Security Target

Symantec Altiris IT Management Suite 7.1 SP2

Document Version 1.2

March 6, 2013

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 Altiris IT Management Suite 7.1 SP2 . 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 Altiris IT Management Suite 7.1 SP2
ST Revision	1.2
ST Publication Date	March 6, 2013
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	Symantec Altiris IT Management Suite 7.1 SP2

Note: The Altiris name is a brand name owned by Symantec. References to Altiris appear in the product component listing and refer to the TOE. For example, the Altiris brand name is used extensively in the component list and during installation of the TOE.

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

SECTION	TITLE	DESCRIPTION
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 1-1 – 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 *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, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.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 describes the acronyms used in this document:

TERM	DEFINITION
Assets	Information or resources to be protected by the countermeasures of a TOE.
Attack potential	In terms of an attacker's expertise, resources and motivation, the perceived potential for the success of an attack, when an attack is launched.
Authentication Data	Information used to prove the claimed identity of a user.
Class	A grouping of families that share common security objectives for the CC
Component	The smallest selectable set of elements that may be included in a PP, an ST, or a package.

TERM	DEFINITION
Dependency	A relationship between requirements, such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.
Element	An indivisible security requirement.
Evaluation Assurance Level (EAL)	A package consisting of assurance components from Part 3 that represents a point on the CC pre-defined assurance scale.
Extension	The augmentation to an ST or PP of security functional requirements not contained in Part 2 and assurance requirements not contained in Part 3 of the CC.
External IT Entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Identity	A unique manifestation that can identify an authorized user, which can be either the full or the abbreviated name of that user, or a pseudonym.
Object	An entity within the TSC that contains or receives information, and upon which subjects perform operations.
Organizational Security Policies	One or more security rules, procedures, practices, or guidelines imposed by an organization on its operations.
PP (Protection Profile)	An implementation-independent set of security requirements for a category of TOEs that meets specific consumer needs.
SOF (Strength-of-Function)	A qualification of a TOE security function that expresses the minimum effort required to defeat its expected security behavior by directly attacking its underlying security mechanism.
ST (Security Target)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Subject	An entity within the TSC (TSF Scope of Control) that causes operations to be performed.
Threat Agent	Any unauthorized user or external IT entity that causes threats by attempts of illegal access, modification or deletion to assets.
TOE (Target of Evaluation)	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
TSC (TSF Scope of Control)	The set of interactions that can occur with or within a TOE and that are subject to the rules of the TSP.
TSF (TOE Security Functions)	A set consisting of all the TOE hardware, software, and firmware that must be relied upon for the correct enforcement of the TSP (TOE Security Policy).
TSF Data	Data generated by and for the TOE, which might affect the operation of the TOE.
TSP (TOE Security Policy)	A set of rules that regulate how assets are managed, protected and delivered within a TOE.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Table 1-2 – Terms and Acronyms Used in Security Target

1.6 TOE Overview and Description

1.6.1 IT Management Suite

IT Management Suite (ITMS) is a systems management solution that reduces the total cost of ownership for desktops, notebooks, and handheld devices. Developed for IT professionals who manage computer devices on a regular basis, the suite enables administrators to deploy, manage, and troubleshoot systems from almost anywhere.

IT Management Suite is a collection of solutions that run on the Symantec Management Platform. The platform and solutions of IT Management Suite provide the following key features:

- Central Web-based management console
- Role-and-scope-based security
- Zero-touch OS deployment and migration
- Integrated hardware and software inventory with Web-based reporting
- Policy-based software management
- Automated patch management
- Software license compliance and harvesting
- Centralized management of mixed hardware and OS environments

The TOE is comprised of the following components and described in the following sections:

- ITMS Solutions
- Symantec Management Platform (SMP)
- Management Console
- Agent

1.6.2 ITMS Solutions

ITMS Solutions plugged into the Symantec Management Platform (SMP) improves visibility into IT assets at every point in the lifecycle to reduce costs and fulfill compliance initiatives. Manages, secures, and troubleshoots desktops and servers throughout their entire IT lifecycle.

Manages software licenses to ensure compliance and optimize purchasing decisions. Visualizes the relationships between hardware, software, contracts, users, and organizational units. Automates common processes such as employee on-boarding or asset reallocation.

Manages client PC lifecycles across Windows, Mac, Linux and virtual desktops. Accurately identifies and inventories devices to forecast hardware and software needs. Automates migration to new system rollouts. Provides comprehensive software management simplifies ongoing software maintenance.

Manages heterogeneous servers across Windows, Linux, UNIX and virtual environments. Provides comprehensive software provisioning and patch management. Provides integrated monitoring and remediation functions.

1.6.3 Symantec Management Platform

The Symantec Management Platform (SMP) provides a set of services that IT-related solutions can leverage. Solutions plug into the platform and take advantage of the platform services, such as security, reporting, communications, package deployment, and Configuration Management Database (CMDB) data. Because solutions share the same platform, they can share platform services as well as data. Shared data is more useful than data that is only available to a single solution. For example, one solution collects data about the software that is installed on company computers and another solution uses the data to manage software licenses. A third solution can also use this data to help you update software. This close integration of solutions and the platform makes it easier for you to use the different solutions because they work in a common environment and are administered through a common interface. The platform provides the following services:

- Client communications and management
- Event triggered and scheduled task and policy execution
- Reporting
- Configuration Management Database (CMDB)

The SMP provides the connections to the Management Agent (Agent) to send management tasks and receive reports about the managed systems.

Configuration of Symantec Management Platform is also supported.

- Set up Notification Server and Configuration Management Database
- Customize GUI (Add submenus and submenu items, setup the menu structure, create and modify views, and create and modify portal pages.

1.6.4 Management Console

The Symantec Management Console (Management Console) is a browser-based console that can be accessed from the Management System computer or remotely. It lets an authorized administrator monitor and manage Management System and its solutions. When accessing the console remotely, the

computer must be on the network, running Microsoft Internet Explorer, and be able to access the Management System computer.

Users must authenticate (login with user name and password) through the management console interface before gaining access to the TOE data or services.

1.6.5 Agent

The Management Agent (Agent) software is installed on the computers to be managed by ITMS. The agent facilitates communications between the managed computer and the TOE. The agent also receives tasks from the platform and solutions, helps install software, and sends data that is collected from the managed computer to the management platform.

As the TOE collects data from client machines, the data is stored in the CMDB, where it can be used as follows:

1. The data is used to generate reports that provide insight and a baseline for managing the network.
2. The data can also be used to trigger the actions that help prevent or address issues automatically.

There may be many Agents deployed on managed systems across an enterprise's network.

1.6.6 Physical Boundary

The TOE is a software TOE and is defined as the Symantec Altiris IT Management Suite 7.1 SP2. In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	Symantec Altiris IT Management Suite 7.1 SP2

Table 1-3 – Evaluated Configuration for the TOE

The ITMS product is composed of several individual component products.

COMPONENT/VERSION/BUILD
Symantec Management Platform 7.1 SP2 (7.1.8280)
Altiris CMDB Solution 7.1 SP2 (7.1.6003)
Altiris Asset Management Solution 7.1 SP2 (7.1.7580)
Altiris IT Analytics 7.1 SP2 (7.1.2060)
Altiris Real-Time Console Infrastructure 7.1 SP2 (7.1.7580)
First Time Setup Portal 7.1 SP2 (7.1.7580)
Altiris Patch Management Solution 7.1 SP2 (7.1.7580)
Altiris Patch Management Solution for Windows 7.1 SP2 (7.1.7580)

COMPONENT/VERSION/BUILD
Altiris Patch Management Solution for Linux 7.1 SP2 (7.1.7580)
Altiris Patch Management Solution for Mac 7.1 SP2 (7.1.7580)
Altiris Inventory Solution 7.1 SP2 (7.1.7580)
Altiris Software Catalog Data Provider 7.1 SP2 (7.1.7580)
Altiris Inventory for Network Devices 7.1 SP2 (7.1.7580)
Altiris Event Console 7.1 SP2 (7.1.7580)
Altiris Monitor Solution for Servers 7.1 SP2 (7.1.7580)
Altiris Inventory Pack for Servers 7.1 SP2 (7.1.7580)
Altiris Real-Time System Manager 7.1 SP2 (7.1.7580)
Altiris Software Management Solution 7.1 SP2 (7.1.7580)
Altiris IT Management Suite 7.1 SP2 (7.1.3)
Altiris Asset Management Suite 7.1 SP2 (7.1.2)
Symantec Barcode Solution 7.1 SP2 (7.1.1180)
Altiris IT Analytics Client Server Management Pack 7.1 SP2 (7.1.2060)
Wise Connector 7.1 SP2 (7.1.7580)
Altiris IT Analytics ServiceDesk Pack 7.1 SP2 (7.1.2060)
Altiris Client Management Suite 7.1 SP2 (7.1.3)
Altiris Out-of-Band Management 7.1 SP2 (7.1.7580)
Altiris Power Scheme Task 7.1 SP2 (7.1.1304)
Symantec pcAnywhere 12.6 SP2 (12.6.7580)
Altiris Client Management Suite Portal Page (7.1.1005)
Symantec Endpoint Protection Integration Component 7.1 SP2 (7.1.1037)
Altiris IT Analytics Symantec Endpoint Protection Pack 7.1 SP2 (7.1.2060)
Altiris Deployment Solution Complete Suite 7.1 SP1aMR1a (7.1.2320)
Altiris Deployment Solution Linux Support 7.1 SP1 MR1 (7.1.2316)
Altiris Deployment Solution WinPE Support 7.1 SP1 MR1 (7.1.2316)
Altiris Deployment Solution Core 7.1 SP1 MR1 (7.1.2316)
Activity Center 7.1 SP2 (7.1.7580)
Altiris Server Management Suite 7.1SP2 (7.1.3)
Altiris Monitor Pack for Servers 7.1 SP2 (7.17580)
Altiris Virtual Machine Management 7.1 SP2 (7.1.7580)
Altiris Server Management Suite Portal Page (7.1.1036)
Altiris Network Topology Viewer (7.1.1043)

Table 1-4 - ITMS Component List

1.6.7 Excluded Functioanlity

The following features are excluded from the evaluated configuration:

- Site Services
- Network Discovery

The following product components are required by the product but are excluded from the evaluated TOE configuration:

- Altiris Patch Management Solution for Linux
- Altiris Patch Management Solution for Mac
- Altiris Deployment Solution Linux Support

1.6.8 TOE Diagram

The TOE boundary is shown below (note that TOE components are shaded):

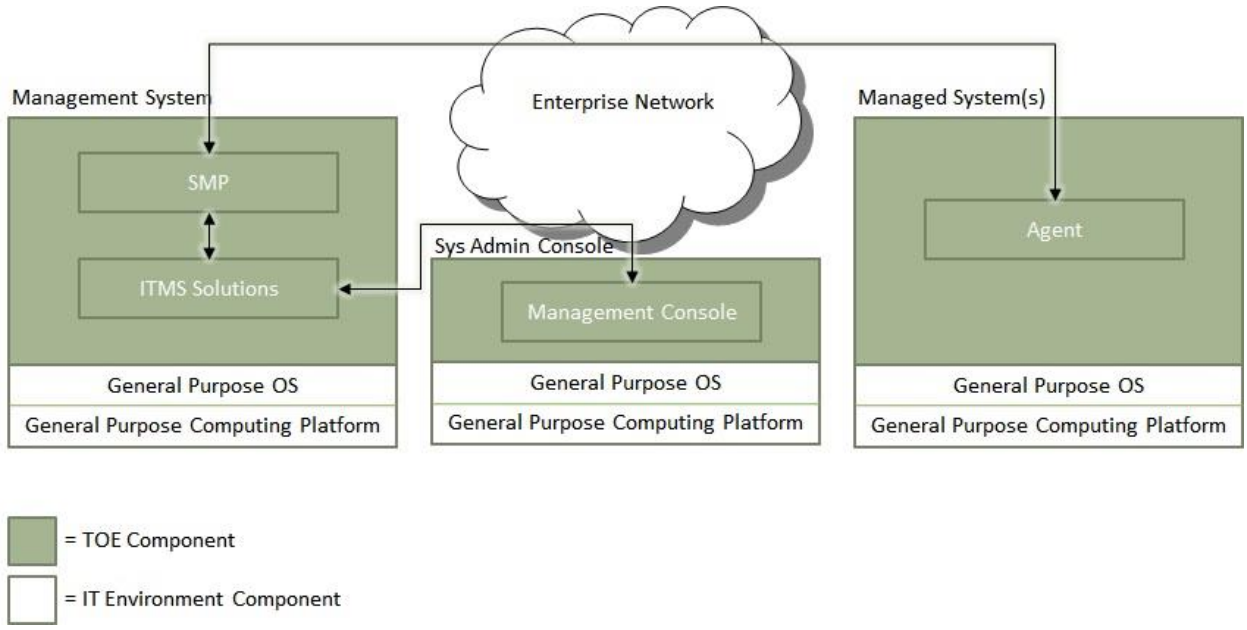

Figure 1 – TOE Boundary

1.6.9 Hardware and Software Supplied by the IT Environment

The following tables identify the minimum hardware and software requirements for components provided by the IT Environment.

	Minimum Requirement
Hardware requirements for all Servers and Agents	General purpose workstation with 8-core 2.4GHz processor, 8GB DDR2 RAM, 6MB L2 cache, Gigabit network, 10GB disk space on 10,000 RPM SCSI or better with RAID 5 or 1+0
Software requirements for systems running the Management System	• NET Framework 3.5 SP1 or above • Internet Explorer 7.0 or above • SQL Server 2005 or SQL Server 2008 • Windows Server 2008 R2 x64

	Minimum Requirement
Software requirements for systems running the Windows Agents	• Windows XP SP3 or later x64/x86 • Windows Vista SP1 or later x64/x86 • Windows 7 x64/x86 • Windows Server 2003 SP2 or later • Windows Server 2008 GA or later x64/x86

Table 1-5 – Hardware and Software Requirements for IT Environment for Less Than 10,000 Managed Endpoints

1.6.10 Logical Boundary Summary

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
Identification and Authentication	The TOE supports identity-based Identification and Authentication of an Operator. Operators authenticate via a Web-based GUI, and operators can assume a defined role based on their user name.
Security Audit	The TOE provides a mechanism to record security-relevant events.
User Data Protection	The TOE provides and enforces user access controls.
Managed Systems	The TOE performs scans of managed systems using configured scanning policies.
Security 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 TOE configuration, CMS Access Control, and audit.

Table 1-6 – Logical Boundary Descriptions

2 Conformance Claims

2.1 CC Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 conformant and Part 3 conformant augmented with ALC_FLR.2 – Flaw Reporting Procedures.

2.2 PP Claim

The TOE does not claim conformance to any registered Protection Profile.

2.3 Package Claim

The TOE claims conformance to the EAL2 assurance package (augmented with ALC_FLR.2 – Flaw Reporting Procedures) defined in Part 3 of the Common Criteria Version 3.1 Revision 3 (July 2009). The TOE does not claim conformance to any functional package.

2.4 Conformance Rationale

No conformance rationale is necessary for this evaluation since this Security Target 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 and IT Environment addresses the following threats:

THREAT	DESCRIPTION
T.ACCESS	An authorized user of the TOE may attempt to access TOE information or resources without having permission to do so.
T.EXPLOIT	An attacker may attempt to gain unauthorized access to the resources of the client system(s) managed by the TOE, by exploiting vulnerabilities on a client system(s).
T.IMPERSON	An attacker may attempt to gain access to the TOE security functions and data by impersonating an authorized user of the TOE.

Table 3-1 – Threats Addressed by the TOE and IT Environment

3.2 Organizational Security Policies

The TOE is not required to meet any 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.ADMIN	It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains, and who can be trusted not to deliberately abuse their privileges.
A.INSTALL	It is assumed that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives.
A.LOCATE	The TOE should be located in the physically secure environment and protected from unauthorized physical access.
A.LOG	It is assumed that the Operational Environment will provide a means to review audit logs.
A.USER	Users of the TOE are assumed to possess the necessary privileges to access the information managed by the TOE.

Table 3-2 – 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 shall ensure that only those authorized users and applications are granted access to the security functions, configuration and associated data.
O.AUDIT	The TOE should precisely record and safely maintain security-related events.
O.ROLES	The TOE must distinguish user roles and provide different security policies and functions according to their roles.
O.SCAN	The TSF must be able to configure and run security scans on the TOE managed devices. In addition, data collected by the TOE must be organized in useful report formats.

Table 4-1 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.ADMIN	Any administrator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.LOG	The IT Environment must provide mechanism to review audit logs.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.PROTECT	The IT Environment must protect the TSF data when it is transmitted between separate parts of the TOE.
OE.TIME	The IT environment must provide reliable timestamps for the TOE.
OE.USER	Those responsible for the TOE must ensure that only authorized users will have access to the information managed by the TOE.

Table 4-2 – 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.

THREATS/ ASSUMPTIONS / OBJECTIVES	T.ACCESS	T.EXPLOIT	T.IMPERSON	A.ADMIN	A.INSTALL	A.LOCATE	A.LOG	A.USER
O.ACCESS	✓	✓	✓					
O.AUDIT	✓	✓						
O.ROLES	✓							
O.SCAN		✓						
OE.ADMIN				✓	✓			
OE.INSTALL					✓			
OE.LOG							✓	
OE.PHYSICAL						✓		
OE.PROTECT	✓							
OE.TIME		✓						
OE.USER				✓				✓

Table 4-3 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

4.3.1 Rationale for Security Objectives of the TOE

The table below contains the rationale for the mapping of Security Objectives to Threats, Policies, and Assumptions:

THREAT/POLICY/ ASSUMPTION	RATIONALE
A.ADMIN	OE.ADMIN provides that administrators of the TOE are trusted, and will have access to the TOE information to manage it effectively OE.USER provides that the TOE will allow only authorized users to have access to the information managed by the TOE.
A.INSTALL	OE.INSTALL provides that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. Administrator is the responsible person to install the TOE and he is trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE (OE.ADMIN).
A.LOCATE	OE.PHYSICAL ensures that the TOE is located in a physically secure environment that only an authorized administrator can access.
A.LOG	OE.LOG ensures that IT Environment provides a mechanism to review audit logs.
A.USER	OE.USER provides that the TOE will allow only authorized users to have access to the information managed by the TOE.

THREAT/POLICY/ ASSUMPTION	RATIONALE
T.ACCESS	O.ACCESS addresses this threat by requiring the TOE to provide a controlled interface that will limit access to the tools and devices to users with authorization and appropriate privileges Only administrators will be able manage the TOE and its security functions. O.AUDIT addresses this threat by precisely recording and safely maintaining security-related events. O.ROLES addresses this threat by distinguishing user roles and providing different security policies and functions according to those roles. OE.PROTECT partially address this threat by requiring the IT Environment to protect the TSF data when it is transmitted between separate parts of the TOE.
T.EXPLOIT	O.SCAN provides that the TOE will be able to configure and run security scans on the TOE managed devices and generates reports. OE.TIME provides reliable timestamps that are included within the report information. O.ACCESS provides that TOE provides a controlled interface that limits access to the tools and devices to users with authorization and appropriate privileges and also ensures will effectively manage the TOE and its security functions. O.AUDIT addresses this threat by precisely recording and safely maintaining security-related events.
T.IMPERSON	O.ACCESS provides that only authorized users gain access to the TOE data and its resource and manage the TOE and its security functions in an effective way.

Table 4-4 – Mapping of Threats, Policies, and Assumptions to Objective

5 Extended Components Definition

5.1 Definition of Extended Components

5.2 Managed Systems (FMS) Class

The purpose of this class of requirements is to address the unique nature of IT Management System (ITMS) products and provide for requirements about scanning managed IT systems.

5.2.1 FMS_SCN_(EXT).1 Target Scanning

Family Behavior:

This family defines the requirements for managed system scanning functionality.

Component Leveling:

FMS_SCN_(EXT).1 Target Scanning provides the scanning of managed systems.

Hierarchical to: No other components.

Dependencies: None

FMS_SCN_(EXT).1.1 The TSF shall perform scans of managed systems based on scanning policies.

Management:

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

a) Configuration of the scanning policy actions to be taken.

Audit:

There are no auditable events foreseen.

6 Security Requirements

The security requirements that are levied on the TOE and the IT environment 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:

Security Function Class	Security Function Component	
Security Audit	FAU_GEN.1	Audit Data Generation
User Data Protection	FDP_ACC.1	Subset Access Control
	FDP_ACF.1	Security Attribute Based Access Control
Identification and Authentication	FIA_UAU.1	Timing of Authentication
	FIA_UID.1	Timing of Identification
Managed Systems	FMS_SCN_(EXT).1.1	Target Scanning
Security Management	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles

Table 6-1 – TOE Security Functional Requirements

Hierarchy and dependency detail for each SFR can be found in Part 2 of the Common Criteria.

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) [no other auditable events]

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

a) Date and time of the event, type of event, subject identity (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 6-2 – FAU_GEN.1 Events and Additional Information].

SFR	AUDITABLE EVENTS	ADDITIONAL INFORMATION
FAU_GEN.1	None	Not Applicable
FDP_ACC.1	None	Not Applicable
FDP_ACF.1	None	Not Applicable
FIA_UAU.1	None	None
FIA_UID.1	None	None
FMS_SCN_(EXT).1	None	Not Applicable
FMT_MSA.1	None	Not Applicable
FMT_MSA.3	None	Not Applicable
FMT_MTD.1	None	Not Applicable
FMT_SMF.1	Use of the management functions.	None
FMT_SMR.1	Modifications to the group of users that are part of a role.	Not Applicable

Table 6-2 – FAU_GEN.1 Events and Additional Information

6.1.2 User Data Protection (FDP)

6.1.2.1 FDP_ACC.1 – Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the [SMP Access Control SFP] on.

[Subjects: Operators attempting to configure the TOE

Objects: TSF Data

Operations: Allow, deny].

6.1.2.2 FDP_ACF.1 – Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the [SMP Access Control SFP] to objects based on the following:

[Subjects: User

Objects: System reports, scanning policy configurations, operator account attributes

Operations: all user actions].

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

[

• The user is a valid user of the TOE

• The user belongs to a group with defined permissions and privileges

].

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

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

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_UAU.1– Timing of Authentication

FIA_UAU.1.1 The TSF shall allow [no administrative actions] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.2 FIA_UID.1 – Timing of Identification

FIA_UID.1.1 The TSF shall allow [no administrative actions] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4 Managed Systems (Extended)

6.1.4.1 FMS_SCN_(EXT).1 - Target Scanning

FMS_SCN_(EXT).1.1 The TSF shall perform scans of managed systems based on scanning policies.

6.1.5 Security Management (FMT)

6.1.5.1 FMT_MSA.1 – Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [SMP Access Control SFP] to restrict the ability to [*query, modify*] the security attributes [Security Settings] to [the authorized administrator].

6.1.5.2 FMT_MSA.3 – Static Attribute Initialization

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

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

6.1.5.3 FMT_MTD.1 – Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to *query, modify,* [no other operations] the [

a) Security settings,

b) Scanning policies,

c) using and customizing report configurations,

d) managing the software catalog and software library

]

to [the Administrator].

6.1.5.4 FMT_SMF.1 – Specification of Management Functions

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

a) Manage security settings,

b) Using and customizing reports

].

6.1.5.5 FMT_SMR.1 – Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Administrator, Guest, Level 1 Worker, Level 2 Worker, Software Librarian, Supervisor].

6.2 Security Requirements Rationale

6.2.1 Security Functional Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

OBJECTIVE / SFR	O.ACCESS	O..AUDIT	O.ROLES	O.SCAN
FAU_GEN.1	✓	✓		
FDP_ACC.1	✓		✓	
FDP_ACF.1	✓		✓	
FIA_UAU.1	✓			
FIA_UID.1	✓			
FMS_SCN_(EXT).1				✓
FMT_MSA.1	✓			
FMT_MSA.3	✓			
FMT_MTD.1	✓		✓	
FMT_SMF.1			✓	✓
FMT_SMR.1	✓		✓	

Table 6-3 – Mapping of TOE Security Functional Requirements and Objectives

6.2.2 Sufficiency of Security Requirements

The following table presents a mapping of the TOE Objectives to TOE Security Requirements.

SFR	RATIONALE
FAU_GEN.1	This component satisfies O.ACCESS and O.AUDIT among TOE security objectives, as it defines auditable events and ensures that audit records are generated.
FDP_ACC.1	This component satisfies O.ACCESS and O.ROLES by ensuring that all user actions resulting in the access to TOE security functions and configuration data are controlled and role separation maintained.

SFR	RATIONALE
FDP_ACF.1	This component satisfies O.ACCESS and O.ROLES by ensuring that access to TOE security functions, configuration data, and account attributes is based on the user privilege level and their allowable actions.
FIA_UAU.1	This component satisfies O.ACCESS among TOE security objectives because it ensures the ability to successfully authenticate a user.
FIA_UID.1	This component satisfies O. ACCESS among TOE security objectives because it ensures the ability to successfully identify an authorized administrator/user.
FMS_SCN_(EXT).1	This component satisfies O.SCAN among TOE security objectives because it provides scanning capabilities of managed systems.
FMT_MSA.1	This component satisfies O. ACCESS among TOE security objectives by ensuring that only privileged administrators can access the TOE security settings..
FMT_MSA.3	This component satisfies O. ACCESS among TOE security objectives by ensuring that the default values of security attributes are restrictive in nature as to enforce the access control policy for the TOE.
FMT_MTD.1	This component satisfies O.ACCESS and O.ROLES among TOE security objectives because it provides an authorized administrator with the ability to manage TSF data related to security settings, report configurations, and scanning policies.
FMT_SMF.1	This component satisfies O.ROLES and O.SCAN among TOE security objectives because it requires the specification of management functions provided by the TSF, such as SMP Access Control SFP, and using and customizing reports .
FMT_SMR.1	This component satisfies O.ACCESS and O.ROLES among TOE security objectives because it ensures that the TSF maintains identified roles.

Table 6-4 – Rationale for TOE Objectives

6.2.3 Dependency Rationale

Table 6-5 – TOE SFR Dependency Rationale 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	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN.1	No other components.	FPT_STM.1	See note below table
FDP_ACC.1	No other components.	FDP_ACF.1	Satisfied
FDP_ACF.1	No other components.	FDP_ACC.1 FMT_MSA.3	Satisfied Satisfied
FIA_UAU.1	No other components.	FIA_UID.1	Satisfied
FIA_UID.1	No other components.	none	Satisfied
FMS_SCN_(EXT).1	No other components.	none	Satisfied
FMT_MSA.1	No other components.	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied Satisfied
FMT_MSA.3	No other components.	FMT_MSA.1 FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	No other components.	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FMT_SMF.1	No other components.	none	Satisfied
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied

Table 6-5 – TOE SFR Dependency Rationale

Note: Although the FPT_STM.1 requirement is a dependency of FAU_GEN.1, it has not been included in this TOE because the timestamping functionality is provided by the IT Environment (OE.TIME). The audit mechanism within the TOE uses this timestamp in audit data, but the timestamp function is provided by the operating system in the IT Environment.

6.2.4 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) augmented with ALC_FLR.2. 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
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
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 6-6 – Security Assurance Requirements at EAL2

6.2.5 Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 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, offering essentially no opportunity for an attacker to subvert the security policies without physical access.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

6.2.6 Security Assurance Requirements Evidence

This section identifies the measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_ARC.1 Security Architecture Description	Security Architecture: Symantec Altiris IT Management Suite 7.1 SP2 from Symantec
ADV_FSP.2 Security Enforcing Functional Specification	Functional Specification: Symantec Altiris IT Management Suite 7.1 SP2 from Symantec
ADV_TDS.1 Basic Design	Basic Design: Symantec Altiris IT Management Suite 7.1 SP2 from Symantec
AGD_OPE.1 Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: Symantec Altiris IT Management Suite 7.1 SP2 from Symantec
AGD_PRE.1 Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: Symantec Altiris IT Management Suite 7.1 SP2 from Symantec
ALC_CMC.2 Use of a CM System	Security Measures: Symantec Altiris IT Management Suite 7.1 SP2 from Symantec
ALC_CMS.2 Parts of the TOE CM coverage	Security Measures: Symantec Altiris IT Management Suite 7.1 SP2 from Symantec
ALC_DEL.1 Delivery Procedures	Secure Delivery Processes and Procedures: Symantec Altiris IT Management Suite 7.1 SP2 from Symantec
ALC_FLR.2 Flaw Reporting Procedures	Flaw Remediation: Symantec Altiris IT Management Suite 7.1 SP2 from Symantec
ATE_COV.1 Evidence of Coverage	Testing Evidence Supplement: Symantec Altiris IT Management Suite 7.1 SP2 from Symantec
ATE_FUN.1 Functional Testing	Testing Evidence Supplement: Symantec Altiris IT Management Suite 7.1 SP2 from Symantec

Table 6-7 – Security Assurance Rationale and Measures

7 TOE Summary Specification

7.1 TOE Security Functions

The security functions performed by the TOE are as follows:

- Security Audit
- Identification and Authentication
- Managed Systems
- Security Management
- Protection of Security Functions

7.2 Security Audit

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

- FAU_GEN.1

The TOE generates audits for the following actions:

- Use of the management functions specified in FMT_SMF.1
- Modifications to the group of users that are part of a role.

The audit log entries include:

- Time stamp
- Action
- UserId
- Machine

7.3 Identification and Authentication

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_UAU.1
- FIA_UID.1

The TOE requires identification and authentication of operators before allowing access to any configurable security functions. Operators authenticate via username/password dialog, and these parameters are set by the administrator. Identification and Authentication occurs via web-based management GUI (Symantec Management Console) interfacing with the Symantec Management Platform component. Administrators are allowed to log in to the TOE as whichever user is logged into the Windows server without further identifying or authenticating. The Administrator will be prompted if the currently logged on Windows user cannot be authenticated as a valid ITMS user. For example, if the current logged on user is in another domain, or is a local system account, etc. they will be prompted to authenticate using credentials for a valid ITMS account.

The Symantec Management Platform uses role-based security, which means that user access is based on the user's security role. A security role is a set of privileges and permissions that is granted to all members of that role. Each user is then assigned to the appropriate role, rather than assign specific privileges and permissions to each individual user.

A security role controls user access to the Symantec Management Platform using the following parameters associated with a valid username/password:

- Privileges
    - A privilege applies system-wide. A privilege lets a user perform a particular action on the Symantec Management Platform or in the Symantec Management Console. In some cases, the user's role requires the corresponding permissions.
- Permissions on folders and items
    - Permissions specify the access that each security role has to a Symantec Management Console folder. A permission on a folder applies to all of the items that are contained directly in that folder.
- Permissions on organizational views and groups
    - An organizational view is a hierarchical grouping of resources (as organizational groups) that reflects a real-world structure, or "view", of the users. A permission that is assigned to an organizational group applies to all resources in that group. By default, the permission applies to all of its child groups. Permissions cannot be assigned directly to a particular resource.

7.4 Managed Systems

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

- FMS_SCN_(EXT).1

The TOE provides scanning capabilities of managed systems with an Agent deployed on them. The specific scanning actions are determined by policies configured by authorized administrators. ITMS refers to scanning as “software discovery”. These software discovery policies are managed through the Management Console/ Settings interface. See the ITMS Implementation Guide section entitled “Finding Software” for more information.

7.5 Security Management and User Data Protection

The Security Management and User Data Protection functions are designed to satisfy the following security functional requirements:

- FDP_ACC.1
- FDP_ACF.1
- FMT_MSA.1
- FMT_MSA.3
- FMT_MTD.1
- FMT_SMF.1
- FMT_SMR.1

The functionality in the TOE requires management to ensure proper configuration control. These pieces of Security Management functionality are described in the following subsections. The Administrator role in the TOE is responsible for all management functions of the TOE, including management of TOE security settings, and definition of access control.

The TOE ensures that only privileged administrators can access the TOE security functions and related configuration data. Further, only secure values can be used in configuration of security functions and related configuration data based on the design of the management console. The management console ensures the default values of security attributes are restrictive in nature as to enforce the access control policy for the TOE.

7.5.1 Access Control

The TOE implements an access control SFP named SMP Access Control SFP. This SFP determines and enforces the privileges associated with operator roles. An authorized administrator can define specific services available to administrators and users via the management console.

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 7-1 – Description of Roles Supported in the TOE). The Administrator can define services available to each roles without granting full System Administrator privileges. Additionally, the Administrator can create new Security Roles and modify the privileges and permissions as appropriate.

By default, the TOE maintains the roles defined in the following table, which contains a description of each role:

ROLE	DESCRIPTION
Administrator	Has all security privileges and permissions assigned, so it has complete access to all aspects of the Symantec Management Platform and any installed solutions. This security role cannot be modified.
Guest	Has highly restrictive privileges assigned.
Level 1 Worker	Has restricted read-only privileges assigned.
Level 2 Worker	Has complete Management and Right-click Menu privileges assigned.
Software Librarian	Has Software Management Framework privileges assigned. The privileges are limited to those needed to create and manage software packages.
Supervisor	Has complete Management and Right-click Menu privileges, and limited System privileges assigned.

Table 7-1 – Description of Roles Supported in the TOE

7.5.2 TOE Configuration

The TOE provides GUI-based management of client computers via the Symantec Management Console. Via the console, authenticated operators with the appropriate privileges can perform the following client management tasks:

- Configure Security
    - Define Security Roles per the Access Control SFP
    - User permissions
    - Account management
- View and customize resource data via reports
    - View and manage resource data with reports
    - Extract and view report results
    - Save report results to a file
- Manage the software catalog and software library

    - Configure software library
    - Populate and view the software catalog
- Manage scanning policies
    - Configure schedules for scanning
    - Configure which targets are to be scanned.