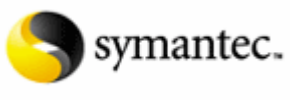

Security Target

for

Symantec LiveState Delivery

version 6.0.1

Reference: Symantec LiveState Delivery\ST

August 2006

Issue: 1.2

Symantec Corporation
275 Second Avenue
Waltham, MA 02451
USA

Copyright notice

DOCUMENT AUTHORISATION

Document Title	Security Target for Symantec LiveState Delivery version 6.0.1

Reference	**Issue**	**Date**	**Description**
Symantec LiveState Delivery\ST	1.0	June 2006	First Issue
Symantec LiveState Delivery\ST	1.2	Aug 2006	Minor updates during certification

Contents

REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004 (aligned with ISO 15408).

GLOSSARY AND TERMS

ADK	Application Development Kit
Authorised Administrators	People on the network allowed to administer the TOE.
BOOTP	BOOTstrap Protocol (Internet)
CC	Common Criteria
CCM	Comprehensive Client Management
CCM TFTP	TFTP (trivial file transfer protocol) transfers the CCM Boot Agent from the server on which it resides to the managed computer.
DHCP	Dynamic Host Configuration Protocol
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
FTP	File Transfer Protocol
IP	Internet Protocol
IT	Information Technology
MAC	Media Access Control
Managed System	Networked PC on which an Agent has been installed
MMC	Microsoft Management Console
NAT	Network Address Translation
NTP	Network Time Protocol
Platform	Any hardware platform and operating system that has a component of the TOE installed on it.
PP	Protection Profile
PROM	Programmable Read Only Memory
PXE	Pre-Boot Execution Environment

SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification
Unauthorised user	Users not authorised to use the TOE.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User data	Data created by and for the user that does not affect the operation of the TSF.
VPN	Virtual Private Network
WAN	Wide Area Network

1 Introduction to the Security Target

1.1 Security Target Identification

1 Title: Security Target for Symantec LiveState Delivery version 6.0.1, issue 1.2.

2 Assurance Level: EAL2.

3 TOE: Symantec LiveState Delivery version 6.0.1.

1.2 Security Target Overview

4 The Symantec LiveState Delivery is an enterprise-class system for remotely delivering operating systems, applications, and programs across networks to desktops, mobile PCs, handheld devices and servers. However, mobile PCs and handheld devices are outside the scope of the evaluation. Symantec LiveState Delivery uses scheduled push and pull technology to deliver software from centralized servers to multiple PCs or servers simultaneously.

5 Symantec LiveState Delivery provides a suite of administrative tools that allow identified and authorised administrators (with a variety of roles) to manage the unattended deployment of business-critical software from centralized Windows servers to multiple PCs or servers simultaneously.

1.3 CC Conformance Claim

6 This TOE has been developed using the functional components as defined in the Common Criteria version 2.2 [CC] part 2, with the assurance level of EAL2, as identified in part 3 of [CC].

7 The TOE conforms to [CC] Part 2 extended and [CC] Part 3 conformant with the assurance level of EAL2.

2 TOE Description

2.1 Overview of Symantec LiveState Delivery

8 This section presents an overview of Symantec LiveState Delivery to assist potential users in determining whether it meets their needs.

9 The Symantec LiveState Delivery provides an enterprise-class system for remotely delivering operating systems, applications, and programs across networks to desktops, mobile PCs, handheld devices, and servers. However, mobile PCs and handheld devices are outside the scope of the evaluation. Symantec LiveState Delivery uses scheduled push and pull technology to deliver software from centralized servers to multiple PCs or servers simultaneously.

10 Diagram 2-1 shows the evaluated network environment for the Symantec LiveState Delivery.

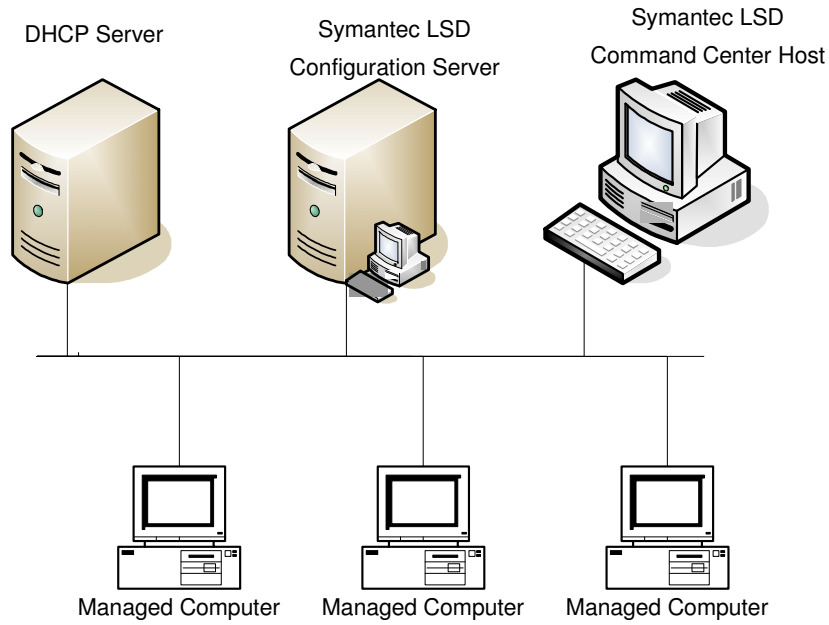

Diagram 2-1: Network Environment

11 Diagram 2-2 shows the configuration of Symantec LiveState Delivery and the scope of the evaluation.

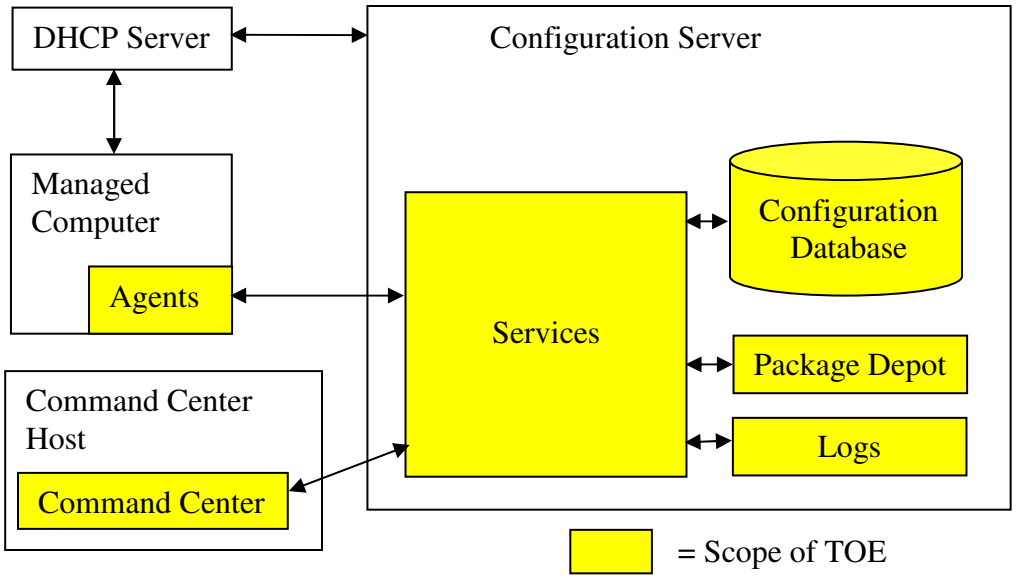

Diagram 2-2: Symantec LiveState Delivery

12 The Symantec LiveState Delivery consists of three fundamental system areas and their corresponding components:

System Area	Components
Server	The Configuration Server supplies: • A Package Depot with all operating systems and applications delivered to managed computers. • The Database for tracking all installation and configuration actions on managed computers. • Services for remotely administering PCs over the network. • Generates and stores the log files that are generated by Symantec LiveState Delivery.
Command Center	The Command Center is used to administer managed computers and manage the Configuration Server.

Managed Computers	The agents reside on the managed computer and carry out any installation and/or configuration that is required. The Command Center is used to install the agents onto the managed computer. The Agents query the configuration server to discover what tasks are scheduled to be performed, download the packages required, and execute the tasks.

13 The administration of a Symantec LiveState Delivery network is an asynchronous operation. Authorised administrators deploy software to managed computers by first copying this software to the Package Depot on the Configuration Servers and then scheduling tasks to be executed from these servers.

14 Tasks are performed by the Agents on targeted managed computers at a defined time or Symantec LiveState Delivery pushes tasks that are immediately executed on managed computers. Completed work is reported back to the server. The authorized administrators can then use the Command Center to determine the status of the managed computers.

15 Symantec LiveState Delivery data exchange is based on IP, the worldwide standard protocol. Symantec LiveState Delivery can be set up in both BOOTP and DHCP (Dynamic Host Configuration Protocol) environments. For the evaluation the DHCP environment will be used. DHCP dynamically allocates IP addresses to computers on a local area network.

16 For the evaluation, the evaluated configuration will be on a network not connected to any other network. The network cards used will be PXE-compatible network card.

2.2 Scope and Boundaries of the Evaluated Configuration

17 The TOE configuration consists of:

- Symantec LiveState Delivery 6.0.1 Configuration Server;
- Command Center 6.0.1;
- Agent for Windows;
- Boot Agent;
- Pre-OS Agent.

18 The TOE is a software only TOE.

2.2.1 Physical Scope

19 The physical scope of the TOE is identified in Table 2-1.

Software	**Symantec LiveState Delivery 6.0.1**

Table 2-1: TOE Component Identification

2.2.2 Hardware and Software for the Command Center and Symantec LiveState Delivery Configuration Server

20 The Command Center is the administration interface to the Symantec LiveState Delivery. For the evaluated configuration the Command Center and Symantec LiveState Delivery Configuration Server will be located on separate machines.

21 The required platform for the TOE is identified in Tables 2-2 and 2-3.

Software	Symantec LiveState Delivery Configuration Server
Operating System	Windows 2000 Advanced Server Service Pack 4
Network Interface Cards	One 10/100 Ethernet card
CPU	One Intel Pentium IV 2.5 GHz processor
Memory	4 GB
Disk	34 GB

Table 2-2: Configuration Server Underlying Platform Minimum Specification

Software	Symantec LiveState Delivery Command Center.
Operating System	Windows XP Professional Service Pack 2
Network Interface Cards	One 10/100 Ethernet card
CPU	One Intel Pentium IV 2.8 GHz processor
Memory	1 GB
Disk	75 GB

Table 2-3: Command Center Host Underlying Platform Minimum Specification

22 The Command Center software has to be loaded onto the Command Center Host in order for the machine to run Command Center.

23 Although the TOE can be accessed from any machine connected to the network that has the Command Center software installed, in the evaluated configuration the authorized administrators are instructed to only access the TOE via the Command Center installed on the Command Center Host.

2.2.3 Hardware and Software Requirements for the Managed Computer

24 The managed computers are accessible on the network. Table 2-4 identifies the tested platform for the managed computer. The minimum specification is for a PC with screen resolution of 1024 x 768 (256 colours) and a single PXE 2.1 or later network card.

Software	The Symantec LiveState Delivery Agents.
Operating System	Windows XP Professional Service Pack 2
Network Interface Cards	Intel Pro/100 VE
CPU	One Intel Celeron 2.4 GHz processor
Memory	128 MB
Disk	40 GB

Table 2-4: Managed Computer Tested Underlying Platform

2.2.4 Security Functions of the TOE

25 The TOE Security Functions (TSF) are:

2.2.4.1 Identification

26 The TOE will identify administrators by means of a username and will authenticate them by use of a password mechanism.

2.2.4.2 User Data Protection and Security Management

27 All administrators will be assigned a role that will determine what functions they can access. There are five roles within the TOE.

2.2.4.3 Audit Function

28 The TOE records when administrators perform certain actions, noting what was performed, by whom and when. This function is active as long as the Configuration Server component of the TOE is running.

2.2.4.4 Protection of TOE Security Functions

29 The TOE provides self protection from untrusted entities. Functions that enforce TOE security always take place before other functions to ensure security is maintained. The TOE Audit Function uses the time from the Configuration Server component operating system.

2.2.5 Outside of the Scope

30 Software and hardware features outside the scope of the defined TSF and thus not evaluated are:

- Wizards;
- Remote Administration;
- Live update support;
- Replicator;
- Web Admin;
- Multiplatform (Java) Agent;
- Web Self Service;
- Pocket PC agent;
- Wake on LAN proxy;
- Locator;
- User profile manager;
- Image Delivery;
- LiveState Delivery Enterprise Manager;
- LiveState Delivery Package Manager;
- Client Migration;
- AutoInstall;
- Auto Discover Agent.

3 Security Environment

3.1 Introduction

31 This section provides the statement of the TOE security environment, which identifies and explains all:

1. known and presumed threats countered by either the TOE or by the security environment;

2. organisational security policies the TOE must comply with;

3. assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects.

3.2 Threats

32 This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment.

33 The TOE is designed to manage many computers across an enterprise. If an attacker is able to gain access to the TOE then every managed computer can be compromised. This will be much faster than compromising each computer individually. Hence, it is important to protect the computer management functions of the TOE.

3.2.1 Threats addressed by the TOE

34 The threats that must be countered by the TOE are listed below.

T.NOIDENT	A user not identified to use the TOE may attempt to bypass the security of the TOE so as to access and use security function and/or non-security functions provided by the TOE.
T.REPEAT	A user not authorised to use the TOE may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.

Table 3-1 Threats to be addressed by the TOE

3.2.2 Threats addressed by both the TOE and the IT Environment

35 The following table identifies the threats that are partially met by the TOE and partially met by the IT Environment.

Threat	Description
T.AUDACC	A user without legitimately acquired logon credentials interacting with the Configuration Server via the network may escape detection because the audit logs are not reviewed.
T.SELPRO	A user attempting unauthorised interaction with the Configuration Server via the network may read, modify or destroy TOE data.
T.AUDFUL	A user attempting unauthorised interaction with the Configuration Server via the network may cause audit records to be lost by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
T.CONFIG	A user attempting unauthorised physical interaction with the Command Center and/or Configuration Server may succeed in reading, modifying or destroying TOE data.

Table 3-2 Threats met by the TOE & IT Environment

3.2.3 Threats countered solely by the IT Environment

36 The threats that must be countered by technical and/or non-technical measures in the IT environment, or must be accepted as potential security risks are listed below.

TE.USAGE	The TOE may be inadvertently configured, used and administered in an insecure manner by either authorised administrators or unauthorised users.

37 Table 3-2 identifies the threats that are partially met by the IT environment.

3.3 Organizational Security Policies

38 There are no organizational security policies or rules with which the TOE must comply.

3.4 Assumptions

39 The following assumptions are assumed to exist.

3.4.1 Physical Assumptions

A.PHYSEC	The Configuration Server and Command Center Host are physically protected to prevent unauthorised use / user access.
A.REMOS	The platforms are delivered to the user's site, installed and administered in a secure manner.

3.4.2 Personnel Assumptions

A.TRUST	The users of the network on which the TOE is installed are trusted not to connect that network to any other network.
A.NOEVIL	Authorised administrators for the TOE and platforms are non-hostile and follow all administrator guidance; however, they are capable of error.

3.4.3 Connectivity Assumptions

A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.COMMS	The communication links between the TOE components are physically protected.
A.ONENET	The network the TOE is installed on is not connected to any other network.

4 Security Objectives

4.1 TOE Security Objectives

4.1.1 IT Security Objectives

40 The IT security objectives are listed below.

O.IDAUTH	The TOE must uniquely identify and authenticate all users, before granting authorised administrators access to the security functions.
O.ACCESS	The TOE must only allow authorised administrators to access TOE functions and data when their role contains the permissions to do so.

4.1.2 IT Security Objectives addressed by both the TOE and the IT Environment

41 The following table identifies the IT Security objectives listed that are partially met by the TOE and partially met by the IT Environment.

Objective	Description
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources.
O.SELPRO	The TOE must protect itself against attempts by unauthorised users to bypass, deactivate, or tamper with TOE security functions.
O.AUDIT	The TOE must record the account management actions of logged in users, with accurate dates and times, in a form readable by authorised administrators.
O.SECFUN	The TOE must provide functionality that enables authorized administrators to use the TOE security functions.
O.PARTSEP	The TSF must maintain a domain for its own execution that protects itself and its resources from external interference or tampering.

Table 4-1 IT Security Objective partially met by IT Environment and TOE

4.2 Environment Security Objectives

4.2.1 IT Security Objectives

42 The following IT security objectives are met by the environment.

OE.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
OE.AUDREV	The TOE must provide a means to read the audit trail.

4.2.2 Non-IT Security Objectives

43 The non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

NOE.PHYSEC	The Command Center and Configuration Server platforms are physically secure.
NOE.NOEVIL	Authorized administrators of the TOE are non-hostile and follow all administrator guidance; however, they are capable of error.
NOE.GUIDAN	The TOE must be delivered to the user's site, installed, and administered in a secure manner.
NOE.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policies and practices.
NOE.REMOS	The Configuration Server, Command Center Host and managed computers must be delivered to the user's site, installed and administered in a secure manner.
NOE.COMMS	The communication links between the Configuration Server, Command Center Host and managed computers must be physically protected.
NOE.TRUST	The users of the network the TOE is installed on must not connect the TOE network to any other network.
NOE.ONENET	The network the TOE is installed on must not be connected to any other network.

5 IT Security Requirements

5.1 TOE Security Requirements

5.1.1 TOE Security Functional Requirements

44 The TOE security functional requirements consist of components from Part 2 of the CC, refined as indicated **[ ]** and two explicitly stated requirements. They are listed in the following table.

Functional Components	
FIA_UID.2	User Identification before any action
FIA_ATD.1	User attribute definition
FIA_UAU.2	User Authentication before any action
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FMT_SMR.1	Security roles
FMT_MOF.1	Management of Security Functions Behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FPT_RVM.1	Non-Bypassability of the TSP
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User identity association
FAU_STG.4	Prevention of audit data loss
FPT_STM.1_EXP	Reliable time stamps
FPT_SEP.1_EXP	TSF domain separation

Table 5-1: Functional Requirements

Identification

45 This section addresses the requirements for functions to establish and verify a claimed user identify.

46 **FIA_UID.2 User Identification before any action**

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

47 **FIA_ATD.1 User attribute definition**

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to the individual users: [user identity, password, association of a user with an authorized administrator role].

48 **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.

User Data Protection

49 This section specifies requirements for the TOE security functions and TOE security function policies relating to protecting user data.

50 **FDP_ACC.1 Subset access control**

FDP_ACC.1.1	The TSF shall enforce the [access control SFP] on [Manipulation of TSF data and security attributes by an authorised administrator (as specified in FMT_MSA.1 and FMT_MTD.1)].

51 **FDP_ACF.1 Security attribute based access control**

FDP_ACF.1.1	The TSF shall enforce the [access control SFP] to objects based on the following:[an authorised administrator with functionality as listed in Table 5-3].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled

objects is allowed: [Manipulation of TSF data and security attributes by an authorised administrator (as specified in FMT_MSA.1 and FMT_MTD.1)].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [None].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [role].

Security Management

52 This section defines requirements for the management of security attributes that are used to enforce the TSF.

53 **FMT_SMR.1 Security Roles**

FMT_SMR.1.1 The TSF shall maintain the roles [HelpDesk, Package, Computer, Computer / Package, Server].

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

54 **FMT_MOF.1 Management of security functions behavior**

FMT_MOF.1.1 The TSF shall restrict the ability to [modify the behaviour of] the functions [listed in Table 5-2] to [the authorised identified roles listed in Table 5-2].

Role	Functions
HelpDesk	• Assign, update, uninstall non-system packages • Extend sql query for computers • Find computers, computer groups, packages, profiles • Wakeup, push computers
Package	• Manage CCM packages • Extend sql query for computers • Find computers, computer groups, packages, profiles • Wakeup, push computers
Computer	• Configure disks • Open computer log files • Reset computers

	• Unlock computers • Assign, update, uninstall system packages • Assign, update, uninstall non-system packages • Extend sql query for computers • Find computers, computer groups, packages, profiles • Wakeup, push computers
Computer / Package	• Manage CCM packages • Configure disks • Open computer log files • Reset computers • Unlock computers • Assign, update, uninstall system packages • Assign, update, uninstall non-system packages • Extend sql query for computers • Find computers, computer groups, packages, profiles • Wakeup, push computers
Server	• Manage CCM packages • Configure disks • Open computer log files • Reset computers • Unlock computers • Assign, update, uninstall system packages • Assign, update, uninstall non-system packages • Extend sql query for computers • Find computers, computer groups, packages, profiles • Wakeup, push computers

Table 5-2: Authorised Roles and Associated Functions

55 **FMT_MSA.1 Management of security attributes**

FMT_MSA.1.1 The TSF shall enforce the [access control SFP] to restrict the ability to [operations listed in Table 5-3] the security attributes [listed in Table 5-3] to [the authorised administrator role listed in Table 5-3].

Security Attribute	Operations	Role: Server
Admin Roles, Admin Accounts	Modify	✓
Server Properties	Change_default	✓
	Modify	✓

Table 5-3: Authorised Roles and Associated Operations

56 **FMT_MSA.3 Static attribute initialization**

FMT_MSA.3.1 The TSF shall enforce the [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 [computer, computer/package, server and siadm] to specify alternative initial values to override the default values when an object or information is created.

57 **FMT_MTD.1 Management of TSF data**

FMT_MTD.1.1 The TSF shall restrict the ability to [operations listed in Table 5-4] the [TSF data listed in table 5-4] to [the authorised administrator roles listed in Table 5-4].

TSF Data	Operations	Role		
		Computer	Computer / package	Server
Organisational computer groups[i]	Modify, delete, create	✔	✔	✔
Computers	Modify	✔	✔	✔
	Delete, create		✔	✔
Computer profiles	Modify, delete, create	✔	✔	✔
Job parameter and Job phase	Modify	✔	✔	✔
Job line	Delete	✔	✔	✔

Table 5-4: Authorised Roles and Operation on TSF Data

58 **FMT_SMF.1 Specification of Management Functions**

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [those for which FMT_MOF.1 and FMT_MSA.1 restrict use to the authorised administrators].

Protection of the TOE Security Functions

59 This section specifies functional requirements that relate to the integrity and management of the mechanisms providing the TSF and TSF data.

60 **FPT_RVM.1 Non-bypassability of the TSP**

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

[i] Temporary computer groups may also be created, modified and deleted by administrators but these actions are security irrelevant and have been excluded from the SFRs.

61 **FPT_SEP.1_EXP TSF domain separation**

FPT_SEP.1.1_EXP	The TSF shall maintain a security domain that protects from interference and tampering by untrusted subjects in initiating actions through its own TSFI.
FPT_SEP.1.2_EXP	The TSF shall enforce separation between the security domains of subjects in the TSC

62 **FPT_STM.1_EXP Reliable time stamps**

FPT_STM.1.1_EXP	The TSF shall be able to obtain time stamps for its own use from a designated time source.

Security Audit

63 This section involves recognizing, recording and storing information related to security relevant activities.

64 **FAU_GEN.1 Audit data generation**

FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the not specified level of audit and c) [the events listed in Table 5-5]
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 operation, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [none]]

Auditable Event
Login of a user
User changing own password
User changing another user's password
Creation of a new user account
Deletion of a user account

Table 5-5: Auditable Event

65 **FAU_GEN.2 User identity association**

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

66 **FAU_STG.4 Prevention of audit data loss**

FAU_STG.4.1 The TSF shall [overwrite the oldest stored audit records] if the audit trail is full.

5.2 Security requirements for the IT Environment

67 This section details the IT security requirements that are met by the IT environment of the TOE. Table 5-6 lists the IT security requirements to be provided by the IT environment:

Functional Components	
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps
FAU_STG.1	Protected audit trail storage
FAU_SAR.1	Audit review

Table 5-6: IT Security Requirements of the Environment

68 **FPT_SEP.1 TSF domain separation**

FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.

69 **FPT_STM.1 Reliable time stamps**[ii]

FPT_STM.1.1	The TSF shall be able to provide reliable time stamps for its own use.

70 **FAU_STG.1 Protected audit trail storage**[iii]

FAU_STG.1.1	The TSF shall protect the stored audit records from unauthorized deletion.
FAU_STG.1.2	The TSF shall be able to [prevent] unauthorised modifications to the audit records in the audit trail.

71 **FAU_SAR.1 Audit review**

FAU_SAR.1.1	The TSF shall provide [all authorised administrators] with the capability to read [all audit trail 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.

5.3 TOE Security Assurance Requirements

72 The assurance requirements for this Security Target, taken from Part 3 of the CC, comprise the EAL2 level of assurance. The assurance components are summarized in the following table.

[ii] FPT_STM.1 is met by the LiveState Delivery Server's platform.
[iii] FAU_STG.1 is fully met by the LiveState Delivery Server's operating system.

Assurance Class	Assurance Components	
Configuration management	ACM_CAP.2	Configuration Items
Delivery and operation	ADO_DEL.1	Delivery Procedures
	ADO_IGS.1	Installation, generation and start-up procedures
Development	ADV_FSP.1	Informal Functional Specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 5-7: Assurance Requirements: EAL2

73 Further information on these assurance components can be found in [CC] Part 3.

5.4 Strength of Function Claim

74 A Strength of Function (SOF) claim of SOF-basic is made for the TOE.

75 FIA_UAU.2 meets the claim of SOF-basic for the strength of the password part of the authentication function.

76 For a justification of the Strength of Function claim see Section 8.3.6.

6 TOE Summary Specification

6.1 TOE Security Functions

77 This section describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in Section 5.1.

6.1.1 Identification

78 **I.1 -** Authorized administrators must be identified and authenticated to the TOE via the Command Center before any administration functions can be completed.

79 **I.2** – Authorized administrators are identified by

- User identity;
- Password;
- Role.

80 **Functional Requirements Satisfied:** FIA_UID.2, FIA_ATD.1, FIA_UAU.2[iv]

6.1.2 User Data Protection and Security Management

81 **M.1 -** The TOE maintains 1 default user account:

- **siadm** - an authorized site primary administrator uses the *siadm* account, which cannot be deleted. This account has the same privileges as the Server role, which grants the highest level of access privileges and allows all CCM tasks to be performed.

82 **M.2 -** Every Administrator account is assigned a role that grants permission to perform certain CCM tasks. The Predefined roles are:

- Server,
- Computer,
- Computer/Package,
- Package,
- Helpdesk.

83 Tasks for predefined roles cannot be changed. Authorised administrators assigned with the role Server can define new roles.

84 **M.3 –** The table below describes the functions that each role / user account is allowed to perform.

[iv] FIA_UAU.2 is subject to strength of function analysis for the authentication mechanism using passwords.

Role / Account	Functions
HelpDesk	• Assign, update, uninstall non-system packages • Extend sql query for computers • Find computers, computer groups, packages, profiles • Wakeup, push computers
Package	• Manage CCM packages • Extend sql query for computers • Find computers, computer groups, packages, profiles • Wakeup, push computers
Computer	• Delete organisational computer groups • Create, Edit organisational computer groups • Edit computers • Create, Edit, delete computer profiles • Edit Job Parameter, delete job line, change job Phase • Configure disks • Open computer log files • Reset computers • Unlock computers • Assign, update, uninstall system packages • Assign, update, uninstall non-system packages • Extend sql query for computers • Find computers, computer groups, packages, profiles • Wakeup, push computers
Computer / Package	• Delete organisational computer groups • Create, Edit organisational computer groups • Edit computers • Add computers • Delete computers • Create, Edit, delete computer profiles • Edit Job Parameter, delete job line, change job Phase • Manage CCM packages • Configure disks • Open computer log files • Reset computers

Role / Account	Functions
	• Unlock computers • Assign, update, uninstall system packages • Assign, update, uninstall non-system packages • Extend sql query for computers • Find computers, computer groups, packages, profiles • Wakeup, push computers
Server	• Manage Admin Roles • Manage Admin Accounts • Edit Server Properties • Delete organisational computer groups • Create, Edit organisational computer groups • Edit computers • Add computers • Delete computers • Create, Edit, delete computer profiles • Edit Job Parameter, delete job line, change job Phase • Manage CCM packages • Configure disks • Open computer log files • Reset computers • Unlock computers • Assign, update, uninstall system packages • Assign, update, uninstall non-system packages • Extend sql query for computers • Find computers, computer groups, packages, profiles • Wakeup, push computers

Table 6-1 User Roles and Associated Functions

85 **Functional Requirements Satisfied:** FMT_SMF.1, FMT_SMR.1, FMT_MOF.1, FMT_MSA.3, FMT_MSA.1, FMT_MTD.1, FDP_ACC.1, FDP_ACF.1.

6.1.3 Audit Function

86 **A.1 -** The accounting mechanisms cannot be disabled. The start-up and shutdown of audit functions is synonymous with the start-up and shutdown of the TOE. Start-up and shut-down of the TOE must be recorded in the audit trail.

87 **A.2 –** The TOE generates, at log level 3, a log file (the Configuration Database Service log file) that provides an audit trail of actions performed by the authorised administrators. The events that are recorded are:

- Login of an authorised administrator;
- Authorised administrator changing own password;
- Authorised administrator changing another user's password;
- Creation of a new user account;
- Deletion of a user account.

88 **A.3 –** For each event the Audit Function will record the following:

- Date and time of the event;
- Type of operation;
- Subject identity;
- Success and failure of event;
- User identity.

89 **A.4 –** The audit trail data will be generated in a format suitable for interpretation by the authorised administrator.

90 **A5 –** When the maximum log file size is reached for the log file, the current log file is renamed to "ccmdb.old" and a new log file, "ccmdb.log" is created. The existing ".old" file is deleted. Archiving is a manual process that is performed on the log files. The files are retained as long as there is space available.

91 **Functional Requirements Satisfied:** FAU_GEN.1, FAU_GEN.2, FAU_STG.4.

6.1.4 Protection of TOE Security Functions

92 **P.1 -** The functions that enforce the TOE Security Policy (TSP) are always invoked and completed, before any function within the TSF Scope of Control (those interactions within the TOE that are subject to the rules of the TSP) is allowed to proceed.

93 **P.2 -** The TOE provides self-protection from external modification or interference of the TSF code or data structures by untrusted subjects by using authentication techniques, domains and privileged user accounts.

94 **P.3** – Time will be derived from Configuration Server operating system time and will be used during auditing.

95 **Functional Requirements Satisfied:** FPT_RVM.1, FPT_SEP.1_EXP, FPT_STM.1_EXP.

6.2 Identification and Strength of Function Claim for IT security Functions

96 This Security Target claims that the general strength of the security functions provided by the TOE is SOF-basic.

97 Section 6.1.1 Identification meets the claim of SOF-basic for the strength of the password mechanism within the authentication function.

6.3 Assurance Measures

98 Assurance measures will be produced to comply with the Common Criteria Assurance Requirements for EAL2. Table 8-6 maps the assurance measures to the assurance requirements.

7 Protection Profiles Claims

No claims against a protection profile are made.

8 Rationale

8.1 Introduction

99 This section demonstrates that the TOE provides an effective set of IT security countermeasures within the security environment and that the TOE summary specification addresses the requirements.

8.2 Security Objectives for the TOE Rationale

100 Table 8-1 demonstrates how the IT security objectives and environment objectives of the TOE counter the IT threats and environment threats identified in Section 3.2.1 and 3.2.2.

Threats/ Assumptions / Objectives	T.NOIDENT	T.REPEAT	T.AUDACC	T.SELPRO	T.AUDFUL	T.CONFIG	TE.USAGE	A.PHYSEC	A.LOWEXP	A.NOEVIL	A.ONENET	A.REMOS	A.COMMS	A.TRUST
O.IDAUTH	✓	✓		✓										
O.ACCESS	✓			✓										
O.SECSTA				✓										
O.SELPRO				✓										
O.AUDIT			✓											
O.SECFUN				✓										
O.PARTSEP				✓		✓								
OE.LOWEXP									✓					
OE.AUDREV			✓		✓									
NOE.GUIDAN							✓							
NOE.ADMTRA			✓		✓	✓	✓							
NOE.PHYSEC			✓	✓	✓	✓		✓						
NOE.NOEVIL						✓				✓				
NOE.ONENET											✓			
NOE.REMOS												✓		
NOE.COMMS													✓	
NOE.TRUST						✓								✓

Table 8-1 Mapping of Objectives to Threats and Assumptions

101 The following are justifications for Objectives that are met solely by the TOE.

102 **O.IDAUTH**

103 This security objective is necessary to counter the threats: T.NOIDENT, T.REPEAT and T.SELPRO because it requires that users be uniquely identified and authenticated before accessing the TOE.

104 **O.ACCESS**

105 This security objective is necessary to counter the threats: T.NOIDENT and T.SELPRO as it requires the TOE to prevent unauthorized management of TOE data or functions by users.

106 The following are justifications for Objectives that are partially met by the TOE and partially by the IT Environment.

107 **O.SECSTA**

108 This security objective is necessary to counter the threats: T.SELPRO because it requires that no information is compromised by the TOE upon start-up or recovery.

109 The Configuration Server Operating System must also not compromise TOE information during start-up or recovery.

110 **O.SELPRO**

111 This security objective is necessary to counter the threat: T.SELPRO because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

112 The Configuration Server Operating System must protect the TOE files from unauthorised interference.

113 **O.AUDIT**

114 This security objective is necessary to counter the threat: T.AUDACC because it requires that a record of actions of logged in users is produced to be available for review by authorised administrators.

115 The Configuration Server operating system provides the time for the TOE and maintains the log file.

116 **O.SECFUN**

117 This security objective is necessary to counter the threat: T.SELPRO by requiring that the TOE allows the authorised administrators access to the TOE security functions.

118 The Configuration Server Operating System provides the MMC that the Command Center relies upon.

119 **O.PARTSEP**

120 This security objective is necessary to counter the threats: T.SELPRO and T.CONFIG because it requires that the TOE protect itself and its resources from external interference, tampering or unauthorized disclosure of the TOE security functions.

121 The Configuration Server platform provides memory management and separation within the CPU.

122 The following are justifications for Objectives that are met by the IT Environment.

123 **OE.LOWEXP**

124 This environmental security objective is necessary to support the assumption: A.LOWEXP because it requires that the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

125 **OE.AUDREV**

126 This security objective is necessary to counter the threats: T.AUDACC and T.AUDFUL by requiring functions to allow the audit trail to be read and thus allowing authorised administrators to see what security relevant events have taken place and how full the audit trail is.

127 The Configuration Server Operating System maintains the log file.

128 **NOE.GUIDAN**

129 This environmental security objective is necessary to counter the threat: TE.USAGE because it requires that those responsible for the TOE ensure that it is delivered to the user's site, installed, administered, and operated in a secure manner.

130 **NOE.ADMTRA**

131 This environmental security objective is necessary to counter the threats: T.AUDACC, T.AUDFUL, T.CONFIG and TE.USAGE because it ensures that authorised administrators receive the proper training.

132 **NOE.PHYSEC**

133 This environmental security objective is necessary to support the threats and assumption: T.AUDACC, T.SELPRO, T.AUDFUL, T.CONFIG and A.PHYSEC because it requires that the Configuration Sever is physically protected to prevent tampering.

134 **NOE.NOEVIL**

135 This environmental security objective is necessary to support the Threat and assumption: T.CONFIG and A.NOEVIL because it requires that authorised administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

136 **NOE.ONENET**

137 This environmental security objective is necessary to support the assumption: A.ONENET because it requires that the network the TOE is installed is not connected to any other network.

138 **NOE.REMOS**

139 This environmental security objective is necessary to support the assumption: A.REMOS because it requires that the Configuration Server and managed computers are delivered to the user's site, installed and administered in a secure manner.

140 **NOE.COMMS**

141 This environmental security objective is necessary to support the assumption: A.COMMS because it requires that the communication links between the Configuration Server and managed computers are physically protected.

142 **NOE.TRUST**

143 This environmental security objective is necessary to support the assumption: A.TRUST because it requires that the users of the TOE network are trusted not to connect the TOE network to any other network.

144 The following are justifications for IT security threats that are partially met by the TOE and partially by the IT Environment.

145 **T.AUDACC**

146 The TOE produces audit events of user actions and writes them into a log file.. The Configuration Server Operating System maintains the log and audit configuration files, provides the authorized administrators with the means to view

the audit trail and provides the facilities for setting what level of audit is carried out. The authorized administrators must ensure that the audit facilities are used and managed correctly including inspecting the logs on a regular basis.

147 **T.SELPRO**

148 Access to the internal data of the TOE is only possible through the machine that the TOE is installed on. The TOE relies on the physical environment to ensure that only the authorised administrators have physical access to the TOE.

149 **T.AUDFUL**

150 The TOE renames the log file to ccmdb.old, overwriting any previously written file of that name, when the audit trail is close to being full and starts a new log file, ccmdb.log (also overwriting any previously written file of that name), so that the audit trail can be backed up. The Configuration Server Operating System maintains the audit log and provides the facilities for backing up the log. The authorized administrators must ensure that the audit log is backed up when necessary. The TOE relies on the physical environment to ensure that only the authorised administrators have physical access to the Configuration Server.

151 **T.CONFIG**

152 The Configuration Server Operating System maintains the TOE files and runtime environment. The authorized administrators must ensure that the TOE is administered correctly. The TOE relies on the physical environment to ensure that only the authorised administrators have physical access to the Configuration Server.

8.3 Security Requirements Rationale

8.3.1 Security Requirements are appropriate

153 Table 8-2 identifies which SFRs satisfy the Objectives as defined in Section 4.1.1.

Objective	Security Functional Requirement(s)
O.IDAUTH	FIA_UID.2, FIA_ATD.1, FIA_UAU.2, FMT_SMR.1
O.ACCESS	FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FMT_SMF.1, FMT_MTD.1, FMT_MSA.1, FMT_MOF.1
O.SECSTA	FMT_MOF.1, FMT_MSA.3, FMT_MSA.1
O.SELPRO	FPT_RVM.1, FPT_SEP.1_EXP, FAU_STG.4
O.AUDIT	FAU_GEN.1, FAU_GEN.2, FPT_STM.1_EXP

Objective	Security Functional Requirement(s)
O.SECFUN	FAU_STG.4, FMT_MOF.1, FMT_SMF.1, FMT_MSA.3, FMT_MTD.1, FMT_MSA.1
O.PARTSEP	FPT_SEP.1_EXP

Table 8-2 Mapping of Objectives to SFRs

154 **O.IDAUTH:** The TOE must uniquely identify all users, before granting authorized administrators access to the security functions. O.IDAUTH is addressed by:

- FIA_UID.2 User identification before any action, which requires that authorized administrators be successfully identified before allowing access to the TOE.
- FIA_ATD.1 User attribute definition, which requires that the TSF maintain security attributes of users.
- FIA_UAU.2 User authentication before any action, which requires that authorised administrators be successfully authenticated before allowing access to the TOE.
- FMT_SMR.1 Security roles, which requires that the TSF be able to associate authorised administrators with roles.

155 **O.ACCESS:** The TOE must allow authorised administrators access only to manage appropriate TOE functions and data according to role. O.ACCESS is addressed by:

- FDP_ACC.1 Subset access control, which requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE.
- FDP_ACF.1 Security attribute based access control, which requires the TSF enforce access controls based on specified security attributes. In addition, the TSF can explicitly authorize and deny access to specified subjects.
- FMT_MSA.3 Static attribute initialization, which requires the TSF enforce access control for specified default values of security attributes.
- FMT_SMF.1 Specification of management functions, which requires that the TSF provide specific management functions.

- FMT_MTD.1 Management of TSF data, which requires that only authorized administrators of the system may query network event data and can delete alert data.

- FMT_MSA.1 Management of security attributes, which requires only authorized administrators can query, modify, and delete specified security attributes.

- FMT_MOF.1 Management of security function behaviour, which requires the authorized administrators (roles) to manage the behaviour of functions in the TSF that use rules or have specified conditions that may be manageable.

156 **O.SECSTA:** Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network. O.SECSTA is addressed by:

- FMT_MOF.1 Management of security function behavior, which requires the authorized administrators (roles) to manage the behavior of functions in the TSF that use rules or have specified conditions that may be manageable.

- FMT_MSA.3 Static attribute initialization, which requires the TSF enforce access control for specified default values of security attributes.

- FMT_MSA.1 Management of security attributes, which requires only authorized administrators can query, modify, and delete specified security attributes.

157 **O.SELPRO:** The TOE must protect itself against attempts by unauthorised users to bypass, deactivate, or tamper with TOE security functions. O.SELPRO is addressed by:

- FPT_RVM.1 Non-bypassability of the TSP, which required that the TSF ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

- FPT_SEP.1_EXP TSF domain separation, which requires that the TSF maintain a security domain for its own execution that protects it from interference and tampering by unauthorised users. The TSF must enforce separation between security domains of subjects in the TSC.

- FAU_STG.4 Prevention of audit data loss, which requires that the TSF take action if the audit trail exceeds a specified limit.

158 **O.AUDIT:** The TOE must record audit records of TOE data access and use of the TOE functions, with accurate dates and times, in a form readable by authorised administrators. O.AUDIT is addressed by:

- FAU_GEN.1 Audit data generation, which requires the ability to audit specified events.
- FAU_GEN.2 User identity association, which requires that the TSF shall associate auditable events to individual user identities.
- FPT_STM.1_EXP Reliable time stamps, which requires the ability to retrieve the date and time from a designated time source.

159 **O.SECFUN:** The TOE must provide functionality that enables authorized administrators to use the TOE security functions. O.SECFUN is addressed by:

- FAU_STG.4 Prevention of audit data loss, which requires that the TSF take action if the audit trail exceeds a specified limit.
- FMT_MOF.1Management of security function behavior, which requires the authorized administrators (roles) to manage the behavior of functions in the TSF that use rules or have specified conditions that may be manageable.
- FMT_SMF.1 Specification of management functions, which requires that the TSF provide specific management functions.
- FMT_MSA.3 Static attribute initialization, which requires the TSF enforce access control for specified default values of security attributes.
- FMT_MTD.1 Management of TSF data, which requires that only authorized administrators of the system may query network event data and can delete alert data.
- FMT_MSA.1 Management of security attributes, which requires only authorized administrators can query, modify, and delete specified security attributes.

160 **O.PARTSEP:** The TSF must maintain a domain for its own execution that protects itself and its resources from external interference or tampering. O.PARTSEP is addressed by:

- FPT_SEP.1_EXP TSF domain separation, which requires that the TSF maintain a security domain for its own execution that protects it from interference and tampering by unauthorized users. The TSF must enforce separation between security domains of subjects in the TSC.

8.3.2 Environmental Security Requirements are appropriate

161 Table 8-3 identifies which environmental SFRs satisfy the Objectives as defined in Sections 4.1.1 and 4.2.1

Objective	Security Functional Requirement(s)
O.SECSTA	FPT_SEP.1, FAU_STG.1
O.SELPRO	FPT_SEP.1, FAU_STG.1
O.AUDIT	FPT_STM.1
O.SECFUN	FAU_STG.1
O.PARTSEP	FPT_SEP.1
OE.LOWEXP	FPT_SEP.1
OE.AUDREV	FAU_SAR.1, FAU_STG.1

Table 8-3 Mapping of Objectives to environmental SFRs

162 **O.SECSTA:** Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network. O.SECSTA is addressed by:

- FPT_SEP.1 TSF domain separation, which requires that the TSF maintain a security domain for its own execution that protects it from interference and tampering by unauthorised users. The TSF must enforce separation between security domains of subjects in the TSC,

- FAU_STG.1 Protective audit trail storage, which requires that requirements are placed on the audit trail. It will be protected from unauthorized deletion and / or modification.

163 **O.SELPRO:** The TOE must protect itself against attempts by unauthorised users to bypass, deactivate, or tamper with TOE security functions. O.SELPRO is addressed by:

- FPT_SEP.1 TSF domain separation, which requires that the TSF maintain a security domain for its own execution that protects it from interference and tampering by unauthorised users. The TSF must enforce separation between security domains of subjects in the TSC,

- FAU_STG.1 Protective audit trail storage, which requires that requirements are placed on the audit trail. It will be protected from unauthorized deletion and / or modification.

164 **O.AUDIT:** The TOE must record audit records for data access and use of the TOE functions. O.AUDIT is addressed by:

- FPT_STM.1 Reliable time stamps, which requires that the TSF provide reliable time stamps for TSF functions.

165 **O.SECFUN:** The TOE must provide functionality that enables authorized administrators to use the TOE security functions. O.SECFUN is addressed by:

- FAU_STG.1 Protective audit trail storage, which requires that requirements are placed on the audit trail. It will be protected from unauthorized deletion and / or modification.

166 **O.PARTSEP:** The TSF must maintain a domain for its own execution that protects itself and its resources from external interference or tampering. O.PARTSEP is addressed by:

- FPT_SEP.1 TSF domain separation, which requires that the TSF maintain a security domain for its own execution that protects it from interference and tampering by unauthorised users. The TSF must enforce separation between security domains of subjects in the TSC.

167 **OE.LOWEXP** The threat of malicious attacks from the external network aimed at discovering exploitable vulnerabilities is considered low. OE.LOWEXP is addressed by:

- FPT_SEP.1 TSF domain separation, which requires that the TSF maintain a security domain for its own execution that protects it from interference and tampering by unauthorised users. The TSF must enforce separation between security domains of subjects in the TSC.

168 **OE.AUDREV:** The environment must provide a means to read the audit trail. OE.AUDREV is addressed by:

- FAU_STG.1 Protective audit trail storage, which requires that requirements are placed on the audit trail. It will be protected from unauthorized deletion and / or modification.

- FAU_SAR.1 Audit review, which provides the capability to read information from the audit records.

8.3.3 Security Requirement dependencies are satisfied

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FIA_UID.2	None	None
FIA_ATD.1	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2 See note below
FMT_SMR.1	FIA_UID.1	FIA_UID.2 See note below
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_ MSA.1 FMT_SMR.1.
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1. FMT_SMF.1
FMT_SMF.1	None	None
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2 See note below
FAU_SAR.1[v]	FAU_GEN.1	FAU_GEN.1
FAU_STG.1[vi]	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1

[v] FAU_SAR.1 is a security requirement for the IT environment.

[vi] FAU_STG.1 is a security requirement for the IT environment.

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FPT_RVM.1	None	None
FPT_SEP.1_EXP	None	None
FPT_STM.1[vii]	None	None
FPT_STM.1_EXP	None	None
FPT_SEP.1[viii]	None	None

Table 8-4 Mapping of TOE SFR Dependencies

169 The security functional requirements are hierarchical and may satisfy the dependency.

170 There are dependencies on FIA_UID.1. The functional component FIA_UID.2 is being used and satisfies this requirement as the components are hierarchical.

8.3.4 IT security functions satisfy SFRs

171 Mapping of Section 6 IT functions to SFRs (Section 5.1 and 5.2).

IT Function	Security Functional Requirement(s)
Identification	
I.1	FIA_UID.2, FIA_UAU.2
I.2	FIA_ATD.1
User Data Protection and Security Management	

[vii] FPT_STM.1 is a security requirement for the IT environment.
[viii] FPT_SEP.1 is a security requirement for the IT environment.

M.1	FMT_SMF.1, FMT_SMR.1
M.2	FMT_SMF.1, FMT_SMR.1
M.3	FMT_MOF.1, FMT_SMF.1, FMT_SMR.1, FMT_MSA.3, FMT_MSA.1, FMT_MTD.1, FDP_ACC.1, FDP_ACF.1
Audit	
A.1	FAU_GEN.1
A.2	FAU_GEN.1
A.3	FAU_GEN.1, FAU_GEN.2
A.4	FAU_GEN.1
A5	FAU_STG.4
Protection of TOE Security Functions	
P.1	FPT_RVM.1
P.2	FPT_SEP.1_EXP
P.3	FPT_STM.1_EXP

Table 8-5 Mapping of IT Functions to SFRs

172 Table 8-5 demonstrates that the IT security functions map to TOE Security Functional Requirements provided by the TSS. Each of the IT Security Functions maps to at least one of the TOE security functional requirements, and all the TOE Security Function Requirements are covered. Therefore, by implementing all of the IT Security Functions, all of the TOE Functional Requirements are met.

8.3.5 IT security functions mutually supportive

173 The mutually supportive nature of the IT security functions can be derived from the mutual support of the SFRs (demonstrated in Section 8.3.3), as each of the IT security functions can be mapped to one or more SFRs, as demonstrated in Table 8-5.

8.3.6 Strength of Function claims are appropriate

174 The SOF claim made by the TOE is SOF-basic.

175 The Security Function Requirement FIA_UAU.2 is subject to strength of function analysis for the authentication mechanism using passwords. This SFR is provided by security functions I.1 and I.2, see Section 6.1.1, and is consistent with the claims made in Section 5.4.

176 Products such as the Symantec LiveState Delivery are intended to be used in a variety of environments and used to connect networks with different levels of trust in the users. A number of deployments are possible. The Strength of Function of SOF-basic for the TOE will be appropriate to a number of deployments, in both government and other organisations.

8.3.7 Explicit Requirements Rationale

177 The explicit requirement FPT_SEP.1_EXP has been added as the TOE is software only and can not fully meet the requirements as written of FPT_SEP.1 that requires the TOE and not its environment to protect itself from external interference and tampering.

178 FPT_SEP.1_EXP ensures that the TOE works in context with the hardware environment to aid in enforcing domain separation.

179 The explicit requirement FPT_STM.1_EXP has been added as the TOE is software only and retrieves the time from the Configuration Server's operating system.

8.3.8 Justification of Assurance Requirements

180 EAL2 is defined in the CC as "structurally tested".

181 Products such as the Symantec LiveState Delivery are intended to be used in a variety of low threat environments, and used to distribute policies and operating systems with different levels of trust in the users. A number of deployments are possible. The EAL2 assurance level will be appropriate to a number of deployments, in both government and other organisations, where the overall threat is considered low. The assumptions A.LOWEXP and A.ONENET are indicative of a low threat environment and hence EAL2 is suitable.

8.3.9 Assurance measures satisfy assurance requirements

182 Assurance measures in the form of deliverables will be produced to meet EAL2 assurance requirements.

183 Table 8-6, below, provides a tracing of the Assurance Measures to the assurance requirements that they meet. From the table it can be seen that all assurance requirements trace to at least one assurance measure.

184 The assurance requirements identified in the table are those required to meet the CC assurance level EAL2. As all assurance requirements are traced to at least one of the assurance measures, the identified assurance measures are sufficient to meet the assurance requirements. It is also asserted that the assurance measures have been produced with EAL2, in mind and as a consequence contains sufficient information to meet the assurance requirements of the TOE.

Assurance Measures	Assurance Requirements Met by Assurance Measure	
The implementation and documentation of procedures for the development of the TOE. Included in the procedures document, the "Configuration Management Document for Symantec LiveState Delivery Version 6.0.1", are: • The use of an automated configuration management system to support the secure development of the TOE, with user restrictions. • Procedures for authorising changes and implementing changes. The configuration items are detailed within the "Configuration List for Symantec LiveState Delivery Version 6.0.1".	ACM_CAP.2	Configuration items
The implementation and documentation of procedures for delivering the TOE to a customer in a secure manner are detailed in "Configuration Management and Delivery Procedures for Symantec LiveState Delivery Version 6.0.1".	ADO_DEL.1	Delivery Procedures

Assurance Measures	Assurance Requirements Met by Assurance Measure	
Documentation provided to the customers instructing the customer how to install and configure the TOE in a secure manner. This combines the "Symantec LiveState Delivery Version 6.0 Implementation Guide" and the "Release notes for The Certified Symantec LiveState Delivery Version 6.0.1".	ADO_IGS.1	Installation, generation and start-up procedures
"Functional Specification for the Symantec LiveState Delivery 6.0.1" describing the TSF and the TOE's external interfaces.	ADV_FSP.1	Informal Functional Specification
"High-Level Design for the Symantec LiveState Delivery 6.0.1" providing descriptions of the TSF structure in the form of subsystems and the functionality of each subsystem.	ADV_HLD.1	Descriptive high-level design
The documentation of the correspondence between all the TSF representations in specifically provided deliverables is detailed in the "Correspondence Representation for Symantec LiveState Delivery Version 6.0".	ADV_RCR.1	Informal correspondence demonstration
Documentation provided to the customers instructing the customer how to configure the TOE in a secure manner. This combines the "Symantec LiveState Delivery Reference Guide", the "Symantec LiveState Delivery Migration Guide" and the" Release notes for The Certified Symantec LiveState Delivery Version 6.0.1".	AGD_ADM.1	Administrator guidance

Assurance Measures	Assurance Requirements Met by Assurance Measure	
No specific user documentation is relevant as there are no non-administrative users.	AGD_USR.1	User guidance
Documented correspondence between the security functions and tests is detailed in “Symantec LiveState Delivery 6.0.1 QA Test Plan for Common Criteria Certification”.	ATE_COV.1	Evidence of coverage
The implementation and documentation of the test procedures including expected and actual results is detailed in “Symantec LiveState Delivery 6.0.1 QA Test Plan for Common Criteria Certification”.	ATE_FUN.1	Functional testing
The TOE was provided to the evaluators.	ATE_IND.2	Independent testing
The documentation for the Strength of Function Assessment is the “Strength of Function Analysis for Symantec LiveState Delivery Version 6.0.1”.	AVA_SOF.1	Strength of TOE security function evaluation
Vulnerability Assessment of the TOE and it's deliverables is performed and documented to ensure that identified security flaws are countered. It is documented in the “Vulnerability Analysis for Symantec LiveState Delivery Version 6.0”.	AVA_VLA.1	Developer vulnerability analysis

Table 8-6 Mapping of Assurance Measures to Assurance Requirements