Commercial In Confidence

Oullim Information Technology, Inc.
ActiveTSM V3.0

Security Target
Version 1.8

Update date: June 03, 2006

< Contents >

Commercial In Confidence

Commercial In Confidence

< List of Figure >

< List of Table >

Commercial In Confidence

1 Security Target Introduction

Chapter 1 provides identification information and overview of Security Target (ST). This ST document also describes product type, TOE scope and boundaries in Chapter 2, threats and assumptions of TOE in Chapter 3, Security Objectives and requirements in Chapters 4 and 5, security functions for TOE requirements in Chapter 6, and the Rationale in Chapter 7.

1.1 ST and TOE Identification

Section 1.1 provides the information necessary for identification and control of this ST and the Target of Evaluation (TOE) - ActiveTSM V3.0.

ST Title:	Oullim Information Technology, Inc. ActiveTSM V3.0 Security Target Version 1.8
ST Version	V1.8
ST Specification prepared on:	July 3, 2006
Authors	Oullim Information Technology, Inc. Lee, Su-Yeon
TOE Identification	ActiveTSM V3.0
CC Identification:	Common Criteria for Information Technology Security Evaluation V2.3 (MIC Notice No. 2005-25)
PP Identification	None
Evaluation Assurance Level	EAL4
ST Evaluation	Korea Information Security Agency (KISA)
Keywords	Security Management, Identification and Authentication, Intrusion Detection System(IDS), Firewall, Intrusion Prevention System(IPS), Access Control

Commercial In Confidence

1.2 Conventions, Terminology, and Acronyms

This section identifies the formatting conventions used to convey additional information and terminology having specific meaning. It also defines the meanings of abbreviations and acronyms used throughout the remainder of the document.

1.2.1 Conventions

This section describes the conventions used to denote CC operations on security requirements and to distinguish test with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, iteration

- Refinement

Refinements are added to requirements of CC to further restrict the requirements. Results of refinement operations are expressed in **bold letters.**

- Selection

Selection is used to select one or more options provided in CC when describing requirements. Result of a selection is expressed in *underlined italic*.

- Assignment

Assignment is used to assign a specific value to a parameter unspecified in CC. (e.g. password length). Result of an assignment operation is expressed in large parenthesis, i.e. [assigned_value].

- Iteration

Iteration is used when a component is repeated in an operation. Result of an iteration is expressed as the number of iterations in parentheses behind the component identifier, i.e. (iteration frequency).

'Application Note' is provided to clarify meaning of requirements; to provide information on options during implementation; and to define 'sat/unsat' criteria for requirements. Application Note is provided together with relevant requirements as needed.

1.2.2 Terminology

The following terms include terms defined in CC 1.3 that help understanding of this ST Specification and those terms used by the ST authors.

Commercial In Confidence

Audit Trail – The set of disk records that record users that access the system and their actions.

Audit Record – Audit data that is kept to record TOE security related events.

Object – An entity within the TSC that contains or receives information and upon which subjects perform operations.

Attack potential – The perceived potential for a successful attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.

Strength of Function (SOF) – A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.

SOF-medium – A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

Enterprise Security Management – The system used to collect data on user activities of control subject assets, analyze the data and use it to conduct integrated control, operation and management based on a consistent set of policies at the enterprise level to maximize efficiency of security management and the security level.

Enterprise Security Management Agent System – A system that is a subject of TOE security control.

Security Target (ST) – A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Security attribute - Characteristics of subjects, users, objects, information, and/or resources that are used for the enforcement of the TSP(TOE Security Policy).

Security Device Log – An audit log that records security related events that occur in an enterprise security management agent system of TOE.

Security Device Data – Data including the status information of TOE enterprise security management agent system including their CPU, memory capacity and network traffic; and the packet information that is blocked or allowed at devices such as a firewall.

Distributed System – A system that is distributed physically over several computers and executed logically as a single program.

Human User – Any person who interacts with 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.

Identity – A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Role – A predefined set of rules establishing the allowed interactions between a user and the TOE. (e.g. User, Administrator)

Operation – Actions to enable a component to counter a specific threat or to satisfy a specific security policy specification in the CC. (e.g. Iteration, Selection, Refinement, Assignment)

Threat Agent – An unauthorized user or external IT entity that causes threats such as unauthorized access, editing or deletion on an information asset.

External IT Entity - any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Authorized Administrator – TOE administrators include the Top Level Admin, Control Admin and Monitoring Admin depending on levels of authority. Unless otherwise stated, the Authorized Admin used in this ST specification refers to the Top Level Admin. Lower level Admin users are configured by the Top Level Admin and any Authorized Admin is not allowed to perform any control functions besides the permitted privileges.

- Top Level Admin: The Authorized Admin with all privileges
- Management Admin: Authorized Admin with all privileges except addition, deletion and editing of Admin ID; and deletion of audit logs.
- Monitoring Admin: Authorized Admin who is permitted to perform event monitoring and system monitoring functions only.

Authentication Data - information used to verify the claimed identity of a user.

Java Virtual Machine (Java VM) – Software that functions as a virtual CPU for executing Java compiled class files in a CPU.

Assets - information or resources to be protected by the countermeasures of a TOE.

Information Protection System Common Criteria – Refers to the common criteria announced in MIC Notice of May 21, 2005. This CC is a Koreanized version of CC v. 2.3, which has been developed internationally based on common language and understanding to accommodate various criteria existing in different countries of the world.

Organizational Security Policies - One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

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.

Subject - an entity within the TSC that causes operations to be performed.

Abstract machine – An abstract machine could be a hardware or firmware platform or a combination of hardware and software that is known or evaluated to operate as a virtual machine. An abstract virtual machine used in this functional package could be an operating system if the TOE is an application software and a firmware or hardware in case the TOE is an operating system.

Intrusion Detection System (IDS) – A system that collects and analyzes user activities of assets under protection to detect real-time illegal events and takes countermeasures to protect the system based on analysis results.

Intrusion Prevention System (IPS) – A system that detects illegal intrusion attempts or worms on a network and blocks such detected traffic.

Firewall – A system that blocks unauthorized access by controlling service requests on a network.

Target of Evaluation (TOE) - an IT product or system and its associated guidance documentation that is the subject of an evaluation.

Evaluation Assurance Level (EAL) - a package consisting of assurance components from CC Part 3 that represents a point on the CC predefined assurance scale.

TOE Security Function (TSF) – a set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy(TSP) – a set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Data – data created by and for the TOE, that might affect the operation of the TOE.

TSF Scope of Control (TSC) – the set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

Remote Method Invocation (RMI) – Technique that forms the base of Java distributed system.

Commercial In Confidence

1.3 Security Target Overview

This ST document defines TOE threats, assumptions, organizational security policy and security requirements; and describes Security Objectives, security functional requirements and assurance requirements.

This ST specification provides the Rationale on the proposed Security Objectives and requirements.

The TOE described in this ST specification has the following architecture.

- **ActiveTSM V3.0** – Enterprise Security Management Agent System

The TOE is a software based product that is installed on a Java VM environment (multi-platform support) to provide security management functions. TOE is a security product that performs effective centralized security control of security products such as Firewalls or VPN.

1.4 Common Criteria Compliance

This ST specification is in compliance of following evaluation criteria:

- Common Criteria (MIC Notice No. 2005-25)
- CC V2.3 Part 2 compliant
- CC V2.3 Part 3 compliant
- Evaluation Assurance Level 4 (EAL4) compliant

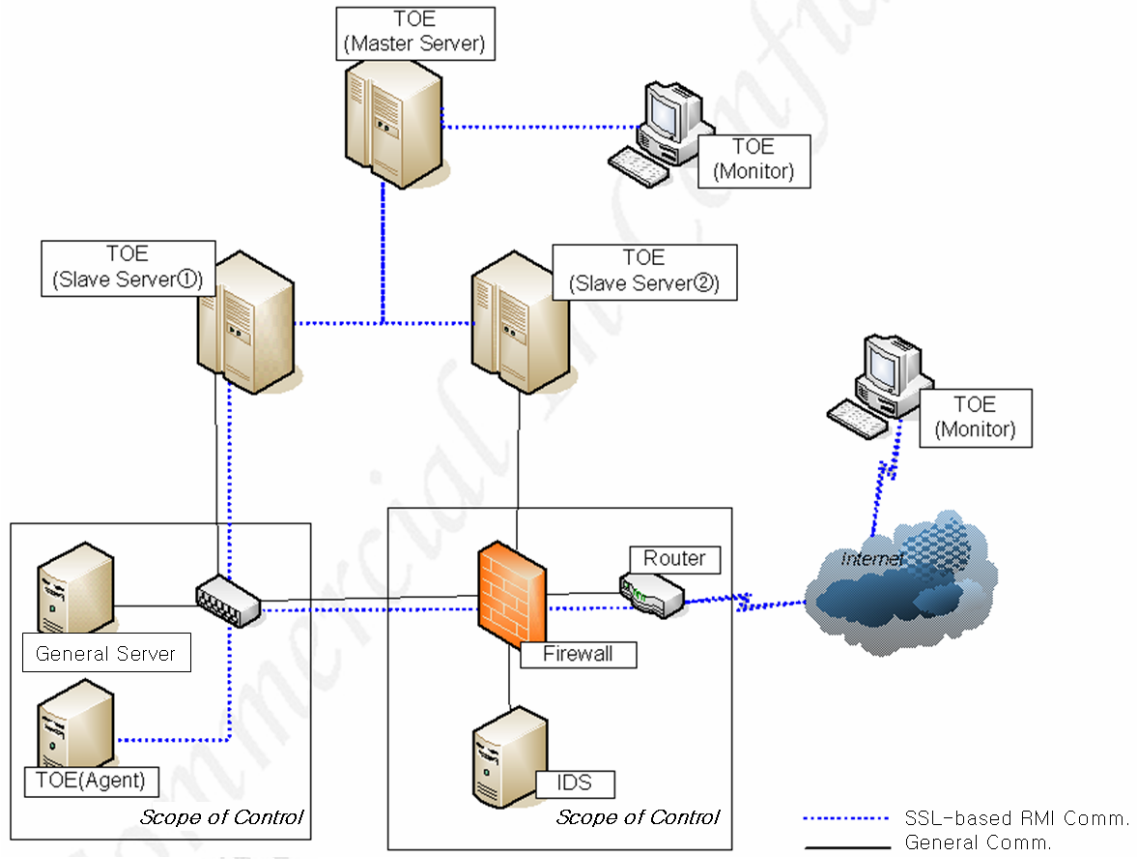
Commercial In Confidence

2 TOE Description

This chapter provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

TOE satisfies EAL4 grade of the assurance requirements of CC V2.3 Part 3.

2.1 Product Type



[Figure 2-1] General TOE Network Architecture

TOE is installed for operation at locations of connection with enterprise security management agent system of an internal network as in Figure 2-1. Enterprise security management agent systems of TOE include Intrusion Detection System (IDS), Firewall, Intrusion Protection System (IPS), general servers and network devices (such as routers).

TOE is an integrated security management system that collects/analyzes user activities of enterprise security management agent system; performs integrated control, operation and management of said systems at the enterprise level based on a consistent set of policies towards maximizing the efficiency of security control activities and the security level. Detailed functions of integrated security management provided by TOE are as follows:

- Event Monitoring
- System Performance Monitoring

- Map Monitoring
- Correlation Analysis Monitoring

TOE (Slave Server) collects and stores data (security equipment logs and security equipment information) of enterprise security management agent system (IT entities) that are within the scope of control.

Methods of information collection consist of direct collection method from enterprise security management agent system via standard interfaces such as SNMP(RFC 1157, 1901) and Syslog (RFC 3195); and the indirect method where a TOE (Agent) is installed on enterprise security management agent system so that said Agent delivers the data via API. In case TOE (Agent) sends data to TOE (Slave Server), SSL-based RMI communication is used.

TOE users include IT entities and Authorized Administrators, which include Top Level Admin, Management Admin and Monitoring Admin. Unless stated otherwise, an Authorized Admin refers to the Top Level Admin with all privileges and the roles of Management Admin or Monitoring Admin are stated where necessary.

Authorized Admin performs security Admin functions using TOE (Monitor), which can be used within the internal network where enterprise security management agent systems reside or from an external network. Configured security Admin functions are sent to TOE (Master Server), which requests information when needed to TOE (Slave Server). Communication between TOE (Monitor) and TOE (Master) is done via SSL-based RMI communication.

TOE(Master Server) and TOE(Slave Server) may be installed on the same system or in separate systems. For separate installation, TOE (Master) can be connected to multiple TOEs (Slave Servers) for security functions. A TOE (Slave) also collects information from multiple enterprise security management agent systems. Therefore, the security function performance of TOE can be done in a tree structure. Communication between TOE (Master) and TOE (Slave) is via SSL-based communication.

TOE controls data sent from outside of TOE based on the security policy. TOE enforces access control policy and data receive security policy on security control target systems.

TOE communication between TOE(Monitor) and TOE(Master Server), TOE(Slave Server), or TOE(Agent) is done via SSL-based RMI communication.

Commercial In Confidence

2.1.2 TOE Environment

2.1.2.1 IT Environment

TOE IT environment includes DBMS (Oracle), character message server and mail server. TOE uses DBMS to manage TOE's security attributes, TSF data, user data and audit data. TOE sends information on management countermeasure activities or correlation analysis to the Admin e-mail via e-mail server. It uses a character message server to send correlation analysis information as a character message.

2.1.2.2 Operational Environment

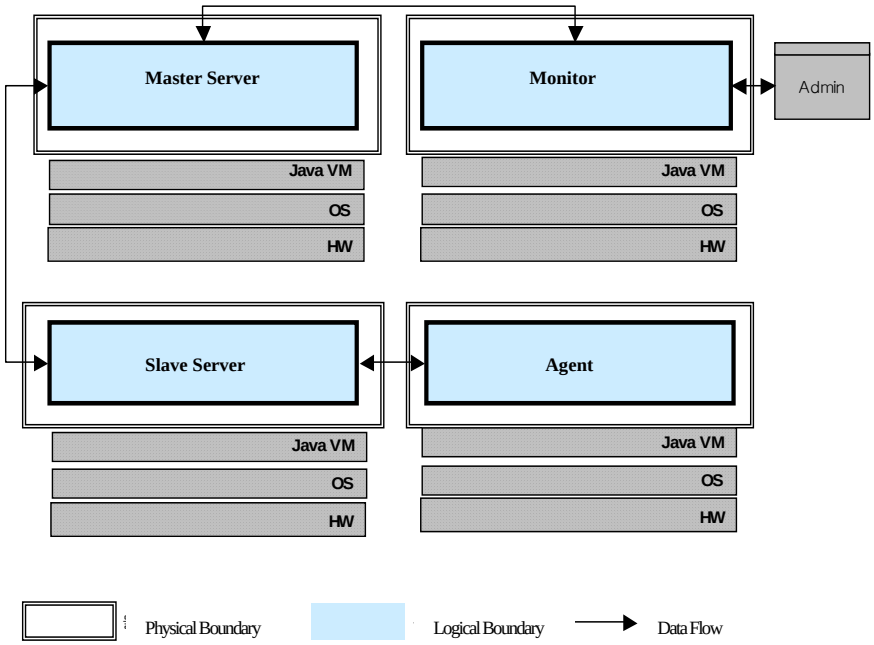
TOE is installed in an internal network that is connected to enterprise security management agent system and is used in an environment which may include threat sources of low knowledge level. Attackers of low level professional knowledge can easily acquire information on exploitable vulnerability and attack tools from Internet, use them to damage or acquire targeted assets. TOE can be used by the Admin to identify such attacks of low level threat sources against enterprise security management agent systems.

Commercial In Confidence

2.2 Product Components

TOE has a four-tier architecture consisting of Master, Slave, Monitor and Agent (installed on Firewall, IPS or IDS). Components of TOE for security functions are as follows:

Master Server
Slave Server
Monitor
Agent



[Figure 2-2] TOE Logical Architecture Diagram

Admin ID and authentication process is required to allow only Authorized Admin to access a monitor to request information to the Master. Information exchanged between access channels is safeguarded via SSL-based RMI communication.

Monitor can be used to send requests for information stored in Master or in Slave through Master; and sending commands to the Master to implement a policy. Master functions include Management Activity Retrieve, Event Monitoring, System Performance Info Monitoring, Account Monitoring, Event Rule Configuration Retrieve, Audit data Retrieve, Security Log Search, Report Generation, and Code Retrieve. Management Activity Retrieve allows viewing of events for special control. Event Monitoring shows events defined from the Master. System Performance Info Monitoring receives performance info from the Master and displays it. Account Monitoring receives account data from Master and displays it. Event Rule Configuration Retrieve receives filtering, leveling, compression, and correlation analysis rules from the Master and displays them. Audit data Retrieve receives audit data from the Master and displays them. Security Log Search receives logs of intrusion detection, intrusion blocking, control target severs, accounts and correlation analysis from the Master and displays them. Report Generation receives report info from the Master and displays it. Code

Retrieve receives code info from the Master and displays it.

The Master component is responsible for processing requests from the Monitor. Most information configured at a Monitor is stored through the Master, which calls the Slave to perform security management functions requested from Monitor. Functions of the Master include Management Activity Management, Event Log Transfer, System Performance Info Transfer, Account Log Transfer, Event Rule Configuration Management, Audit data Transfer, Report Generation and Code Management. Management Activity Management stores/edits/retrieves management activity information in DB. Event Log Transfer applies event rules on events collected from Slave and sends them to Monitor. System Performance Info Transfer sends collected account log from Slave to Monitor. Event Rule Configuration Management stores/edits/retrieves event rules received from Monitor to DB. Audit data Management stores/edits/retrieves audit data that occur at Monitor or the system. Security Log Transfer sends security log data from Slave to Master. Report Generation receives basic data for report generation from DB and sends it to Monitor. Code Management stores/edits/retrieves code information from Monitor to DB.

The Slave component is responsible for storage and management of information sent from Agent. Also, when the Master sends a request for security equipment log, Slave retrieves this log from DB and delivers it to the Master. Slave functions include Event Log Collect, System Performance Info Collect, Account Log Collect and Security Log Search. Event Log Collect collects event related info from log info received from Agent. System Performance Info Collect collects performance related info from log data received from Agent. Account Log Collect collects account info from log data received from Agent. Security Log Search performs searches of security log data of Agent based on requests from the Master.

The Agent component collects log data of enterprise security management agent system and system performance info and delivers them to Slave. Agent functions include Log Collect and Log Transfer. Log Collect and Log Transfer perform collection of log data from equipment where Agents are installed and transfers the data to Slave at the same time.

Commercial In Confidence

2.3 Scope and Boundaries of the Evaluated configuration

This section provides a general description of the physical and logical scope and boundaries of the TOE.

2.3.1 Physical Scope and Boundaries

TOE consists of software components and its physical scope refers to software installed on OS. Table 2-1 shows the hardware system specification and operating environment where TOE is to be installed. Software environment is categorized based on whether the Master and Slave servers are installed on the same system (integrated system environment) or on different systems (distributed system environment).

[Table 2-1] Software

Components (Softwate)		**Environment**	
		Hardware	**Operating Environment**
Distributed System Environment	**Master Server**	CPU – 1Ghz or more Memory - 1Gbyte or more Ethernet Card – 1 ea or more HDD - 20GB or more	Sun Solaris 9 for Sparc Java(v. 1.4.2_10) VM Environment DBMS – Oracle 9i(v. 9.2.0.8)
	Slave Server	CPU – 1Ghz or more Memory - 1Gbyte or more Ethernet Card – 1 ea or more HDD - 40GB or more	Sun Solaris 9 for Sparc Java(v. 1.4.2_10) VM Environment Syslog, SNMP support DBMS – Oracle 9i(v. 9.2.0.8)
Integrated System Environment	**Master /Slave Server**	CPU – 1.5Ghz * 2 ea or more Memory - 4 Gbyte or more Ethernet Card – 1 ea or more HDD - 73GB * 4 ea or more	Sun Solaris 9 for Sparc Java(v. 1.4.2_10) VM Environment Syslog, SNMP support DBMS – Oracle 9i(v. 9.2.0.8)
Monitor		CPU – 1Ghz or more Memory - 1Gbyte or more Ethernet Card – 1 ea or more HDD – 100MB or more	Windows2000 (Service Pack 4) or WindowsXP (Service Pack 2) Java(v. 1.4.2_10) VM Environment
Agent		CPU – 300Mhz or more Memory – 128Mbyte or more Ethernet Card – 1 ea or more HDD – 100MB or more	Sun Solaris 9 for Sparc Java(v. 1.4.2_10) VM Environment

ActiveTSM V3.0 consists of the above four products. Master Server, Slave Server and Agent are installed on Sun Solaris 9 for Sparc, where Java VM environment is supported, for operation. Monitor for managing the Master server is installed either in Windows 2000 or Windows XP for operation. Oracle DBMS is outside of the TOE and is hence excluded from evaluation.

2.3.2 Logical Scope and Boundaries

2.3.2.1 TOE Security Functions (TSF)

TOE provides the following security functions as a whole.

Security Management – TOE permits only Authorized Admin to manage and operate the access control policy. This function uses coded communication channel using SSL-based RMI.. Also, only Authorized Admin can perform retrieval and configuration management including Event Monitoring, System Performance Monitoring, Map Monitoring, Security Policy Configuration, Enterprise Security Management Agent Systems Log Analysis, TOE related data such as countermeasures, Security Attributes and Authentication Data.

Security Audit – TOE permits only the Authorized Admin to perform retrieval of audit data. Significant TOE security events are time stamped and stored in a storage in time sequence. Stored audit data can be categorized and retrieved for various conditions.

Protection of User Data – TOE performs user data protection function through Security Management Access Control Policy and Enterprise Security Management Agent System Data Receive Security Policy. TOE performs access control on data sent from IT entities of Authorized Admin. Also, TOE enforces access control policy on data sent to TOE from external IT entities.

Identification and Authentication – TOE performs ID and authentication to ensure that only authorized external IT entities and Authorized Admin have access to TOE. TOE provides general password function as an authentication mechanism for Authorized Admin. TOE forms a safe data channel using SSL-based RMI to ensure safety of Admin authentication data sent from the Admin main console.

Protection of Security Functions - TOE conducts periodic security check on whether security functions are being performed normally. In case of an abnormality, the relevant function is re-executed. TOE performs integrity test of TOE data and execution program to ensure safety of TOE data and functions. TOE demon status is checked periodically and stopped demons are re-executed.

Commercial In Confidence

2.3.2.2 Out of Scope

Functions outside of TOE scope are as follows:

a) Data management via DBMS(Database Management System) Oracle 9i

b) Java provided RMI communication

Commercial In Confidence

3 TOE Security Environments

TOE Security Environment consists of assumptions, which describe security requirements; threats that can be targeted against TOE assets or environment by threat sources; and the organizational security policy, which consists of rules, procedures and practices that TOE is required to comply.

3.1 Assumptions

The following shows assumptions that must be implemented or maintained in the operating environment of TOE.

[Table 3-1] Assumptions

Name	Description
A.DYNAMIC	TOE shall be managed to appropriately handle dynamic variations of enterprise security management agent system.
A.PHYSEC	TOE shall be located in physically safe environment where only authorized users have access.
A.TADMIN	TOE's Authorized Admin shall have no malice, be trained on TOE Admin functions, and perform his/her duties in accordance with the Admin guideline.
A.REINFOCEOS	OS services and tools that are not needed by TOE shall be removed and OS weaknesses shall be augmented to ensure reliability and safety of OS.
A.REINFOCEOE	Weaknesses of Java VM environment shall be augmented to ensure its reliability and safety.
A.ACCESS	Slave and Agent, components of TOE, shall have access to all enterprise security management agent systems for security management purposes.
A.DBINSTLIMIT	DBMS for TOE data management shall be installed in the same system where TOE is installed to ensure reliability and safety of the DB access.
A.TEXTSERVER	Reliability and safety of the following servers, which reside outside of TOE in support of TOE functions, shall be ensured. - SMTP server for sending mails to admin. - SMS server for sending character messages to admin.

Commercial In Confidence

3.2 Threats

The following threats are categorized as those against TOE and those against the environment. Assets for protection by TOE are computer resources that the organization operates. Threat sources have low level of professional knowledge, resources and motives.

3.2.1 Threats Against TOE

This section addresses threats against TOE. The following threats are derived by either TOE or the operating environment. Sources of such threats are unauthorized users without TOE privileges or external IT entities.

[Table 3-2] Threats against TOE

Name	Description
T.DISGUISE	An external attacker can get an authentication data and use it to disguise as an Authorized Admin to access TOE and to damage TSF data.
T.RECFAIL	Storage capacity can be depleted by a threat source to disable security event logging. Depletion of TOE storage refers to use of a normal method to change TSF data or to generate audit data to be stored in audit data DB.
T.WRONGINFO	An external threat source can bring in unauthorized information from an external IT entity to cause damage to security equipment log or security equipment within TOE.
T.REPEAT	An external attacker can make continual authentication attempts to find out authentication data, then access the TOE and damage TSF data.
T.CHGTSFD	An external threat source can expose, change or delete TSF data in unauthorized ways. External threat sources refer to external attackers that access TSF data storage using illegal methods.

The following threats are against assets under TOE protection.

[Table 3-3] Threats against Assets under TOE security protection

Name	Description
T.ABNORMALSVC	A threat source can access TOE to use a service resource of an enterprise security management agent system in excess of normal use and thus cause the enterprise security management agent system to operate abnormally.
T.ABNORMALRES	Due to System Error (external attack including worm, virus or DOS attack; system malfunction due to hardware or software error) an enterprise security management agent system's resources can be depleted and the system operates abnormally.

COMMERCIAL IN CONFIDENCE

3.2.2 Threats against Operating Environment

The following are threats against the TOE operating environment.

[Table 3-4] Threats against TOE Operating Environment

Name	Description
TE.WEAKMGT	An Authorized Admin can configure, manage or use the TOE in an unsafe manner.
TE.DELNINST	TOE security can be damaged by an external threat source during distribution or installation process. An external threat source refers to an unauthorized person who attempts to change, damage or erroneously install TOE during the TOE distribution process.
TE.CHGTSFD	TSF data sent by TOE can be exposed, changed or deleted by an external threat source in unauthorized ways.

3.3 Organization Security Policy

An organization that operates the TOE implemented in accordance with this ST Specification shall have its own security policy and the Authorized Admin utilizes the TOE to implement such security policy.

The following organizational security policy shall be applicable to TOE operating environment.

[Table 3-5] Security Policy

Name	Description
P.AUDIT	Security events shall be recorded and maintained to enable accountability tracking of all security related actions, and the recorded data shall be reviewed.
P.SECMGT	Authorized Admin shall manage the TOE using safe methods.
P.STAT	Authorized Admin should be able to perform statistical processing of audit data and data from integrated security management.

Commercial In Confidence

4 Security Objectives

Security objectives are categorized into those for TOE and those for the environment. TOE security objectives are those addressed by the TOE directly while those for the environment are those addressed by IT areas or non-technical/procedural means.

4.1 TOE Security Objectives

This section lists the security objectives for the TOE.

[Table 4-1] TOE Security Objectives

Name	Description
O.AUDIT	TOE shall record and maintain security related events to enable accountability tracking of security related actions. TOE shall also provide the means to review recorded security related data.
O.MANAGE	TOE shall provide the management tools to enable Authorized Admin to efficiently manage the TOE in safe ways.
O.ID	TOE shall identify all external IT entities that are under TOE's access control and all users that attempt to access TOE.
O.AUTH	TOE shall authenticate Admin ID after its identification prior to granting access to TOE. Application Note: It is possible for a threat source to make repeated attempts for authentication using an Admin ID. To block such repeated authentication attempts, a proper authentication mechanism shall be implemented as suitable to the desired security strength level.
O.COLLECTINFO	TOE shall collect data generated from activities of enterprise security management agent systems.
O.ACCESS	TOE shall control the TOE access of external users based on the security policy.
O.ABNORMALOP	TOE shall perform appropriate countermeasures based on analysis result of collected information to ensure normal operation enterprise security management agent systems.
O.SECTSFD	TOE shall protect TSF data stored within TOE from any unauthorized exposure, editing and deletion attempts.
O.STAT	TOE shall provide the Authorized Admin the statistical processing capability of audit data and data generated from integrated security management.

Commercial in Confidence

4.2 Security Objectives for the Environment

Security objectives for the environment are addressed or resolved through assumptions and the organization's security policy. The following are security objectives for the environment.

[Table 4-2] Security Objectives for the Environment

Name	Description
OE.DYNAMIC	TOE shall be managed to appropriately handle dynamic variations of enterprise security management agent systems.
OE.PHYSEC	TOE shall be located in physically safe environment where only authorized users have access.
OE.TADMIN	TOE's Authorized Admin shall have no malice, be trained on TOE Admin functions, and perform his/her duties in accordance with the Admin guideline.
OE.SECMGT	TOE shall be distributed and installed in safe ways and be safely configured, managed and used by Authorized Admin.
OE.REINFORCEOS	OS services and tools that are not needed by TOE shall be removed and OS weaknesses shall be augmented to ensure reliability and safety of OS.
OE.REINFORCEOE	Weaknesses of Java VM environment shall be augmented to ensure its reliability and safety.
OE.ACCESS	TOE shall allow access to enterprise security management agent system defined as the security control scope by the security policy for normal security management activities.
OE.DBINSTLIMIT	DBMS for TOE data management shall be installed in the same system where TOE is installed to ensure reliability and safety of the DB access.
OE.SECCH	TOE shall send or receive TSF data through safe channels for communication between physically separated TOEs, or between external IT entities and the admin.
OE.SECTSF	The operating system where TOE is installed shall periodically verify the TOE status to ensure safe operation of TSF.
OE.EXTSERVER	Reliability and safety of the following servers, which reside outside of TOE in support of TOE functions, shall be ensured. - SMTP server for sending mails to admin. - SMS server for sending character messages to admin.

Commercial In Confidence

5 IT Security Requirements

This chapter presents security functional requirements and assurance requirements of TOE. These requirements consist of the security functional components in Part 2 of CC (v. 2.3) and the assurance components of Part 3 (Assurance Grade). CC is categorized into the following two categories.

- TOE Security Functional Requirements: Provide security functions including Security Violation Analysis, Security Violation Countermeasure, Security Management, Audit data and Identification & Authentication.

- TOE Security Assurance Requirements: Provide a reliable basis of verifying if TOE satisfies security objectives.

.

5.1 TOE Security Functional Requirements

This section presents security functional requirements (SFR) of TOE, which are explained in the following two parts.

- Security Functional Requirements (SFRs): SFRs are defined using those components selected from Part 2 of CC to satisfy security objectives identified in the previous chapter.

- SFRs with Strength of Function (SOF): SOFs used in this ST are described in 5.1.2.

Commercial In Confidence

5.1.1 Security Functional Requirements (SFRs)

SFRs listed in Table 5-1 are names of SFR components used in this ST Specification. They have been quoted from Part 2 of CC. Those with incomplete operations have been completed by the author of this ST Specification.

[Table 5-1] Security Functional Requirements (SFRs)

Security Functional Class	Functional Component ID	Functional Component
Security Audit Class	FAU_ARP.1	Security alarm
	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Select audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
User Data Protection Class	FDP_ACC.1(1)	Subset access control(1)
	FDP_ACF.1(1)	Security attribute based access control (1)
	FDP_ACC.1(2)	Subset access control(2)
	FDP_ACF.1(2)	Security attribute based access control (2)
	FDP_ITC.1	Import of user data without security attributes
Identification & Authentication Class	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1(1)	User attribute definition (1)
	FIA_ATD.1(2)	User attribute definition (2)
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2(1)	User identification before any action (1)
	FIA_UID.2(2)	User identification before any action (2)
Security Management Class	FMT_MOF.1	Management security function action
	FMT_MSA.1	Management of security attribute
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1(1)	Management of TSF data (1)
	FMT_MTD.1(2)	Management of TSF data (2)
	FMT_MTD.1(3)	Management of TSF data (3)
	FMT_MTD.1(4)	Management of TSF data (4)
	FMT_MTD.2(1)	Management limits on TSF data (1)
	FMT_MTD.2(2)	Management limits on TSF data (2)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TOE Security Functional Class	FPT_TST.1	TSF Testing
	FPT_STM.1	Security alarm

Commercial in Confidence

FAU_ARP.1 Security alarm

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take the following actions upon detection of a potential security violation;

a) Authentication Failure: TERMINATE relevant Admin account.
b) Correlation analysis trigged by configured value for correlation analysis: An action configured by Authorized Admin.

FAU_GEN.1 Audit data generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamp

FAU_GEN.1.1 The TSF shall be able to generate an audit data of the following auditable events:

a) Start-up and shutdown of the audit functions

b) All auditable events for *minimal or basic* level of audit specified in Table 5-4

c) [Refer to [Table 5-3] Audit Target Event]

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

a) Event Date/Time , Event Type, Entity ID, Event Result (Success or Failure)

b) For each audit target event defined in functional components of ST Specification, record the following info. [Refer to [Table 5-2] and [Table 5-3] Audit Target Events]

- Object ID (Admin ID, Master, Slave, Enterprise Security Management Agent Systems)
- Event Significance (ERROR, WARNING, NOTICE, MANAGE)
- Sequence No.
- Event Detail

Commercial In Confidence

[Table 5-2] Minimum Audit Target Events

Component ID	Minimum Audit Target Events	Additional audit info
FAU_ARP.1	Action caused by an urgent security violation	-
FAU_SAA.1	Automated action due to Action Start, Action Stop or Tool of analysis mechanism.	Authorized Admin ID (Admin ID)
FDP_ACF.1	Successful request for an operation on an object handled by SFP.	Entity & Object Identification Info
FDP_ITC.1	Successful entry of user data including Security Attributes	-
FIA_AFL.1	Reaching the limit of authentication failures and subsequent actions taken and subsequent return to normal condition, as necessary.	Unauthorized Users and Authorized Admin Identification
FIA_UAU.2	Failed use of Authentication mechanism	User ID provided to TOE (User ID)
FIA_UID.2	Failed use of Admin ID mechanism including Admin ID provided.	User ID provided to TOE (User ID)
FMT_SMF.1	Use of a Management Function	Authorized Admin ID (Admin ID)
FMT_SMR.1	Change in user groups that share roles	Authorized Admin ID (Admin ID)
FPT_STM.1	Time change	Authorized Admin ID (Admin ID)

[Table 5-3] Additional Audit Target Event

Component ID	Additional Audit Target Event	Additional audit info
FAU_STG.3	Alarm for audit data storage space shortage	-
FIA_UAU.2	Authentication Success	Authorized Admin ID (Admin ID)
FMT_MSA.1	All changes of Security Attribute values	Security AttributeValue
FMT_MSA.3	Change in basic configuration on authorization rules or limiting rules. All changes to initial values of security attributes.	Security Attribute Value
FMT_MTD.1	All changes to TSF Data	Changed TSF Data Value
FMT_MTD.2	All changes to TSF Data limits	Changed TSF Data limit
FPT_TST.1	TSF Self Diagnose Result	
FPT_AMT.1	TOE error status	-
Other	DB HASH computation error	

Commercial in Confidence

FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) The TSF shall enforce the following rules for monitoring audited events: [Authentication Failure or Correlation Analysis trigger by Correlation Analysis Configuration Value] known to indicate a potential security violation
b) [None]

FAU_SAR.1 Audit review

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Security alarm

FAU_SAR.1.1 The TSF shall provide [an Authorized Administrator] with the capability to read [all audit trail data] from the audit data

FAU_SAR.1.2 The TSF shall provide the audit data in a manner suitable for the user to interpret the information.

Application Note: Authorized Admin refers to Top Level Admin or Management Admin.

Commercial In Confidence

FAU_SAR.3 Select audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform *searches and sorting* of audit data based on [

- Event Date/Time (Date & Time)
- Object ID
- Event Category
- Event Significance (Event Type)
- Keyword (Event Detail)

]

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall prevent the stored audit data from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to *prevent* modifications to the audit data

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [Send Notice to Authorized Admin] if the audit trail exceeds [Authorized disk space specified by Authorized Admin].

Application Note: Authorized Admin refers to Top Level Admin or Management Admin.

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall ***terminate TOE and TSF services to prevent Audit Target Events*** and [Send email to Authorized Admin] if the audit trail is full.

FDP_ACC.1(1) Subset access control(1)

Commercial In Confidence

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [Security Management Access Control Policy] on [
a) Entity List: Authenticated Admin with FIA_UAU.2 completed.
b) Object List: TOE Security Management Functional Process
c) Operation: Permitted in case of Authenticated Admin access
]

FDP_ACF.1(1) Security attribute based access control (1)

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [Security Management Access Control Policy] to objects based on the following: [
a) Entity List: Authenticated Admin with FIA_UAU.2 completed
b) Entity Security Attributes:
- Privilege(Top Level Admin, Management Admin, Monitoring Admin)

c) Object List: TOE Security Management Functional Process
d) Object Security Attributes:
- Security Management Function

]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[
- Permitted if FDP_ACF.1.1 Entity Security Attributes are normal Authentication status, and
- FDP_ACF.1.1 Entity Security Attribute Privilege is the same as Object Operation Privilege]

FDP_ACF.1.3 The TSF shall explicitly authorize 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 [None]

Commercial in Confidence

FDP_ACC.1(2) Subset access control (2)

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1The TSF shall enforce the [Enterprise Security Management Agent Systems Data Receive Security Policy] on [

a) Entity List: Unauthenticated external IT entity on the sender side
b) Object List: File that stores equipment security log of enterprise security management agent system
c) Operation: Permitted when entity IP address is registered as the asset's security IP

]

FDP_ACF.1(2) Security Attribute-based Access Control (2)

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [Enterprise Security Management Agent Systems Data Receive Security Policy] to objects based on the following: [

a) Entity List: Unauthenticated external IT entity on the sender side
b) Entity Security Attributes:
- IP address of external IT entity that sends info to TOE
- Protocol type of info sent by an external IT entity to TOE
c) Object List: File that stores equipment security log of Enterprise Security Management Agent systems
d) Object Security Attributes: File name and storage location

]

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

- FDP_ACF.1.1 Entity Security Attribute, external IT entity's IP Address is the same as the security attribute IP of the asset registered by the Authorized Admin, and
- FDP_ACF.1.1 Entity Security Attribute, protocol type is permitted by TOE.]

FDP_ACF.1.3 The TSF shall explicitly authorize 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 [None]

Application Note: Authorized Admin includes Top Level Admin and Management Admin.

Commercial In Confidence

FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialization

FDP_ITC.1.1 The TSF shall enforce the [Enterprise Security Management Agent Systems Data Receive Security Policy] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [None]

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*3*] unsuccessful authentication attempts occur related to [Admin Authentication attempts].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent authentication until a countermeasure action by Authorized Admin]

Application Note: Authorized Admin refers to the Top Level Admin.

FIA_ATD.1(1) User attribute definition (1)

Hierarchical to: No other components

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to each **IT entity:** [
a) IP Address
].

Commercial In Confidence

FIA_ATD.1(2) User attribute definition (2)

Hierarchical to: No other components

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to each **administrator**: [

a) ID
b) User Security Attributes
   - Password
   - Authentication Failure Frequency Configuration Value
   - Privilege

].

Application Note: Admin includes Top Level Admin, Management Admin and Monitoring Admin.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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

Application Note: Admin includes Top Level Admin, Management Admin and Monitoring Admin.

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [Asterisk marked Password] to the **administrator** while the authentication is in progress.

Application Note: Admin includes Top Level Admin, Management Admin and Monitoring Admin.

Commercial in Confidence

FIA_UID.2(1) User identification before any action (1)

Hierarchical to: FIA_UID.1

Dependencies: No dependencies.

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

FIA_UID.2(2) User identification before any action (2)

Hierarchical to: FIA_UID.1

Dependencies: No dependencies.

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

Application Note: Admin includes Top Level Admin, Management Admin and Monitoring Admin.

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to *disable, enable* the functions [

- Event
  - Apply Event Compression
- Correlation Analysis
  - Apply Correlation Analysis Performance Info Security Policy
  - Apply Correlation Analysis Event Security Policy
  - Apply Correlation Analysis YELLOW List
  - Apply Correlation Analysis BLACK List
  - Send Correlation Analysis Info e-mail
  - Send Correlation Analysis Info character message
- Other
  - Generate alarm sound or warning screen.
  - Send e-mail on management countermeasure

] to [an Authorized Administrator].

Application Note: Authorized Admin refers to Top Level Admin or Management Admin.

FMT_MSA.1 Management of security attribute

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [Security Management Access Control Policy, Enterprise Security Management Agent Systems Data Receive Security Policy] to restrict the ability *query, modify* the security attributes [
[Table 5-4] Security Attribute List

Security Attribute	Action	Related Security Policy
Admin Privilege	Query, Modify	Security Management Access Control Policy

] to [the Authorized Administrator].

Application Note: Authorized Admin refers to Top Level Admin or Management Admin.

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components

Dependencies: FMT_MSA.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [Security Management Access Control Policy, Enterprise Security Management Agent Systems Data Receive Security Policy] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

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

Application Note: Authorized Admin includes Top Level Admin and Management Admin.

FMT_MTD.1(1) Management of TSF data (1)

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to *query, modify, delete, [create]* the [

- Identification & Authentication Data
- Control Activity Management
- Event
  - Event Filtering Security Policy

Commercial In Confidence

- Event Leveling Security Policy

- Correlation Analysis
  - Correlation Analysis Performance Info Security Policy
  - Correlation Analysis Event Security Policy
  - Correlation Analysis YELLOW List Security Policy
  - Correlation Analysis BLACK List Security Policy
- Security Equipment Info Management
- Code Management

] to [an Authorized Administrator].

Application Note: Authorized Admin refers to Top Level Admin or Management Admin. Here, Identification & Authentication Data handling can only be performed by Top Level Admin.

FMT_MTD.1(2) Management of TSF data (2)

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to *query, modify* the [

- Event Pattern Number
- Event Pattern Initialization(Time, Interval)
- Event Screen Display Number
- TOE Time Stamp used for Audit Data accumulation
- Management Environment Configuration
- Map Management Function
- Disk reserve space
- Integrity Test frequency

] to [an Authorized Administrator].

Application Note: Authorized Admin refers to Top Level Admin or Management Admin.

FMT_MTD.1(3) Management of TSF data(3)

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to *query* the [

- Event Monitoring (IDS, Firewall, Account)
- Event Search (IDS, Firewall, Account)

Commercial In Confidence

- Performance Monitoring (CPU, Memory, Traffic)
- Correlation Analysis Monitoring
- Correlation Analysis Search
- Audit Info
  - Object History
  - System History
  - User History
  - Audit Data Retrieve
- Trend Report
  - Performance Management Trend Report
  - Event Trend Report
- Knowledge Management Info Search
- Map Node Search
- Event Pattern Monitoring

] to [an Authorized Administrator].

Application Note: Top Level Admin and Management Admin can perform this activity while Monitoring Admin is allowed only Map Node Search and various Monitoring Functions. (Monitoring Functions: Event Monitoring, Performance Monitoring and Correlation Analysis Monitoring)

FMT_MTD.1(4) Management of TSF data(4)

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to [*Statistical Processing*] the [

- Security Equipment Log
- Security Equipment Info

] to [an Authorized Administrator].

Application Note: Authorized Admin refers to Top Level Admin, Management Admin or Monitoring Admin.

Commercial In Confidence

FMT_MTD.2(1) Management limits on TSF data (1)

Hierarchical to: No other components

Dependencies: FMT_MTD.1 Management of TSF data
FMT_SMR.1 Security roles

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [Audit Storage Capacity] to [the Authorized Administrator]

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed the indicated limits: [FAU_STG.3 specified Countermeasure or FAU_STG.4 specified Countermeasure].

Application Note: Top Level Admin and Management Admin can perform this activity.

FMT_MTD.2(2) Management limits on TSF data (2)

Hierarchical to: No other components

Dependencies: FMT_MTD.1 Management of TSF data
FMT_SMR.1 Security roles

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [Integrity Test를 수행하는 Time Interval] to [the Authorized Administrator]

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed the indicated limits: [Integrity Test & Self Diagnosis].

Application Note: Top Level Admin and Management Admin can perform this task.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components

Dependencies: No dependencies.

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

a) TSF Function Management
   - Items specified in 5.1.1.1 FMT_MOF.1

b) TSF Security Attributes Management
   - Items of 5.1.1.1 FMT_MSA.1

c) TSF Data Management
   - Items of 5.1.1.1 FMT_MTD.1

d) TSF Data Limit Management
   - Items of 5.1.1.1 FMT_MTD.2

e) Security Role Management
   - Items of 5.1.1.1 FMT_SMR.1

].

FMT_SMR.1 Security roles

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [
a) Top Level Admin
b) Management Admin
c) Monitoring Admin
].

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

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components

Dependencies: No dependencies.

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

Application Note: As a way of maintaining own time stamps, TOE shall allow Authorized Admin to configure own system time stamp provided by own OS through TOE and use this system.

FPT_TST.1 TSF Testing

Hierarchical to: No other components

Dependencies: FPT_AMT.1 Abstract machine testing

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation, and upon request from an authorized user* to demonstrate the correct operation of the *TSF*.

FPT_TST.1.2 The TSF shall provide **the Authorized Administrator** with the capability to verify the integrity of *TSF data*.

FPT_TST.1.3 The TSF shall provide **the Authorized Administrator** with the capability to verify the integrity of stored TSF executable code.

Application Note: Authorized Admin includes Top Level Admin and Management Admin.

Commercial In Confidence

5.1.2 **SOF Declarations**

This ST Specification selects SOF-Medium. Thus, the ST considers threats of low level professional knowledge, resources and motives. To counter such threats TOE has to satisfy minimum SOF-basic. Since this ST Specification provides security functions whose strength level is 'medium,' said TOE satisfies the requirement.

Commercial In Confidence

5.2 TOE Security Assurance Requirements

Table 5-5 shows security assurance components of TOE. These are from the Assurance Requirements of Part 3 of CC [1] and the assurance level is EAL4.

[Table 5-5] EAL4 Assurance Requirements

Assurance Class	Assurance Component ID	Assurance Component Name
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life-cycle support activity	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

Commercial in Confidence

5.2.1 Configuration Management

ACM_AUT.1 Partial CM automation

Dependencies: ACM_CAP.3 Authorization controls

Developer action elements:

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2D The developer shall provide a CM plan.

Content and presentation of evidence elements:

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

Evaluator action elements:

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

ACM_CAP.4 Generation support and acceptance procedures

Dependencies: ALC_DVS.1 Identification of security measures

Developer action elements:

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labeled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

Commercial In Confidence

ACM_CAP.4.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.6C The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.

ACM_CAP.4.7C The CM system shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.4.8C The CM plan shall describe how the CM system is used.

ACM_CAP.4.9C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.10C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.11C The CM system shall provide measures such that only authorized changes are made to the configuration items.

ACM_CAP.4.12C The CM system shall support the generation of the TOE.

ACM_CAP.4.13C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

Evaluator action elements:

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.2 Problem tracking CM coverage

Dependencies: ACM_CAP.3 Authorization controls

Developer action elements:

ACM_SCP.2.1D The developer shall provide a list of configuration items for the TOE.

Content and presentation of evidence elements:

ACM_SCP.2.1C The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.

Evaluator action elements:

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

5.2.2 Delivery and operation

ADO_DEL.2 Detection of modification

Dependencies: ACM_CAP.3 Authorization controls

Developer action elements:

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

Evaluator action elements:

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

ADO_IGS.1 Installation, generation, and start-up procedures

Dependencies: AGD_ADM.1 Administrator guidance

Developer action elements:

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

Content and presentation of evidence elements:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

Evaluator action elements:

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

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up

Commercial In Confidence

procedures result in a secure configuration.

Commercial In Confidence

5.2.3 Development

ADV_FSP.2 Fully defined external interfaces

Dependencies: ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

Evaluator action elements:

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

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.2 Security enforcing high-level design

Dependencies: ADV_FSP.1 Informal functional specification

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

Commercial In Confidence

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Evaluator action elements:

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

ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_IMP.1 Subset of the implementation of the TSF

Dependencies: ADV_LLD.1 Descriptive low-level design

ADV_RCR.1 Informal correspondence demonstration

ALC_TAT.1 Well-defined development tools

Developer action elements:

ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF.

Content and presentation of evidence elements:

ADV_IMP.1.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be internally consistent.

Evaluator action elements:

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

Commercial In Confidence

ADV_IMP.1.2E The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

ADV_LLD.1 Descriptive low-level design

Dependencies: ADV_HLD.2 Security enforcing high-level design

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

Content and presentation of evidence elements:

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

Evaluator action elements:

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

ADV_LLD.1.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

Commercial In Confidence

ADV_RCR.1 Informal correspondence demonstration

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

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

ADV_SPM.1 Informal TOE security policy model

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements:

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements:

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

Commercial In Confidence

5.2.4 Guidance documents

AGD_ADM.1 Administrator guidance

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

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

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

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

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

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

Evaluator action elements:

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

Commercial In Confidence

AGD_USR.1 User guidance

Since this TOE is not a general user product, there is no user management content in the FMT class within the TOE security functional requirements. Therefore, we do not provide Users' Manual and assurance mechanism on AGD_USR.1 is not applicable.

Commercial In Confidence

5.2.5 Life cycle support

ALC_DVS.1 Identification of security measures

Dependencies: No dependencies.

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

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

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

ALC_LCD.1 Developer defined life-cycle model

Dependencies: No dependencies.

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation of evidence elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all

Commercial In Confidence

requirements for content and presentation of evidence.

ALC_TAT.1 Well-defined development tools

Dependencies: ADV_IMP.1 Subset of the implementation of the TSF

Developer action elements:

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

Content and presentation of evidence elements:

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

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

Commercial In Confidence

5.2.6 Tests

ATE_COV.2 Analysis of coverage

Dependencies: ADV_FSP.1 Informal functional specification

ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator action elements:

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

ATE_DPT.1 Testing: high-level design

Dependencies: ADV_HLD.1 Descriptive high-level design

ATE_FUN.1 Functional testing

Developer action elements:

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator action elements:

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

Commercial In Confidence

ATE_FUN.1 Functional testing

Dependencies: No dependencies.

Developer action elements:

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

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

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

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

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

Evaluator action elements:

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

ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.1 Informal functional specification

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

ATE_FUN.1 Functional testing

Developer action elements:

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

Content and presentation of evidence elements:

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

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that

Commercial In Confidence

were used in the developer's functional testing of the TSF.

Evaluator action elements:

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

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

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

Commercial In Confidence

5.2.7 Vulnerability assessment

AVA_MSU.2 Validation of analysis

Dependencies: ADO_IGS.1 Installation, generation, and start-up procedures

ADV_FSP.1 Informal functional specification

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Developer action elements:

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements:

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

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

Commercial In Confidence

AVA_SOF.1 Strength of TOE security function evaluation

Dependencies:

ADV_FSP.1 Informal functional specification

ADV_HLD.1 Descriptive high-level design

Developer action elements:

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

Content and presentation of evidence elements:

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

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

Evaluator action elements:

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

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

AVA_VLA.2 Independent vulnerability analysis

Dependencies:

ADV_FSP.1 Informal functional specification

ADV_HLD.2 Security enforcing high-level design

ADV_IMP.1 Subset of the implementation of the TSF

ADV_LLD.1 Descriptive low-level design

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Developer action elements:

AVA_VLA.2.1D The developer shall perform a vulnerability analysis.

AVA_VLA.2.2D The developer shall provide vulnerability analysis documentation.

Commercial In Confidence

Content and presentation of evidence elements:

AVA_VLA.2.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

AVA_VLA.2.2C The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

AVA_VLA.2.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.2.4C The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

Evaluator action elements:

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

AVA_VLA.2.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.2.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.2.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.2.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

Commercial In Confidence

5.3 Security Requirements for the IT Environment

Requirements for IT Environment are as follows.

FDP_ITT.1 Basic internal transfer protection

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDT_ITT.1.1 The **IT environment** shall enforce the [Enterprise Security Management Agent Systems Data Receive Security Policy] to prevent the *disclosure, modification* of user data when it is transmitted between physically-separated parts of the TOE.

FPT_AMT.1 Abstract machine testing

Hierarchical to: No other components

Dependencies: No dependencies.

FPT_AMT.1.1 The **IT environment** shall run a suite of tests *during initial start-up, periodically during normal operation* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Application Note: TOE uses commands supported by own OS to perform configuration processing and DB status check monitoring periodically. Through these processes TOE monitors and checks status of each TOE processor performance and DB status. In case of a halt, the hated processor or DB is re-executed to provide normal TOE operation.

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components

Dependencies: No dependencies.

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

Application Note: TOE calls SSL functions provided as a part of the IT environment to form SSL protocol and thus safe channels.

6 TOE Summary Specification

This Chapter presents a functional overview of the TOE; the security functions implemented by the TOE; and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE Security Functions

This section describes TOE security functions. It describes how all SFRs specified in Chapter 5 are satisfied by the security functions of ActiveTSM V3.0, which is an enterprise security management system.

6.1.1 Security Management (AT_ADMIN)

Basically, the Top Level Admin has privileges to directly manage Admin ID and related information necessary for system management. When an Authorized Admin successfully logs into the Master server using own ID, he/she can perform functions to manage TOE's security related data. If an Authorized Admin enters any value outside of limit or inappropriate value when entering security attributes, TOE sends a system management error message to notify the error.

Security Management Role (Privilege Management)

Top Level Admin, who is basically created when TOE is installed, has all privileges. Top Level Admin can add, delete or modify specific privilege admins (Management Admin or Monitoring Admin).

Functional scope of privilege admins are as follows:

- Management Admin cannot perform the following major functions that can impact the overall system.
  - Retrieve, Add, Delete of all Admin IDs
  - Audit Data Delete

- Monitoring Admin functions are limited to monitoring of security equipment log and system performance status. Specifically, Monitoring Admin is authorized to perform the following functions.
  - Event Monitoring (IDS, Firewall, ACCOUNT)
  - Performance Monitoring (CPU Load, Memory Status, Network Status)
  - Correlation Analysis Monitoring

Security Access Management

TOE Monitor can access the Master Server via RMI communication. Here, TOE Admin accesses the Master Server using SSL protocol, which is implemented within RMI communication. SSL communication provides coding of Admin traffic as well as data integrity.

TOE Security Management functions consist of the following:

- Event Monitoring
- Performance Monitoring

- Agent Log Management
- Security Info Management
- Security Correlation Analysis Management
- Security Object Management
- Security Environment Configuration Management

Event Monitoring

Event Monitoring provides the basic information to enable Authorized Admin to perform real-time monitoring of security status (Intrusion Detection, Intrusion Block, Traffic, System Load, etc.) of Enterprise Security Management Agent Systems to devise necessary countermeasures.

Each Enterprise Security Management Agent System generates a considerable amount of security equipment log, which is collected by the Agent and sent to the Slave, which receives such security equipment log and stores it in a relevant DB. Since real-time monitoring of all security equipment log for all systems stored in DB by Authorized Admin is practically impossible, this function extracts and transmits only the significant security equipment logs configured beforehand by Authorized Admin. Such refined security equipment log is referred as 'event.'

Log info that is generated at each Enterprise Security Management Agent System is collected by the TOE Agent. This log data is stored in a DB via interfaces of Master and Slave. At the same time, Authorized Admin can monitor any security status of Enterprise Security Management Agent Systems via TOE's Monitor from real-time extracted security info.

Event info is displayed on a monitoring screen whenever an event occurs. Admin can freeze event info based on date/time for analysis or send specific info directly to event related functions (Event Filtering/ Level Management, Correlation Analysis Rule Registration, KMS (Attack Info, Virus Info, Management History Info) Search or Management Receive).

Information for an event consists of the following data:

- Log Type (Firewall/IDS)
- Occurrence Object
- Occurrence Date/Time
- System Time
- Actual Equipment Name
- Attack Name
- Attacker IP, Port
- Target IP, Port
- Threat Level
- Frequency
- Other

TOE provides Event Filtering Method, Event Compression and Event Leveling to enable event extraction upon security equipment log refinement. Extracted events can be monitored using certain event data selectively based on Admin choice (e.g. Intrusion Block or Intrusion Detection).

Event Filtering

Collected security equipment log is analyzed and configured event filtering rules are applied. The result is then sent to Monitor via Master. Authorized Admin can add, delete or modify the event filtering rules.

Event Compression

Sometimes the same attack causes multiple security equipment logs. That is, when an attacker makes repeated attacks, the log information is almost identical except the occurrence number and the time data. Therefore, these log records can be compressed into a single log. Event compression is a basic TOE function and the Authorized Admin simply sets whether to use this feature or not.

Event Level Management

Security equipment log analysis system uses the log significance (level) to judge severity of pertinent security problem. However, sometimes the security equipment log does not maintain accurate level information. Therefore, the Authorized Admin can use the Event Level Management function to modify the level info in accordance with the leveling rule, which is configured by the Authorized Admin, applied in the similar manner as Event Filtering to events extracted from security equipment logs. Thus, existing level info can be adjusted to higher or lower levels.

For leveling rule generation, information necessary for leveling rule configuration is automatically filled in while the Admin only adds the level info to modify. TOE provides the functions to edit, delete or retrieve event leveling rules.

Event Pattern Monitoring

When the number of Enterprise Security Management Agent Systems that TOE manages is numerous, the number of events extracted from security equipment logs can be considerable. Therefore, the Admin cannot possibly monitor all events. For this reason, TOE provides the function to extract only the top N number of events in sequence of their occurrence frequency from among extracted events.

Extracted event patterns are displayed in a pie chart in terms of detailed info units (Attack Name, Attacker IP, Target IP, Occurrence Object, Attack Port, Target Port, etc.) on the monitor screen. Normally, the Admin uses such graphic info to monitor security status of TOE rather than focusing on detailed event info.

For event pattern configuration, since basic values are configured at the time of TOE installation and this function is used for processing of the entire TOE event patterns, only the value of event patterns to view is configured. That is, the upper limit of the most frequent event patterns for view is configured for extraction.

Event Monitoring

Event Monitoring allows simultaneous display of event monitoring results of IDS and Firewall as well as Event Pattern Monitoring result.

COMMERCIAL IN CONFIDENCE

ACCOUNT Monitoring: TOE provides the function to monitor packets that are either blocked or allowed at Enterprise Security Management Agent Systems such as a Firewall.

ACCOUNT info consists of the following data:

- Log Type (Intrusion Block)
- Occurrence Object
- Occurrence Date/Time
- System Time
- Actual Equipment Name
- Service
- Action
- Source IP, Port
- Destination IP, Port
- Frequency
- Other

Performance Monitoring

TOE provides the function to real-time monitoring at Monitor of system status info (CPU Load Rate, Network Traffic/ Packet Volume, Memory Status, etc.) of Enterprise Security Management Agent Systems. Thus, the operating status of Enterprise Security Management Agent Systems and security & network status can be verified.

Agent Log Management

TOE provides the function to collect and manage Security Equipment Logs, which are basic data that occurs at Enterprise Security Management Agent Systems. Security Equipment Log Management function consists of the following three sub-functions.

- Security Equipment Log Collection (Agent)
- Security Log Event Processing (Slave)
- Collected Log Search (Monitor)

Interfaces that an Agent uses for security equipment log collection are SNMP, SYSLOG and custom APIs, where the former two are standard interfaces that enable log collection from all Enterprise Security Management Agent Systems regardless of their type via common interfaces. In case of custom API, TOE Agent provides collection interface to representative products.

TOE Agent functions are performed in two types of modes: internal mode and external mode. The internal mode enables TOE to directly conduct log collection remotely via standard interfaces (SNMP or SYSLOG) from Enterprise Security Management Agent Systems and interfaces with Slave. On the other hand, in the external mode, Enterprise Security Management Agent Systems do not provide standard interfaces but only custom interfaces so that they perform Agent function directly for equipment log collection. SSL-based RMI communication channel is used to transfer log collected by Agent using the external mode to Slave.

Commercial In Confidence

a) Security Equipment Log Collection

TOE provides the function for its Agent to collect security log and status info from Enterprise Security Management Agent Systems. Collected info includes Intrusion Detection, Intrusion Block, Management Target Server, Security Equipment Log, CPULoad, Network Traffic and Memory. Collected info is sent to Slave of TOE.

b) Security Log Event Processing

TOE Slave receives security logs collected by Agent and stores them in their primitive form in a DB. At the same time, the Slave applies Event Filtering Rules and Event Compression Rules configured by the Authorized Admin to security logs and delivers the refined security log-in events to the Master at real-time.

Event Filtering rules defined at Monitor by Authorized Admin are stored in DB by Master. However, the defined event filtering and event compression are performed directly by Slave at real-time and the results are sent to TOE Master.

Event Filtering rules defined at Monitor by Authorized Admin are stored in DB by Master. However, the defined event filtering rules and event compression are performed directly by Slave at real-time.

c) Event Search

Event Search function is categorized into event search of events that occurs at Enterprise Security Management Agent Systems and the search for Firewall Account Log Types.

Admin normally uses either Event Monitoring or Event Pattern Monitoring for security monitoring tasks. However, in case a specific Enterprise Security Management Agent System incurs a heavy volume of security log or experiences a serious security problem, its primitive security log needs to be retrieved. Security Equipment Log Search is conducted by Slave, where the search criteria are as follows. Storing of search files in external text files is also provided.

Events

- Log Type (Intrusion Detection, Intrusion Block)
- Area
- Entity
- Attack Name
- Threat Level
- Actual Equipment Name
- Attacker IP/Port
- Target IP/Port
- Begin / End Date
- Max Search Result Number

Account

Commercial In Confidence

- Log Type (Intrusion Block)
- Occurrence Object
- Occurrence Date/Time
- System Time
- Actual Equipment Name
- Service
- Action
- Source IP, Port
- Destination IP, Port
- Frequency
- Other

Security Info Management

TOE's security info management function includes Security Management Admin, Security Knowledge Management System (KMS), Security Management Report and Admin Function to support Authorized Admin to review collected security log data, analyze security issues and take appropriate countermeasures. That is, the Admin utilizes this function to analyze performance (CPU, memory, traffic) of Enterprise Security Management Agent Systems and the external attack info to take measures on Enterprise Security Management Agent Systems or to establish appropriate security policy.

a) Security Management Admin
Authorized Admin analyzes major security event info that is delivered real-time to Monitor, makes judgment on the seriousness of current problems, takes appropriate measures to counter them and record the results.

Basic functions of security management are Add, Edit, Delete and Retrieve of management records. Also, management records can proceed through the steps of Receive, Analysis and Countering as the Admin completes each process in sequence. If a further process is required at Analysis or Countering step, then a record can be held temporarily, while if no further processing is required, the record is returned to previous process.
Upon management acceptance of a record, requester info is required on the requester who makes a request for analysis and countering on the occurred security problem, where the requester can be a Management Admin, Monitoring personnel, or System Admin. Requester Info (name, position, team, e-mail, phone number, company) Management function (Add, Edit, Retrieve, Delete) is provided.

Also, the info on a general equipment that caused a security problem is required. Therefore, a function, including Add, Edit, Retrieve and Delete, is provided to manage problem equipment info as follows:

- Host Name
- Domain Name
- Equipment Type (PC, Router, Server, Switch, External Server, etc.)
- Location
- Host IP, Port

- OS Version
- Other Info

b) Knowledge Management System (KMS)

TOE provides the security knowledge management function that supports systematic accumulation of diverse knowledge management info and rapid countering of security events that occur. The types of security knowledge managed by KMS include Virus Info, Attack Info and Management History Info. Virus and Attack info are automatically stored in DB via a web robot while the Management History is stored in Security Management.

Therefore, KMS only provides the function to retrieve security info that has been collected and stored. This is used for security info analysis based on reference info including analyzed info history and virus attack info while conducting Management tasks. Virus info and attack info include URL info so that web content of relevant URL for each info record can be retrieved and detailed management history info also can be retrieved.

Virus Info includes the following data.

- Virus Name
- Type (Trojan Horse, Harmful, etc.)
- Threat Level (Average, Serious, Unknown, etc.)
- Symptom Detail
- Date Detected
- Target Platform
- Symptom
- Occurrence Location
- Treatment
- URL

Attack Info includes the following data:

- Attack Name
- Attack Code
- Attack Type
- Overview
- URL

Management History Info includes the following data:

- Receive No.
- Receive Title
- Attack Type
- Attack Method
- Receive Detail
- Analyzer
- Countermeasure

Commercial In Confidence

- Countermeasure Result
- Modify Data
- Modifier

c) Trend Report Retrieve

This function allows Authorized Admin to generate a trend report based on collected security logs and event data. That is, an Authorized Admin can analyze collected info through such reports and take appropriate actions. Reports are only generated for Admin verification but are not stored. Here, reports can be stored in the admin's local computer in file forms based on Admin requests.

Trend Reports include performance trend reports on CPU, traffic, packet and memory as well as event trend reports.

Security Correlation Analysis

TOE provides correlation analysis function that allows extraction of significant info from various info and events that occur in large quantities at numerous Enterprise Security Management Agent Systems. Correlation analysis is necessary because it is practically difficult to track and monitor security logs and events of such target systems and such security logs are usually mutually correlated.

Although an external attack can be identified through analysis of a specific system, usually an attack symptoms occur in multiple systems. Therefore, instead of analyzing a single event, IDS attack names, firewall blocking rules and event extraction rules on CPU/memory/network load conditions can be configured as elements that generate security logs on all Enterprise Security Management Agent Systems so that the countermeasures configured by the Admin are performed when such rules are satisfied simultaneously. Thus, multiple events' correlations are configured to enable accurate analysis of security problems.

Rule management for correlation analysis provides management of rules on performance and events, whereas info to be configured is as follows:

a) Performance Threshold Management

Thresholds on performance (CPU load, memory load, or network load) are set by equipment and by network so that when such a threshold is reached, pertinent action configured by the Admin for the event is performed. This function provides correlation analysis of performance info not only of individual equipment but all equipment in group networks or areas. Performance correlation analysis manages (add, edit, delete, retrieve) the following configuration data.

- Rule Name
- Applicability
- Entity (Network, Black List, Firewall, Area (Domain), Yellow List)
- Threshold
- Action

Threshold data used in performance correlation analysis are separately managed. Load variations by specific time periods (by date) under normal operating conditions are analyzed or average values per time periods (a day, three days, a week, a month or average by day of week) and the respective Threshold values are adjusted accordingly to prevent unnecessary triggering of security events. Also, event triggers are configured only when a configured Threshold is held for a certain length of time continuously. The following Thresholds are managed (add, edit, delete, retrieve) within performance security policy configuration for correlation analysis.

- Threshold Name
- Description
- Code Type (CPU Load, Memory Load, Network Load)
- Continuity Threshold (seconds, minutes, number of times)
- Frequency (daily average, 3-day average, weekly average, monthly average, average by day of week)
- Threshold value by date or day of week

b) Event Security Policy Management

The Admin can configure event correlations to extract those events that satisfy these rules. Logical relationships between events that occur in one or more Enterprise Security Management Agent Systems are configured. When an event that satisfies any of such relationships occurs, it is delivered to the Admin according to the configured alarm process.

When configuring event correlation rules, rules can be generated on three different related Enterprise Security Management Agent Systems. However, existing event correlation rules can be used in other correlation rules as if they are rules for other related target systems. Thus, an infinite number of event correlation rules can be configured as connected rules. Event correlation rules include the following data.

- Rule Name
- Applicability
- Target Equipment Entity/Event/Occurrence Count (Condition)
- Related Equipment 1 Entity/Event/Occurrence Count (Condition)
- Related Equipment 2 Entity/Event/Occurrence Count (Condition)
- Action (Alarm Sound, Warning Screen, Logging, E-mail, Character Message)
- Threat Level(High/Medium/Low/Event Surge)

c) Correlation YELLOW/ BLACK List Management

Black List is the list of attack IPs that cause security problems and it is managed (add, edit, delete, retrieve) together with the following info.

- System Title
- Attack IP

Oullim Information Technology, Inc.
COMMERCIAL IN CONFIDENCE

- Description
- Applicability

On the other hand, Yellow List is systems that have been attacked. It is managed (add, edit, delete, retrieve) with the following info.

- System Title
- System IP
- Service Name
- Description
- Applicability

Security Object Management

TOE components such as Master, Slave, Agent and Enterprise Security Management Agent Systems must be registered as security objects to enable security functions on them. Thus, they are all managed as TOE assets. Relationships among TOE security objects must be configured via Management Maps to enable normal application of security functions. Therefore, security objects registered in Asset Management must be added to map info within Map Management to define interrelationships and roles among security objects. In case multiple Slaves are registered as TOE assets, Map Management is used to configure which of them is connected to the Master and to what Agents each Slave is connected.

a) Asset Management

This function manages (add, edit, delete, retrieve) information required for security management of all TOE components, excluding Monitor and Agents, and Enterprise Security Management Agent Systems. Major info consists of the following data and this info can be stored as an external text file.

- Control No.
- Category (Hardware/Software)
- Item (Master/ Slave/ Intrusion Detection/ Intrusion Block/ Management Target Server/ Network Equipment)
- Host Name, IP
- Usage

b) Map Management

Security objects registered in asset management must be configured to interconnect within TOE. Such relationships are configured by registering them as objects in a visual map. Relationships of Master-Slave-Agent-Equipment are registered in map management to enable TOE security functions. When a problem occurs with a system registered in the map, then the system's status is visually displayed on the map.

In case the number of registered equipment is large, their map display can be very complicated and difficult. Thus, the following map display options can be used.

- Actual Group: This map shows actual TOE execution architecture that shows

configuration among physical security objects.

- Equipment Group: Equipment is grouped for display by their type including Intrusion Detection, Intrusion Block, Router and Management Target Server.
- Area Group: This map displays numerous Enterprise Security Management Agent Systems by area such as localities or organizational groups.

Within map management, Areas, Slaves and Agents are managed (add, edit, delete, retrieve) to initialize or store the entire map info.

Master is basically displayed on the map always. Therefore, it does not need registration in the map. Slaves are managed with the following info. Asset info registered in Asset Management can be utilized for Slave registration in the map.

- Slave Name
- Slave Description
- Control No.
- Item
- Detail Category
- Host Name, IP
- Connected Master
- Area
- Port

The following data are used for Agent registration.

- Agent Name
- Agent Description
- Control No.
- Item
- Host Name, IP
- Community
- CPU OID
- Memory OID
- Memory Total OID
- Memory free OID
- Memory used OID
- Connected Slave
- Area
- Port

c) Map Node Search

A specific node can be searched using node name from map screen.

The network interface status between TOE system and Enterprise Security Management Agent Systems can be verified using ICMP ping.

COMMERCIAL IN CONFIDENCE

Since SSL-based RMI is used for communication among all TOE components (Monitor, Master, Slave, Agent), data transferred through RMI interfaces are protected using the confidentiality algorithm (3DES) and integrity algorithm (SHA-1).

Security Management Environment Configuration

a) Code Management

Codes used for TOE security functions are managed (add, edit, delete, retrieve) and the Authorized Admin can modify them as necessary. Codes configured by Authorized Admin include Item (System Type), Control No., Product Category, Nation, Equipment Type, Attack Type and Attack Method.

b) TOE allows the following configuration on security management configuration data.

- Integrity Test Frequency Configuration
- Disk Space Configuration
- TOE System Time Configuration
- Function to turn on/off of Alarm Sound or Warning Screen in case of excessive generation.
- Max number of events in a real-time event list
- Management Environment Configuration
  - Add/Delete of Character Message Server Access Info (SMS Server IP, Port, User ID/Password) and Receiver Info (SMS No., Description, Applicability)
  - Frequency of Monitor and Master event processing
  - Frequency of TOE status check
  - Frequency of DB status check
  - No. of screens displayed on Monitor
  - Mail server IP

Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.2(1), FMT_MTD.2(2), FMT_SMF.1, FMT_SMR.1, FPT_ITT.1

Commercial in Confidence

6.1.2 Audit (AT_AUDIT)

Security audit functions described in this sub-section include Audit Data Generation, Audit Data Retrieve, Audit Data Storage and selective Audit Data Retrieve.

Audit data generated at each module is sent to Log Module, which checks the audit data and generates an alarm in case of an alarm condition and the audit data is stored in the log table within a relevant DB.

Audit data generation

a) Audit info generated by TOE is categorized into changes in TOE security configuration and errors or major messages generated within TOE system.
Whenever Authorized Admin processes Add, Edit or Delete requests on security configuration info, this action is stored as an audit data record. In addition, errors that occur during TOE system performance and results of major security functions that are applicable for audit are stored as audit data. Major target items are as follows. All security audit events incur audit data, which is delivered to Log Module for storage in the order of their occurrence time.
   - All functional errors that occur
   - Self Diagnose Results
   - Integrity Test Results

b) For audit target events described in Table 5-2 and Table 5-3 are stored as audit data records with the following data at minimum.

   - Event Date/Time
   - Object ID (Admin ID, Agent, Master, Slave, Agent)
   - Event Significance (ERROR, WARNING, NOTICE, MANAGE)
   - Sequence No.
   - Event Detail

c) TOE converts all actions of security policy implementation by Authorized Admin specified in AT_ADMIN as audit data.

d) TOE monitors generated audit data and in case a pre-configured alarm condition occurs with any audit data, this event is sent to Authorized Admin via e-mail and a warning screen is displayed.

e) When generating audit data, Event Significance log (ACCOUNT, WARNING, ERROR, MANAGE) is sent to Log Process Module.

f) When Admin authentication occurs three times consecutively for an Admin ID, the status of this Admin ID is changed to 'TERMINATE.' In this condition, a normal authentication info entry fails authentication.

Commercial In Confidence

g) In the event of exceeding a Threshold for correlation analysis configured by Admin is exceeded or any specified event occurs, this creates an audit data record and the action specified for the correlation analysis condition is executed (such as an alarm to admin).

Audit review

a) Audit Data Retrieve

TOE provides Retrieve and Search functions to Authorized Admin on all audit data records based on conditions. However, Monitoring Admin is not allowed to retrieve audit data. Authorized Admin can retrieve audit data by audit data type based on specific date and time.

Authorized Admin (Top Level Admin, Management Admin) can retrieve desired audit data from stored audit data by specific conditions. Retrieved search result can be viewed via TOE Monitor.

- Event Date/Time (Date & Time)
- Object ID
- Event Category
- Event Significance (Event Type)
- Event Detail (Arbitrary search key)

b) Real-time Audit Data Retrieve

Authorized Admin can view audit data upon retrieve at real-time. If Authorized Admin wishes to view current audit data using any of the following conditions, he/she may enter values for such conditions and retrieve desired audit data at real-time.

- Event Date/Time (Date & Time)
- Object ID
- Event Category
- Event Significance (Event Type)
- Event Detail (Arbitrary search key)

c) Object History

History of Master, Slave, Agent or Area can be retrieved.

d) System History

Execution and Stop of Master and Slave's Master Access History can be retrieved.

e) User History

Admin can retrieve TOE log-on or log-out history.

COMMERCIAL IN CONFIDENCE

TOE Audit Data Configuration

TOE Security Management function allows configuration of audit data generation level within audit data environment configuration.

Admin can set OS Time for Master, Slave and Monitor systems to ensure consistency of log times.

All security configuration changes of TOE by Authorized Admin are left in audit data as are TOE internal problems. When storing audit data, audit data significance level can trigger an Alarm Send to Admin or display of a warning screen.

TOE uses DBMS as the audit data storage. When its storage capacity is less than the configured value, an alarm is sent to Admin or service is terminated. Action for this case is the DB Admin modifies DB partition configuration to secure additional storage space.

Upon checking the DB partition storage space, if the storage space reaches the first Admin Alarm Percent Value (default value 5%: in case available space is less than or equal to 5%), TOE sends e-mails to all admins and displays a warning message at Monitor.

If the storage space reaches Total Service Terminate Percentage (default value 3%), both Slave and Master components are terminated and log info is no longer stored in DB. Also, e-mails are sent to admins and a warning message is displayed on the TOE Monitor.

TOE time stamp

To ensure consistency of audit data times, the Top Level Admin configures time stamp directly. Then times of all systems that perform TOE functions are set simultaneously. That is, OS times of Agent, Master and Slave systems are all modified at real-time.

Functional Requirements Satisfied: FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, FAU_STG.3, FAU_STG.4, FPT_STM.1

Commercial In Confidence

6.1.3 User Data Protection (AT_UDP)

TOE performs access control on Admin and all Enterprise Security Management Agent Systems.

Enterprise Security Management Agent Systems request access to send audit data and system status info generated within them to TOE. TOE then verifies Ips of Enterprise Security Management Agent Systems. If IP and Port data match, then access is granted, upon which a session is established to exchange actual data. Upon session creation, an Enterprise Security Management Agent System uses the session to send user data, which is stored in a TOE storage.

When the Admin requests security management screen to retrieve or edit TSF data, TOE first authenticate the Admin as an Authorized Admin (successful authentication and verification of relevant TSF privilege), then security management screen is displayed to authenticated Authorized Admin only.

Functional Requirements Satisfied: FDP_ACC.1(1), FDP_ACF.1(1), FDP_ACC.1(2), FDP_ACF.1(2), FDP_ITC.1, FDP_ITT.1

Commercial In Confidence

6.1.4 Identification and Authentication (AT_INA)

Admin authentication function allows an Admin to request authentication to TOE via only RMI interface so that only Authorized Admins are authenticated to use TOE security management. That is, authentication is possible only through pre-registered system Ips.

General Identification & Authentication Method –Authorized Admin

a) TOE has authentication mechanism for admins. Authentication method includes ID and password. All admins use the same authentication mechanism.

b) Identification & Authentication function is implemented using permutation mechanism (Password based Admin Authentication). Strength of Function satisfies SOF-Medium level.

c) Identification & Authentication Function performs authentication of remote Authorized Admins via password based SSL protocol. The function receives safely remote admin's ID and password via SSL based RMI, which is supported in the IT environment, and performs Admin authentication.

d) TOE Password Authentication mechanism is used to authenticate admins using the following coded characters.

- Password has min 6 and max 20 alphanumeric characters.
- Permitted characters are total 93 including a-z(26), A-Z(26), 0-9(10) '&' but excluding! @ # $ % ^ * ( ) _ + | ` - = \ { } : " < > ? [ ] ; ' , . / "
- Admin ID and password of an Admin account being configured are not permitted.

e) When an admin, including specific privilege admins, requests security management function, the admin's authentication status is checked and access is granted only if the status is normal. Also, even if the authentication status is normal, if the requested security management function is not a part of the admin's assigned privileges, access is blocked.

While an Admin performs authentication, TOE shows only the admin's ID but echoes its password as a series of asterisks (*).

f) TOE receives directly security logs and equipment info from Agents or Enterprise Security Management Agent Systems. Here, TOE identifies the IT entity that sends such info to TOE. The source IP address of info source is checked against the registered IP list of Enterprise Security Management Agent Systems so that, if the source is not included in the registered source IP list, the info receive is blocked.

FIA_UAU.2 satisfies SOF-Medium level.

Authentication Failure Process Method

When Admin authentication fails three times, the Admin ID is converted to TERMINATE status, where the ID can no longer enable authentication unless the Top Level Admin releases the TERMINATE status.

Functional Requirements Satisfied: FIA_AFL.1, FIA_ATD.1(1), FIA_ATD.1(2), FIA_UAU.2, FIA_UAU.7, FIA_UID.2(1), FIA_UID.2(2)

Commercial In Confidence

6.1.5 Protection of Security Function (AT_PT)

TOE stores hash values of TSF environment data and TSF execution data to protect TSF area against unauthorized entities so that, when an Admin accesses security management server and makes requests, such requests are compared against stored hash values to verify integrity. TOE also checks the status of the RMI interface that connects TOE components as well as the status of components that are connected to the interface.

TSF Data Transfer via Safe Channel

Since TOE uses SSL-based RMI communication between all components (Monitor, Master, Slave, Agent), data transferred via RMI interface is protected using confidentiality algorithm (3DES) and integrity algorithm (SHA-1). This is the same for Admin authentication so that SSL certificate created during TOE installation is used to create a trust SSL channel, which is then used for Admin authentication.

All TOE components uses RMI based communication interface provided by Java language for mutual connection. Each Java RMI interface has a unique internal ID so that connection is not possible unless the interface ID matches when connecting with RMI interface of another system. Also, Java RMI interface selectively uses SSL. Thus, TOE's Monitor, Master, Slave and Agents all use Java RMI for mutual identification.

TOE Self Diagnosis

TOE ensures safety of environment files and execution files of TSF through integrity test, which ensures safe execution of security functions. To protect TSF data, TOE stores hash values of TSF environment data and TSF execution files so that when an Admin accesses the security management server, frequent comparison is made against the stored hash values to check integrity. Any deviation identified is sent to the Authorized Admin.

When an Admin accesses TOE via a security server and an integrity error occurs from TSF protection function, it is displayed on a security management screen for resolution. The Authorized Admin can re-create hash values of the error files to resolve the integrity problem. Integrity test and TOE process checks are periodically conducted during system operation.

TOE Self Diagnose is conducted at each TOE start-up and periodically conducted at every minute. Integrity tests are conducted at start-up, at frequency defined by FMT_MTD.2(2) and upon request from Admin.

TSF Protection Function is implemented using a permutation mechanism (SHA-1 based TSF Data Integrity Test).

a) Environment Configuration Data Integrity Management
   Integrity test ensures safety of TSF environment files and execution files. To protect TSF data, TOE stores hash values of TSF environment data and TSF execution files so that when an

Admin accesses the security management server, frequent comparison is made against the stored hash values to check integrity. Any deviation identified is sent to the Authorized Admin.

TOE provides the Integrity Test Result View function to Authorized Admin. Also, TOE provides the Initialization function for Integrity Test execution and Integrity Test Time Configuration function as well as retrieval of recent integrity test results. Authorized Admin can re-create hash values of integrity error files.
TOE Self Diagnose is conducted at each TOE start-up and periodically conducted at every minute. Integrity tests are conducted at start-up, at frequency defined by FMT_MTD.2(2) and upon request from Admin.

b) System Status Management
TOE checks status of its major components to ensure their normal operations. Targets of system status check include Master, Slave, Agent and DBMS. Abnormal status info is sent to the Admin as follows. In case TOE Master Operation is abnormal, TOE Monitor can detect the status and send a message to the Admin. For abnormal status of Slave, Agent or DBMS, TOE Master in normal condition detects the problem and sends a message to the admin.

Functional Requirements Satisfied: FPT_TST.1, FPT_AMT.1, FPT_ITT.1

Commercial In Confidence

6.2 Assurance Measures

Assurance requirements of this ST follow those of Part 3 of CC (1). TOE provides documents to verify the assurance requirements of Chapter 5 as in Table 6-1.

[Table 6-1] Traced Assurance Measures

Assurance Component ID	Assurance Component Name	Assurance Measure
ACM_AUT.1	Partial CM automation	Configuration Management
ACM_CAP.4	Generation support and acceptance procedures	Configuration Management
ACM_SCP.2	Problem tracking CM coverage	Configuration Management
ADO_DEL.2	Detection of modification	Delivery Documentation
ADO_IGS.1	Installation, generation, and start-up procedures	Installation guidance
ADV_FSP.2	Fully defined external interfaces	Function Specification
ADV_HLD.2	Security enforcing high-level design	High-level Design
ADV_IMP.1	Subset of the implementation of the TSF	Implementation Representation
ADV_LLD.1	Descriptive low-level design	Low-Level Design
ADV_RCR.1	Informal correspondence demonstration	Analysis of Correspondence
ADV_SPM.1	Informal TOE security policy model	Security Policy Model
AGD_ADM.1	Administrator guidance	Administrator guidance
AGD_USR.1	User guidance	*N/A
ALC_DVS.1	Identification of security measures	Development Security
ALC_LCD.1	Developer defined life-cycle model	Life Cycle definition Document
ALC_TAT.1	Well-defined development tools	Development Tool Document
ATE_COV.2	Analysis of coverage	Test Documentation
ATE_DPT.1	Testing: high-level design	Test Documentation
ATE_FUN.1	Functional testing	Test Documentation
ATE_IND.2	Independent testing - sample	Test Document, Testable TOE
AVA_MSU.2	Validation of analysis	Misuse Analysis
AVA_SOF.1	Strength of TOE security function evaluation	Strength of Function Analysis
AVA_VLA.2	Independent vulnerability analysis	Vulnerability Analysis

* TOE does not allow general users. Since there is no mention of general user management in FMT class within the TOE security function requirements, users' manual is not provided. Therefore, assurance measure for AGD_USR.1 is not applicable.

Commercial in Confidence

7 Rationale

This chapter describes evidences used in evaluation. These evidences are complete and concentrated collection of ST requirements, provides efficient IT security measures within the TOE security environment, and supports the fact that the TOE summary specification addresses the TOE requirements properly.

[Table 7-1] Logical mapping between Security Environment and TOE security objectives

IT Security Objectives (TOE) / IT Security Environments	O.AUDIT	O.MANAGE	O.SECTSFD	O.ID	O.AUTH	O.COLLECTINFO	O.ACCESS	O.ABNORMALOP	O.STAT
A.DYNAMIC									
A.ACCESS									
A.TADMIN									
A.PHYSEC									
A.REINFOCEOS									
A.REINFOCEOE									
A.DBINSTLIMIT									
A.TEXTSERVER									
T.DISGUISE	X			X	X				
T.RECFAIL	X								
T.WRONGINFO	X	X					X		
T.REPEAT	X			X	X				
T.CHGTSFD	X		X	X	X		X		
T.ABNORMALSVC						X		X	
T.ABNORMALRES						X		X	
TE.WEAKMGT		X							
TE.DELNINST									
TE.CHGTSFD									
P.AUDIT	X			X	X				
P.SECMGT		X							
P.STAT									X

Commercial In Confidence

[Table 7-2] Logical mapping between Security Environment and IT Environment security objectives

IT Security Objectives (TOE) / IT Security Environments	OE.PHYSEC	OE.TADMIN	OE.SECMGT	OE.REINFORCEOS	OE.REINFORCEOE	OE.DYNAMIC	OE.ACCESS	OE.DBINSTLIMIT	OE.SECCH	OE.SECTSF	OE.EXTSERVER
A.DYNAMIC						X					
A.ACCESS							X				
A.TADMIN		X									
A.PHYSEC	X		X								
A.REINFOCEOS				X						X	
A.REINFOCEOE					X						
A.DBINSTLIMIT								X			
A.TEXTSERVER											X
T.DISGUISE											
T.RECFAIL											
T.WRONGINFO											
T.REPEAT											
T.CHGTSFD											
T.ABNORMALSVC											
T.ABNORMALRES											
TE.WEAKMGT		X	X								
TE.DELNINST		X	X								
TE.CHGTSFD									X		
P.AUDIT											
P.SECMGT		X	X								
P.STAT											

Commercial In Confidence

7.1 Rationale for IT Security Objectives

The following is the rationale for security objectives.

[Table 7-3] Rationale for security objectives equivalent to IPSPP

Security Objective	Description
O.AUDIT	When a user uses a security function, TOE shall record each user audit event based on audit data policy and provide a mechanism to maintain safely and to review such recorded audit event data. Audit data policy is as follows. ▪ Audit events of Admin Identification & Authentication shall be recorded. ▪ TOE shall provide a countermeasure when audit data reaches a saturation level. ▪ TOE shall record unauthorized access attempts as audit events. ▪ In case of repeated authentication attempts, TOE shall ensure detection of such attacker ID using audit data. ▪ TOE shall record integrity errors as audit events. Thus, this TOE security objective is to counter unauthorized modification of threats T.DISGUISE, T.RECFAIL, T.WRONGINFO, T.REPEAT and T.TSF Data using audit data; and to support the organization's security policy P.AUDIT.
O.MANAGE	TOE configures access control rules to execute security policy and control unauthorized TOE access. For this purpose, TOE shall provide the means to safely manage TSF data and TOE including TOE configuration data creation and management. Thus, this security objective is to counter the threats of T.WRONGINFO and TE.WRONGMGT and support organizational security policy P.SECMGT by providing means to Authorized Admin to safely manage TOE.
O.SECTSFD	TSF data can be modified through an external, unexpected access without Admin's awareness to disable normal execution of security policy. To prevent this condition, TSF data is checked for intentional/unintentional modification to ensure its integrity and thus ensure normal TSF functioning. Thus, this TOE security objective is to counter the threat of T. CHGTSFD.
O.ID	When an external IT entity sends user data to TOE, the entity has to be identified and the Admin has to be authenticated to allow only Authorized Admin access. By identifying Admin and external IT entities, TOE uses ID info for audit data generation, permits access to only registered IT entities and Authorized Admins and prevents unauthorized modification of TSF data. Also, repeated authentication failures cause termination of relevant Admin ID. Thus, this security objective is to counter the threats of T.DISGUISE, T.REPEAT, T.CHGTSFD and to support P.AUDIT.
O.AUTH	An Admin that wishes to access TOE has to secure authentication. And only authenticated Admin can access TOE and modify TSF data. However, authentication is vulnerable to repeated authentication attempts by an external attacker. Therefore, this security objective is to counter the threats of T.DISGUISE, T.REPEAT and T.CHGTSFD; and to support P.AUDIT.
O.COLLECTINFO	TOE collects user data of system resource usage and security actions from Agents that reside in TSC external systems. Collected info is used to check status of Agent service and resource usage. Thus, this TOE security objective is to counter T.ABNORMALSVC and T.ABNORMALRES.

O.ACCESS	TOE controls user's unauthorized use of TOE security management functions. TOE blocks unauthenticated user's access to security management functions. TOE receives user data from Enterprise Security Management Agent Systems that are external IT entities. This security objective is to ensure blocking of user data transfer from any unauthorized external IT entity based on Agent Data Receive Security Policy, and to block access of unauthorized user based on Admin Access Control Policy. Thus, this security objective counters the threats of T.WRONGINFO and T.CHGTSFD.
O.ABNORMALOP	TOE sends an alarm to Admin in case Agent services or resources are used abnormally by checking Agent collected info. Therefore, TOE shall ensure Admin's countermeasure against abnormal Agent operational status via alarm system. Thus, this security objective counters the threats of T.ABNORMALSVC, and T.ABNORMALRES.
O.STAT	TOE performs statistical processing of Security Equipment Log and Security Equipment Info collected from Agents based on Statistical Processing Policy. Thus, this TOE security objective supports Security Policy P.STAT.

Commercial In Confidence

7.2 Rationale For Security Objectives For The Environments

The following are rationale for Environment Security Objectives.

[Table 7-4] Rationale for Security Objectives for the Environment

Security Objective	Description
OE.DYNAMIC	This environment security objective is to counter A.DYNAMIC by ensuring dynamic variations of Enterprise Security Management Agent Systems.
OE.PHYSEC	This environment security objective is to ensure that TOE is installed in a physically safe location to defend against external physical attacks and TOE modification attempts, thus ensuring the physical safety of TOE. Thus, it supports the assumption A.PHYSEC.
OE.TADMIN	This environment security objective ensures trustworthiness of Authorized Admin so that it supports the assumption A.TADMIN and security policy P.SECMGT; and counters TE.WRONGMGT and TE.DELNINST.
OE.SECMGT	This environment security objective ensures that TOE is distributed/installed in a safe way, configured and used safely by Authorized Admin so that it counters threats of TE.WRONGMGT and TE.DELNINST; and is needed to support the assumption A.PHYSEC and the security policy P.SECMGT
OE.REINFORCEOS	This environment security objective is to ensure safe and reliable OS by removing all unnecessary services and means in OS and augmenting all OS vulnerabilities. Thus, it supports the assumption A.REINFORCEOS.
OE.REINFORCEOE	This environment security objective ensures safety and reliability of Java VM operating environment by augmenting its vulnerabilities. Thus, it supports the assumption A.REINFORCEOE.
OE.ACCESS	This environment security objective ensures TOE access to Enterprise Security Management Agent Systems defined as the scope of protection in security policy to perform normal security Management functions. Thus, it supports A.ACCESS.
OE.DBINSTLIMIT	This environment security objective ensures reliability and safety of DB access via DBMS for TOE data management installed in the same system as TOE. Thus, it supports A.DBINSTLIMIT.
OE.SECCH	This environment security objective ensures that TSF data transfer to a physically separated TOE or receive from an external entity is done through a safe communication channel. Thus, it counters the threat TE.CHGTSFD.
OE.SECTSF	This environment security objective is to ensure that OS detects any abnormal TSF operation and takes appropriate action. Thus, it supports the assumption A.REINFOCEOS.
OE.EXTSERVER	This environment security objective ensures that external servers that TOE interacts for normal functions are safe. Thus, it supports the assumption A.TEXTSERVER.

Commercial In Confidence

7.3 Rationale for TOE Security Requirements

[Table 7-5] Rationale for Security Functional Requirements

IT Security Objectives (TOE) / Security Function Requirements	O.AUDIT	O.MANAGE	O.SECTSFD	O.ID	O.AUTH	O.COLLECTINFO	O.ACCESS	O.ABNORMALOP	O.STAT
FAU_ARP.1								X	
FAU_GEN.1	X								
FAU_GEN.2	X								
FAU_SAA.1	X							X	
FAU_SAR.1	X								
FAU_SAR.3	X								
FAU_STG.1	X								
FAU_STG.3	X								
FAU_STG.4	X								
FDP_ACC.1(1)			X				X		
FDP_ACF.1(1)			X				X		
FDP_ACC.1(2)							X		
FDP_ACF.1(2)							X		
FDP_ITC.1						X			
FIA_AFL.1				X	X				
FIA_ATD.1(1)				X			X		
FIA_ATD.1(2)				X			X		
FIA_UAU.2			X		X				
FIA_UAU.7					X				
FIA_UID.2(1)				X			X		
FIA_UID.2(2)			X	X					
FMT_MOF.1		X							
FMT_MSA.1		X	X						
FMT_MSA.3		X	X						
FMT_MTD.1(1)		X	X						
FMT_MTD.1(2)		X	X						
FMT_MTD.1(3)		X	X						
FMT_MTD.1(4)		X	X						X
FMT_MTD.2(1)		X							
FMT_MTD.2(2)		X							
FMT_SMR.1		X		X	X				
FMT_SMF.1		X							
FPT_STM.1	X								
FPT_TST.1			X						

The following are descriptions of the rationale for the security functional requirements of TOE.

FAU_ARP.1 Security alarm

This component ensures admin's ability to take a countermeasure against three authentication attempts and correlation analysis results. Thus, TOE security objective O.ABNORMALOP is satisfied.

FAU_GEN.1 Audit data generation

This component ensures audit target event definition and audit data generation. Thus, TOE security objective O.AUDIT is satisfied.

FAU_GEN.2 User identity association

This component ensures that user identification is required to define audit target events and to track user relation with audit data. Thus, TOE security objective O.AUDIT is satisfied.

FAU_SAA.1 Potential violation analysis

This component ensures identification of security violations through audit event review. Thus, TOE security objective O.AUDIT, O.ABNORMALOP is satisfied.

FAU_SAR.1 Audit review

This component ensures Authorized Admin's capability to review audit data. Thus, TOE security objective O.AUDIT is satisfied.

FAU_SAR.3 Select audit review

This component ensures audit data search and ordering based on logical relations. Thus, TOE security objective O.AUDIT is satisfied.

FAU_STG.1Protected audit trail storage

This component ensures protection of audit records from unauthorized modifications and deletions. Thus, TOE security objective O.AUDIT is satisfied.

FAU_STG.3Action in case of possible audit data loss

This component ensures countermeasures in case accumulated audit data exceeds a pre-configured limit. Thus, TOE security objective O.AUDIT is satisfied.

FAU_STG.4Prevention of audit data loss

This component ensures countermeasures in case audit data storage saturation. Thus, TOE security objective

Commercial In Confidence

O.AUDIT is satisfied.

FDP_ACC.1(1) Subset access control(1)

This component ensures that Security Management Access Control Policy and its scope are defined. Thus, TOE security objective O.ACCESS, O.SECTSFD is satisfied.

FDP_ACF.1(1) Security attribute based access control (1)

This component ensures attribute-based Security Management Access Control Policy is executed properly. Thus, TOE security objective O.ACCESS, O.SECTSFD is satisfied.

FDP_ACC.1(2) Subset access control(2)

This component ensures that Enterprise Security Management Agent Systems Data Receive Security Policy for access control is defined and the scope of Enterprise Security Management Agent Systems Data Receive Security Policy is defined. Thus, TOE security objective O.ACCESS is satisfied.

FDP_ACF.1(2) Security attribute based access control (2)

This component ensures that Enterprise Security Management Agent Systems Data Receive Security Policy Rules for attribute-based access control are provided. Thus, TOE security objective O.ACCESS is satisfied.

FDP_ITC.1 Import of user data without security attributes

This component ensures that for SFP controlled User Data inflow from a TSC External System, proper Enterprise Security Management Agent Systems Data Receive Security Policy is applied. Thus, TOE security objective O.COLLECTINFO is satisfied.

FIA_AFL.1 Authentication failure handling

This component ensures that the admin's max number of failed authentication attempts is defined and the ability of take a countermeasure in case of reaching or exceeding this predefined limit. Thus, TOE security objective O.ID, O.AUTH is satisfied.

FIA_ATD.1(1)User attribute definition (1)

This component requires that external IT entities provide IP addresses as security attributes, which identify them and provide the basis for access control. Thus, Security objectives O.ID and O.ACCESS are satisfied.

FIA_ATD.1(2)User attribute definition (2)

This component requires that Admin Security Attributes of ID(ID) and User Security Attributes are maintained for Admin identification and as basis for access control. Thus, the Security objectives O.ID and O.ACCESS are satisfied.

FIA_UAU.2 User authentication before any action

This component ensures the capability to successfully authenticate Admin prior to any action and allow only authenticated Admin to manage TSF data. Thus, TOE security objective O.SECTSFD, O.AUTH is satisfied.

FIA_UAU.7 Protected authentication feedback

This component ensures that only designed authentication feedback is provided while authentication is in process. Thus, TOE security objective O.AUTH is satisfied.

FIA_UID.2(1) User identification before any action (1)

This component requires IP address identification of external IT entities, where the IP addresses provide the basis for their identification, audit data generation and access control. Thus, Security objective O.ID, and O.ACCESS are satisfied.

FIA_UID.2(2) User identification before any action (2)

This component ensures that ID is required of all Admin and that only those identified Admin that succeed in authentication are allowed to manage TSF data. Thus, Security objective O.SECTSFD and O.ID are satisfied.

FMT_MOF.1 Management security function action

This component ensures the Authorized Admin's ability to terminate or initiate security functions. Thus, TOE security objective O.MANAGE is satisfied.

FMT_MSA.1 Management of security attribute

This component ensures that only Authorized Admin has the access to security attributes as TSF data required for executing TOE security functions. Thus, TOE security objective O.MANAGE, O.SECTSFD is satisfied.

FMT_MSA.3 Static attribute initialization

This component ensures that only Authorized Admin has access to security attributes that are TSF data necessary to perform TOE security functions. Thus, TOE security objective O.MANAGE, O.SECTSFD is satisfied.

FMT_MTD.1(1) Management of TSF data (1)

This component ensures the Authorized Admin capability to manage Identification & Authentication Data, Management tasks, Event & Correlation Analysis Data. Thus, TOE security objective O.MANAGE, O.SECTSFD is satisfied.

FMT_MTD.1(2) Management of TSF data (2)

Commercial In Confidence

This component ensures the Authorized Admin capability to manage Event Compression Security Policy, Event Pattern Number, Event Pattern Initialization (Time, Interval), Event Screen Number, Master Info, Management Environment Configuration and Monitoring Screen Configuration. Thus, TOE security objective O.MANAGE, O.SECTSFD is satisfied.

FMT_MTD.1(3) Management of TSF data (3)

This component provides the Authorized Admin capability to manage Enterprise Security Management Agent Systems statistical reporting, Management System reporting, Correlation Analysis Results, History & Trend Reporting. Thus, TOE security objective O.MANAGE, O.SECTSFD is satisfied.

FMT_MTD.1(4) Management of TSF data (4)

This component provides the Authorized Admin capability to perform statistical processing of Security Equipment Log and Security Equipment Info. Thus, TOE security objective O.MANAGE, O.SECTSFD, O.STAT is satisfied.

FMT_MTD.2(1) Management limits on TSF data (1)

This component ensures availability of major TOE resources through authorized Admin control of storage capacity limit and countermeasures in the event of any limit excess. Thus, TOE security objective O.MANAGE is satisfied.

FMT_MTD.2(2) Management limits on TSF data (2)

This component ensures that authorized admin manages the integrity test interval limit so that proper actions are taken in the event of limit violation, thus ensuring major availability of TOE. Thus, TOE security objective O.MANAGE is satisfied.

FMT_SMF.1 Specification of Management Functions

This component requires that Admin functions are specified for TSF Security Attributes, TSF Data and Security Function. Thus, TOE security objective O.MANAGE is satisfied.

FMT_SMR.1 Security roles

This component requires that TOE Admin roles are limited to Authorized Admin roles. Thus, TOE security objective O.MANAGE, O.ID, O.AUTH is satisfied.

FPT_STM.1 Reliable time stamps

This component requires reliable time stamp function for TSF use and ensures that generated time stamps ensure sequential recording of Security Audit Events for audit data generation. Thus, TOE Security objective O.AUDIT is satisfied.

FPT_TST.1 TSF Testing

This component ensures self diagnosis for precise TSF operation and that Authorized Admin checks integrity of TSF data and TSF execution code. Thus, TOE security objective O.SECTSFD is satisfied.

Commercial In Confidence

7.4 Rationale for Security Requirements of IT Environment

The following describes rationale for security functional requirements for IT environment.

FDP_ITT.1 Basic internal transfer protection

This component ensures that data receive security policy is implemented when sending user data between TOE components via internal safe channels. Thus, TOE security objective OE.SECCH is satisfied.

FPT_AMT.1 Abstract machine testing

This component ensures a series of tests are performed by IT environment OS to show precise operation of TSF abstract machine. Thus, TOE security objective OE.SECTSF is satisfied.

FPT_ITT.1 Basic internal TSF data transfer protection

This component requires that a safe channel is formed to receive TSF data transfer between physically separated TOE components. Thus, TOE security objective OE.SECCH is satisfied.

Commercial In Confidence

7.5 Rationale for Assurance Requirements

This ST chose assurance requirements to satisfy EAL4. EAL4 provides sufficient assurance in the TOE security environment. Assurance means for satisfying EAL4 package requirements are described in the assurance documents referenced in 6.2 and each document is sufficient to satisfy the assurance requirements. For AGD_USR.1 Users' Manual Assurance Component, since there is no general user for TOE based on its characteristics, users' manual is not available. Thus, no assurance means for this component is provided here.

7.6 Rationale for SOF

This ST chooses SOF-medium, where threats are considered to have low level of professional knowledge, resources and motives. To counter threat sources having low level of attack success rate, SOF-basic has to be satisfied at minimum. Since this ST provides security functions of intermediate strength levels, this requirement is satisfied.

Commercial In Confidence

7.7 Rationale for TOE Summary Specification

This section describes whether TOE security functions and assurance methods are appropriate for TOE security requirements.

7.7.1 TOE Security Functions

Certain special TOE security functions must be performed together to satisfy a security requirement. Table 7-5 shows that TOE SFRs map to all security functions.

[Table 7-5] Mapping of SFRs to Security Functions

Security Function	Security Functional Requirement
Security Management (AT_ADMIN)	FMT_MOF.1
	FMT_MSA.1
	FMT_MSA.3
	FMT_MTD.1(1)
	FMT_MTD.1(2)
	FMT_MTD.1(3)
	FMT_MTD.1(4)
	FMT_MTD.2(1)
	FMT_MTD.2(2)
	FMT_SMF.1
	FMT_SMR.1
	FPT_ITT.1
Audit (AT_AUDIT)	FAU_ARP.1,
	FAU_GEN.1
	FAU_GEN.2
	FAU_SAA.1
	FAU_SAR.1
	FAU_SAR.3
	FAU_STG.1
	FAU_STG.3
	FAU_STG.4
	FPT_STM.1
User Data Protection (AT_UDP)	FDP_ACC.1(1)
	FDP_ACF.1(1)
	FDP_ACC.1(2)
	FDP_ACF.1(2)
	FDP_ITC.1
	FDP_ITT.1
Identification and Authentication (AT_INA)	FIA_AFL.1
	FIA_ATD.1(1)
	FIA_ATD.1(2)
	FIA_UAU.2
	FIA_UAU.7
	FIA_UID.2(1)
	FIA_UID.2(2)
Protection of Security Function (AT_PT)	FPT_ITT.1
	FPT_TST.1
	FPT_AMT.1

FMT_MOF.1- Management of security function action – TOE provides security management interfaces to Authorized Admin to stop or initiate configuration of various environment elements such as Event Compression and Correlation Analysis Security Policy. Thus, this function is satisfied. (AT_ADMIN)

FMT_MSA.1- Management of security attribute – TOE provides interface to manage security attributes to implement Access Control Policy and Enterprise Security Management Agent Systems Data Receive Security Policy. (AT_ADMIN)

FMT_MSA.3- Static attribute initialization – TOE ensures basic values are maintained for Security Management Access Control Policy and Security Control Target Systems Data Receive Security Policy. (AT_ADMIN)

FMT_MTD.1(1)-Management of TSF data(2) – TOE enables Authorized Admin to retrieve, create, edit and delete to manage Identification & Authentication Data, Management Tasks, Event Security Policy, Correlation Analysis Security Policy, Security Equipment Info Management and Code Management. (AT_ADMIN)

FMT_MTD.1(2)-Management of TSF data(3) – TOE enables Authorized Admin to retrieve and modify configuration values including Event Pattern Number, Event Pattern Initialization, Event Screen Number, TOE Time Stamp, Management Environment Configuration, Map Management Function, Disk Space and Integrity Test Frequency. (AT_ADMIN)

FMT_MTD.1(3)-Management of TSF data(4) – TOE enables Authorized Admin to retrieve/perform Event Monitoring, Event Search, Performance Monitoring, Correlation Analysis Monitoring, Correlation Analysis Search, Audit Info, Trend Report, Knowledge Management Info Search, Map Node Search and Event Pattern Monitoring. (AT_ADMIN)

FMT_MTD.1(4)-Management of TSF data(5) – TOE enables Authorized Admin to perform statistical processing of Security Equipment Log & Security Equipment Info from Enterprise Security Management Agent Systems. (AT_ADMIN)

FMT_MTD.2(1)- Management limits on TSF data (1)– TOE enables definition of audit storage capacity limit via security management interface. (AT_ADMIN)

FMT_MTD.2(2)- Management limits on TSF data (2)– TOE enables definition of time interval for integrity tests via security management interface. (AT_ADMIN)

FMT_SMR.1- Security roles – TOE can assign or add Admin privileges to Management Admin and Monitoring Admin. (AT_ADMIN)

FMT_SMF.1- Specification of Management Functions – TOE provides security management interface to Authorized Admin to perform TSF Function Management, TSF Security Attributes Management, TSF Data Management and TSF Data Limit Management. (AT_ADMIN)

FAU_ARP.1- Security alarm – TOE stops use of Admin account in case of authentication failures and takes a countermeasure configured by Authorized Admin in the event correlation analysis result reaches a threshold value. (AT_AUDIT)

FAU_GEN.1- Audit data generation – TOE generates audit data for Error, Warning, Notice and Manage for all events that occur within TOE. (AT_AUDIT)

FAU_GEN.2- User identity association – TOE can relate user ID and audit target events for all events

that occur within TOE. (AT_AUDIT)

FAU_SAA.1- Potential violation analysis – In the event of three consecutive generation of audit data per Admin authentication failures or abnormal action from correlation analysis, TOE categorizes such as security violations and take appropriate countermeasures. (AT_AUDIT)

FAU_SAR.1- Audit review – TOE allows Authorized Admin to receive security audit data via security management interface. (AT_AUDIT)

FAU_SAR.3- Select audit review – TOE allows Authorized Admin to retrieve desired audit data using various search conditions. (AT_AUDIT)

FAU_STG.1- Protected audit trail storage – TOE stores generated audit data to DBMS that is accessible only by Authorized Admin. (AT_AUDIT)

FAU_STG.3- Action in case of possible audit data loss – TOE displays available storage space to Authorized Admin and generates alarm as necessary. (AT_AUDIT)

FAU_STG.4- Prevention of audit data loss – TOE negates all services in case audit storage is saturated and sends a warning e-mail to Authorized Admin. (AT_AUDIT)

FDP_ACC.1(1)- Subset access control(1)– TOE implements Security Management Access Control Policy to negate access from any Admin without normal authentication status and security management requests that are not compliant with assigned privileges. (AT_UDP)

FDP_ACF.1(1)- Security attribute based access control (1)– TOE either negates or grants Admin access or request based on admin's authentication status and privilege when implementing Security Management Access Control Policy. (AT_UDP)

FDP_ACC.1(2)- Subset access control(2)– TOE controls access of external IT entities to TOE via Enterprise Security Management Agent Systems Data Receive Security Policy. (AT_UDP)

FDP_ACF.1(2)- Security attribute based access control (2)- TOE performs access control based on source IP address and protocol type of info transferred when implementing Enterprise Security Management Agent Systems Data Receive Security Policy. (AT_UDP)

FDP_ITC.1- Import of user data without security attributes – TOE applies Enterprise Security Management Agent Systems Data Receive Security Policy for transfer of Security Equipment Log, Security Equipment Info from external IT entities outside of TOE Management scope. (AT_UDP)

FDP_ITT.1- Basic internal transfer protection- TOE applies Enterprise Security Management Agent Systems Data Receive Security Policy for transfer of Security Equipment Log, Security Equipment Info received from external IT entities among TOE components. (AT_UDP)

FIA_AFL.1- Authentication failure handling – TOE sends an alarm to authorized Admin in case a specific Admin authentication fails three times or more. (AT_INA)

FIA_ATD.1(1)- User attribute definition (1)– TOE requires Authorized Admin to define security attributes of IT entities for implementing security policy on external IT entities. (AT_INA)

FIA_ATD.1(2)- User attribute definition (2)– TOE requires Authorized Admin to define and apply Admin security attributes for implementation of Admin based security policy. (AT_INA)

FIA_UAU.2– User authentication before any action – TOE applies security policy on authenticated Admin for admins that require authentication. (AT_INA)

FIA_UAU.7- Protected authentication feedback – TOE uses a special character for Admin password during Admin authentication to prevent password display on the Admin interface. (AT_INA)

FIA_UID.2(1)– User identification before any action (1)– TOE identifies IP address for IT identification prior to allowing the IT entity to use any TOE security function. (AT_INA)

FIA_UID.2(2)– User identification before any action (2)– TOE receives Admin ID prior to allowing an Admin to use TOE security function. (AT_INA)

FPT_ITT.1- Basic internal TSF data transfer protection– TOE implements SSL-based coded communication for communication between TOE internal components that are physically separated. (AT_ADMIN, AT_PT)

FPT_STM.1- Reliable time stamps– TOE allows an Authorized Admin to modify TOE time, which is uniformly applied to all TOE components. (AT_AUDIT)

FPT_AMT.1- Abstract machine testing– TOE checks TOE status periodically using functions provided by IT environment OS and performs restart-up in case of an abnormal condition. (AT_PT)

FPT_TST.1- TSF Testing – TOE performs integrity test on own execution binary files at start-up, during operation and based on Authorized Admin request and the results are displayed to Authorized Admin. (AT_PT)

Commercial In Confidence

7.7.2 TOE SOF Claims

SOF of this TOE is SOF-Medium as defined in CC Part 1, which is the level against attackers with low level attack success probability. Security functions of SOF application are Identification and Authentication, which utilize a permutation and probabilistic mechanism.

TOE is installed in an internal network that is connected to Enterprise Security Management Agent Systems. Attackers in this environment are assumed to have low level of professional knowledge, resources and motives and the probability of a threat source to find system vulnerability is low.

Commercial In Confidence

7.7.3 TOE Assurance Requirements

Table 7-6 provides methods of assurance verification for assurance requirements specified in 5.2.

[Table 7-6] Assurance Measure Compliance Table

Assurance Measure / Assurance Component ID	Configuration Management	Delivery Documentation	Installation guidance	Function Specification	High-level Design	Implementation	Low-Level Design	Analysis of Correspondence	Security Policy Model	Administrator guidance	Development Security	Life Cycle definition	Development Tool	Test Documentation	Misuse Analysis	Vulnerability Analysis	Strength of Function Analysis	**TOE to Test**
ACM_AUT.1	X																	
ACM_CAP.4	X																	
ACM_SCP.2	X																	
ADO_DEL.2		X																
ADO_IGS.1			X															
ADV_FSP.2				X														
ADV_HLD.2					X													
ADV_IMP.1						X												
ADV_LLD.1							X											
ADV_RCR.1								X										
ADV_SPM.1									X									
AGD_ADM.1										X								
ALC_DVS.1											X							
ALC_LCD.1												X						
ALC_TAT.1													X					
ATE_COV.2														X				
ATE_DPT.1														X				
ATE_FUN.1														X				
ATE_IND.2														X				X
AVA_MSU.2															X			
AVA_SOF.1																	X	
AVA_VLA.2																X		

ACM_AUT.1- Partial CM automation – TOE provides **Configuration Management** that provides the automated feature to allow only the permitted modifications occur in TOE implementation expressions and the automated TOE creation mechanism.

ACM_CAP.4- Generation support and acceptance procedures – TOE provides **Configuration Management** to ensure that proper control is implemented to prevent unauthorized modifications and appropriate functionality and usage of the configuration management system.

ACM_SCP.2- Problem tracking CM coverage – TOE provides **Configuration Management** to ensure that all configuration items are modified in accordance with controlled methods with appropriate authorization process.

ADO_DEL.2- Detection of modification – TOE provides **Delivery Documentation** where system control, distribution facility and process ensure data sent by a sensor is sent without being modified.

ADO_IGS.1- Installation, generation, and start-up procedures – TOE provides **Installation Guidance** to ensure that TOE is installed, created and operated in a safe manner intended by the developer.

ADV_FSP.2- Fully defined external interfaces – TOE provides **Functional Specification** to define all external interfaces and to implement basic descriptions of interfaces visible to TSF users and actions as well as TOE security functional requirements.

ADV_HLD.2- Security enforcing high-level design – TOE provides **High-Level Design** to describe TSF in terms of major components (subsystems), describe their functions and relationships, and ensures TOE architecture is appropriate for implementing the TOE security functional requirements.

ADV_IMP.1- Subset of the implementation of the TSF – TOE provides **Implementation Representation** to ensure identification of detailed actions of TSF and to facilitate their analysis.

ADV_LLD.1- Descriptive low-level design – TOE provides **Low-Level Design** to describe TSF internal actions, mutual relationships and dependencies between modules and to ensure that TSF subsystems are accurately and effectively detailed.

ADV_RCR.1- Informal correspondence demonstration – TOE provides **Analysis of Correspondence** to ensure consistency of diverse expressions of TSF (descriptions of TOE Summary Specification, Functional Specification, Basic Design, Detailed Design and Implementation).

ADV_SPM.1- Informal TOE security policy model – TOE provides **Security Policy Model** to describe rules and characteristics of all TSP policies and to ensure consistency and completeness of all policies.

AGD_ADM.1- Administrator guidance – TOE provides **Administrator Guidance** as an documentation for use by those responsible for configuration, maintenance and management of TOE in precise ways to maximize TOE security.

ALC_DVS.1- Identification of security measures – TOE provides **Development Security** to protect TOE by utilizing physical, procedural, human and other security measures for development environment.

ALC_LCD.1- Developer defined life-cycle model – TOE provides **Life Cycle Definition Document** to ensure controls necessary for development and maintenance of models.

ALC_TAT.1- Well-defined development tools – TOE provides **Development Tool Document** to ensure that wrongly defined, inconsistent or inaccurate development tools are not used for TOE development.

ATE_COV.2- Analysis of coverage – TOE provides **Test Documentation** to ensure that TSF is tested systematically according to function specification.

ATE_DPT.1- Testing: high-level design – TOE provides **Test Documentation** to ensure that TSF subsystems are implemented correctly.

ATE_FUN.1- Functional testing – TOE provides **Test Documentation** to ensure that all security functions are executed according to their specifications.

ATE_IND.2- Independent testing - sample – TOE provides **Test Documentation & TOE for Testing** to ensure that security functions are performed according to their specifications.

AVA_MSU.2- Validation of analysis – TOE provides **Misuse Analysis** to ensure that system documentation does not contain any errors, inconsistencies or conflicting guidelines and that all operating modes are based on safe procedures.

AVA_SOF.1- Strength of TOE security function evaluation – TOE provides **Strength of Function Analysis** to determine the quantitative or statistical analysis results on security actions of sub-security mechanisms and the strength of security actions to overcome the problems.

AVA_VLA.2- Independent vulnerability analysis – TOE provides **Vulnerability Analysis** to ensure that certain security vulnerabilities exist and that such vulnerabilities cannot be misutilized within the intended environment of TOE.

Commercial In Confidence

7.8 Rationale for SFR Dependencies

Security functional requirements used in this SF satisfy the dependencies of Table 7-7 and there are no components that do not satisfy dependencies.

[Table 7-7] Satisfaction of Dependency of SFR Security Functional Requirements

No.	Functional Component ID	Dependency (ies)	Reference Number
1	FAU_ARP.1	FAU_SAA.1	4
2	FAU_GEN.1	FPT_STM.1	34
3	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	2 19, 20 (Select FIA_UID.2 as upper dependency)
4	FAU_SAA.1	FAU_GEN.1	2
5	FAU_SAR.1	FAU_GEN.1	2
6	FAU_SAR.3	FAU_SAR.1	5
7	FAU_STG.1	FAU_GEN.1	2
8	FAU_STG.3	FAU_STG.1	7
9	FAU_STG.4	FAU_STG.1	7
10	FDP_ACC.1	FDP_ACF.1	11
11	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	10 23
12	FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	10 23
13	FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	10
14	FIA_AFL.1	FIA_UAU.1	17 (Select FIA_UAU.2 as upper dependency)
15	FIA_ATD.1(1)	-	-
16	FIA_ATD.1(2)	-	-
17	FIA_UAU.2	FIA_UID.1	19 (Select FIA_UID.2 as upper dependency)
18	FIA_UAU.7	FIA_UAU.1	17 (Select FIA_UAU.2 as upper dependency)
19	FIA_UID.2(1)	-	-
20	FIA_UID.2(2)	-	-
21	FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	31 30
22	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	10 31 30
23	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	22 31
24	FMT_MTD.1(1)	FMT_SMF.1 FMT_SMR.1	30 31
25	FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	30 31
26	FMT_MTD.1(3)	FMT_SMF.1 FMT_SMR.1	30 31
27	FMT_MTD.1(4)	FMT_SMF.1	30

		FMT_SMR.1	31
28	FMT_MTD.2(1)	FMT_MTD.1 FMT_SMR.1	24, 25, 26, 27 31
29	FMT_MTD.2(2)	FMT_MTD.1 FMT_SMR.1	24, 25, 26, 27 31
30	FMT_SMF.1	-	-
31	FMT_SMR.1	FIA_UID.1	20 (Select FIA_UID.2 as upper dependency)
32	FPT_AMT.1	-	-
33	FPT_ITT.1	-	-
34	FPT_STM.1	-	-
35	FPT_TST.1	FPT_AMT.1	32

Commercial In Confidence

REFERENCES

[1] CC V2.3
[2] Configuration Management CMP-TSM-v30.doc Version 1.2
[3] Delivery Documentation DEL-TSM-v40.doc Version 1.2
[4] Function Specification FSP-TSM-v40.doc Version 1.7
[5] High-level Design HLD-TSM-v40.doc Version 1.2
[6] Low-Level Design LLD-TSM-v40.doc Version 1.2
[7] Implementation Representation IMP-TSM-v40.doc Version 1.1
[8] Security Policy Model SPM-TSM-v40.doc Version 1.4
[9] Analysis of Correspondence RCR-TSM-v40.doc Version 1.1
[10] Administrator guidance ADM-Admin-TSM-v40.doc Version 1.4
[11] Installation guidance IGS-TSM-v40.doc Version 1.6
[12] Test Documentation TST-K1-v40.doc Version 1.3
[13] Development Security DVS-K1-v40.doc Version 1.2
[14] Life Cycle definition Document LCD-K1-v40.doc Version 1.2
[15] Development Tool Document TAT-K1-v40.doc Version 1.2
[16] Misuse Analysis MSU-K1-v40.doc Version 1.3
[17] Strength of Function Analysis SOF-K1-v40.doc Version 1.3
[18] Vulnerability Analysis VLA-K1-v40.doc Version 1.2

Commercial In Confidence