of Management Functions

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

- [Management of TSF data
- management of security attributes
- Management of TSF functions].

6.1.3.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Global Administrator, Global User, Global Auditor, and user defined roles].

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

6.1.4 Data Collection, Analysis, Display, and Reporting (SDC_ADR_EXT)

6.1.4.1 SDC_ADR_EXT.1 System data collection

SDC_ADR_EXT.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) configuration information consisting of *installed software*, *patches*, *vulnerabilities*, *user accounts*, and [no other system information]; and

b) discoverable network information;

c) discoverable hosts information; and

d) discoverable application information.

6.1.4.2 SDC_ADR_EXT.2 System data analysis

SDC_ADR_EXT.2.1 The TSF shall perform the following analysis function(s) on data received:

a) *Compliance evaluation*, *metrics calculation*, *vulnerability analysis*, *inventory identification*, *patch analysis*, and *statistical analysis*]; and

b) [no other analytical functions]

6.1.4.3 SDC_ADR_EXT.3 System data display

SDC_ADR_EXT.3.1 The TSF shall provide data collected and analyzed in SDC_ADR_EXT.1 and SDC_ADR_EXT.2 to [Global Administrator, Global User, Global Auditor, and user defined roles].

6.1.4.4 SDC_ADR_EXT.4 System data actions

SDC_ADR_EXT.4.1 The TSF shall permit [Global Administrator, Global User, Global Auditor, and user defined roles] to *add*, *edit*, and *delete* collected data and its associated meta data.

6.2 IT 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 3 (EAL3) augmented with ALC_FLR.1 Flaw Reporting Procedures. The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.3	Functional Specification with Complete Summary
	ADV_TDS.2	Architectural Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.3	Authorization Controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Identification of Security Measures
	ALC_FLR.1	Basic Flaw Remediation
	ALC_LCD.1	Developer defined life-cycle model
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.2	Analysis of Coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing – Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 13 – Security Assurance Requirements at EAL3

6.2.1 Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 3 augmented with ALC_FLR.1. EAL3 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL3 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is Basic, the security environment provides physical protection, and the TOE itself offers a very limited interface.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements for the TOE

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

SFR \ OBJECTIVE	O.ACCESS	O.ANALYZE	O.AUDIT	O.AUTHENTICATE	O.INTEGRITY	O.MANAGE	O.SCAN
FAU_GEN.1			✓				
FAU_GEN.2			✓				
FAU_SAR.1			✓				
FAU_STG.1			✓		✓		
FIA_AFL.1	✓						
FIA_ATD.1	✓						
FIA_SOS.1	✓						
FIA_UAU.2	✓			✓	✓		
FIA_UID.2	✓			✓	✓		
FMT_MOF.1					✓	✓	
FMT_MTD.1					✓	✓	
FMT_SMF.1					✓	✓	
FMT_SMR.1					✓	✓	
SDC_ADR_EXT.1		✓					
SDC_ADR_EXT.2		✓					
SDC_ADR_EXT.3					✓		
SDC_ADR_EXT.4							✓

Table 14 – Mapping of TOE SFRs to Security Objectives

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

OBJECTIVE	RATIONALE

OBJECTIVE	RATIONALE
O.ACCESS	This objective is met by FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, and FIA_UID.2. FIA_UAU.2 and FIA_UID.2 ensure that users are identified and authenticated prior to allowing access while the other SFRs address authentication failures and password requirements. Once authenticated TOE allows access to management functions based on user account status and associated role.
O.ANALYZE	This objective is met by SDC_ADR_EXT.2 and SDC_ADR_EXT.3 which provide for the analysis and reporting functions on the collected data.
O.AUDIT	This objective is met by FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, and FAU_STG.1. FAU_GEN.1, FAU_GEN.2, and FAU_STG.1 provide for the generation/storage of audit records which FAU_SAR.1 ensures that the records can be reviewed.
O.AUTHENTICATE	This objective is met by FIA_UAU.2 and FIA_UID.2 which ensure that users are identified and authenticated prior to allowing access.
O.INTEGRITY	This objective is met by FAU_STG.1, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, and SDC_ADR_EXT.3. These requirements ensure that audit records cannot be deleted or modified by an unauthorized user. Users are required to be identified and authenticated and are allowed access to management functions based on their associated role. Collected and analyzed data is only provided to authorized users.
O.MANAGE	This objective is met by FMT_MOF.1, FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1 which provide for user roles and rights to limit TOE access.
O.SCAN	This objective is met by SDC_ADR_EXT.4 which provides for the collection, display, reporting, and performing of actions on information from targeted IT resources.

Table 15 – Rationale for Mapping of TOE SFRs to Objectives

6.4 Dependency Rationale

Table 16 - Functional Requirement Dependencies identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency. Notes are provided for those cases where the dependencies are satisfied by components which are hierarchical to the specified dependency.

SFR	Dependencies	Dependency Satisfied?	Notes
FAU_GEN.1	FPT_STM.1	Yes	The TOE uses time provided by the IT Environment
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Yes	FAU_GEN.1 and FIA_UID.2 are in the ST
FAU_SAR.1	FAU_GEN.1	Yes	FAU_GEN.1 is in the ST
FAU_STG.1	FAU_GEN.1	Yes	FAU_GEN.1 is in the ST
FIA_AFL.1	FIA_UAU.1	Yes	FIA_UAU.2 is in the ST
FIA_ATD.1	None	Yes	
FIA_SOS.1	None	Yes	
FIA_UAU.2	FIA_UID.1	Yes	FIA_UID.2 is in the ST

SFR	Dependencies	Dependency Satisfied?	Notes
FIA_UID.2	None	Yes	
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	Yes	FMT_SMF.1 and FMT_SMR.1 are in the ST.
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Yes	FMT_SMF.1 and FMT_SMR.1 are in the ST.
FMT_SMF.1	None	Yes	
FMT_SMR.1	FIA_UID.1	Yes	FIA_UID.2 is in the ST
SDC_ADR_EXT.1	None	Yes	
SDC_ADR_EXT.2	SDC_ADR_EXT.1	Yes	SDC_ADR_EXT.1 is in the ST
SDC_ADR_EXT.3	SDC_ADR_EXT.1	Yes	SDC_ADR_EXT.1 is in the ST
SDC_ADR_EXT.4	SDC_ADR_EXT.1	Yes	SDC_ADR_EXT.1 is in the ST

Table 16 - Functional Requirement Dependencies

Note: Although the FMT_SMF.1 requirement is a dependency of FMT_MOF.1 and FMT_MTD.1, FMT_SMF.1 has not been included in this ST. The requirements FMT_MOF.1 and FMT_MTD.1 express the functionality required by the TSF to provide the specified functions to manage TSF data, security attributes and management functions. These requirements make it clear that the TSF has to provide the functions to manage the identified data, attributes and functions. Therefore FMT_SMF.1 is not necessary.

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 6.1 – Security Functional Requirements. The security functions performed by the TOE are as follows:

- Security Audit
- Identification and Authentication
- Scanning and Security Assessment
- Security Management

7.1.1 Security Audit

The TOE automatically creates audit records of authentication events and changes made by user accounts. The records include the time that the event occurred and the identity of the user attempting to perform the action. For failed authentication attempts the IP address is also recorded. The audit records are stored in the RAS database. The TOE is able to utilize the reliable time stamp provided by the IT environment for its own use.

Access to view the log is determined by the user's assigned rights. Audit logs can be viewed by category, sorted by any available column, and filtered by keywords or regular expressions. Users can page through the audit records or view specific results per page.

There is no provision for deleting audit records via the RAS Portal. Audit records can not be modified.

7.1.2 Identification and Authentication

The RAS Portal is accessed by using a desktop web browser to browse to the RAS Portal. The TOE is installed with SSL enabled and required for all user and client connections[4], therefore pre-pending the RAS Portal URL with *https://* is necessary. The user interface login page does not allow any actions other than specifying a username and password for authentication. The minimum length for passwords is configurable by an administrator and can be 3-18 characters. Additionally, passwords can contain at least one number and one letter as well as at least one special character.

The TSF detects when an administrator specified number of authentication failures have occurred and will lock the account until a Global Administrator or a user with sufficient rights unlocks the account. The failure limit is selected from the range of values specified in FIA_AFL.1. Accounts on the RAS Portal also have an associated status which is active, suspended, or locked out. A Global Administrator or a user with sufficient rights is able to activate or suspend an account.

[4] Note that this functionality is provided by the IT environment

The user logs into the RAS Portal with their user name and password or with their Active Directory (AD) credentials, if AD authentication has been enabled in the RAS Portal[5]. An AD user level account is required to be entered into the RAS Portal to enable this option. Once entered, the user level account will be used to query the Active Directory and list AD user accounts to be given access to the RAS Portal. Once added, users will sign into the RAS Portal, authentication will be passed to AD, and if successful, the users will be granted access. Object level authorization and role-based access is performed natively in the TOE.

7.1.3 Scanning and Security Assessment

Configuration information is collected from the system by authenticating to it using stored credentials or by an authorized agent connecting to the Web Services API. Information gathered from the system is gathered through interfaces that are specific to the scanned operating system. Network, host, and application information is discovered using Internet Protocol (IP) and higher level protocols. Users with appropriate rights can define system wide scan parameters to narrow or expand the scope of the scanning process.

Data is collected by a predefined schedule or an ad hoc scan. All scans can be controlled and scheduled to run based on user-selected factors. This includes time of day, frequency, type of device to be scanned (e.g. operating system), specific groups of devices (e.g. asset classes, asset categories), locations, or business unit. By combining these options, users have extensive command and control over exactly what gets scanned and when. The schedules are set separately for each scanning process.

Scanner registration is performed by a user with the appropriate rights. Each scanner integrated into the TOE has options for throttling the scans. Limits can be set uniquely per network, so that scans can occur much faster on high capacity networks, while conserving bandwidth on slower or smaller network connections. Limits can also be set uniquely for each scanning process and can be set differently based on time of day.

Compliance analysis is performed by analyzing data against defined rules to determine if asset data is compliant or not. The convention for analysis is done using a proprietary method and/or SCAP protocols. Metrics calculations are done by summarizing detailed data using fixed or user defined formulas to compare against user defined measurements. Vulnerability analysis is performed using SCAP protocols. Inventory identification and patch analysis is done using SCAP protocols and a proprietary method. Statistical analysis is done by summarizing detailed data using fixed or user defined formulas.

The system displays data using charts, tables, grid views to provide different views into the data. The data can be sorted or filtered using regular expressions. Users can also customize the data display by modifying the page size or specifying search functions.

[5] The AD capability is defined as part of the TOE's operational environment.

If a user has sufficient rights they can perform system data actions on security issues such as filtering or closing vulnerabilities by modifying the meta data associated with the scan results. A user with appropriate rights can authorize a host or network and can accept an issue or assign it to another user.

7.1.4 Security Management

The TOE has default roles consisting of Global Auditor, Global User, and Global Administrator. The Global Auditor role can be assigned to any user who will have rights to view data within the TOE but who is not allowed to change anything within the application. The Global Administrator role can perform all RAS Portal functions. The Global User role has limited change rights. In addition the TOE supports user-defined roles. User defined roles can be restricted by organization, host category, OS type, and OS version in conjunction with specific user rights. Each action a user attempts to perform is checked against the user's rights and must match before the action is allowed.

Audit records are time stamped using time provided by the operating system.

User rights/roles changes and changes to applications are restricted to the Global Administrator or a user with sufficient rights.

Before allowing access or a data's Organizational assignment is checked against the user's organization assignment(s). In addition access to collected data is also determined based on the asset's host category, OS type, and OS version.

SFR \ SECURITY FUNCTION	Security Audit	Identification and Authentication	Scanning and Security Assessment	Security Management
FAU_GEN.1	✓			
FAU_GEN.2	✓			
FAU_SAR.1	✓			
FAU_STG.1	✓			
FIA_AFL.1		✓		
FIA_ATD.1		✓		
FIA_SOS.1		✓		
FIA_UAU.2		✓		
FIA_UID.2		✓		
FMT_MOF.1				✓
FMT_MTD.1				✓

SFR \ SECURITY FUNCTION	Security Audit	Identification and Authentication	Scanning and Security Assessment	Security Management
FMT_SMF.1				✓
FMT_SMR.1				✓
SDC_ADR_EXT.1			✓	
SDC_ADR_EXT.2			✓	
SDC_ADR_EXT.3			✓	
SDC_ADR_EXT.4			✓	

Table 17- Mapping of Security Functions to SFRs