SenSage, Inc.
SenSage 4.6.2

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 1.2

Prepared for:

SenSage, Inc.
55 Hawthorne Street
San Francisco, CA 94105
United States of America

Phone: +1 (415) 808-5900
Email: info@sensage.com
http://www.sensage.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, 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 CONTENTS **2**

TABLE OF FIGURES **3**

TABLE OF TABLES **3**

1 INTRODUCTION **4**
1.1 PURPOSE 4
1.2 SECURITY TARGET AND TOE REFERENCES 4
1.3 PRODUCT OVERVIEW 5
1.3.1 Clarification on Terminology *6*
1.4 TOE OVERVIEW 6
1.4.1 Brief Description of the Components of the TOE *7*
1.4.2 TOE Environment *9*
1.5 TOE DESCRIPTION 10
1.5.1 Physical Scope *10*
1.5.2 Logical Scope *11*

2 CONFORMANCE CLAIMS **14**

3 SECURITY PROBLEM **15**
3.1 THREATS TO SECURITY 15
3.2 ORGANIZATIONAL SECURITY POLICIES 15
3.3 ASSUMPTIONS 16

4 SECURITY OBJECTIVES **17**
4.1 SECURITY OBJECTIVES FOR THE TOE 17
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 17
4.2.1 IT Security Objectives *17*
4.2.2 Non-IT Security Objectives *18*

5 EXTENDED COMPONENTS **19**
5.1 EXTENDED TOE SECURITY FUNCTIONAL COMPONENTS 19
5.1.1 Class FAU: Security Audit *19*

6 SECURITY REQUIREMENTS **22**
6.1.1 Conventions *22*
6.2 SECURITY FUNCTIONAL REQUIREMENTS 22
6.2.1 Class FAU: Security Audit *24*
6.2.2 Class FCS: Cryptographic Support *28*
6.2.3 Class FDP: User Data Protection *30*
6.2.4 Class FIA: Identification and Authentication *33*
6.2.5 Class FMT: Security Management *34*
6.2.6 Class FPT: Protection of the TSF *37*
6.3 SECURITY ASSURANCE REQUIREMENTS 38

7 TOE SPECIFICATION **39**
7.1 TOE SECURITY FUNCTIONS 39
7.1.1 Security Audit *40*
7.1.2 Alert Generation *40*
7.1.3 Cryptographic Support *41*
7.1.4 User Data Protection *42*
7.1.5 Identification and Authentication *44*
7.1.6 Security Management *44*
7.1.7 Protection of the TSF *47*

8 RATIONALE 48
8.1 CONFORMANCE CLAIMS RATIONALE 48
8.2 SECURITY OBJECTIVES RATIONALE 48
8.2.1 Security Objectives Rationale Relating to Threats 48
8.2.2 Security Objectives Rationale Relating to Policies 50
8.2.3 Security Objectives Rationale Relating to Assumptions 50
8.3 RATIONALE FOR EXTENDED SECURITY FUNCTIONAL REQUIREMENTS 51
8.4 RATIONALE FOR EXTENDED TOE SECURITY ASSURANCE REQUIREMENTS 51
8.5 SECURITY REQUIREMENTS RATIONALE 51
8.5.1 Rationale for Security Functional Requirements of the TOE Objectives 51
8.5.2 Security Assurance Requirements Rationale 54
8.5.3 Dependency Rationale 54

9 ACRONYMS 57
9.1 ACRONYMS 57

Table of Figures

FIGURE 1 – DEPLOYMENT CONFIGURATION OF THE TOE 6
FIGURE 2 – PHYSICAL TOE BOUNDARY 11
FIGURE 3 – EXT_FAU_EDC EVENT DATA COLLECTION FAMILY DECOMPOSITION 19
FIGURE 4 – EXT_FAU_SAA POTENTIAL SECURITY VIOLATION ANALYSIS FAMILY DECOMPOSITION 20

Table of Tables

TABLE 1 – ST AND TOE REFERENCES 4
TABLE 2 – CC AND PP CONFORMANCE 14
TABLE 3 – THREATS 15
TABLE 4 – ASSUMPTIONS 16
TABLE 5 – SECURITY OBJECTIVES FOR THE TOE 17
TABLE 6 – IT SECURITY OBJECTIVES 17
TABLE 7 – NON-IT SECURITY OBJECTIVES 18
TABLE 8 – EXTENDED TOE SECURITY FUNCTIONAL REQUIREMENTS 19
TABLE 9 – TOE SECURITY FUNCTIONAL REQUIREMENTS 22
TABLE 10 – CRYPTOGRAPHIC KEY GENERATION STANDARDS 28
TABLE 11 – CRYPTOGRAPHIC OPERATIONS 29
TABLE 12 – MANAGEMENT OF TSF DATA (SENSAGE) 36
TABLE 13 – MANAGEMENT OF TSF DATA (SKV) 36
TABLE 14 – ASSURANCE REQUIREMENTS 38
TABLE 15 – MAPPING OF TOE SECURITY FUNCTIONS TO SECURITY FUNCTIONAL REQUIREMENTS 39
TABLE 16 – AUDIT RECORD CONTENTS 40
TABLE 17 – PREDEFINED PERMISSIONS FOR SENSAGE CONSOLE 42
TABLE 18 – THE STRUCTURE OF THE SPECIAL USER CLASS 45
TABLE 19 – THE STRUCTURE OF THE INDIVIDUAL USER CLASS, AND PREDEFINED ROLES & PERMISSIONS 45
TABLE 20 – THREATS:OBJECTIVES MAPPING 48
TABLE 21 – ASSUMPTIONS:OBJECTIVES MAPPING 50
TABLE 22 – OBJECTIVES:SFRS MAPPING 51
TABLE 23 – FUNCTIONAL REQUIREMENTS DEPENDENCIES 54
TABLE 24 – ACRONYMS 57

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is SenSage 4.6.2, and will hereafter be referred to as the TOE throughout this document. The TOE is a system which offers customers the ability to collect, store, and query log data from their enterprise computing environment, and thereby reduce security, fraud, and compliance risks. The TOE enables customers to easily query years of data from multiple sources at any detail level to support business requirements. The TOE is a software-only TOE.

1.1 Purpose

This ST contains the following sections to provide mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish or mitigate the defined threats:

- 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), Protection Profile (PP), 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 (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target and TOE References

Table 1 – ST and TOE References

ST Title	SenSage, Inc. SenSage 4.6.2 Security Target
ST Version	Version 1.2
ST Author	Corsec Security
ST Publication Date	7/7/2011
TOE Reference	SenSage 4.6.2
Keywords	Event Data Warehouse

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

SenSage 4.6.2 is an Event Data[1] Warehouse solution that handles massive amounts of log and event data. Event data contains evidence directly pertaining to and resulting from the execution of a business process or system function. Below are several examples of systems or devices that generate event data, as well as different kinds of event data:

- Network and security devices
- Physical access systems
- Identity management systems
- Workstations, servers, and operating systems
- Enterprise applications – 3rd party and in-house
- Database activity
- Email, Windows, network and other systems management activity events
- Banking transactions such as online, ATM[2] and debit card use
- Historical prices of stocks and other financial instruments
- Telephone Call Detail Records (CDRs[3])
- Internet Protocol Detail Records (IPDRs) of web based access and transactions

When properly configured, the Event Data Warehouse contains the records of all system activities – users logging in and logging out, users accessing confidential files, activities on the firewall, emails being sent and received, information on processed transactions, the web sites being accessed, etc.

Given the massive daily volumes of audit logs and the myriad sources across the network in a typical enterprise computing environment, efficiently collecting and aggregating all relevant events in a structured way for analysis can be a challenging task. SenSage 4.6.2 enables the user to easily collect and store large volumes of event data. It also provides the user an ability to query and perform analysis on the event data that are available.

The core components of the SenSage 4.6.2 that are responsible for collecting, storing and analyzing the event data run on a Linux platform. These components can be deployed on a single Linux machine or they can be deployed across a large number of Linux platform machines. When deployed over a multiple machines, depending on the volume of event data being stored and processed, the deployment can have multiple instances of the Scalable Log Server (SLS) component, which is a proprietary columnar database on a Linux platform that serves as event data repository. It should be noted that the actual deployment is determined by the customer's network architecture and performance requirements, therefore the configuration varies by each customer's computing environment.

The SenSage 4.6.2 also includes a management console component, which provides a browser-based graphical user interface (GUI) to the end-users of the TOE. The management console component runs on a Windows operating system platform (Windows XP, Windows Vista 32 or 64-bit, Windows Server 2008 64

[1] Event Data – also referred to as an "audit trail" or "system of record"; this is a set of chronologically sequenced data records that capture information about an event.

[2] ATM – Automatic Teller Machine

[3] CDR – A Call Detail Records (CDR) is the computer record produced by a telephone exchange containing details of a call that passed through it. It is the automated equivalent of the paper toll tickets that were written and timed by operators for long distance calls in a manual telephone exchange.

bit, or Windows 7). Again, depending on the customer's environment, either a single console or multiple consoles can be deployed.

1.3.1 Clarification on Terminology

It should be noted that while SenSage 4.6.2 is a software application that collects and analyzes event data from numerous sources across the network, it also generates event data (i.e., audit logs) for itself and collects and analyzes its own event data (audit logs).

Throughout this document, the terms "event data" and "audit logs" will be used. The context of this terminology is explained below.

1. Event Data – this is a general and comprehensive term. It refers to an "audit trail" or "system of record" generated by all the entities which include source machines (hosts that send event data to SenSage), and also SenSage 4.6.2, itself.

2. Audit Logs – this term is specifically referring to event data generated only by SenSage 4.6.2. It excludes all other instances of event data generated by entities other than SenSage 4.6.2.

1.4 TOE Overview

This 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.

SenSage 4.6.2 is a software-only TOE that consists of several separate executable components. Figure 1 below shows the detailed view of the CC-evaluated configuration of the TOE.

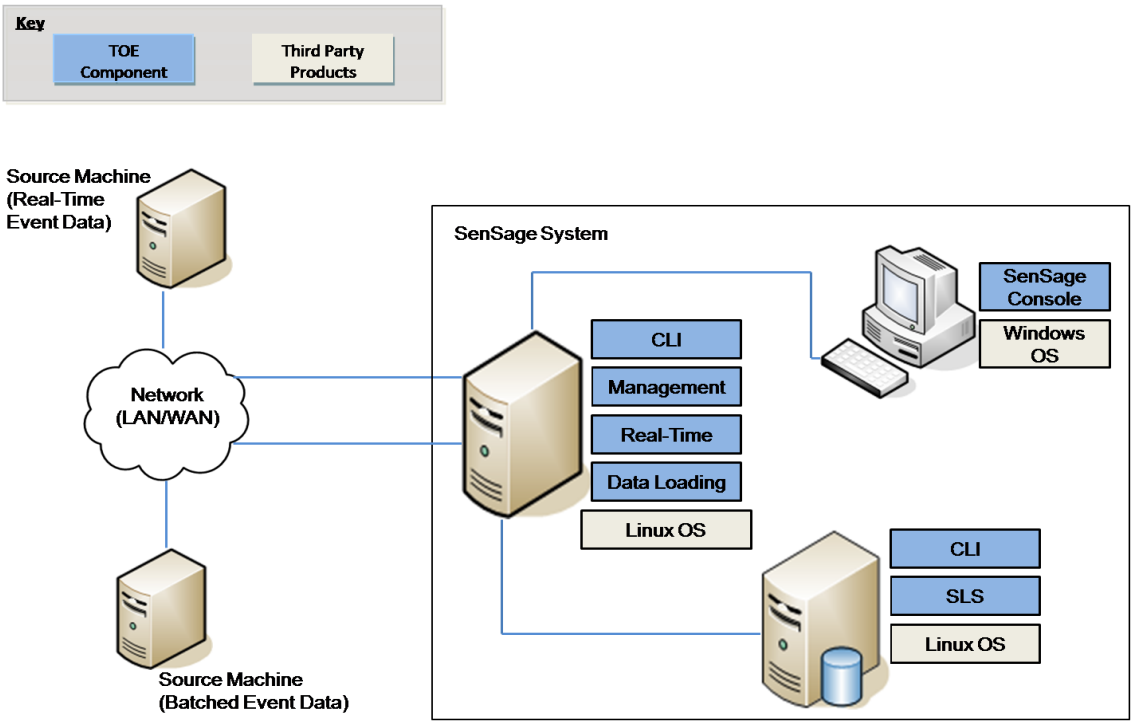

Figure 1 – Deployment Configuration of the TOE

The TOE includes a management console component, which provides a browser-based graphical user interface (GUI) to the end-users of the TOE. In the environment of the CC evaluated configuration of the TOE, the console component runs on a Windows 7 machine.

All the components of the TOE that run on Linux OS machines provide a Command Line Interface (CLI), through which the administrative users of the TOE and the TOE system processes can execute SenSage-associated commands and scripts.

In summary, the environment of the CC-evaluated configuration of the TOE is composed of a single Linux-architecture machine, hosting the SLS component and the CLI component, another Linux machine , hosting the Management, Real-Time, Data Loading and CLI, and a single Windows operating system machine, hosting the SenSage console.

1.4.1 Brief Description of the Components of the TOE

The following paragraphs provide a brief description of the components of the TOE.

1.4.1.1 Scalable Log Server (SLS) Component

The TOE is composed of several components, the most important of these being the Scalable Log Server. The SLS is a high-performance, read-only columnar database with clustering ability. The SLS is coded in the C++ programming language, and is compiled and run on Red Hat Linux 5.1 or 5.5. It uses the application level clustering technique to perform all load and query tasks in parallel, across any number of SLS database instances. This architecture allows users to load and query massive volumes of data in a single, logical database instance without partitioning. The SLS stores user data (*i.e.* the event data from source machines) in a special filesystem directly on disk. It also generates its own audit logs.

1.4.1.2 Management Component

The Management Component of the TOE is responsible for processing the user requests. It acts as a communication agent between the SenSage Console and the SLS. The Management Component performs the following tasks:

- Authenticates, authorizes, and maintains SenSage Console sessions.
- Manages definitions for reports, libraries[4], dashboards, namespaces, schedules, users, roles and permissions.
- Stores rules for parsing the event data, rules for analyzing the event data, and conditions for triggering alerts.
- Processes queries against the SLS.
- Sends reports, alerts, and email with scheduled reports to SenSage Console.

The Management Component includes a set of Java applications and Perl applications that interact with the other TOE components and TOE Environment components. These applications use the JBoss Application Server (Java) and Perl Application Server, installed and running on the Linux platform machine that houses the Management Component. Third party products such as the JBoss Application Server and the Perl Application Server are excluded from the scope of CC evaluation for the TOE.

1.4.1.3 Data Loading Component

Before the user is able to analyze event data, original event data must be collected into the SenSage system. The event data needs to be gathered and loaded into the SLS component.

There are two ways in which the TOE collects the event data:

[4] Library – A group of shared code. SenSage 4.6.2 enables users to create libraries, which allow common SQL fragments and Perl codes to be shared across queries.

- Batches – events are collected from log files and other event repositories maintained by network devices and software applications. The Data Loading component is responsible for loading the batches of event data into the SLS component.

- Streams – events flow into the SenSage system as a real-time stream of event-log entries from network devices and software applications that generate the events. The Real Time component is responsible for loading the streams of real-time event data into the SLS component.

As stated above, it is the Data Loading Component that gathers the batches of log data from the source, parses and transforms the log file as specified by the PTL (Parser, Transform, and Load), and loads the data into a specified SLS instance, name space and table. Collected batch event data is able to be analyzed by users connecting through the SenSage Console component.

1.4.1.4 Real Time Component

The Real Time Component of the TOE is responsible for collecting the real-time event data that is sent to the SenSage system by the source machines. The Real Time Component receives the event data streams by listening on designated network ports. It accepts event data from various systems, reformats them into a standard format, and then parses them into a normalized data structure so they can be ready for loading into the database in the SLS Component.

In addition to performing these tasks, the Real Time Component performs real-time correlation analysis on parsed normalized event data. If the analysis detects a predefined condition for raising alerts, the Real Time Component relays the information to the Management Component, which in turn sends the security alerts to the SenSage Console Component.

In analyzing the real-time event data for possible security alerts, the Real Time Component uses a set of SenSage-supplied "Rules" files which it applies against the incoming stream of event data for specific patterns indicative of potential threats, and raises alerts when these patterns are detected. Below lists a few examples of SenSage-supplied rules:

- Rules for detecting User Object Modification Attacks

- Rules for detecting Process Termination Attacks

- Rules for detecting DNS[5]Zone Transfer Attacks

- Rules for detecting Generic Well Known Service Attacks

- Rules for detecting Web Server Attacks

- Rules for detecting Dictionary Password Attacks

In addition to the rules that are supplied by SenSage, the users of the TOE can create their own rules, to be used by the Real Time Component. The rules must be in XML[6] format.

1.4.1.5 SenSage Console Component

The SenSage Console Component is a Java application installed on the user's Windows workstation through the Java Web Start framework (a standard part of the JRE[7] as of JRE 1.6.0_13 or greater). Since

[5] DNS – Domain Name Server

[6] XML – Extensible Markup Language

[7] JRE – Java Runtime Environment

the SenSage Console Component is written in Java, the SenSage Console Component provides the end-users a graphical user interface for monitoring, analyzing, resolving, and reporting real-time and historical event data.

The SenSage Console Component communicates with a Java Servlet running inside the Management Component. Through the Management Component, the SenSage Console Component is able to access the event data stored in the SLS component.

1.4.1.6 CLI Component

The CLI Component of the TOE is responsible for providing a CLI through which the administrative users of the TOE and the TOE system processes can execute SenSage-associated commands and scripts. The CLI is used for administering the SLS, Management, Real-Time, and Data Loading components which run on Linux OS machines.

1.4.2 TOE Environment

The TOE has the following hardware requirements for the Linux-architecture machine:

- CPU[8] – Dual Xeon processor (or higher) running at 3.0 GHZ[9](or higher)
- Memory – 8 Gigabytes (GB) RAM[10] or more
- 1 GB network adapter
- Disk Space
    - Operating System (RAID[11] 1) – 2 x 72 GB SCSI[12] hard drives
    - Log data (RAID 5) – Approximately 1 Terabytes (TB) per node
    - 16 GB in the SLS temporary workspace directory on hosts where an SLS instance runs
    - 10 GB in the SenSage home directory
    - 1.5GB in /tmp directory for installation

The TOE runs on the following types of Linux operating systems:

- Red Hat Enterprise Linux Server 5.1
- Red Hat Enterprise Linux Server 5.5,

The TOE also deploys the following two applications on the Linux-architecture machine that houses the Management Component of the TOE:

- JBoss Application Server (Java)
- Perl Application Server

The TOE requires that a Syslog server be configured on the Linux machines to support retrieving Syslog data.

SenSage Console Workstation has the following requirements:

- One of the following Windows operating systems: Windows XP, Windows Vista 32 or 64 bit, or Windows Server 2008 64 bit, Windows 7

[8] CPU – Central Processing Unit

[9] GHZ – Gigahertz

[10] RAM – Random Access Memory

[11] RAID – Redundant Array of Inexpensive Disks

[12] SCSI – Small Computer System Interface

- JRE 1.6_13, or a later version

Optional Component:
External LDAP Authentication Authority:

- Active Directory
- SunOne

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

As stated in the Section 1.4, the TOE is composed of modular components and thus numerous deployment scenarios are possible. For the purpose of the CC evaluation, the following evaluation configuration of the TOE is used:

- One (1) Linux-architecture machine running the Management Component, Real Time, Data Loading and CLI components
- One (1) Linux-architecture machine each running the SLS and CLI components
- One (1) machine (for SenSage Console) running the GUI on Windows operating system (XP, Vista, Server 2008, or Windows 7) with JRE 1.6_13 or later

For the CC-evaluation, the TOE boundary includes all of the SenSage-created software components. It excludes the underlying operating system and its filesystem, any third party system software such as JBoss Application Server and Perl Application Server, and external entities such as LDAP Server and Log source machines.

Figure 2 below 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.

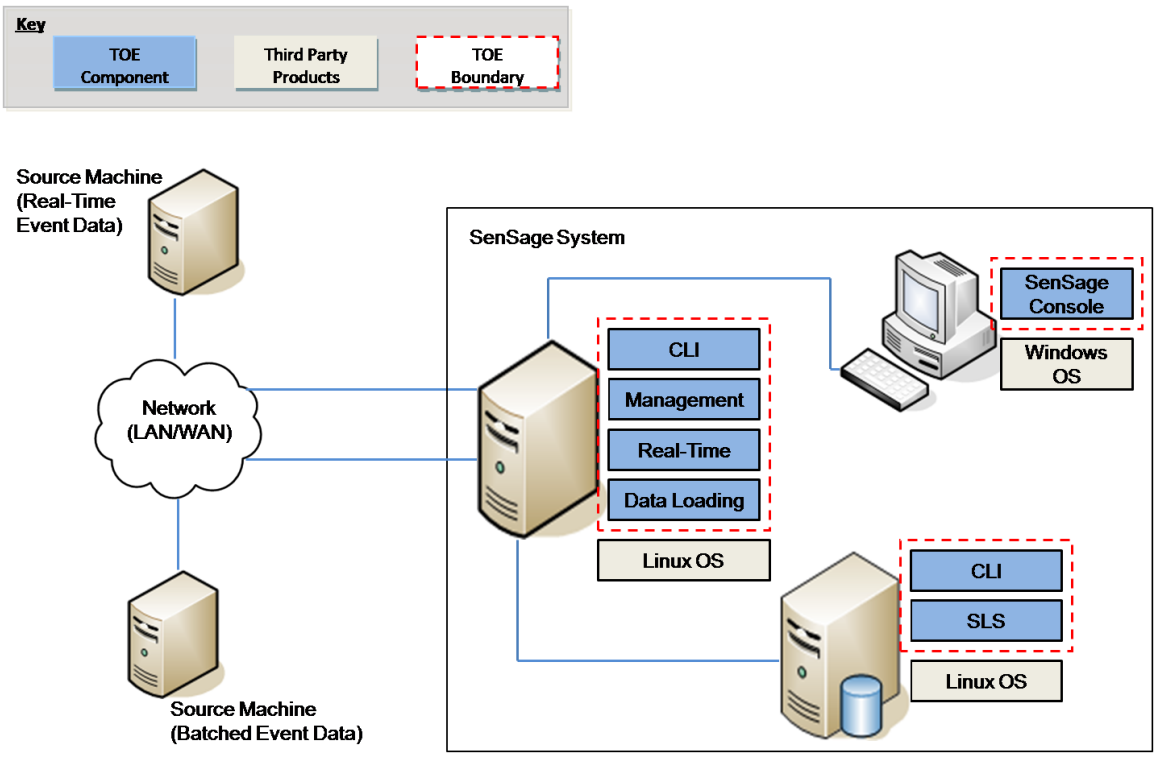

Figure 2 – Physical TOE Boundary

1.5.1.1 Guidance Documentation

The following guides are required reading and part of the TOE

- SenSage 4.6.2 Installation, Configuration, and Upgrade Guide
- SenSage 4.6.2 Administration Guide
- SenSage 4.6.2 Event Collection Guide
- SenSage 4.6.2 Reporting Guide
- SenSage 4.6.2 Glossary
- SenSage 4.6.2 Guidance Documentation Supplement

1.5.2 Logical Scope

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

- Security Audit
- Alert Generation
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management

1.5.2.1 Security Audit

The TOE performs auditing of *authentication attempts and administrative actions*, and can be configured to store these events. The TOE audit logs include all of the following information: date and time of the event

occurrence, date and time of the event completion, status of the event, type of event, and the subject identity.

1.5.2.2 Alert Generation

The TOE provides the end-users timely visibility into events that may require immediate attention or further investigation. That is, the TOE raises alerts in response to the pre-specified conditions, which are either user-defined or pre-defined by the TOE. The users can view alerts via the SenSage Console, view the events that contributed to raising the alert, and define email notifications that are sent when the alert is raised. The Alert Generation security function applies to both the event data generated by the source machines (and collected by the TOE), and the audit logs for the TOE itself, generated and kept by the TOE.

1.5.2.3 Cryptographic Support

The TOE offers an ability to protect the TOE deployment and the data stored inside the TOE from unauthorized inspection or tampering by individuals or applications. The TOE accomplishes this by applying encryption to "data at rest". The *data at rest* in the SenSage deployment refers to:

- Event Data stored in the SLS Component
- Configuration files used by the SenSage Components

When the *data at rest* is encrypted, the SenSage deployment is operating in an encrypted mode. An encrypted SenSage deployment functions exactly like an unencrypted deployment except that users must enter a special *pass phrase* to start, stop, or reconfigure the deployment. FIPS 140-2 validated cryptographic module performs all cryptographic operations for the "data at rest" encryption. The FIPS 140-2 validated cryptographic module also encrypts user data in transit using TLS[13] and SSH[14], for users connecting via SenSage Console and the CLI.

1.5.2.4 User Data Protection

The TOE enforces an Access Control mechanism. SenSage Access Control decisions are made based on the permission information available for a given subject and a given object. When a TOE user requests an operation to be performed on a particular object, the SenSage Access Control determines if the user's role(s) for the object contain permissions sufficient for performing the requested operation on behalf of the requesting user. If the sufficient permissions are found, the requested operation is performed. Otherwise, the requested operation is denied.

1.5.2.5 Identification and Authentication

The TOE requires that all TOE users are authenticated by the TOE or an external authentication authority prior to being granted access to the TOE functionality. The TOE is responsible for the identification of all authenticated users.

1.5.2.6 Security Management

Users are assigned roles. Roles are assigned role permissions. Access to the administrative interface of the TOE is determined based on role permissions. The TOE ensures that the ability to create, modify and delete security attributes and TSF[15] data such as user accounts, roles and permissions are restricted to a user

[13] TLS – Transport Layer Security

[14] SSH – Secure Shell

[15] TSF – TOE Security Function

with *administrator* role or a user with *analyzer.admin* role. For the Report object in SenSage Console, the owner of a Report (the user who created the Report) also has ability to assign specific permissions (View, Edit, Run) to specific roles. Users are also assigned with a role when they access the SKV with a passphrase with the CLI.

2 Conformance Claims

This section provides the identification for any CC, Protection Profile, 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 2 – 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 Interpreted CEM as of 2009/07/31 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with Flaw Remediation (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 individuals who are not authorized to use the TOE. The threat agents are assumed to:

- have public knowledge of how the TOE operates
- possess a low skill level
- have limited resources to alter TOE configuration settings
- have no physical access to the TOE
- possess a low level of motivation
- have a low attack potential

The Information Technology (IT) assets requiring protection are the event data collected by the TOE and the audit logs for the TOE itself. Removal, diminution and mitigation of the threats are through the objectives in Section 4 – Security Objectives.

The following threats are applicable:

Table 3 – Threats

Name	Description
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

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 4 – Assumptions

Name	Description
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.PHYSICAL	The TOE resides in a physically controlled access facility that prevents unauthorized physical access.
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 5 – Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE data.
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 gather audit logs of actions on the TOE and alerts which may be indicative of misuse.
O.IDAUTH	The TOE must identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.INTEGRITY	The TOE must ensure the integrity of all TOE data through its own interfaces.
O.ENCRYPT	The TOE must encrypt the all TOE data at rest and user data in transit.
O.NOTIFICATION	The TOE shall generate and deliver alerts upon detecting the patterns of event data indicative of potential security violations.

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 6 – IT Security Objectives

Name	Description
OE.SEP	The TOE environment must protect itself and the TOE from external interference or tampering.
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 7 – Non-IT Security Objectives

Name	Description
NOE.NOEVIL	Users are non-hostile, appropriately trained, and follow all user guidance.
NOE.PHYSICAL	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

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 8 identifies all extended SFRs implemented by the TOE.

Table 8 – Extended TOE Security Functional Requirements

Name	Description
EXT_FAU_SAA.1	Potential security violation analysis
EXT_FAU_EDC.1	Event data collection

5.1.1 Class FAU: Security Audit

Families in this class address the requirements for functions to recognize, record, store, and analyze information related to security relevant activities.

The extended family "EXT_FAU_EDC: Event data collection" was modeled after FAU_GEN.

5.1.1.1 Event data collection (EXT_FAU_EDC)

Family Behavior

This family defines the set of rules which SenSage 4.6.2 uses in collecting event data to be stored in the SLS database.

Component Leveling

Figure 3 – EXT_FAU_EDC Event data collection family decomposition

EXT_FAU_EDC.1 Event data collection, defines the set of rules which SenSage 4.6.2 uses when collecting event data to be stored in the SLS database. It was modeled after FAU_GEN.1

EXT_FAU_EDC.1 Event Data Collection

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable Time Stamps

Event data collection defines the type of event data collected.
EXT_FAU_EDC.1.1 The TSF shall be able to collect event records based on the following:

a) All events collected from event data sources using [assignment: *protocols*]; and
b)[assignment: *other specifically defined events*].

EXT_FAU_EDC.1.2 The TSF shall be able to collect event records with the following:

a) Date and time of the event and type of event; and
b) For each event type, based on the event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

5.1.1.2 Potential security violation analysis (EXT_FAU_SAA)

The extended family "EXT_FAU_SAA: Potential security violation analysis" was modeled after FAU_SAA.

Family Behavior

This family defines the set of rules which SenSage 4.6.2 uses in analyzing the event data to detect a potential security violation.

Component Leveling

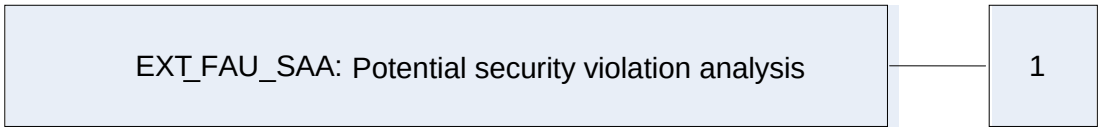

Figure 4 – EXT_FAU_SAA Potential security violation analysis family decomposition

EXT_FAU_SAA.1 Potential security violation analysis, defines the set of rules which SenSage 4.6.2 uses when analyzing event data to detect a potential security violation. It was modeled after FAU_SAA.1

EXT_FAU_SAA.1 Potential security violation analysis

Hierarchical to: No other components

Dependencies: FAU_GEN.1

This component will provide users the capability to detect a potential security violation by analyzing the event data by using a set of predefined rules and/or user-created rules.
EXT_FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the event data and based upon these rules, indicate a potential security violation.

EXT_FAU_SAA1.2 The TSF shall enforce the following rules for monitoring event data:

- **Accumulation or combination of [assignment: *subset of event data*] known to indicate a potential security violation;**
- **[assignment: *any other rules*]**

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 Parts 2 and 3 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 italicized 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 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_ARP.1	Security Alarms		✓	✓	
FAU_GEN.1	Audit data generation	✓	✓		
EXT_FAU_EDC.1	Event data collection		✓		
EXT_FAU_SAA.1	Potential security violation analysis		✓		
FAU_SAR.1	Audit review		✓		
FAU_STG.1	Protected audit trail storage	✓			
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
FDP_ACC.1(a)	Subset access control (SenSage Console)		✓		✓
FDP_ACC.1(b)	Subset access control (SenSage SLS)		✓		✓
FDP_ACF.1(a)	Security attribute based access control (SenSage Console)		✓		✓
FDP_ACF.1(b)	Security attribute based access control (SenSage SLS)		✓		✓
FIA_UAU.2	User authentication before any action				

Name	Description	S	A	R	I
FIA_UID.2	User identification before any action				
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialization	✓	✓		
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FMT_MTD.1(a)	Management of TSF Data (SenSage)	✓	✓		
FMT_MTD.1(b)	Management of TSF Data (SKV)	✓	✓		
FPT_ITC.1	Inter-TSF confidentiality during transmission				

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

6.2.1 Class FAU: Security Audit

FAU_ARP.1 Security alarms

Hierarchical to: No other components.

FAU_ARP.1.1

The TSF shall ~~**take**~~ [*notify the end-users of the TOE and a predetermined list of recipients via sending alerts to the SenSage console and sending alert e-mail messages to the email addresses associated with the list of recipients, respectively]* upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis

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) [*authentication attempts and administrative actions*].

FAU_GEN.1.2

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

Dependencies: FPT_STM.1 Reliable time stamps

EXT_FAU_EDC.1 Event Data Collection

Hierarchical to: No other components.

EXT_FAU_EDC.1.1

The TSF shall be able to collect event records based on the following:

a) All events collected from event data sources using [*SFTP, SCP, RCP, Syslog, Syslog(syslog-ng), SNMP, LEA, and HL-7*]; and

b) [*Patterns of event data indicative of User Object Modification Attack*

- *Patterns of event data indicative of Process Termination Attack*
- *Patterns of event data indicative of DNS Zone Transfer Attack*
- *Patterns of event data indicative of Generic Well Known Service Attack*
- *Patterns of event data indicative of Web Server Attack*
- *Patterns of event data indicative of Dictionary Password Attack*
- *Patterns of event data indicative of Many to one Threshold Attack*
- *Patterns of event data indicative of One to Many Threshold Attack*
- *Patterns of event data indicative of One to One Threshold Attack*]

].

EXT_FAU_EDC.1.2

The TSF shall be able to collect event records with the following:

a) Date and time of the event and type of event; and
b) For each event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

Dependencies: FPT_STM.1 Reliable time stamps

EXT_FAU_SAA.1 Potential security violation analysis

Hierarchical to: No other components.

EXT_FAU_SAA.1.1

The TSF shall be able to apply a set of rules in monitoring the event data and based upon these rules, indicate a potential security violation.

EXT_FAU_SAA.1.2.

The TSF shall enforce the following rules for monitoring event data:

- Accumulation or combination of [*following events:*
  - *Patterns of event data indicative of User Object Modification Attack*
  - *Patterns of event data indicative of Process Termination Attack*
  - *Patterns of event data indicative of DNS Zone Transfer Attack*
  - *Patterns of event data indicative of Generic Well Known Service Attack*
  - *Patterns of event data indicative of Web Server Attack*
  - *Patterns of event data indicative of Dictionary Password Attack*
  - *Patterns of event data indicative of Many to one Threshold Attack*
  - *Patterns of event data indicative of One to Many Threshold Attack*
  - *Patterns of event data indicative of One to One Threshold Attack*]

known to indicate a potential security violation;

- [*additional rules as follows:*
  - *User-Created Rules that specify conditions for triggering security alarms*]

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1 Audit Review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*administrator and analyzer.admin*] with the capability to read [*all audit events*] from the audit records.

FAU_SAR.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

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 key generation algorithms listed in the Key Generation Method column of Table 10*] and specified cryptographic key sizes [*the key sizes listed in the Cryptographic Key Size column of Table 10*] that meet the following: [*the standards listed in the Standards column of Table 10*].

Table 10 – Cryptographic Key Generation Standards

Key Generation Method	Cryptographic Key Size	Standards
X9.31	All key sizes specified in the Key Sizes (bits) column of Table 11 below	X9.31 (cert #xxx)

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

Note to Evaluator: The final certificates for the cryptographic functions have not yet been completed. The certificate numbers will be added when the FIPS evaluation has been finalized.

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 zeroization requirements*].

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

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1

The TSF shall perform [*the cryptographic operations listed in the Cryptographic Operations column of Table 11*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms listed in the Cryptographic Algorithm column of Table 11*] and cryptographic key sizes [*the cryptographic key sizes listed in the Key Sizes (bits) column of Table 11*] that meet the following: [*the list of standards in the Standards (Certificate #) column of Table 11*].

Table 11 – Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Symmetric encryption and decryption	Triple-DES[16] (2-Key, 3-Key) ECB,CBC,CFB, and OFB	128, 192	FIPS 46-3 (cert #xxx)
	AES[17] (128, 192, 256) ECB, CBC,CFB, and OFB	128, 192, 256	FIPS-197 (cert #xxx)
Random Number Generation	ANSI X9.31 RNG	Any	X9.31 (cert #xxx)

Dependencies: [FCS_CKM.1 Cryptographic key generation, or

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

Note to Evaluator: The final certificates for the cryptographic functions have not yet been completed. The certificate numbers will be added when the FIPS evaluation has been finalized.

[16] DES – Data Encryption Standard

[17] AES – Advanced Encryption Standard

6.2.3 Class FDP: User Data Protection

FDP_ACC.1(a) Subset access control (SenSage Console)
Hierarchical to: No other components.

FDP_ACC.1.1(a)

The TSF shall enforce the [*SenSage Console Access Control Policy*] on [

a. Subjects: TOE users

b. Objects: Reports, Report Folders, Dashboards, Dashboard Folders

c. *Operations: View, Edit, Run*].

Dependencies: FDP_ACF.1(a) Security attribute based access control (SenSage Console)

FDP_ACC.1(b) Subset access control (SenSage SLS)
Hierarchical to: No other components.

FDP_ACC.1.1(b)

The TSF shall enforce the [*SenSage SLS Access Control Policy*] on [

a. Subjects: TOE users

b. Namespaces[18]

c. *Operations: create, rename, view, load, drop, select, compact, retire, canceltask*].

Dependencies: FDP_ACF.1(b) Security attribute based access control (SenSage SLS)

FDP_ACF.1(a) Security attribute based access control (SenSage Console)
Hierarchical to: No other components.

[18] The namespace includes tables, views, column filters, and processes.

FDP_ACF.1.1(a)

The TSF shall enforce the [*SenSage Console Access Control Policy*] to objects based on the following: [

a. *Subjects: TOE users*

b. *Subject security attributes: User Identity, Roles*

c. *Objects: Reports, Report Folders, Dashboards, Dashboard Folders*

d. *Object attributes: Object Identity, Object Role-Permission pairs*

].

FDP_ACF.1.2(a)

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

a) If a user's assigned role is assigned permissions to access an object as defined in Object Role-Permission pairs, permit access;

b) If a user's assigned role lacks permissions to access an object as defined in Object Role-Permission pairs, deny access.

].

FDP_ACF.1.3(a)

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*The system user account and the administrator user account*].

FDP_ACF.1.4(a)

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*].

Dependencies: FDP_ACC.1(a) Subset access control (SenSage Console)
FMT_MSA.3 Static attribute initialization

FDP_ACF.1(b) Security attribute based access control (SenSage SLS)

Hierarchical to: No other components.

FDP_ACF.1.1(b)

The TSF shall enforce the [*SenSage SLS Access Control Policy*] to objects on the following: [

a. *Subjects: TOE users*

b. *Subject security attributes: User Identity, Roles,*

c. *Objects: Namespaces*

d. *Object attributes: Object Identity, Object Role-Permission pairs*

].

FDP_ACF.1.2(b)

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*The SenSage SLS Access Control Policy shall ensure objects are protected from unauthorized access according to the following rules:*

a) *If a user's assigned role is assigned permissions to access a namespace as defined in Object Role-Permission pairs, permit access;*

b) *If a user's assigned role lacks permissions to access a namespace as defined in Object Role-Permission pairs, deny access.*

].

FDP_ACF.1.3(b)

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*The system user account and the administrator user account*].

FDP_ACF.1.4(b)

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*].

Dependencies: FDP_ACC.1(b) Subset access control (SenSage SLS)
FMT_MSA.3 Static attribute initialization

6.2.4 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1

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

Dependencies: FIA_UID.1 Timing of identification

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

6.2.5 Class FMT: Security Management

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*SenSage Console Access Control SFP and SenSage SLS Access Control Policy*] to restrict the ability to [*query, modify, delete*] the security attributes [*Object Role-Permission pairs*] to [*administrator and analyzer.admin and for reports, the owner of a report*].

Dependencies: FDP_ACC.1(a) Subset access control (SenSage Console)
FDP_ACC.1(b) Subset access control (SenSage SLS)
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialization
Hierarchical to: No other components.

FMT_MSA.3.1

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

FMT_MSA.3.2

The TSF shall allow the [*User with Administrator role*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MOF.1 Management of security functions behavior
Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to [*determine the behavior of, disable, enable, modify the behavior of*] the functions [

a) event data parsing

b) event data analysis

c) data encryption

] to [*administrator and analyzer.admin*].

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: [*security attribute management, security audit management, security function management, user account management, SKV user account management, SKV key management, and role management*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*system; administrator; analyzer.admin; guest; analyzer.alerts; analyzer.reports; analyzer.dashboard; analyzer.reports.creator; Key Store Manager; Key Store User*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

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

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*perform operations identified in column 1 of Table 12*] the [*list of TSF data identified in column 2 of Table 12*] to [*administrator, analyzer.admin*].

Table 12 – Management of TSF Data (SenSage)

Operation	TSF data
Select	audit event data
add, view, modify, and delete	user identity and its associated roles and role-permissions

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

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

Hierarchical to: **No other components.**

FMT_MTD.1.1

The TSF shall restrict the ability to [*perform operations identified in column 1 of Table 13*] the [*list of TSF data identified in column 2 of Table 13*] to [*Key Store Manager*].

Table 13 – Management of TSF Data (SKV)

Operation	TSF data
add, view, modify, and delete	SKV user identity and its associated roles and role-permissions

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

6.2.6 Class FPT: Protection of the TSF

FPT_ITC.1 Inter-TSF confidentiality during transmission
Hierarchical to: No other components.

FPT_ITC.1.1

The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorized disclosure during transmission.

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 14 – Assurance Requirements summarizes the requirements.

Table 14 – Assurance Requirements

Assurance Requirements	
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 15 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
Alert Generation	FAU_ARP.1	Security alarms
	EXT_FAU_SAA.1	Potential security violation analysis
	EXT_FAU_EDC.1	Event Data Collection
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_ACC.1(a)	Subset access control (SenSage Console)
	FDP_ACC.1(b)	Subset access control (SenSage SLS)
	FDP_ACF.1(a)	Security attribute based access control (SenSage Console)
	FDP_ACF.1(b)	Security attribute based access control (SenSage SLS)
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
	FMT_MTD.1(a)	Management of TSF data (SenSage)
	FMT_MTD.1(b)	Management of TSF data (SKV)

TOE Security Function	SFR ID	Description
Protection of the TSF	FPT_ITC.1	Inter-TSF confidentiality during transmission

7.1.1 Security Audit

The TOE provides the ability to conduct security audit checks on the event data collected from the source machines. The TOE adds the timestamp to the event data collected from the source machines as it is received by the TOE. The TOE also performs audit (logging) for the TOE itself throughout various components of the TOE, and these audit logs are stored within each component and the SLS database. Some of the audit logs generated by the TOE are collected by the TOE on a scheduled basis, in the same way that third-party system event data are collected. Other audit logs for the TOE remain in-place where they were created and must be manually accessed and reviewed by administrators.

The TOE performs auditing of all events. Audit records without an error code and error message are successful. Audit records with an error code and error message are failures.

Table 16 – Audit Record Contents

Field	Content
Time	Time the activity occurred (yyyy-mm-dd hh:mm:ss)
Account	User account used to perform the activity
Source IP	IP address from which the user logged in
Action	Activity performed by the user
Object Accessed	Name of SenSage object accessed
Error Code	Error message code
Error Message	Text of error message

The TOE provides the end-users an ability to view the event data and the audit logs in the report from the SenSage Console.

The TOE provides the administrative TOE users an option to specify the level of detail for one of the audit logs generated by the TOE. The “activity.log” file, which gathers logs about all the activities in regards to the report functionality of the TOE (creating, editing, viewing, and running of the report), can be configured to collect different levels of details, ranging from “least verbose” to “intermediately verbose” to “most verbose”.

None of the event data received by the TOE and stored in the SLS database can be tampered with by unauthorized users. Once loaded into the SLS database, they cannot be modified or deleted. All event data stored in the SLS database is encrypted with keys stored in the SKV to protect against modification. The SLS database is read-only so data can never be deleted but only retired from the system by administrators connecting over the CLI.

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

7.1.2 Alert Generation

One of the primary features provided by the TOE is its ability to generate alerts and thereby notify the intended recipients of the possible security violations. This Alert Generation security function applies to

both the event data generated by the source machines (and collected by the TOE), and the audit logs for the TOE itself, generated and kept by the TOE.

The TOE performs an analysis on both incoming real time event data and historical event data from the source machines to determine if the condition to trigger an alert has been met. If so, the TOE generates an alert and notifies the intended recipients. The TOE can be configured to perform the same tasks for its own audit logs. These types of alerts are named *Security Alerts* (real-time) and *Exception Reports Alerts* (historical) respectively, and discussed below in more detail.

In addition to the alerts derived from the event data and the audit logs, the TOE raises alerts and notifies the intended recipients when the TOE Components are not functioning properly. This type of alert – known as *System Alerts* – is generated to indicate the status of the TOE's operation.

To summarize, the TOE categorizes three types of alerts as follows:

1. **Security Alerts** are raised in response to activity in monitored systems. For example, a security alert can be triggered when a particular user logs in, when certain servers are accessed, or when specified patterns of activity are detected. Security Alerts are a feature of the SenSage Real-Time Component and require *Parser Rules* to parse the incoming streams of event data and *Correlator Rules* to define the conditions that trigger an alert. As described in the section 1.4.1.4, the TOE supplies a set of predefined rules files and also allows the users to create their own rules files. The primary use of the Security Alerts is for the events generated by source machines that send their event data to the TOE.

2. **Exception Reports Alerts** are raised when a scheduled SenSage report triggers an exception report alert. The alerts are triggered when a designated report returns one or more rows. For example, a report that lists after-hours logins could trigger an alert when a user logs in after hours. In contrast to the Security Alerts, which are alerts raised when the TOE detects the alert-triggering conditions from analyzing the incoming real-time event data, Exception Reports Alerts are alerts raised from scheduled exception reports having run the SQL query over data already loaded in the SLS Component. In other words, Exception Report Alerts are alerts generated from the historical event data. It should be noted that the Exception Report Alerts are primarily used on the event data (historical) of the source machines that the TOE collects. However, the TOE can be configured so that it uses the Exception Reports Alerts on its own historical audit logs. The SLS and Real-Time components are responsible for generating exception report alerts.

3. **System Alerts** are raised in response to most important failures within the SenSage system itself. For example, an alert is raised when data fails to load as expected into the SLS Component. All SenSage components can generate system alerts in response to failures.

Users can view alerts via the SenSage Console, view the events that contributed to raising the alert, and define email notifications that are sent when the alert is raised.

The TOE shall be able to collect event data over the following protocols: SFTP, SCP, RCP, Syslog, Syslog(syslog-ng), SNMP, LEA, and HL-7.

TOE Security Functional Requirements Satisfied: FAU_ARP.1, EXT_FAU_SAA.1, EXT_FAU_EDC.1

7.1.3 Cryptographic Support

Encryption protects the data stored in the SLS Component from inspection or tampering by individuals or applications. An encrypted SenSage deployment functions exactly like an unencrypted deployment except that users must enter a special *pass phrase* to start, stop, or reconfigure the deployment. The encryption

applies only to "data at rest ", such as event data stored in the SLS component and the TOE configuration files.

Encryption-related information is stored and managed in the *Secure Key Vault* (SKV). The SKV maintains its own set of SKV *UserIDs* and *pass phrases* to control access to the SKV and encryption functionality. The SKV acts as a gate keeper for encryption in a SenSage deployment. SenSage modules gain access to encryption and decryption services through the SKV, which is implemented as a file stored on the local file system of each instance of the SLS component in the SenSage deployment.

The TOE implements a FIPS 140-2 validated cryptographic module that handles all cryptographic functions for the encryption of the data at rest. The FIPS 140-2 validated cryptographic module generates keys, which are stored in the SKV.

The FIPS 140-2 validated cryptographic module also encrypts user data in transit using TLS and SSH, for users connecting via SenSage Console and the CLI.

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

7.1.4 User Data Protection

The TOE has two different access control policies that work together to determine the access to objects. The SenSage Console Access Control Policy is applied to Report, Report Folder, Dashboard, and Dashboard Folders. The SenSage SLS Access Control Policy operates on namespaces which include Tables, Views, Column Filters, Tasks, and Child Namespaces. The subjects of the TOE are users. Each user has a user name, and a role.

Both access control policies determine access based on the Object Role-Permission pairs. It should be noted that the user must be allowed access by both access control policies. The TOE first checks the SenSage Console Access Policy and then the SenSage SLS Access Control Policy.

Access Control decisions on the objects are made based on the Object Role-Permission pairs defined for the requested object.

Below lists the predefined permissions that are available to TOE users who access the SLS component via CLI or SenSage Console

SLS Permissions

- sls.admin – users can view and manipulate authorization
- sls.create – users can create SLS objects, such as tables, views, and column filters
- sls.rename – users can rename SLS tables and views
- sls.drop – users can drop SLS objects, such as tables and column filters
- sls.canceltask – users can cancel SLS tasks in progress
- sls.compact – users can compact SLS tables
- sls.load – users can load data into SLS tables
- sls.retire – users can retire/delete rows from SLS tables
- sls.select – users can select data from SLS tables and views
- sls.namespace – users can access SLS objects only in specific namespaces. Users must also have one or more of the above permissions.

Below lists the predefined permissions that are available to TOE users who access the SenSage Console

Table 17 – Predefined permissions for SenSage Console

Permission	Context			
	Reports	Report Folders	Dashboard	Dashboard Folders
View	View reports cache entries; View the SQL and Search Criteria	View shortcut cache entries for reports to which the users has view permissions; View the Folder in the navigator	View the dashboard and its widgets The user can only view report and alert widgets for which the user has view permission	View the Folder in the navigator; View the dashboards contained in a folder; The user can only view dashboards for which the user has permission; The user can only view report and alert widgets for which the user has View permission
Edit	Edit the report definition; Change roles and permissions on the report;	Delete shortcuts to reports for which the user has Edit permission; Add short cuts to reports for which the user has View, Edit, or Run permission; Changes roles and permissions on the folder	Change a dashboard; The user can only add reports for which the user has View, Edit, or Run permission; The user must have analyzer.alerts permission to add alert widgets to the dashboard; Changes roles and permission on the dashboard	Add or delete dashboards contained in the folder; The user must have Edit permission on individual dashboards; Change roles and permissions on the folder
Run	Run the report	Run reports contained in the report folder; The user can only run reports for which the user has Run permission	Run reports contained in the dashboard; The user can only run reports for which the user has Run permission	n/a

TOE Security Functional Requirements Satisfied: FDP_ACC.1(a), FDP_ACC.1(b), FDP_ACF.1(a), FDP_ACF.1(b)

7.1.5 Identification and Authentication

The Identification and Authentication function ensures that the TOE user who is requesting a service has provided a valid username and password and is authorized to access that service.

The TOE performs the Identification and Authentication in one of two ways, depending on whether the TOE is configured to use the local SenSage authentication mechanism or the external authorization authority of the TOE environment.

When a TOE user enters his username and password from the SenSage Console UI or from the CLI, the information is checked against either an external authentication authority such as Active Directory, or against the local SenSage credentials data. After the user is identified and authenticated, the TOE allows the user to perform only those tasks and access only the data allowed by user's roles and permissions. A user cannot perform any other functions on the TOE without first completing the authentication steps.

When a TOE user has been successfully identified and authenticated by the TOE over the CLI, they may access the SKV functions by entering an additional passphrase. This additional passphrase will grant the user access to the SKV as a Key Store Manager or Key Store User. Only Key Store Managers may add additional SKV users.

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

7.1.6 Security Management

The TOE implements roles by assigning role permission to roles, and users to roles. It is the role permission that defines what functions of the CLI or SenSage Console that a given user can access and execute.

Users, roles, and role-permissions are related in the following ways:

- Role-Permissions specify what areas of the SLS, the SenSage Console, and event-log data users can access and what action they can perform.
- Role-Permissions are granted to roles.
- Users are assigned to roles and inherit each role's permissions.
- An Administrator can assign users to multiple roles and multiple permissions to roles.
- An Administrator cannot grant a permission directly to a user.

The TOE has two different user classes: *Special* user class and *Individual* user class. Because user accounts and roles under the *Special* user class are considered critical, they cannot be deleted. The System and Administrator user accounts are *Special* user accounts that are not required to follow the SenSage Access Control policy. The TOE provides the following predefined *Special* user accounts and roles assigned to them:

- ***System*** user account – is assigned the *system* role and is used by internal, automated processes to perform work requiring system authorization. The system user account and role are never assigned to an end user; they are strictly for the use of internal, automated processes. The system user has read access to all information and processes within an SLS instance.

- ***Administrator*** user account – is assigned to two roles:

    - *administrator* – grants full permission to view, create, modify, and delete all SenSage objects (such as table and views) in the SLS; this role is required for an end-user to administer an SLS instance.

- *analyzer.admin* – grants full permission to view, create, modify, and delete all SenSage objects (such as reports, dashboards, and folders) in all SenSage Console components, but does not grant permission to view, create, modify, and delete all SenSage objects in the SLS; this role is required for a user to administer the SenSage Console.

- ***Guest*** user account – is assigned the *guest* role and does not have any permissions by default. This role was created only to enable backward compatibility for early SenSage releases. It is suggested by SenSage not to assign the *guest* role to any end-user.

Table 18 below summarizes the structure of the Special User Class.

Table 18 – The Structure of the Special User Class

User Class	User Account	User Role	Permission
Special	System	system	Read access to all information and processes in the SLS
	Administrator	administrator	View, create, modify, and delete all SenSage objects in the SLS
		analyzer.admin	View, create, modify, and delete all SenSage objects in the SenSage Console
	Guest	guest	No permissions by default

Under the *Individual* user class, the TOE provides a set of predefined roles. Each of these predefined roles has permissions associated with them. The analyzer.admin, analyzer.reports, analyzer.reports.creator, analyzer.dashboard, and analyzer.alerts user roles listed in Table 19, refer to roles that can only connect via the SenSage Console. The analyzer.admin, analyzer.reports, analyzer.reports.creator, analyzer.dashboard, and analyzer.alerts user roles are required to follow the SenSage Access Control policy. Table 19 below lists a set of predefined roles that are available to the administrator-defined unique user accounts in the *Individua*l user class.

Table 19 – The Structure of the Individual User Class, and Predefined Roles & Permissions

User Class	User Account	User Role	Permission
Individual	Unique User ID[19]	analyzer.admin	Able to view, create, modify, and delete all SenSage objects in the SenSage Console
		analyzer.reports	Access to SenSage Console Report mode to view, edit, run the reports
		analyzer.reports.creator	Able to create new reports in SenSage Console
		analyzer.dashboard	Access to SenSage Dashboard mode to edit, view, and run dashboards and reports and to view alerts
		analyzer.alerts	Access to exception security and system alert widgets in the Chooser area in SenSage Console Dashboard mode
		administrator	Able to view, create, modify, and delete all SenSage objects in the SLS

[19] For the Individual user class, as no account names such as "System", "Administrator", or "Guest" are assigned by SenSage 4.6, any unique User ID defined by an administrator is equivalent to an Individual user class User Account.

User Class	User Account	User Role	Permission
		guest	No permission by default;

Any user (Special or Individual) with *administrator* role privilege can create users and roles, manage the relationships between the users and roles, and assign any of the existing permissions to any role. This user can also assign another user to the *administrator* and *analyzer.admin* roles. When *individual* users are assigned to these roles, they have the full privileges granted to the roles. *Individual* users, however, can be deleted. The inability to delete the *special* administrator user prevents system lock out.

It should be noted that when a new user account (e.g., johndoe) is created, the TOE creates a role named identically to the user account id and assigns the user to that role (e.g., johndoe). In TOE terminology, this is referred as a "shadow" role. The administrative TOE user can delete this shadow role and replace it with one of the SenSage-supplied user roles (for individual user class) in Table 19. Alternatively, the administrative TOE user can assign one or more of the SenSage-supplied permissions to the shadow role or rename the shadow role to something else and assign one or more the SenSage-supplied permissions.

Any user with *administrator* role can enable or disable or modify certain functionalities of the TOE. These include the ability to modify the parser rules and analysis rules in the Real Time Component, ability to enable or disable functions such as encryption of data at rest. In addition, any user with *administrator* role or *analyzer.admin* role can modify the Object Role-Permission pairs for any objects. For the Report object, in addition to the user with *administrator* role or *analyzer.admin* role, an owner of the report (a user with *analyzer.report.creator* role who created the report) can also assign specific View, Edit, and Run permissions to specific roles.

It should be noted that when namespace is created off of a root, it has no permissions granted. Child namespace inherits the permission of their parents. For Console object, when the object is created, it inherits the permissions of a parent container. Also, TOE does not allow the alternative initial values for object-permission pairs to be defined.

Only authorized administrators can perform the operations identified in Table 12 using the SenSage Console UI or the CLI. The CLI is used for initial system configuration, viewing status information, user administration, and system administration. SenSage Console provides a GUI Console for reports, alerts, asset management, user administration, and system administration.

In addition to the administrator roles that can be assigned to users connecting over the CLI, an additional role is assigned to administrators connecting to the SKV. An administrator connecting to the SKV can be assigned a Key Store Manager or Key Store User role. The Key Store Manager role has privileges to perform cryptographic operations on the SKV, create other SKV users with the Key Store Users role, re-key the SKV, and rotate master keys for data stored in the SLS columnar database. The Key Store User role has the privileges required to perform cryptographic operations. Only authorized administrators with the Key Store Manager role can perform the operations identified in Table 13 on the SKV using the CLI.

When a TOE user requests an operation to be performed on a particular object, the access control policy determines if the user's role(s) contains permission(s) that is sufficient for performing the requested operation on behalf of the requesting user. If the sufficient permissions for that particular object are found in the role of that TOE user, the requested operation on that object is performed. Otherwise, the requested operation is denied.

The SenSage Console queries the SKV on behalf of SenSage Console users to obtain the necessary information to encrypt or decrypt SLS objects accessed through the SenSage Console. Users connecting over the SenSage Console cannot directly retrieve key data and are only returned a filtered view for all data that is not allowed to be viewed with their SLS permissions.

TOE Security Functional Requirements Satisfied: FMT_MSA.1, FMT_MSA.3, FMT_MOF.1 FMT_SMF.1, FMT_SMR.1, FMT_MTD.1(a), FMT_MTD.1(b)

7.1.7 Protection of the TSF

TSF data is protected from unauthorized disclosure during transmission between the TSF and another trusted IT product by a FIPS 140-2 validated cryptographic module which encrypts user data in transit using TLS and SSH, for users connecting via SenSage Console and the CLI.

TOE Security Functional Requirements Satisfied: FPT_ITC.1

8 Rationale

8.1 Conformance Claims Rationale

There are no protection profile conformance claims for this security target.

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, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives is 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.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE data.	The O.ACCESS objective ensures that unauthorized modifications and access to data is prevented by the access control policies.
	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.	The O.ADMIN objective requires that only authorized users are able to manage the security attributes of the TOE.
	O.ENCRYPT The TOE must encrypt all TOE data at rest and user data in transit.	The O.ENCRYPT objective ensures that TOE data is protected from unauthorized inspection or tampering by individuals or applications.
	O.IDAUTH The TOE must identify and authenticate users prior to allowing access to TOE administrative functions and data.	By ensuring that the TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data, O.IDAUTH mitigates this threat.
	O.NOTIFICATION The TOE shall generate and deliver alerts upon detecting the patterns of event data indicative of potential security violations.	O.NOTIFICATION requires that the TOE generate and deliver alerts upon detecting potential security violations or the failure of any of its functional components. These alerts allow administrators of the TOE to help protect the TOE against unauthorized users.
	OE.SEP The IT Environment will protect the TOE from external interference or tampering.	The OE.SEP objective supports these objectives by requiring that the IT environment protect the TOE from interference that would

Threats	Objectives	Rationale
		prevent it from performing its functions.
	OE.TIME The IT Environment must provide reliable timestamps to the TOE.	The OE.TIME objective mitigates this threat by providing reliable time stamps to audit data and the event data collected by the TOE.
T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE data.	The O.ACCESS objectives ensure that unauthorized modifications and access to data is prevented. The O.ACCESS objective provides that the TOE must allow authorized operators to access only appropriate TOE data.
	O.INTEGRITY The TOE must ensure the integrity of all TOE data through its own interfaces.	O.INTEGRITY supports the mitigation of this threat by ensuring that only authorized users with appropriate permissions are able to delete the TOE data.
	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 supports the mitigation of this threat by ensuring that only authorized users may configure the TOE security mechanisms.
T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE data.	The O.ADMIN and O.ACCESS objectives together ensure that policies will not be subverted or changed by unauthorized users. The O.ACCESS objective provides that the TOE must allow authorized operators to access only appropriate TOE data.
	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.	The O.ADMIN and O.ACCESS objectives together ensure that policies won't be subverted or changed by unauthorized users. The O.ADMIN objective ensures that only TOE operators with appropriate privileges can manage the data of the TOE.
	O.AUDIT The TOE must gather audit logs of actions on the TOE and alerts which may be indicative of misuse.	The O.AUDIT objective provides defense in depth, by requiring the recording and availability of audit logs for review by an authorized operator of the TOE.
	O.IDAUTH The TOE must identify and authenticate users prior to allowing access to TOE administrative functions and data.	This threat is primarily diminished by the O.IDAUTH objective, which requires that the TOE must identify and authenticate operators prior to allowing access to TOE functions and data.

Threats	Objectives	Rationale
	O.NOTIFICATION The TOE shall generate and deliver alerts upon detecting the patterns of event data indicative of potential security violations.	O.NOTIFICATION requires that the TOE generate and deliver alerts upon detecting potential security violations or the failure of any of its functional components. This allows administrators of the TOE to protect the TOE against unauthorized users.
	OE.SEP The TOE environment must protect itself and the TOE from external interference or tampering.	The OE.SEP objective supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.
	OE.TIME The IT Environment must provide reliable timestamps to the TOE.	The OE.TIME objective mitigates this threat by providing reliable time stamps to audit data and the event data collected by the TOE.

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 Policies

There are no Organization Security Policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 21 – Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	NOE.NOEVIL Users are non-hostile, appropriately trained, and follow all user guidance.	The NOE.NOEVIL objective ensures that operators are non-hostile, appropriately trained, and follow all operator guidance.
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 satisfies the assumption that the IT environment provides reliable timestamps for the TOE.
A.PHYSICAL The TOE resides in a physically controlled access facility that prevents unauthorized physical access.	NOE.PHYSICAL The TOE will be located within controlled access facilities which will prevent unauthorized physical access.	The NOE.PHYSICAL objective requires that the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

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

The TOE contains the following explicitly stated security functional requirements for which there is no CC Part 2 equivalent:

- EXT_FAU_EDC.1
- EXT_FAU_SAA.1

The extended family "EXT_FAU_EDC: Event data collection" defines the set of rules which SenSage 4.6.2 uses when collecting event data to be stored in the SLS database. It is modeled after FAU_GEN.1. EXT_FAU_EDC.1 is explicitly stated because the TOE is capable of gathering event data which is used to generate alerts which may be indicative of misuse.

The extended family "EXT_FAU_SAA: Potential security violation analysis" defines the set of rules which SenSage 4.6.2 uses in analyzing the event data to detect a potential security violation. It is modeled after FAU_SAA.1. EXT_FAU_SAA is explicitly stated because the TOE is able to analyze the event data for detecting potential security violation.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended TOE security assurance requirements.

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.ACCESS The TOE must allow authorized users to access only appropriate TOE data.	FDP_ACC.1(a) Subset access control (SenSage Console)	The TOE has an access control policy that ensures that only authorized SenSage Console users gain access to TOE data.
	FDP_ACC.1(b) Subset access control (SenSage SLS)	The TOE has an access control policy that ensures that only authorized SenSage SLS users gain access to TOE data.
	FDP_ACF.1(a) Security attribute based access control (SenSage Console)	The TOE is required to provide authorized SenSage Console users access to TOE data.
	FDP_ACF.1(b) Security attribute base access control (SenSage SLS)	The TOE is required to provide authorized SenSage SLS users access to TOE data.
	FIA_UAU.2	The TOE will not give any user

Objective	Requirements Addressing the Objective	Rationale
	User authentication before any action	access to the TOE's data and functions until the TOE has authenticated the user.
	FIA_UID.2 User identification before any action	The TOE will not give any user access to the TOE's data and functions until the TOE has identified the user.
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with appropriate privileges and only those TOE users, may exercise such control.	FMT_MSA.1 Management of security attributes	Only the appropriately authorized users of the TOE are given the right to modify or set defaults for TOE security attributes.
	FMT_MSA.3 Static attribute initialization	Restrictive values for TOE functions and data are provided, and the authorized administrator can change them when a data object is created.
	FMT_MOF.1 Management of security functions behavior	The requirement meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate role permissions
	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 role	The TOE defines a set of roles.
	FMT_MTD.1(a) Management of TSF data (SenSage)	FMT_MTD.1(a) supports this objective by ensuring that the TOE will restrict the ability to perform the operations identified in Table 12.
	FMT_MTD.1(b) Management of TSF data (SKV)	FMT_MTD.1(b) supports this objective by ensuring that the TOE will restrict the ability to perform the operations identified in Table 13.
O.AUDIT The TOE must gather audit logs of actions on the TOE and alerts which may be indicative of misuse.	FAU_ARP.1 Security alarms	The requirement meets this objective by ensuring that the TOE notifies the intended recipients of the potential security threats by sending alerts.
	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.
	EXT_FAU_SAA.1 Potential security violation analysis	The requirement meets this objective by ensuring that the TOE is able to analyze the event data

Objective	Requirements Addressing the Objective	Rationale
		for detecting potential security violation.
	EXT_FAU_EDC.1 Event Data Collection	The requirement meets the objective by gathering event data which is used to generate alerts which may be indicative of misuse.
	FAU_SAR.1 Audit review	The TOE provides the ability to review the audit trail of the system.
O.ENCRYPT The TOE must encrypt the all TOE data at rest and user data in transit.	FCS_CKM.1 Cryptographic key generation	This requirement supports O.ENCRYPT by requiring that cryptographic keys are generated according to an assigned standard.
	FCS_CKM.4 Cryptographic key generation	This requirement supports O.ENCRYPT by ensuring that cryptographic keys are destroyed according to FIPS 140-2 zeroization requirements.
	FCS_COP.1 Cryptographic operation	This requirement supports O.ENCRYPT by requiring cryptographic operations be performed according to the specified algorithms with the specified key sizes.
	FPT_ITC.1 Inter-TSF confidentiality during transmission	This requirement supports O.ENCRYPT by ensuring all TSF data is protected from unauthorized disclosure during transmission between the TSF and another trusted IT product.
O.IDAUTH The TOE must identify and authenticate users prior to allowing access to TOE administrative functions and data.	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that users are authenticated before access to TOE administrative functions is allowed.
	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.INTEGRITY The TOE must ensure the integrity of all TOE data through its own interfaces.	FAU_STG.1 Protected audit trail storage	The TOE protects the audit data from unauthorized deletion.
	FDP_ACF.1(a) Security attribute based access control (SenSage Console)	Only authorized TOE users with the appropriate permissions may access TOE data.
	FDP_ACF.1(b) Security attribute based access control (SenSage SLS)	Only authorized TOE users with the appropriate permissions may access TOE data.
	FDP_ACC.1(a) Subset access control(SenSage	The TOE has an access control policy that ensures that only

Objective	Requirements Addressing the Objective	Rationale
	Console)	authorized users gain access to TOE data.
	FDP_ACC.1(b) (SenSage SLS) Subset access control	The TOE has an access control policy that ensures that only authorized users gain access to TOE data.
	FMT_MSA.1 Management of security attributes	Only authorized users of the TOE may query and modify TOE data.
	FCP_COP.1 Cryptographic operation	This requirement supports O.INTEGRITY by ensuring that cryptographic operations are used to ensure the integrity of data.
O.NOTIFICATION The TOE shall generate and deliver alerts upon detecting the patterns of event data indicative of potential security violations.	FAU_ARP.1 Security alarms	The requirement meets the objective by specifying the actions to be taken by the TOE when potential security violations are detected.
	EXT_FAU_SAA.1 Potential security violation analysis	The requirement meets the objective by specifying the rules that identify potential security violations.

8.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. At EAL2, the TOE will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

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

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_ARP.1	FAU_SAA.1	✓	The dependency is met with EXT_FAU_SAA.1.
FAU_GEN.1	FPT_STM.1	✓	FPT_STM.1 is not included since the TOE environment (the underlying hardware) provides the timestamps that are used by the TOE. Environmental Objective

SFR ID	Dependencies	Dependency Met	Rationale
			OE.TIME satisfies this requirement.
EXT_FAU_EDC.1	FPT_STM.1	✓	FPT_STM.1 is not included since the TOE environment (the underlying hardware) provides the timestamps that are used by the TOE. Environmental Objective OE.TIME satisfies this requirement.
EXT_FAU_SAA.1	FAU_GEN.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FCS_CKM.1	FCS_CKM.4	✓	
	FCS_COP.1	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.4	✓	
	FCS_CKM.1	✓	
FDP_ACC.1(a)	FDP_ACF.1(a)	✓	
FDP_ACC.1(b)	FDP_ACF.1(b)	✓	
FDP_ACF.1(a)	FDP_ACC.1(a)	✓	
	FMT_MSA.3	✓	
FDP_ACF.1(b)	FDP_ACC.1(b)	✓	
	FMT_MSA.3	✓	
FIA_UAU.2	FIA_UID.1	✓	
FIA_UID.2	No dependencies	✓	
FMT_MSA.1	FDP_ACC.1(a)	✓	
	FDP_ACC.1(b)	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	
FMT_MTD.1(a)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(b)	FMT_SMF.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FMT_SMR.1	✓	
FPT_ITC.1	No dependencies	✓	

9 Acronyms

9.1 Acronyms

Table 24 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ATM	Automatic Teller Machine
CBC	Cipher Block Chaining
CC	Common Criteria
CDR	Call Detail Record
CLI	Command Line Interface
CM	Configuration Management
CPU	Central Processing Unit
DES	Data Encryption Standard
DNS	Domain Name Server
EAL	Evaluation Assurance Level
ECB	Electronic Codebook
GB	Gigabyte
GHZ	Gigahertz
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
HTTPS	Secure Hypertext Transfer Protocol
IP	Internet Protocol
IPDR	Internet Protocol Detail Records
ISO	International Organization for Standardization
IT	Information Technology
JRE	Java Runtime Environment
LDAP	Lightweight Directory Access Control
N/A	Not Applicable
OS	Operating System
PP	Protection Profile
RAID	Redundant Array of Inexpensive Disks
RAM	Random Access Memory

Acronym	Definition
RNG	Random Number Generator
PTL	Parser, Transform, and Load
SAR	Security Assurance Requirement
SCSI	Small Computer System Interface
SFR	Security Functional Requirement
SHA	Secure Hashing Algorithm
SKV	Secure Key Vault
SLS	Scalable Log Server
SSH	Secure SHell
ST	Security Target
TB	Terabyte
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
XML	Extensible Markup Language

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

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