Kaseya International Limited
Virtual System Administrator v6.2.1.0

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 1.1

Prepared for:

Kaseya International Limited
Avenue de Gratta-Paille 2
CP 476
CH - 1000 Lausanne 30
Switzerland

Phone: +41 21 641 55 60
Email: sales@kaseya.com
http://www.kaseya.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the Kaseya Virtual System Administrator v6.2.1.0, and will hereafter be referred to as the TOE or VSA throughout this document. The TOE is a software only IT[1] Systems Management system. It provides IT managers with the capability to monitor, manage, and maintain distributed IT networks. VSA provides the capability to automate tasks such as asset management, patch management, checking for network vulnerabilities, and updating software.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 - ST and TOE References

ST Title	Kaseya International Limited Virtual System Administrator v6.2.1.0 Security Target
ST Version	Version 1.1
ST Author	Corsec Security, Inc.
ST Publication Date	11/4/2011
TOE Reference	Virtual System Administrator v6.2.1.0
FIPS 140-2 status	Level 1, Validated crypto module

[1] IT = Information Technology

ST Title	Kaseya International Limited Virtual System Administrator v6.2.1.0 Security Target
Keywords	IT Systems Management, Asset Management, Security Management, Network Management, Patch Management, Software Updates, Network Vulnerabilities

1.3 Product Overview

The Kaseya Virtual System Administrator provides IT managers with the capability to monitor, manage, and maintain distributed IT networks. VSA automates tasks such as asset management, patch management, checking for network vulnerabilities, and updating software. The current number of managed devices supported is approximately 20,000 per Kaseya Server. Customers can scale the deployment of the TOE to their environment by adding more Kaseya Servers.

VSA allows IT managers to perform all these functions using a browser-based web GUI[2]. This Administrator Console can be any computer with a web browser that has access to the local network for VSA. This allows administrators to configure and monitor the product from a computer on the local or remote network.

VSA includes the following product features:

- Agent Technology
- Monitoring
- Ticketing
- Patch Management
- Audit and Inventory
- Remote Access
- Info Center

The VSA is a software solution architected with both a client and server component. The Agent is installed on all the managed devices in an IT infrastructure. The Kaseya Agent component can be installed on servers, desktops, and laptops of various operating systems such as Windows, Macintosh OSX and Linux. The Kaseya Server component can be installed on Windows 2003 or 2008 Server.

[2] GUI = Graphical User Interface

Table 2 below specifies the minimum system requirements for the major components of VSA.

Table 2 – VSA Minimum Requirements

Component	Type	Requirement
Kaseya Server	Operating System	Microsoft Windows : • Server 2003 or 2008
	Hardware	Single processor (1.0 Ghz,160 Mhz[3] front side bus, 1 MB[4] cache)
		3 GB RAM[5]
		40 GB hard drive
		100 Mbps Network Interface Card (NIC)
		DSL[6] or Cable modem connection
	Third Party Software	Microsoft SQL: • SQL Server 2005 or 2008, or • SQL 2005 or 2008 Express Edition with Advanced Services Other: • Microsoft Internet Information Server (IIS) version 5.1 or greater • Microsoft Message Queuing (MSMQ) • Microsoft .NET Framework 2.0 • Microsoft .NET Framework 3.5 • Microsoft SQL Reporting Services
	Configuration	Open ports - configurable: • Web UI: TCP port 80 or 443 inbound and outbound • Email Notifications: TCP port 25 outbound • Agent connections: TCP port 5721 inbound • Live Connect: UDP port 5721 inbound and outbound
Kaseya Agent	Operating System	• Microsoft Windows 98, Me, NT, 2000, XP, 2003, Vista, 2008, 7 • Apple Macintosh OSX version 10.3.9 or above • Linux
	Hardware	• 333 MHz CPU[7] or greater • 128 MB of RAM • 30 MB of free disk space • Network Interface Card (NIC) or modem
	Configuration	• TCP/IP[8] Outbound Port 5721 • No Inbound Ports
Administrator Console	Third Party Software	Internet Explorer 8.0 or greater must have cookies and JavaScript enabled

[3] MHz = megahertz
[4] MB = Megabyte
[5] RAM =Random Access Memory
[6] DSL = Digital Subscriber Line
[7] CPU = Central Processing Unit
[8] TCP/IP = Transmission Control Protocol/Internet Protocol

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The VSA is a software solution architected with both a client and server component. In the evaluated configuration, the Kaseya Agent component will be installed on a Windows XP host. The Kaseya Server component will be installed on a Windows 2003 Server.

Figure 1 shows a simple sample network deployment of the Kaseya Server and Kaseya Agents.

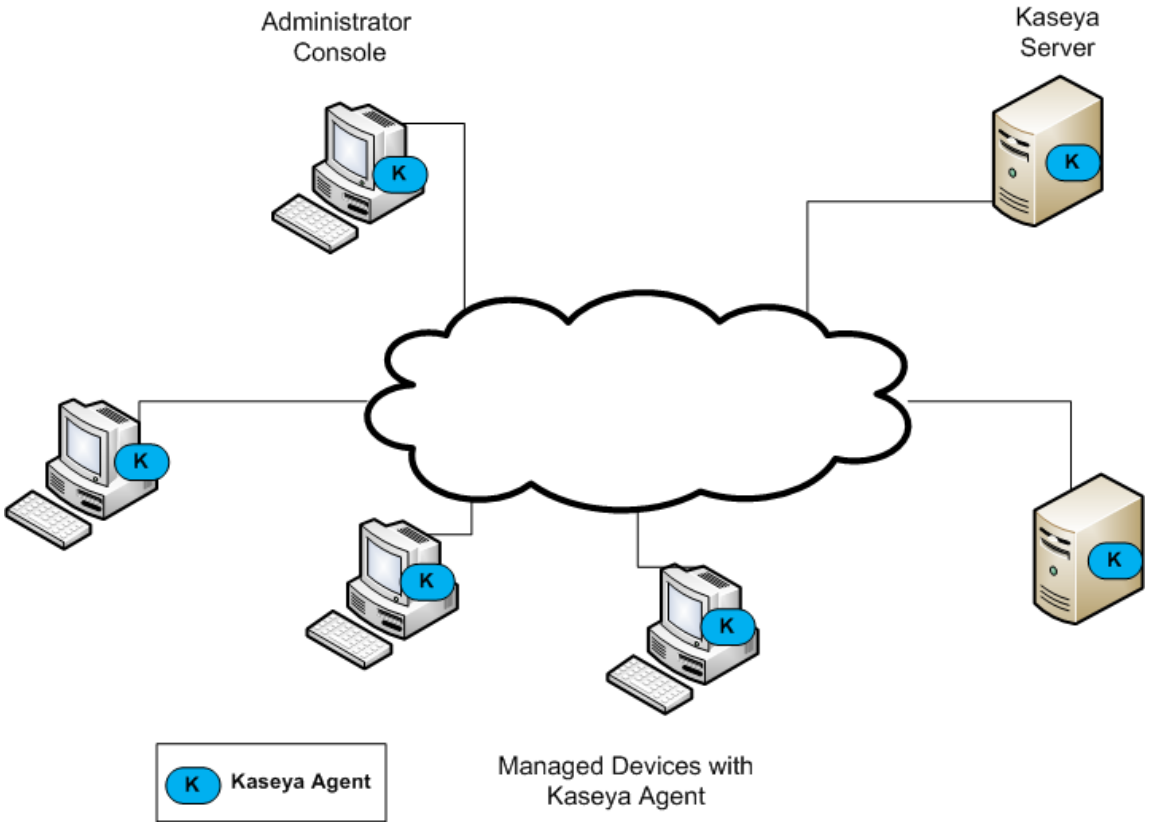

Figure 1 - Deployment Configuration of the TOE

The KaseyaAgent collects the following information from the managed devices:

- Machine hardware information
- All installed software
- System Information
- Current network settings
- Scan information from the local area network
- SNMP information

All of this information is sent to the KaseyaServer and stored in the third party relational database (RDBMS). This information can be used for asset management, network management, and vulnerability management. VSA Administrators can inventory all assets as well as apply software patches automatically. Policies are set through the VSA Administrator Console.

1.4.1 KaseyaVSA Components of the TOE

KaseyaVSA is an IT Systems Management system that is comprised of the KaseyaAgents and Kaseya Server with a web-based Administrator Console.

1.4.1.1 Kaseya Agents

VSA manages machines by installing a software client called the KaseyaAgent on a managed device. The KaseyaAgent will also be referred to as "Agent" throughout this document. The Kaseya Agent is a system service or a daemon that does not require the user to be logged on for the Agent to function and does not require a reboot for the Agent to be installed. The Agent is configurable and can be totally invisible to the end user.

The Kaseya Agents are software applications installed on managed devices. Agents are the components which enact the machine management activities driven by Kaseya Server activities. All Agent activities are driven by policies or requested tasks generated on the Virtual System Administrator Server. However, the Agent must first connect to the Kaseya Server. The Kaseya Server component acting solely as a server will never initiate a connection to the Agent.

1.4.1.2 Kaseya Server

The Kaseya Server contains the majority of the Kaseya-developed logic and functionality to provide the VSA services. The Kaseya Server performs the authentication for all administrators and ensures that all automated tasks that have been scheduled by administrators are performed. The Kaseya Server accepts configuration information and instructions via the web-based Administrator Console to change policies or settings on managed devices as well as instructions to perform scans on the managed devices. In addition to the Administrator Console, the VSA also has an API[9] that allows third party application integration. The API exposes the majority of the actions and functionality available from the web GUI.

The Kaseya Server uses proprietary cryptographic software to provide protection of data transfer between the Kaseya Server and the Agents.

The Microsoft SQL[10] database is the data repository for IT policies, collected information about the IT network, and VSA configuration information.

1.4.2 TOE Environment

It is assumed that there will be no untrusted users or software on the Kaseya Server host. The Kaseya Server relies upon the IT environment to provide protection of data transfer between the Administrator web-based GUI and the Kaseya Server TOE components. Third party SSL is used for a trusted communication path between the Administrator web-based GUI and the Kaseya Server. The Kaseya Server relies on a Web Server to provide web services. Third party software such as WinVNC, pcAnywhere™ (Symantec), RAdmin (Famatech), or Terminal Server (Microsoft) used for the remote control capabilities are considered outside the TOE Boundary.

The Kaseya Server relies upon the underlying operating system (OS) and hardware platform to provide protection and execution of the TOE software, disk storage, and reliable timestamps. A listing of third party software relied upon by the Kaseya Server is given in Table 3.

[9] API = Application Programming Interface
[10] SQL = Structured Query Language

The Kaseya Server is intended to be deployed in a physically secured cabinet, room, or data center with the appropriate level of physical access control and physical protection (e.g. badge access, fire control, locks, alarms, etc.).

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

The TOE includes the following software only components:

- Kaseya Server v6.2.1.0
- Kaseya Agent v6.2.1.0

The evaluated configuration includes the following:

- Kaseya Server v6.2.1.0 installed on a Windows Server 2003 host and is compliant to the minimum software and hardware requirements as listed in Table 2.
- Kaseya Agent v6.2.1.0 installed on a Windows XP host and is compliant to the minimum software and hardware requirements as listed in Table 2.
- Administrator Console with a web browser compliant to the minimum software requirements as listed in Table 2.

Figure 2 below provides a diagram of the TOE and the TOE Environment:

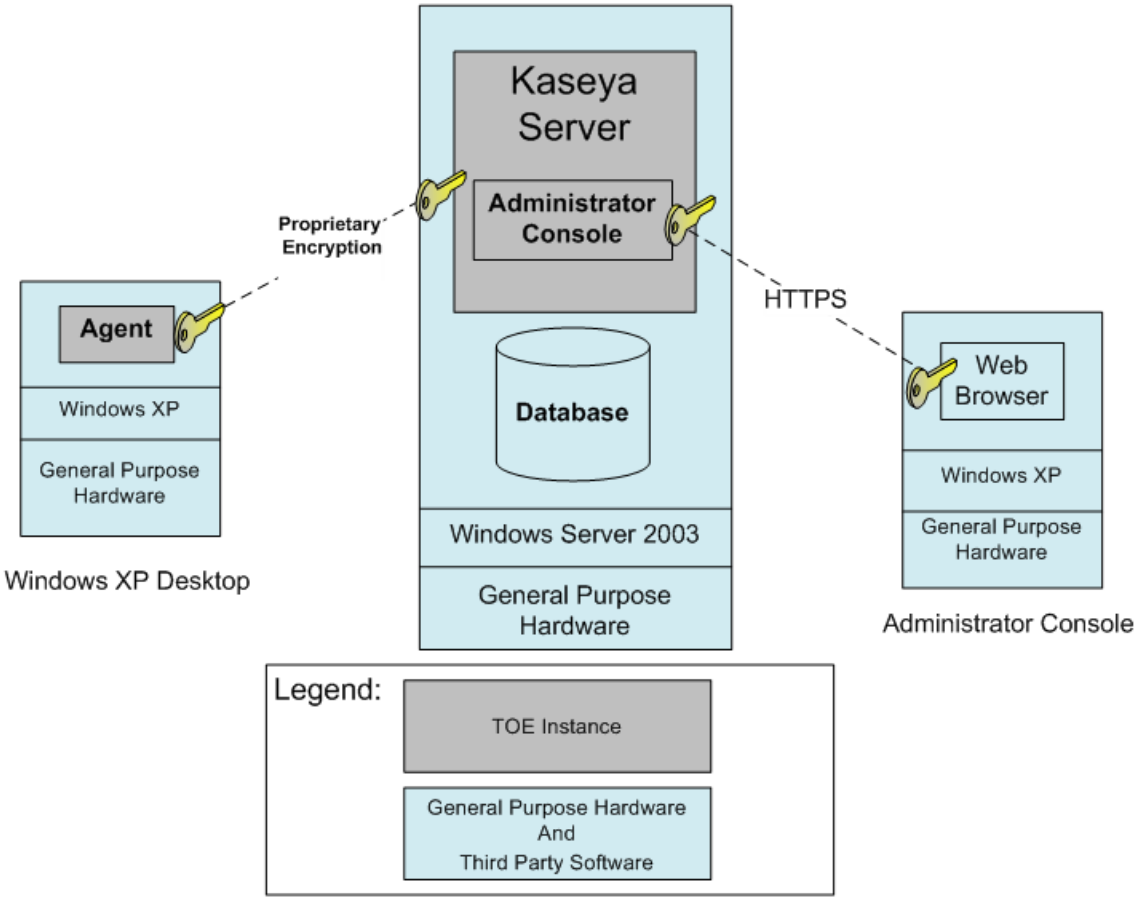

Figure 2 - TOE and TOE Environment[11]

The TOE Boundary includes all the Kaseya-developed parts of the VSA product. The TOE Boundary specifically does not include any of the third party software that the TOE relies upon as described in section 1.4.2 of the ST and Table 3 below. The TOE Boundary also does not include the third party SQL database that stores collected data about the managed devices. This boundary enables Kaseya to respond to Requests for Proposals (RFPs) by stating that the Kaseya-built components of the system have been Common Criteria validated. One of the primary reasons Microsoft IIS is excluded from the evaluation is because it provides SSL functionality that does not have a FIPS 140-2 validation. For remote administrator sessions, the TOE relies on third party software using SSL[12] to secure the communications channel between the browser and Kaseya Server.

Ksubscribers is the Kaseya Server SQL schema and SQL Reporting Services is used to produce reports. Since these are integrated into the SQL database, they are considered outside the TOE Boundary. In addition, the API interface will be outside the TOE Boundary.

[11] XP = Windows XP Operating System
[12] SSL = Secure Sockets Layer

Table 3 below indicates the elements of the product that are included in the TOE boundary and TOE Environment.

Table 3 – Components of the TOE and TOE Environment

Component	TOE	TOE Environment
Kaseya Server Software v6.2.1.0	✓	
Kaseya Agent v6.2.1.0	✓	
Microsoft IIS[13]		✓
Microsoft .NET Framework		✓
Microsoft Message Queuing (MSMQ)		✓
Microsoft SQL Database		✓
Microsoft SQL Reporting Services		✓
Microsoft Terminal Server		✓
Kaseya Server Hardware and operating system		✓
Kaseya Agents Hardware and operating systems		✓
WinVNC		✓
pcAnywhere™		✓
Famatech Radmin		✓

1.5.1.1 Guidance Documentation

The following guides are required reading and part of the TOE:

- Kaseya Virtual System Administrator Online User Assistance [VSA Onl]

1.5.2 Logical Scope

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- FAU Security Audit
- FCS Cryptographic Support
- FIA Identification and Authentication
- FMT Security Management
- FPT Protection of the TSF
- SMS Systems Management System

1.5.2.1 Security Audit

The Kaseya Server component generates audit records for the actions of the Kaseya Server.

From the Kaseya Server component's Administrator Console, an authorized administrator can read the event audit data generated by the Kaseya Server.

[13] IIS = Internet Information Services

1.5.2.2 Cryptographic Support

The TOE uses proprietary encryption for securing the user and TSF data transmitted between the Kaseya Server and Agents.

1.5.2.3 Identification and Authentication

The Kaseya Server provides functionality to allow administrators to verify their claimed identity. The Identification and Authentication TSF ensures that only legitimate administrators can gain access to the configuration settings and management settings of the TOE. Administrators must log in with a valid user name and password before the Kaseya Server will permit the administrators to manage the TOE.

1.5.2.4 Security Management

The Kaseya Server provides a set of commands for administrators to manage the security functions, configuration, and other features of the Kaseya Server and Agents. The Security Management function specifies Master and custom user roles for the Kaseya Server. The Master user role is a super user role that has access to all functions. The Master user can create custom user roles with a specified scope and access permissions to the TOE Management functions.

1.5.2.5 Protection of the TSF

The Kaseya Server protects its programs and data from unauthorized access through its own interfaces. The TSF secures all communications between the Kaseya Server and Agents with proprietary encryption.

1.5.2.6 Systems Management System

The Agents collect information from managed devices. This information includes machine hardware, software, system, and network information. Alarms can be programmed in the Administrator Console based on the collected information. .

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

Most features and functionality of the Kaseya Virtual System Administrator v6.2.1.0 are part of the evaluated configuration of the TOE. The only exception is that the API interface will not be included in the TOE.

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 4 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations from the CEM as of 2010/07/13 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with ALC_FLR.2

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat Agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the user and TSF data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. The following threats are applicable:

Table 5 - Threats

Name	Description
T.ACCOUNT	The security relevant actions of users may go undetected.
T.UNAUTH	An unauthorized user may attempt to disclose, remove, destroy, or compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.EXPLOIT	An attacker may attempt to gain unauthorized access to the resources of the managed devices, by exploiting vulnerabilities on a managed device.
T.SELPRO	An unauthorized user may read, modify, or corrupt security critical TOE configuration data while in transit between the Agent and Server.
T.SPOOF	A hostile entity masquerading as the Server component may receive TSF data from an authorized agent that incorrectly thinks it is communicating with an authorized Server component.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs defined for this ST.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 - Assumptions

Name	Description
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.PROTECT	The components of the TOE critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 7 - Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.
O.AUDIT	The TOE must provide the means of recording any security relevant events, so as to assist an administrator in the detection of potential attacks or misconfiguration of TOE security features as well as hold administrator users accountable for any actions they perform regarding the configuration of TOE Security functions.
O.AUTHEN	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.CRYPTO	The TOE will provide encryption/decryption of all Agent communications with the TOE Server component.
O.ROBUST	The TOE must secure all critical security data so that it is protected from unauthorized disclosure and modification while in transit between the Agent and Server.
O.SCAN	The TOE must be able to collect information from the managed devices and send alerts based on programmable alarms.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 8 - IT Security Objectives

Name	Description
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.

4.2.2 Non-IT Security Objectives

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

Table 9 - Non-IT Security Objectives

Name	Description
OE.MANAGE	Those responsible for the TOE must be competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
OE.PROTECT	Those responsible for the TOE must ensure that the physical environment must be suitable for supporting a computing device in a secure setting.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 10 identifies all extended SFRs implemented by the TOE. The rationale for these extended components is described in Section 8.3.

Table 10 - Extended TOE Security Functional Requirements

Name	Description
EXT_SMS_ARP.1	Security alarms
EXT_SMS_SDC.1	System data collection

5.1.1 Class SMS: Systems Management System function

Systems Management functions involve collecting information from managed devices as well as sending alerts based on programmable alarms. The EXT_SMS: Systems Management function class was modeled after the CC FAU: Security audit class. The extended family and related components for EXT_SMS_SDC: System data collection was modeled after the CC family and related components for FAU_GEN: Security audit data generation. The extended family EXT_SMS_ARP: Security alarms was modeled after the CC family FAU_ARP: Security alarms.

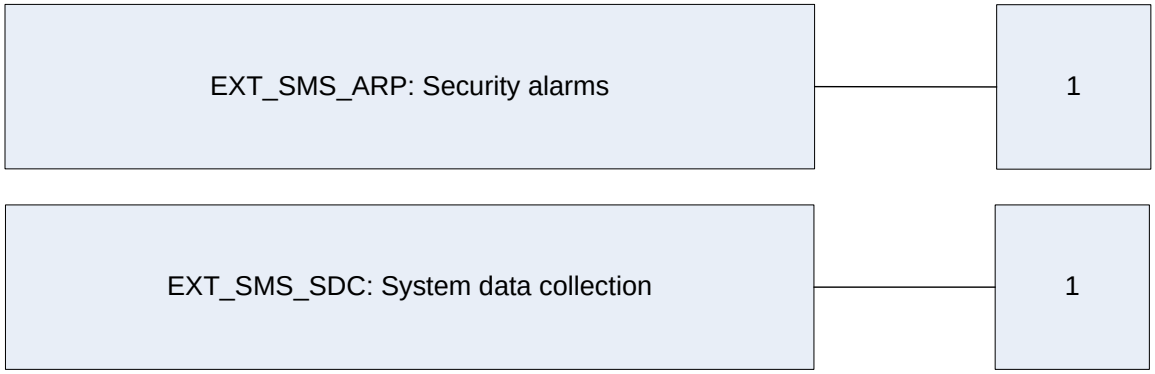

Figure 3 - EXT_SMS: Systems Management System Function Class Decomposition

5.1.1.1 Security alarms (EXT_SMS_ARP)

Family Behaviour

This family defines the requirements for the response to be taken in case of a detected system data change or policy enforcement.

Component Leveling

Figure 4 - Security alarms family decomposition

EXT_SMS_ARP.1 Security alarms, the TSF shall take actions in case a detected system data change or policy enforcement.

Management: EXT_SMS_ARP.1

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

a) the management (addition, removal, or modification) of alarm.

Audit: EXT_SMS_ARP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Actions taken due to a detected system data change or policy enforcement.

[EXT_SMS_ARP.1 Security alarms]
Hierarchical to: No other components
EXT_ SMS_ARP.1.1
The TSF shall take [*assignment: list of actions*] upon the trigger of a programmable alarm.
Dependencies: [EXT_SMS_SDC.1 System data collection]

5.1.1.2 System data collection (EXT_SMS_SDC)]

Family Behaviour

This family defines the requirements for recording the occurrence of Systems Management System events that take place under TSF control. This family identifies the level of system data collection, enumerates the types of events that shall be collected by the TSF, and identifies the minimum set of SMS-related information that should be provided within various SMS record types.

Component Leveling

Figure 5 - System data collection family decomposition

EXT_SMS_SDC.1 System data collection, defines the level of SMS events, and specifies the list of data that shall be recorded in each record.

Management: EXT_SMS_SDC.1

a) There are no auditable events foreseen.

Audit: EXT_SMS_SDC.1

b) There are no auditable events foreseen.

EXT_SMS_SDC.1 System data collection
Hierarchical to: No other components
EXT_SMS_SDC.1.1
The TSF shall be able to collect the following information from the managed device(s): [assignment: *specifically defined events*.]

EXT_SMS_SDC.1.2
At a minimum, the TSF shall collect and record the following information:
- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

Dependencies: No dependencies

5.2 Extended TOE Security Assurance Components

There are no extended TOE Security Assurance Components.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

6.1.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 11 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 11 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_GEN.2	User identity association				
FAU_SAR.1	Audit review		✓		
FAU_SAR.2	Restricted audit review				
FCS_CKM.1	Cryptographic key generation				
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
FIA_UAU.5	Multiple authentication mechanisms		✓		
FIA_UID.2	User identification before any action				
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_ITT.1	Basic internal TSF data transfer protection	✓			
EXT_SMS_ARP.1	Security alarms		✓		

Name	Description	S	A	R	I
EXT_SMS_SDC.1	System data collection		✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation
Hierarchical to: No other components.
FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events, for the [not specified] level of audit; and
c) [*the specifically defined auditable events as listed in the 'Auditable Events' column of Table 12*].

Table 12 - Auditable Events

Server
VSA user login attempts (success and failure)
Administrative actions performed as operations on TSF Data as described in Table 16
Agent
all alarms triggered for the selected machine
alarm conditions that have occurred and the corresponding actions taken in response
Agent and system error messages
VSA settings changes for the selected machine
Agent configuration changes
send/receive data for network applications
successful/failed Agent procedures
successful/failed remote control sessions
windows events
syslog events

FAU_GEN.1.2

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [none].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association
Hierarchical to: No other components.
FAU_GEN.2.1

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

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

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*the authorized users as listed in the 'Authorized User' column of Table 13*] with the capability to read [*the list of audit information as listed in the 'Audit Information' column of Table 13*] from the audit records.

Table 13 - Audit Review

Authorized User	Audit Information
Master User	All logging of application activity on the application server.
VSA Administrator	All logging on the application server.

FAU_SAR.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

FAU_SAR.2.1

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Dependencies: FAU_SAR.1 Audit review

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*the cryptographic key generation algorithm as listed in the 'Key Generation Algorithm' column of Table 14*] and specified cryptographic key sizes [*listed in the 'Cryptographic Key Size' column of Table 14*] that meet the following: [*standards listed in the 'Standards' column of Table 14*].

Table 14- Cryptographic Key Generation Standards

Key Generation Algorithm	Cryptographic Key Size	Standards
AES	All key sizes specified in the Key Sizes (bits) column of Table 14 below.	FIPS-197 for AES

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components.
FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2 Level 1*].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
FCS_COP.1.1

The TSF shall perform [assignment *cryptographic operations listed in the 'Cryptographic Operations' column of Table 15*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms listed in the 'Cryptographic Algorithm' column of Table 15*] and cryptographic key sizes [*listed in the 'Key Sizes (bits)' column of Table 15*] that meet the following: [*the list of standards in the 'Standards' column of Table 15*].

Table 15 - Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards
Symmetric encryption and decryption	AES	256	FIPS-197 , FIPS 140-2 Level 1
Message Digest	SHA[14]	256	FIPS 180-2, FIPS 140-2 Level 1

[14] SHA = Secure Hash Algorithm

Dependencies: **[FDP_ITC.1 Import of user data without security attributes, or**
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

6.2.3 Class FIA: Identification and Authentication

FIA_UAU.5 Multiple authentication mechanisms
Hierarchical to: No other components.
FIA_UAU.5.1
The TSF shall provide [*password and domain authentication*] to support user authentication.
FIA_UAU.5.2
The TSF shall authenticate any user's claimed identity according to the [*following multiple authentication mechanism rules:*
- *VSA users are authenticated by the TSF using a password based authentication mechanism when the Kaseya Server is configured to use a VSA logon password.*
- *VSA users are authenticated by the Windows domain logon password when the VSA Server is configured to use the Windows domain logon.*

].
Dependencies: **No dependencies**

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
FIA_UID.2.1
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: **No dependencies**

6.2.4 Class FMT: Security Management

FMT_MTD.1 Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1

The TSF shall restrict the ability to [query, modify, delete, clear, [*and other operations as defined in column 'Operation' of Table 16*]] the [*TSF data as defined in column 'TSF Data' of Table 16*] to [*the authorized identified roles as defined in column 'Authorized Role' of Table 16*].

Table 16 - Management of TSF Data

Operation	TSF Data	Authorized Role
Server		
configure	preferences	Master User granted permission
set	VSA logon User ID and password	Master User granted permission
set	check-in control	Master User granted permission
set	naming policy	Master User granted permission
enable/disable, logoff	user logons	Master User granted permission
query, add, edit or delete	all scope data objects: organizations, machine groups, machines, departments, and service desks	Master User with Master Scope
query, add, edit or delete	User	Master User granted permission
query, add, edit or delete	Master User	Master User
query, modify, set	Scope	Master User granted permission
view, add, edit or delete	group	Master User granted permission
query, modify, create, set	Role	Master User granted permission
Import/export	Agent Procedures, Monitor Sets, Monitor SNMP Sets, Patch Policies	Master User granted permission
Agent		
configure	log history - number of days to store log data	Master User granted permission
query, create, edit,	machine ID[15] accounts	Master User granted permission

[15] Machine ID = Account name for a managed machine in the VSA database.

Operation	TSF Data	Authorized Role
delete, rename		
create	install packages for installing Agents on single machines	Master User granted permission
reassign to	different machine group or subgroup	Master User granted permission
suspend	all Agent operations	Master User granted permission
configure	check-in control	Master User granted permission
configure	portal access	Master User granted permission
configure	set credential	Master User granted permission
schedule, create	Agent procedures	Master User granted permission
import, export	machine ID account settings	Master User granted permission
configure, download, update	security and patch content	Master User granted permission

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components.
FMT_SMF.1.1
The TSF shall be capable of performing the following management functions: [*management of security function behaviour, management of security attributes*].
Dependencies: No Dependencies

FMT_SMR.1 Security roles
Hierarchical to: No other components.
FMT_SMR.1.1
The TSF shall maintain the roles [*see authorised identified roles as described in Table 17 below*].

Table 17 - Authorized Identified Roles

Type	Role
User Role	End User
	Master User
	Custom
Machine Role	Default
	Custom

FMT_SMR.1.2
The TSF shall be able to associate users with roles.
Dependencies: FIA_UID.1 Timing of identification

6.2.5 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection
Hierarchical to: No other components.
FPT_ITT.1.1
The TSF shall protect TSF data from [*disclosure or modification*] when it is transmitted between separate ~~parts~~ **instances** of the TOE.
Dependencies: No dependencies

6.2.6 Class SMS: Systems Management System

EXT_SMS_ARP.1 Security alarms
Hierarchical to: No other components
EXT_ SMS_ARP.1.1
The TSF shall take [*action to send a notification via e-mail, execute configured procedures, and create job tickets*] upon the trigger of a programmable alarm.
Dependencies: EXT_SMS_SDC.1 System data collection

EXT_SMS_SDC.1 System data collection
Hierarchical to: No other components
EXT_SMS_SDC.1.1
The TSF shall be able to collect the following information from the managed device(s): [
- *All hardware information*
- *All installed software*
- *System Information*
- *Current network settings*
- *Scan information from the local area network*
- *SNMP information*]

EXT_SMS_SDC.1.2
At a minimum, the TSF shall collect and record the following information:
- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

Dependencies: No dependencies

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 18 summarizes the requirements.

Table 18 - Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 19 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Identification and Authentication	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.2	User identification before any action
Security Management	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
Systems Management System	EXT_SMS_ARP.1	Security alarms
	EXT_SMS_SDC.1	System data collection

7.1.1 Security Audit

The Security Audit function provides the TOE with the functionality of generating and viewing audit records. As administrators manage and configure the TOE, their activities are tracked and recorded as audit records in log files.

7.1.1.1 Kaseya Server Security Audit

The Kaseya Server creates multiple log files that tracks all administrator actions. In addition, the Kaseya Server does application logging which logs the activity of all application activity on the application server.

The **System Log** page logs events that cannot be tracked by machine ID, for a specified time period. The System Log is viewable through the Administrator Console. This log is available to VSA Administrators that have the access rights to view the System Log. This log captures events not contained in any of the Agent logs. Examples include:

- Deleting machine IDs
- Failed and successful logon attempts
- Video streaming sessions
- Starting/stopping of the Kaseya Server
- Deleting trouble tickets assigned to a group (not a machine)

The **Application Logging** page controls the logging of application activity on the application server. The Application Log is viewable through the Administrator Console. This function is only visible to master role users.

- It is possible to set the level of logging in the log files, from None to Maximum. The amount of information in these logs depends on how much logging is in each application and the level of detail specified by the **Application Logging** configuration.

7.1.1.2 Agent Security Audit

The Agent creates the following logs:

- **Alarm Log** - Lists all alarms triggered for the selected machine.
- **Monitor Action Log** - The log of alarm conditions that have occurred and the corresponding actions, if any, that have been taken in response to them.
- **Agent Log** - Displays a log of Agent, system, and error messages.
- **Configuration Changes** - Displays VSA settings changes for the selected machine.
- **Network Statistics** - Displays a log of send/receive data for network applications.
- **Event Logs** - Displays event log data collected by Windows. Not available for Win9x. Only event logs that apply to the selected machine display in the event log drop-down list.
- **Agent Procedure Log** - Displays a log of successful/failed Agent procedures.
- **Remote Control Log** - Displays a log of successful/failed remote control sessions.
- **Log Monitoring** - Displays Log Monitoring entries. Allows the monitoring of the data generated by any text-based log.

The VSA is capable of monitoring data collected from many standard log files. **Log Monitoring** extends that capability by extracting data from the output of any text-based log file. Examples include application log files and syslog files created for Unix, Linux, and Macintosh operating systems, and network devices such as Cisco routers. To avoid uploading all the data contained in these logs to the Kaseya Server database, **Log Monitoring** uses parser definitions and parser sets to parse each log file and select only the data an authorized administrator wants to capture. Parsed messages are displayed in Log Monitoring, which can be accessed using the Agent Logs tab of Live Connect > Agent Data or the Machine Summary page. Users can optionally trigger alerts when a **Log Monitoring** record is generated, as defined using Assign Parsing Sets or Parser Summary.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2.

7.1.2 Cryptographic Support

The Cryptographic Support of the TSF function provides cryptographic functions to protect TSF data from disclosure or modification while in transit from the Kaseya Server to the Agent. The information collected by the Agent is securely transmitted to the Kaseya Server over an encrypted channel. This provides a secure and confidential method to transmit the Agent system data. The connection between the Agent and Kaseya Server is secured by proprietary cryptographic functions.

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.4, FCS_COP.1.

7.1.3 Identification and Authentication

The Kaseya Server requires that each administrative user be successfully identified and authenticated with a username and password before being allowed access to the Kaseya Server and Administrative Console.

Kaseya VSA provides two identification and authentication mechanisms:

- Username and password
- Domain logon

One of the authentication mechanisms provided is username and password. A user provides a unique username and password to gain access to the TOE.

A second method is to use their Windows domain logon. This enables the user to logon to the VSA using their Windows domain logon and have their VSA logon name and password managed using Active Directory. At the same time, the user can continue to use all their previous VSA share rights, procedures and other user settings.

TOE Security Functional Requirements Satisfied: FIA_UAU.5, FIA_UID.2.

7.1.4 Security Management

The allowed operations on TSF data and the authorized roles required to execute them are listed in Table 16. Management of the Kaseya Server functions is done through the Administrative Console.

7.1.4.1 Server

The **Preferences** page sets system-wide preferences that apply only to the currently logged on user. This includes the email address where alert messages will be sent.

The **Change Logon** page sets the VSA logon username and password. These preference options apply only to the currently logged on user.

The **Check-in Policy** page defines group ID policies controlling the minimum, maximum and fixed values allowed for a variety of options. These policies prevent users from selecting settings that place undue stress on Windows servers running the Kaseya Server.

The **Naming Policy** page defines the IP address criteria used to automatically re-assign machines to a different machine group. Each machine group can be assigned multiple naming policies.
Naming policies can also force the renaming of a machine ID, if the machine ID name doesn't match the computer name, reducing confusion when administering managed devices.

The Import Center allows for an authorized administrator to import and export multiple objects as described in Table 16.

7.1.4.2 Agent

The Agent can be managed through the Agent Menu. Functions in the **Agent** module allow users to create, edit, delete machine IDs, control Agent check-in frequency, and update the version of Agent software that resides on managed devices.

Through the Administrative Console, the Agent can be configured as follows:

The **Log History** page determines the number of days to store log data in the database on a per log basis for each machine ID.

The **Deploy Agent** page creates and distributes an Agent install package to *multiple* machines.

The **Portal Access** page defines the logon name and password, by machine ID, required to use Live Connect as a machine user *remotely*. A **Live Connect** session run by a machine user is called **Portal Access**. The functions displayed using **Portal Access** are determined by the System > Machine Role page.

The **Set Credential** page registers the credential required by an Agent to perform user level tasks on a managed device. A credential is the logon name and password used to authenticate a user or process's access to a machine or network or some other resource. Most Agent tasks do not require a credential.

The **Import/Export** page imports and exports machine ID account settings as XML files, including scheduled Agent procedures, assigned monitor sets and event sets. Log data is not included in the import or export. **Import/Export** can be used to migrate machine ID account settings, including machine ID templates, from one Kaseya Server to the next.

Use the **Patch Management** Menu to monitor, scan, install, and verify Microsoft patches on managed devices. Patch management automates the process of keeping all the managed devices up to date with the latest patches. Configure how and when updates are applied on a per machine basis. See Methods of Updating Patches, Configuring Patch Management, Patch Processing, Superseded Patches, Update Classification and Patch Failure for a general description of patch management.

7.1.4.3 User Roles

Each user must be assigned at least one role and one scope. Multiple roles and scopes can be assigned to a user, but *only one role and one scope is active at any one time.* The active role and scope are selected using the **Role** and **Scope** drop-down lists in the top-right corner of the page in the Administrator Console. Kaseya licensing is purchased by role type. There are separate role types for licensing users by *user role type* and licensing machines by *machine role type*. Each role type enables selected functions listed in the **Access Rights** tab of User Roles and Machine Roles.

Master Users vs. Standard Users

User Security in the VSA is controlled by two actions: Roles and Scopes. The simplest explanation is that Roles control what a user ***can do*** while Scopes control ***what data*** the user can see.

A user defined as Master then consists of both Master Role and Master Scope. This user can then do everything in the VSA system environment with no restriction on what data they can see.

Roles other than Master are defined by the access rights granted to them and the functions they are able to perform within a particular part of the Administrator Console, such as create, edit, delete, etc.

Scopes other than Master are defined by the organizations, machine groups, machines and departments for which data will be available for the scope. An example would be a scope that is restricted to one particular machine only and the data related to that machine. The term *standard user* is sometimes used to indicate a

user that does not use a Master user role and a Master scope. Master users and Standard users are VSA administrators.

The Master user role provides user access to all functions throughout the VSA. A Master user is a VSA user that uses a Master user role and a Master scope. The Master scope provides access to all scope data objects throughout the VSA. A Master user role can be used with a non-Master scope, but a Master scope cannot be used with a non-Master role. Kaseya Server management configuration and other specialized functions can only be performed by Master role users. Master role users have an additional ability to take ownership of user-defined data objects. The Master User can create custom user roles based on the needs of the organization. *End users* have limited access to VSA functionality. *Machine users* are machines with the Kaseya Agent installed on them.

Master Users

- Any user can be assigned a Master user role and Master scope, if sufficient role type licenses exist.
- Master *role* users can view and operate all navigation and control options provided by the user interface.
- Master *scope* users can view, add, edit or delete all scope data objects: organizations, machine groups, machines, departments, and service desks.
- Masters can add or delete any user, including other master users. Since even a master user can't delete their own account while logged on, the system requires at least one master user be defined at all times.

End Users

- The End User role allows for limited access to the Management Interface. This role only provides for limited access to selected functions in the Management Interface. Users with 'End User' role can logon to the VSA and print reports or look at tickets about their own organizations.

Machine Users

- Machine users use machines with VSA Agents installed on them. They should not be confused with VSA users who can logon to the VSA.
- Machine users can click the Agent icon on the machine's system tray to see a VSA Portal Access window of functions and data related to that single machine. **Portal Access** is called Live Connect when accessed from the VSA.
- Access to **Portal Access** functions are determined by the machine role the machine is assigned to. Managed devices are assigned to the Default machine role by default and have access to all machine user **Portal Access** functions, unless limited by a VSA user.
- Data object access from the machine is determined by the Anonymous scope. Currently, the only data objects enabled by the Anonymous scope are **Service Desk** tickets. All other data seen in **Portal Access** is generated by the machine itself.

TOE Security Functional Requirements Satisfied: FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

7.1.5 Protection of the TSF

The Protection of the TSF function provides protection of TSF data from disclosure or modification while in transit from the Kaseya Agent to the Kaseya Server. The information collected by the Agent is then securely transmitted to the Kaseya Server over an encrypted channel. This provides a secure and confidential method to transmit the Agent system data. The connection between the Agent and Kaseya Server is secured by proprietary cryptographic functions.

TOE Security Functional Requirements Satisfied: FPT_ITT.1.

7.1.6 Systems Management System

Agents can be scheduled to automatically audit the hardware and software configurations of their managed devices on a recurring basis. Agents report the information back to the Kaseya Server so it can be accessed using the VSA even when managed devices are powered down. The Agent always connects to the Kaseya Server. The Kaseya Server never directly initiates a connection to the Agent. Once the Agent initiates a communications channel with Kaseya Server, the Agent connects to the database in order to download any remote procedure calls and tasks that have been configured on the Kaseya Server for the Agent. The system maintains three types of audits for each machine ID:

- **Baseline audit** - The configuration of the system in its original state. Typically a baseline audit is performed when a system is first set up.
- **Latest audit** - The configuration of the system as of the last audit. Once per day is recommended.
- **System Info** - All DMI[16] / SMBIOS[17] data of the system as of the last system info audit. This data seldom changes and typically only needs to be run once.

These are located in the Audit Menu of the Administrator Console. The VSA detects changes in a machine's configuration by comparing the latest audit to the baseline audit. The latest audit record is stored for as many days as specified in the log history.

Two alert types specifically address changes between a baseline audit and the latest audit: **Application Changes** and **Hardware Changes.** Collected audit information includes:

- All hardware, including CPUs, RAM, PCI[18] cards, and disk drives.
- All installed software, including licenses, version numbers, full path, and description.
- System Information from DMI and SMBIOS including PC make, model, serial number, mother board type, and over 40 other pieces of information describing the PC and its configuration.
- OS info with version number and service pack build.
- Current network settings including local IP address, gateway IP address, DNS[19], WINS[20], DHCP[21], and Media Access Control address.

LAN Watch uses an existing Agent on a managed device to periodically scan the local area network for any and all new devices connected to that LAN since the last time LAN Watch ran. These new devices can be workstations and servers without Agents or SNMP devices. Optionally, the VSA can send an alert when a LAN Watch discovers any new device. LAN Watch effectively uses the Agent as a proxy to scan a LAN behind a firewall that might not be accessible from a remote server.

The SNMP Traps Settings are in the Monitor Menu within the Administrator Console. The **SNMP Traps Alert** page triggers an alert when an `SNMP Trap` event log entry is created on a selected managed device.

[16] DMI = Desktop Management Interface; A management system for PCs.
[17] SMBIOS = System Management Basic Input/Output System
[18] PCI = Peripheral Component Interconnect
[19] DNS = Domain Name Server
[20] WINS = Windows Internet Naming Service
[21] DHCP = Dynamic Host Configuration Protocol

SNMP event log entries are created in response to the managed device receiving an SNMP trap message from an SNMP device on the same LAN as the managed device.

When an **SNMP Traps Alert** is assigned to a managed device, the Agent on the machine begins generating SNMP trap events, one for each SNMP trap message it receives. The log type for these event sets is set to `SNMP Trap`. "`<All Events>`" can be assigned to a managed device to create an alert for any SNMP Trap event received by the managed device, or an event set filter criteria can be created that limits the types of SNMP trap events triggering an alert.

Monitor

Monitor provides five methods of monitoring machines and log files:

- **Alerts** - Monitors events on *Agent-installed* machines.
- **Monitor Sets** - Monitors the performance state on *Agent-installed* machines.
- **SNMP Sets** - Monitors the performance state on *non-Agent-installed devices*.
- **System Check** - Monitors events on *non-Agent-installed* machines.
- **Log Monitoring** - Monitors events in *log files*.

Monitor parses the Agent collected data to provide information about the managed devices and SNMP devices on the targeted network. When programmable alarms are triggered, Monitor executes email notifications, procedures, and job ticketing, for problems and state changes that are configured by the VSA Administrator within the Administrator Console. When programmable alarms are triggered, **Monitor** executes email notifications, procedures and job ticketing, for such problems and state changes as:

- When any critical server or desktop computer goes off-line.
- When a machine user disables remote control.
- When any software application is added or removed.
- When the hardware configuration changes.
- When the computer is running low on disk space.
- When a specific event or any event log entry is generated.
- When any protection policy violation occurs.
- When any Agent procedure fails execution.
- When an unapproved application attempts to access the network.
- When an unapproved application attempts to access a protected file.
- When a new device appears on the local area network.
- When an external log records a specific log entry.

In addition to generating alert notifications, when **event log entries** are generated, event log entries collected from the managed devices are stored on the VSA. The event log data is always available, even if the managed device goes offline or suffers a hard failure.

TOE Security Functional Requirements Satisfied: EXT_SMS_ARP.1, EXT_SMS_SDC.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 3.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1 and 8.2.2 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 20 - Threats: Objectives Mapping

Threats	Objectives	Rationale
T.ACCOUNT The security relevant actions of users may go undetected.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN counters this threat by ensuring that access to TOE security data is limited to those users with access to the management functions of the TOE.
	O.AUDIT The TOE must provide the means of recording any security relevant events, so as to assist an administrator in the detection of potential attacks or misconfiguration of TOE security features as well as hold administrator users accountable for any actions they perform regarding the configuration of TOE Security functions.	O.AUDIT counters this threat by ensuring that all relevant TOE security actions are recorded.
T.UNAUTH An unauthorized user may attempt to disclose, remove, destroy, or compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN counters this threat by ensuring that access to TOE security data is limited to those users with access to the management functions of the TOE.
	O.AUDIT The TOE must provide the means	O.AUDIT counters this threat by ensuring that all relevant TOE

Threats	Objectives	Rationale
	of recording any security relevant events, so as to assist an administrator in the detection of potential attacks or misconfiguration of TOE security features as well as hold administrator users accountable for any actions they perform regarding the configuration of TOE Security functions.	security actions are recorded.
	O.AUTHEN The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	O.AUTHEN counters this threat by ensuring that access to TOE security data is limited to those users that have been successfully identified and authenticated.
T.EXPLOIT An attacker may attempt to gain unauthorized access to the resources of the managed devices, by exploiting vulnerabilities on a managed device.	O.SCAN The TOE must be able to collect information from the managed devices and send alerts based on programmable alarms.	O.SCAN counters this threat by ensuring that the TOE collects information from the managed devices and sends alerts based on programmable alarms.
T.SELPRO An unauthorized user may read, modify, or corrupt security critical TOE configuration data while in transit between the Agent and Server.	O.ROBUST The TOE must secure all critical security data so that it is protected from unauthorized disclosure and modification while in transit between the Agent and Server.	O.ROBUST counters this threat by ensuring that the TOE must secure all critical security data so that it is protected from unauthorized disclosure and modification.
T.SPOOF A hostile entity masquerading as the Server component may receive TSF data from an authorized agent that incorrectly thinks it is communicating with an authorized Server component.	O.CRYPTO The TOE will provide encryption/decryption of all Agent communications with the TOE Server component.	O.CRYPTO counters this threat by ensuring that all communications between the Agent and Server are encrypted.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Assumptions

Table 21 - Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the	OE.MANAGE Those responsible for the TOE must be competent, non-hostile TOE administrators who are	OE.MANAGE ensures that competent individuals are assigned to manage the TOE and the TSF.

Assumptions	Objectives	Rationale
information it contains.	appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	OE.MANAGE Those responsible for the TOE must be competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE ensures that the users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.PROTECT The components of the TOE critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.	OE.PROTECT Those responsible for the TOE must ensure that the physical environment must be suitable for supporting a computing device in a secure setting.	OE.PROTECT ensures that the TOE environment provides protection from external interference or tampering.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME ensures that the IT environment provides reliable timestamps to the TOE.

Every Assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

A family of EXT_SMS requirements was created to specifically address the Systems Management functions. The CC Part 2 FAU SFRs are specifically for the auditing of TOE Security Functionality. In this case, the information being collected is from external software and machines that are outside the TOE Boundary. As a result, the FAU SFRs do not apply. The US Government Protection Profile Intrusion Detection System (IDS) System for Basic Robustness Version 1.7 July 25, 2007 was used as a model for creating these requirements. The IDS SFRs from this PP are based on the CC FAU Security audit class Security Functional Requirements of the CC Part 2. Likewise the EXT_SMS SFRs are also based on the CC FAU Security audit class Security Functional Requirements of the CC Part 2. The purpose of this family of requirements is to describe the collecting of information from managed devices as well as sending alerts based on programmable alarms. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation. The CC Part 2 FAU SFRs are specifically for the auditing of TOE Security Functionality. In this case, the information being collected is about external software and machines that are outside the TOE Boundary. As a result, the FAU SFRs do not apply.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no Extended SARs defined for this ST.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 22 - Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that only authorized users are allowed access to TSF data.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
O.AUDIT The TOE must provide the means of recording any security relevant events, so as to assist an administrator in the detection of potential attacks or misconfiguration of TOE security features as well as hold administrator users accountable for any actions they perform regarding the configuration of TOE Security functions.	FAU_GEN.1 Audit Data Generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_GEN.2 User identity association	The requirement meets the objective by ensuring that the TOE associates each auditable event with the identity of the user that caused the event.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensure that the TOE provides the ability to review logs.
	FAU_SAR.2 Restricted audit review	The requirement meets the objective by ensuring that the TOE only allows authorized users to read the audit records.
O.AUTHEN	FIA_UAU.5	The requirement meets the

Objective	Requirements Addressing the Objective	Rationale
The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	Multiple authentication mechanisms	objective by requiring that all users and administrators be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user or administrator.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the users are identified before access to TOE administrative functions is allowed.
O.CRYPTO The TOE will provide encryption/decryption of all Agent communications with the TOE Server component.	FCS_CKM.1 Cryptographic key generation	The requirement meets the objective by ensuring that the TOE can generate cryptographic keys for use during cryptographic operations.
	FCS_COP.1 Cryptographic operation	The requirement meets the objective by ensuring that the TOE provides confidentiality and integrity services for TSF data being transmitted among separate instances of the TOE.
O.ROBUST The TOE must secure all critical security data so that it is protected from unauthorized disclosure and modification while in transit between the Agent and Server.	FCS_CKM.4 Cryptographic key destruction	The requirement meets the objective by ensuring that the TOE destroys cryptographic keys when no longer in use.
	FPT_ITT.1 Basic internal TSF data transfer protection	The requirement meets the objective by protecting TSF data from modification and disclosure while it is transmitted between separate instances of the TOE.
O.SCAN The TOE must be able to collect information from the managed devices and send alerts based on programmable alarms.	EXT_SMS_ARP.1 Security alarms	The requirement meets the objective by ensuring that the TOE sends an alert based on programmable alarm.
	EXT_SMS_SDC.1 System data collection	The requirement meets the objective by ensuring that the TOE collects information from the managed machines.

8.5.2 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL2 assurance package augmented with ALC_FLR.2. EAL2+ was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. Kaseya Virtual System Administrator v6.1 is targeted at an environment with good physical access security (OE.PROTECT) and competent administrators (OE.MANAGE, A.MANAGE), where EAL 2 should provide adequate assurance. Within such environments it is assumed that attackers will have little attack potential. As such, EAL2 is appropriate to provide the assurance necessary to counter the limited potential for attack. ALC_FLR.2 was chosen to assure that the developer is able to act appropriately upon security flaw reports from TOE users. This Security Target conforms to Part 2 extended and Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 3.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 23 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 23 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	FPT_STM.1 is not included because time stamps are provided by the environment. An environmental objective states that the TOE will receive reliable timestamps.
FAU_GEN.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
	FAU_GEN.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	
FCS_CKM.1	FCS_COP.1	✓	
	FCS_CKM.4	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FIA_UAU.5	No dependencies	✓	
FIA_UID.2	No dependencies	✓	
FMT_MTD.1	FMT_SMR.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FMT_SMF.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_ITT.1	No dependencies	✓	
EXT_SMS_ARP.1	EXT_SMS_SDC.1	✓	
EXT_SMS_SDC.1	No dependencies	✓	

9 Acronyms and Terms

This section describes the acronyms and terms.

9.1 Acronyms

Table 24 - Acronyms and Terms

Acronym	Definition
API	Application Programming Interface
ASP	Active Server Pages
CC	Common Criteria
CM	Configuration Management
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DMI	Desktop Management Interface
DNS	Domain Name Server
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GB	Gigabyte
IP	Internet Protocol
IIS	Internet Information Server
IT	Information Technology
LAN	Local Area Network
MB	Megabyte
Mhz	Megahertz
MSMQ	Microsoft Message Queuing
NIC	Network Interface Card
OS	Operating System
PC	Personal Computer
PCI	Peripheral Component Interconnect
RAM	Random Access Memory
RFP	Request for Proposal
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement

Acronym	Definition
SMBIOS	System Management Basic Input/Output System
SQL	Structured Query Language
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
UI	User Interface
VSA	Virtual System Administrator
WINS	Windows Internet Naming Service
XP	Windows XP Operating System

9.2 Terminology

Table 25 - Term

Acronym	Definition
Machine ID	Account name for a managed machine in the VSA database. Each agent installed on a managed machine is assigned a unique machine ID / group ID / organization ID. All machine IDs belong to a machine group ID and optionally a subgroup ID. All machine group IDs belong to an organization ID. An organization typically represents a single customer account. If an organization is small, it may have only one machine group containing all of themachine IDs in that organization. A larger organization may have many machine groups and subgroups, usually organized by location or network.
Managed device	A managed device is an IP host that has the Kaseya Agent installed on it.
System data	The information collected by the Kaseya Agent.

9.3 References

Table 26 - References

Reference	Description
[VSA Onl]	Kaseya Virtual System Administrator Online User Assistance

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Hwy, Suite 220
Fairfax, VA 22033

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com