Hewlett-Packard Enterprise Development, L.P.

Server Automation Ultimate v10.10.002

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.9

Prepared for:

Hewlett Packard Enterprise

Hewlett-Packard Enterprise Development, L.P.
3000 Hanover Street
Palo Alto, CA 94304
United States of America

Phone: +1 305 267 4220
Email: info@hpe.com
http://www.hpe.com

Prepared by:

Corsec

Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the HP Server Automation Ultimate v10.10.002, and will hereafter be referred to as the TOE throughout this document. The TOE is software-only, which provides complete automated lifecycle management for enterprise servers. It provides a scalable and heterogeneous solution for establishing a baseline, patching, configuration management, script management, and compliance management across physical and virtual servers.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality 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, 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 Security 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 and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 ST and TOE References

ST Title	Hewlett-Packard Enterprise Development, L.P. Server Automation Ultimate v10.10.002 Security Target
ST Version	Version 1.9
ST Author	Corsec Security, Inc.
ST Publication Date	12/17/2015

TOE Reference	HP Server Automation Ultimate v10.10.002 Build 55.0.51417.0
FIPS 140-2 Status	Level 1, OpenSSL FIPS[1] Object Module, Software Version 2.0.5, Certificate No. 1747 Level 1, RSA[2] BSAFE Crypto-J JSAFE and JCE[3] Software Module, Software Version 6.1, Certificate No. 2057

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 introduce the parts of the overall product offering that are specifically being evaluated.

HP Server Automation Ultimate (also referred as SA) is a complete and heterogeneous lifecycle management solution for enterprise servers, which allow customers to standardize, consolidate, and automate server operations in their hybrid data centers. SA provides a single solution for data center automation across Linux, Solaris, Windows® and UNIX® platforms. It is supported on physical hardware, both HPE and non-HPE servers, and on virtualized platforms.

SA is full-scale server automation software that includes:

- OS[4] provisioning and patching
- Server discovery and device explorer
- Application configuration management and deployment
- Audit, remediation, and reporting
- Storage visibility, automation, and Service Automation Visualizer (SAV)
- Virtual server management

The remainder of this section is a brief description of these features.

1.3.1 OS provisioning and patching

SA OS provisioning provides the ability to provision OS baselines onto bare metal and virtual servers. SA automates the following OS installation tasks:

- Preparing hardware for OS installation.
- Defining OS build plans and OS sequences, which are a list of tasks to be performed on a server before and after OS installation.
- Installing a baseline OS and default OS configuration.
- Installing system applications such as SSH[5], anti-virus software, or Java Virtual Machines (JVMs).

SA also provides an automated, centralized, and flexible method of applying the required OS patches for Windows®, Linux, and UNIX®-based managed servers[6].

1.3.2 Server discovery and device explorer

Server discovery allows SA to scan a network for servers, and it allows SA to deploy SA Agents[7] to a large number of discovered servers and place them under SA management. SA's device explorer is used to view information about managed servers in the environment.

[1] FIPS – Federal Information Processing Standards
[2] RSA – Rivest, Shamir, and Adelman
[3] JCE – Java Cryptography Extension
[4] OS – Operating System
[5] SSH – Secure Shell
[6] Managed Servers are the servers on network managed by SA.

1.3.3 Application configuration management and deployment

SA's application configuration management feature is used to design application configuration templates and push these configurations to all SA managed servers. SA is also used to automate the process of deploying software applications onto managed servers in a single step.

1.3.4 Audit, remediation, and reporting

SA audit and remediation allows users to define managed server configuration policies, audit compliance to these policies, and remediates managed servers that are found to be out of compliance with these policies. SA provides an extensive set of comprehensive and configurable reports that present the state of the managed servers.

1.3.5 Storage visibility, automation, and SAV

Storage visibility and automation enables end-to-end visibility and management of the entire storage subsystems. SAV provides a visual environment for automating change and compliance management across data centers. It also maps relationships and dependencies across distributed business applications in the IT[8] environment.

1.3.6 Virtual server management

Virtual server management provisions and manages virtual servers. SA integrates with VMware vCenter, Oracle Solaris, HP Matrix, and Microsoft SCM[9] in order to support the provisioning of virtual machines within VMware vSphere, Oracle Solaris Zones, HP-UX, and Microsoft Hyper-V hypervisors.

1.4 TOE Overview

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

The TOE is an automation software solution, which centralizes and automates server configuration and lifecycle management for the hybrid data center. The TOE scans network to discover servers, and bring them under the TOE management. The TOE installs SA Agent software on the SA Managed Servers to patch, audit, monitor, and maintain those servers. Figure 1 below shows an HP SA deployment scenario in the evaluated configuration.

The following previously undefined acronyms appear in the Figure 1 below.

- API – Application Programming Interface
- HTTPS – Hypertext Transfer Protocol Secure
- LDAP – Lightweight Directory Access Protocol
- OCSP – Online Certificate Status Protocol
- RHEL – Red Hat Enterprise Linux
- TLS – Transport Layer Security

[7] The SA Agent is a SA software component installed on a SA Managed Server.
[8] IT – Information Technology

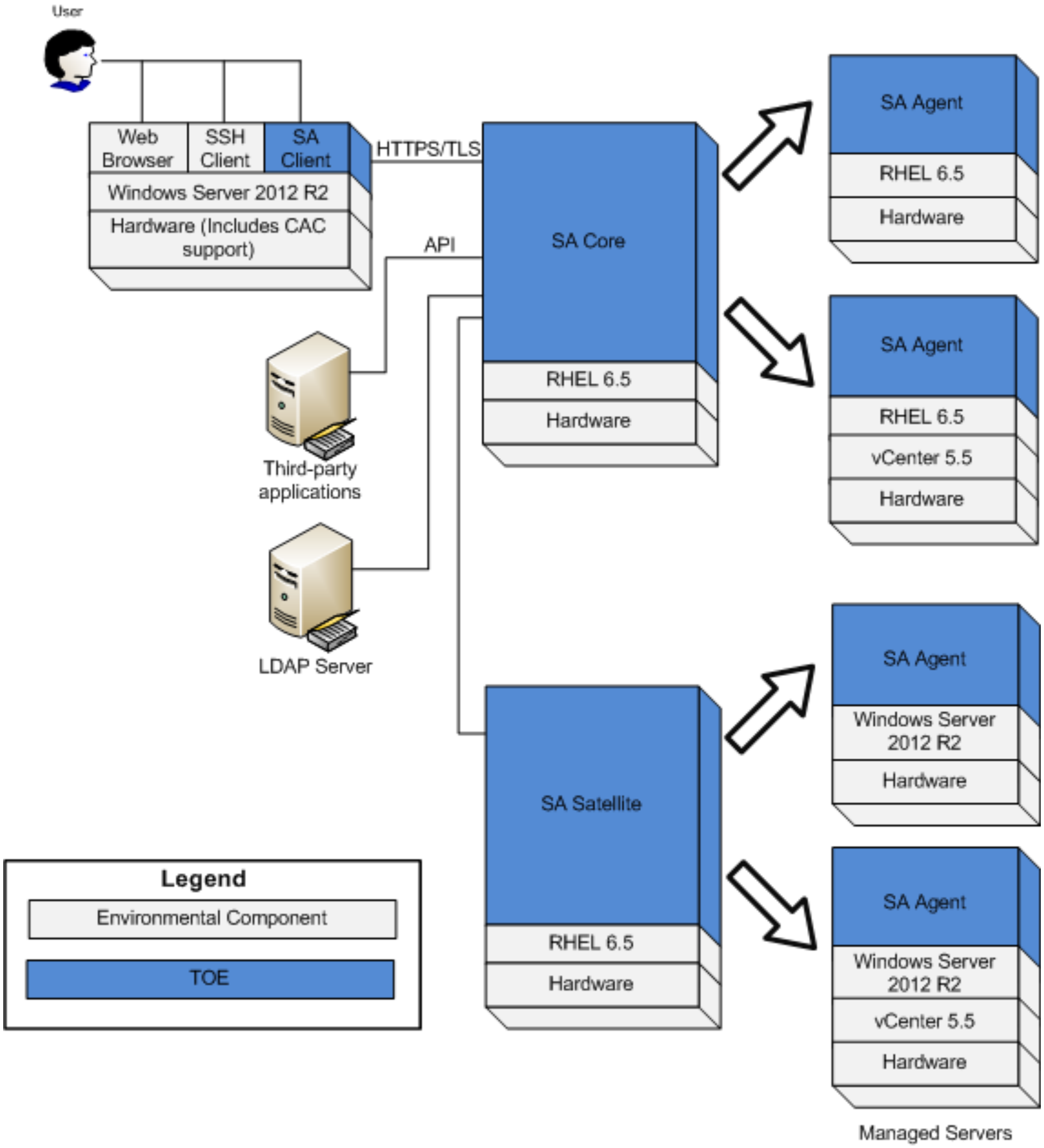

Figure 1 HP SA Deployment Configuration

The TOE consists of the following major components:

- SA Core,
- SA Satellite,
- SA Agent(s), and
- SA Client

The SA Core component is the heart of SA. It allows the TOE to discover unmanaged servers on a network, and place them under TOE management. The SA Core component stores information about the location and configuration of all the SA Managed Servers on network. The SA Core provides management and secure communication capabilities to all those Managed Servers.

The SA Satellite is a lightweight versions of the SA Core. The SA Satellite is a solution for remote sites that do not have a large enough number of Managed Servers. The SA Satellite also facilitates management of devices that reside within network blind spots such as those that are in different networks than a SA Core or in non-public IP[10] spaces.

The SA Agent is a software component installed by SA on Managed Servers. When the SA Agent is installed on an unmanaged server, the unmanaged server is registered with the SA Core and is added to the SA pool of Managed Servers. The SA Agent communicates with the SA Core and responds to commands on behalf of the Managed Server. These commands may:

- install patches,
- install and remove applications,
- perform configuration of software or hardware, and
- report managed server status.

The SA Client is a Microsoft Windows® based interface for managing, monitoring, and configuring the TOE. The TOE also provides a web-based GUI[11] over HTTPS for TOE administration. Additionally, the TOE exposes an API that can be called externally by third-party applications. The API includes libraries for Java RMI[12] clients. All these interfaces are used to connect to the SA Core.

Figure 1 above shows TOE deployed in a Multimaster Mesh configuration. A Multimaster Mesh is a TOE deployment consisting of two or more SA Cores, or a combination of SA Core(s) and SA Satellite(s). The evaluated configuration includes a single SA Core, and single SA Satellite deployed in a Multimaster Mesh configuration managing SA Agents installed on Managed Servers, and virtualization platforms.

The TOE implements Role Based Access Control (RBAC), where only authorized users can perform management actions. In addition to RBAC, the TOE also enforces permissions, which regulate user authorizations to operations performed on Managed Servers. The TOE maintains a detailed audit trail of events performed by TOE users.

The TOE supports password-based authentication, which consists of a username and password for each user, which are used for identity verification and authentication.

All individual TOE components communicate with each other using X.509 certificates and a secure TLS session over an IP network. The TOE establishes TLS v1.0 sessions between the

- SA Core and SA Agent(s)
- SA Satellite and SA Agent(s)
- SA Client and SA Core
- SA Core and SA Satellite

The TOE provides a secure connection with the web GUI using HTTPS (via TLS v1.0). The TOE leverages the FIPS 140-2 validated OpenSSL FIPS Object Module, Software Version 2.0.5 and RSA Crypto-J Software Module, Software Version 6.1 libraries for providing secure communications.

1.4.1 TOE Environment

The TOE environment consists of supported server platforms for SA Core, SA Satellite, SA Agent(s), and SA Client, and hypervisors. Table 2 specifies the TOE environment included in the evaluated configuration.

[10] IP – Internet Protocol
[11] GUI – Graphical User Interface
[12] RMI – Remote Method Invocation

Table 2 TOE Environment

Category	Requirement
SA Core Server	RHEL 6.5 Base Server
SA Satellite Server	RHEL 6.5 Base Server
SA Agent Server	RHEL 6.5 Base Server Microsoft Windows Server 2012 R2
SA Agent Virtualization	VMware vCenter 5.5 VM[13] running Red Hat RHEL 6.5 Base Server VMware vCenter 5.5 VM running Microsoft Windows Server 2012 R2
SA Client	Microsoft Windows Server 2012 R2

The TOE environment also consists of an SSH client capable of negotiating v2 of the SSH protocol, a web browser (Google Chrome 6 or later; or Microsoft Internet Explorer 8 or later), and an LDAP authentication server which is used for user authentication externally using LDAPv3.

1.5 TOE Description

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

1.5.1 Physical Scope

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.

The TOE boundary consists of HP Server Automation Ultimate v10.10.002 software, which comprises the binaries for

- SA Core,
- SA Satellite,
- SA Agent, and
- SA Client

See section 1.4.1 for the essential components for the proper operation of the TOE in the evaluated configuration.

[13] VM – Virtual Machine

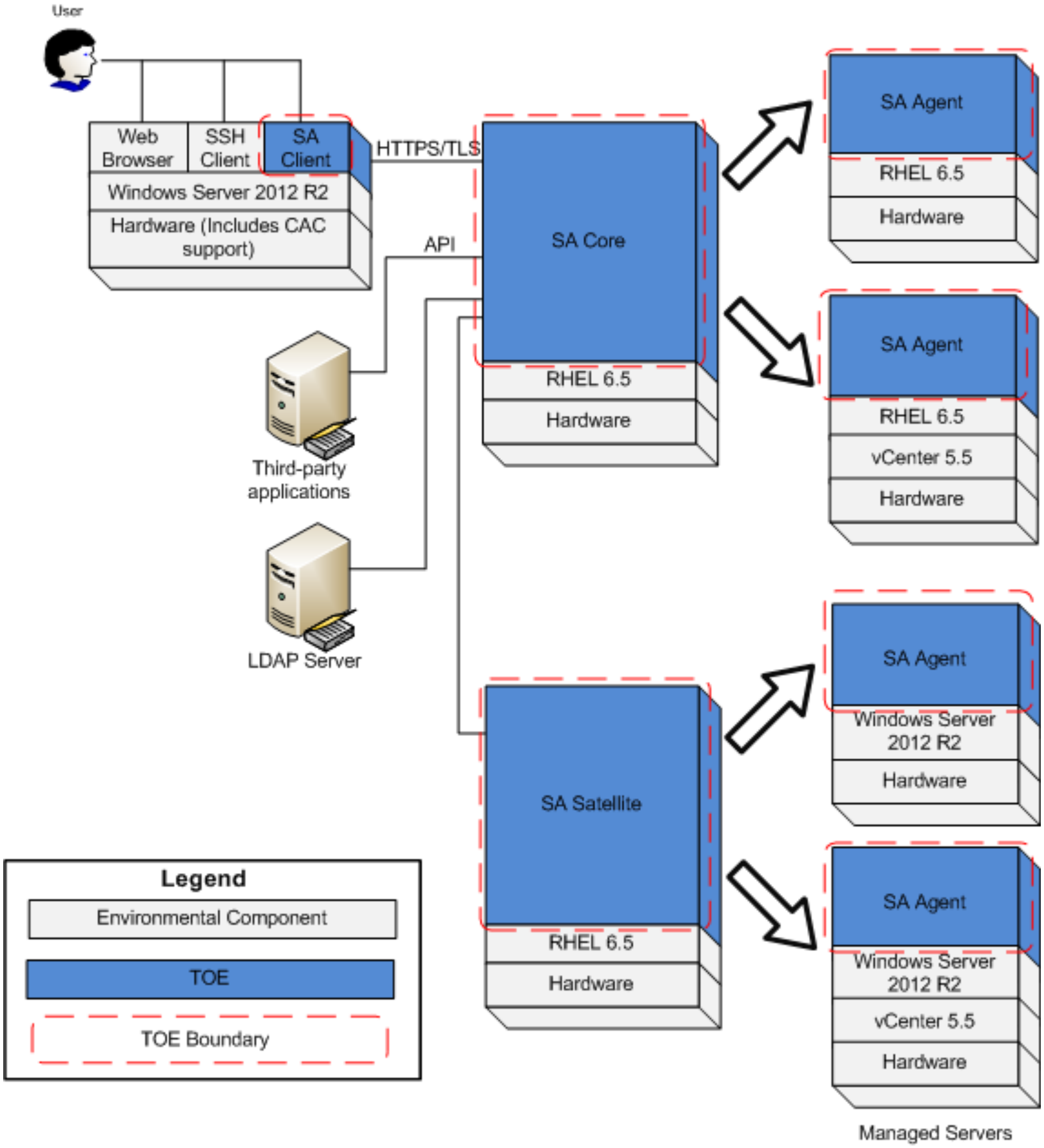

Figure 2 Physical TOE Boundary

1.5.1.1 Guidance Documentation

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

- Hewlett-Packard Enterprise Development, L.P. Server Automation Ultimate v10.10.002 Guidance Documentation Supplement
- HP Server Automation; Ultimate Edition; Software Version 10.10 Administration Guide
- HP Server Automation; Ultimate Edition; Software Version 10.10; Installation Guide
- HP Server Automation; Ultimate Edition; Software Version 10.10; User Guide
- HP Server Automation; Ultimate Edition; Software Version 10.10; User Guide: Virtualization Management

- HP Server Automation; Ultimate Edition; Software Version 10.10; Platform Developer Guide
- *HP Server Automation; Ultimate Edition; Software Version 10.10; Release Notes
- *HP Server Automation; Ultimate Edition; Software Version 10.10; FIPS 140-2 Compliance Statement
- HP Server Automation; Ultimate Edition; Software Version 10.10; Content Utilities
- HP Server Automation; Ultimate Edition; Software Version 10.10; Storage Visibility and Automation Installation & Administration Guide
- HP Server Automation; Ultimate Edition; Software Version 10.10; Overview and Architecture
- HP Server Automation; Ultimate Edition; Software Version 10.10; Reports Guide
- HP Server Automation; Ultimate Edition; Software Version 10.10; Storage Visibility and Automation User Guide
- HP Server Automation; Ultimate Edition; Software Version 10.10; Application Configuration
- HP Server Automation; Ultimate Edition; Software Version 10.10; Application Deployment Manager
- HP Server Automation; Ultimate Edition; Software Version 10.10; Audit & Compliance
- HP Server Automation; Ultimate Edition; Software Version 10.10; Server Patching
- HP Server Automation; Ultimate Edition; Software Version 10.10; Server Automation Visualizer
- HP Server Automation; Ultimate Edition; Software Version 10.10; Software Management

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes, which are further, described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF[14]
- TOE Access
- Trusted Path/Channels

1.5.2.1 Security Audit

The TOE generates log files to record auditable events. The TOE audits the start-up event and user login attempts. The audit logs contain the identity of the user (if applicable) that caused event to occur. The TOE provides all authorized users with the ability to review the audit logs.

1.5.2.2 Cryptographic Support

The FIPS-validated cryptographic modules in the TOE provide all necessary cryptographic services while in the evaluated configuration. The TOE utilizes the FIPS 140-2 validated OpenSSL FIPS Object Module, Software Version 2.0.5 and RSA Crypto-J Software Module, Software Version 6.1 libraries for performing cryptographic operations. The FIPS 140-2 certificates for the cryptographic modules used by the TOE are #1747 and #2057, respectively.

The Cryptographic Support TSF provides cryptographic functions to secure communications between the SA Client or a web browser on the client workstation to the SA Core. The TOE also provides cryptographic functions to secure communications between distributed components of the TOE using

[*] Required reading only, not necessary for installation.

[14] TSF – TOE Security Functionality

certificate-based authentication. The TOE destroys cryptographic keys in accordance with FIPS 140-2 zeroization requirements.

1.5.2.3 User Data Protection

The TOE provides user data protection by enforcing the SA Access Control SFP[15] on Resource[16] and Folder objects. The SA Access Control SFP limits each user's access based on role[17], and object-level permissions, which grant authorizations to perform operations on objects. The TOE provides the following permissions needed to perform an operation on a managed server:

- Resource permissions: Read, Read & Write, or no resource permissions are assigned
- Folder permissions:
    - List contents of folder
    - Read objects within folder
    - Write objects within folder
    - Execute objects within folder
    - Edit folder permissions

1.5.2.4 Identification and Authentication

The TOE identification and authentication functionality requires TOE users to successfully identify and authenticate to the TOE to access its functionality. The TOE provides password-based authentication mechanism. The TOE maintains the username, role, and password belonging to individual users to enforce identification and authentication functionality. During authentication, characters entered during password entry are replaced by bullets ('*') over the SA Client or GUI over web browser. User accounts are suspended when configured number of failed login attempts is met.

1.5.2.5 Security Management

The TOE implements RBAC functionality to selectively grant administrative permissions to roles as needed. Each TOE user is assigned one or more roles, and will assume all capabilities of the combined roles. SA ships with a single Super Administrator account with default credentials, which has full access to SA. Additionally, HPE includes other predefined roles (See section 6.2.5). All object security attributes contain restrictive default values, where an authorized user can modify, query, and change the default values to all object security attributes.

1.5.2.6 Protection of the TSF

SA utilizes cryptographic services to secure communications between distributed components of the TOE to prevent unauthorized disclosure, and modification of TSF data. The TOE employs TLS v1.0 for securing communications between:

- SA Core and SA Agent(s)
- SA Satellite and SA Agent(s)
- SA Client and SA Core
- SA Core and SA Satellite

The TOE provides the ability to run diagnostic and health tests periodically or at the request of an authorized user for SA Cores and SA Agents on SA Managed Servers.

1.5.2.7 TOE Access

The TOE mitigates unauthorized user access by automatically locking the current session for the SA client after a Super Administrator configured time interval of inactivity. In order for a user to regain access of a

[15] SFP – Security Functional Policy

[16] Resources – Resources are one or more SA Managed Servers

[17] Role represents a User Group or a Super Administrator

timed out session, the user must successfully re-authenticate with the credentials of the user owning the locked out session.

1.5.2.8 Trusted Path/Channels

The cryptographic functionality of the TOE provides the TOE with the ability to create trusted channels and trusted paths. The TOE implements trusted channels using HTTPS/TLS v1.0 between itself and a remote LDAP authentication server during remote authentication attempts to provide protection of the credentials during transmission. The TOE also establishes secure communication with external IT entities such as web services clients over HTTPS.

The TOE provides a secure communication path between itself and remote users. The TOE provides trusted paths between TOE operators and the GUI over an HTTPS connection from a web browser. The management communication paths are logically distinct from other communication paths and channels. These paths provide mutual identification and authentication of each end of the communication channel. These communications paths are also protected from modification and disclosure.

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

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- Multimaster Mesh configuration – Cores only
- Agent Tools
- OS Provisioning
- Command Line Interface (CLI) access
- Global File System (OGFS) access

2 Conformance Claims

This section and Table 3 provide the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 3 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 4, September 2012; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM[18] as of 2014/11/28 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)

[18] CEM – Common Methodology for Information Technology Security Evaluation

3 Security Problem

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

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

3.1 Threats to Security

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

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

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

Table 4 Threats

Name	Description
T.ACCESS	The TSF must control access of subjects to objects based on access control. The TSF must allow authorized users to specify which subjects are allowed to access a specific object. A threat agent might gain access to user data stored, processed, or transmitted by the TOE without being appropriately authorized according to the TOE security policy.
T.COMINT	An unauthorized person may attempt to compromise the integrity of the data discovered and events produced by the TOE by bypassing a security mechanism.
T.FAILURE	The failure of an SA Core component or SA Agent could go undetected or cause a breach of the TSF.
T.NOAUDIT	An attacker may perform security relevant operations on the TOE without being held accountable for them.
T.TRANSMIT	A user or process may be able to bypass the TOE's security mechanisms and gain access to the data while the data is in transit.
T.UNATTEND	An unauthorized user could attempt to take over an unattended session and perform malicious activities.
T.UNAUTH	An unauthorized user may bypass the TOE's identification,

Name	Description
	authentication, or authorization mechanisms in order to illicitly utilize the TOE's management functions, or TSF data.

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 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. Table 5 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 5 Assumptions

Name	Description
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware and operating system.
A.DEDICATED	Those responsible for installing the TOE will ensure that the SA Core server is only used for the SA Core and have no other purpose. In addition, the users responsible for installing the TOE will protect the SA Core installation log.
A.LOCATE	The TOE is located within a controlled access facility.
A.NETCON	The TOE environment provides the network connectivity required to allow the TOE to perform its intended functions.
A.NOEVIL	The users who manage the TOE and the security of the information it contains are non-hostile, appropriately trained, and follow all guidance.
A.PROTECT	The TOE software is protected from unauthorized modification.
A.TIMESTAMP	The TOE 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 listed in Table 6 below.

Table 6 Security Objectives for the TOE

Name	Description
O.ACCESS	The TSF must control access of subjects to objects based on access control. The TSF must allow authorized users to specify which subjects are allowed to access objects covered by access control SFP.
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.ATTRIB	The TOE will be capable of maintaining user security attributes.
O.AUDIT	The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review audit records.
O.AUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.AUTO	The TOE must provide the ability to automatically run the health tests for monitoring SA Core components and SA Agents both periodically and at the request of an authorized user.
O.CRYPTO	The TOE must provide the means of protecting cryptographic operations and secure management of cryptographic keys using cryptography that conforms to standards specified in FIPS PUB 140-2.
O.SECURE	The TOE shall securely transfer data with other trusted IT entities and remote users.
O.SESSION	The TOE will provide a mechanism that controls a user's logical access to the TOE.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 7 below lists the IT security objectives that are to be satisfied by the environment.

Table 7 IT Security Objectives

Name	Description
OE.DEDICATED	The hardware and OS from the operating environment that host the SA Core server must be used to only support the SA Core server's functionality.
OE.MONITOR	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.
OE.PLATFORM	The hardware and OS from the operating environment that host the TOE must support all required TOE functions.
OE.PROTECT	The TOE environment must protect itself, the network on which the TOE is deployed, and the TOE from external interference or tampering.
OE.TIME	The underlying Operating System must provide reliable timestamps to the TOE.

4.2.2 Non-IT Security Objectives

Table 8 below lists the non-IT environment security objectives that 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 8 Non-IT Security Objectives

Name	Description
NOE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives.
NOE.NOEVIL	Those responsible for operating the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.

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.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 9 identifies all extended SFRs implemented by the TOE

Table 9 Extended TOE Security Functional Requirements

Name	Description
FAU_GEN_EXT.1	Security Audit Data Generation – SA Core and SA Client

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.

5.1.1.1 Audit Data Generation (FAU_GEN)

Family Behaviour

This family defines requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types.

Component Leveling

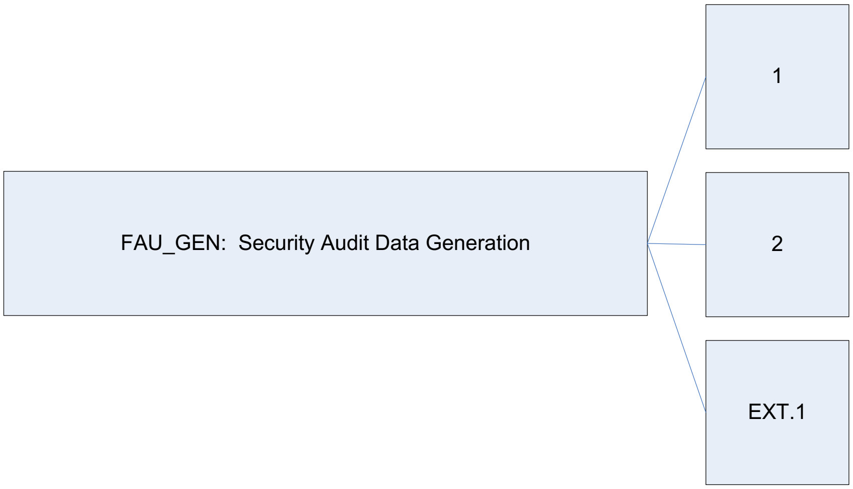

Figure 3 FAU_GEN: Audit data generation Family Decomposition with Extended Component

FAU_GEN_EXT.1: Audit data generation defines the level of auditable events and specifies the list of data that shall be recorded in each record without auditing the shutdown of the audit functions.

Management: FAU_GEN_EXT.1

- There are no management activities foreseen.

Audit: FAU_GEN_EXT.1

- There are no auditable events foreseen.

FAU_GEN_EXT.1 Security Audit Data Generation – SA Core and SA Client
Hierarchical to: No other components
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN_EXT.1.1

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

a) Start-up of the audit functions;
b) All auditable events, for the [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and
c) [assignment: *other specifically defined auditable events*]

FAU_GEN_EXT.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, [assignment: *other audit relevant information*].

5.2 Extended TOE Security Assurance Components

There are no extended TOE security assurance components.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

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

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

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

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN_EXT.1	Security Audit data generation – SA Core and SA Client	✓	✓		
FAU_GEN.2	User identity association				
FAU_SAR.1	Audit review		✓		
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FIA_AFL.1	Authentication Failure Handling	✓	✓		
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.2	User authentication before any action				
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.2	User identification before any action				

Name	Description	S	A	R	I
FMT_MTD.1	Management of TSF Data	✓	✓		
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		✓		
FPT_ITT.1	Basic internal TSF data transfer protection	✓			
FPT_TST.1	TSF Testing	✓	✓		
FTA_SSL.1	TSF-initiated session locking		✓		
FTP_ITC.1	Inter-TSF Trusted Channel	✓	✓		
FTP_TRP.1	Trusted path	✓	✓		

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

6.2.1 Class FAU: Security Audit

FAU_GEN_EXT.1 Security Audit Data Generation – SA Core and SA Client
Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN_EXT.1.1

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

a) Start-up of the audit functions;
b) All auditable events, for the [not specified] level of audit; and
c) [*In the SA client log:*
- *TOE user logins*
- *Invalid login attempts*]

FAU_GEN_EXT.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*].

FAU_GEN.2 User identity association
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1

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

FAU_SAR.1 Audit review
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1

The TSF shall provide [*Super Administrator*] with the capability to read [*all of audit information in the SA client logs using the User Login Reports*] 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.

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Cryptographic key generation algorithm – see Table 11 and Table 12 below*] and specified cryptographic key sizes [*cryptographic key sizes – see Table 11 and Table 12 below*]] that meet the following: [*list of standards – see Table 11 and Table 12 below*].

Table 11 Cryptographic Key Generation Standards (OpenSSL Library)

Key Generation Algorithm	Key Sizes Tested	Standards (Certificate #)
DRBG[19]	CTR[20]DRBG (AES[21])	NIST[22] SP[23] 800-90A (CAVP[24] cert # 342)
RNG[25]	AES – 128, 192, 256	ANSI[26] X9.31 (CAVP cert # 1202)

Table 12 Cryptographic Key Generation Standards (RSA Crypto-J Library)

Key Generation Algorithm	Key Sizes Tested	Standards (Certificate #)
HMAC[27] DRBG	HMAC-SHA[28]-1, 224, 256, 384, 512	NIST SP 800-90A (CAVP cert #273)

FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1

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*].

[19] DRBG – Deterministic Random Bit Generator
[20] CTR – Counter Mode
[21] AES – Advanced Encryption Standard
[22] NIST – National Institute of Standards and Technology
[23] SP – Special Publication
[24] CAVP – Cryptographic Algorithm Validation Program
[25] RNG – Random Number Generator
[26] ANSI – American National Standards Institute
[27] HMAC – Hash-Based Message Authentication Code
[28] SHA – Secure Hash Algorithm

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1

The TSF shall perform [*list of cryptographic operations – see Table 13 and Table 14 below*] in accordance with a specified cryptographic algorithm [*cryptographic algorithm – see Table 13 and Table 14 below*] and cryptographic key sizes [*cryptographic key sizes – see Table 13 and Table 14 below*] that meet the following: [*list of standards – see Table 13 and Table 14 below*].

Table 13 Cryptographic Operations (OpenSSL Library)

Algorithm	Standard and Cert #
Symmetric Key Algorithms	
AES: ECB[29], CBC[30], OFB[31], CFB 1, CFB[32] 8, CFB 128, CTR, CCM[33], GCM[34], CMAC[35] modes for 128-, 192-, and 256-bit key sizes	FIPS 197 (CAVP cert #2484)
AES: XTS[36,37,38] mode for 128- and 256-bit key sizes	FIPS 197 (CAVP cert #2484)
Triple-DES[39]: ECB, CBC, CFB, OFB, CMAC modes for keying option 1 (3 different keys)	SP 800-67 (CAVP cert #1522)
Digital Signature Algorithms	
RSA X9.31, PKCS#1 V.1.5, Signature verification – 1024, 1536, 2048, 3072, 4096-bit	ANSI X9.31; FIPS 186-2 (CAVP cert #1273)
Hashing Functions Asymmetric Key Algorithms	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	FIPS 180-3 (CAVP cert #2102)
Message Authentication Code (MAC) Functions	
HMAC with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	FIPS 198 (CAVP cert #1526)

[29] ECB – Electronic Codebook
[30] CBC – Cipher Block Chaining
[31] OFB – Output Feedback
[32] CFB – Cipher Feedback
[33] CCM – Counter with CBC-MAC
[34] GCM – Galois Counter Mode
[35] CMAC – Cipher-Based Message Authentication Code
[36] XTS – XEX-based tweaked-codebook mode with ciphertext stealing
[37] XEX – XOR-Encrypt-XOR
[38] XOR – Exclusive Or
[39] DES – Data Encryption Standard

Table 14 Cryptographic Operations (RSA Crypto-J Library)

Algorithm	Standard and Cert #
Symmetric Key Algorithms	
AES: ECB, CBC, OFB, CFB128, CCM, GCM, CTR, XTS-128 & XTS-256 bit mode for 128-, 192-, and 256-bit key sizes	FIPS 197, CAVP cert #2249
Triple-DES: ECB, CBC, CFB-64, OFB mode for keying option 1 (3 different keys)	FIPS 46-3, CAVP cert #1408
Digital Signature Algorithms	
RSA X9.31, PKCS#1 V.1.5, Signature verification – 1024-, 2048-, 3072-bit	ANSI X9.31 (FIPS 186-4), CAVP cert #1154
Key Derivation	
KDFTLS10, KDFTLS12 with SHA-256, SHA-384, SHA-512	SP 800-135, CAVP cert #39
Hashing Functions Asymmetric Key Algorithms	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	FIPS 180-2, CAVP cert #1938
Message Authentication Code (MAC) Functions	
HMAC with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	FIPS 198, CAVP cert #1378

6.2.3 Class FDP: User Data Protection

FDP_ACC.1 Subset access control
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1

The TSF shall enforce the [*SA Access Control SFP*] on
[Subjects:

- *TOE users*

Objects:

- *Resources*
- *Folder*

Operations:

- *Resources: Read & Write*
- *Folder: List, Read, Write, Execute and Edit*]

FDP_ACF.1 Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1

The TSF shall enforce the [*SA Access Control SFP*] to objects based on the following:
[*Subjects:*

- *TOE users*

Objects:

- *Resources*
- *Folder*

Security Attributes:

- *Subject – role*
- *Object – facility, customer, device group and permissions*].

FDP_ACF.1.2

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

- *a subject is granted access to perform an operation on an object based on the associated role within the TOE, and*
- *a subject can List, Read, Write, Execute or Edit only if the subject has been granted explicit access]*

FDP_ACF.1.3

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

FDP_ACF.1.4

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

6.2.4 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1

The TSF shall detect when [an administrator configurable positive integer within [*1-255*]] unsuccessful authentication attempts occur related [*to any user attempting to authenticate*.]

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [met] the TSF shall [*suspend the user account*.]

FIA_ATD.1 User attribute definition
Hierarchical to: No other components.
Dependencies: No dependencies

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [

- *Username*
- *Role*
- *Password*
- *Account lockout status*]

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

FIA_UAU.2.1

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

FIA_UAU.7 Protected authentication feedback
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1

The TSF shall provide only [*feedback in the form of bullets ('*') over the SA Client and GUI over web browser*] to the user while the authentication is in progress.

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies

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.

6.2.5 Class FMT: Security Management

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1

The TSF shall enforce the [*SA Access Control SFP*] to restrict the ability to [change default, query, modify, delete] the security attributes [*role, facility, customer, device group and permissions*] to [*Super Administrator*].

FMT_MSA.3 Static attribute initialization
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1

The TSF shall enforce the [*SA 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 [*Super Administrator*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1

The TSF shall restrict the ability to [modify] the [*objects listed in the 'Object' column of Table 15*] to [*the user listed in the 'User' column of Table 14*].

Table 15 Management of TSF Data

Object	User
SA Access Control settings	Super Administrator
Authentication data	Super Administrator or the currently logged in user (only for password changes)
Password Policy	Super Administrator
Action Permissions	Super Administrator
Session timeouts	Super Administrator
User accounts	Super Administrator

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components.
Dependencies: No Dependencies

FMT_SMF.1.1

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

- *Manage the SA Access Control policy*
- *Create and delete user accounts*
- *Manage authentication data*
- *Manage and define password policies*

- *Manage permissions for user accounts*
- *Manage inactivity session timer configuration*

]

FMT_SMR.1 Security roles
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the roles [

- *Super Administrator*
- *Opsware System Administrators*
- *Superusers*
- *Viewers*
- *Reporters*
- *Patch Policy Setters*
- *Patch Deployers*
- *Software Policy Setters*
- *Software Deployers*
- *Compliance Policy Setters*
- *Compliance Auditors*
- *Compliance Enforcers*
- *Virtualization Administrators*
- *Hypervisor Managers*
- *Virtual Machine Managers*
- *VM Lifecycle Managers*
- *VM Template Deployers*
- *VM Template Managers*
- *Command Line Administrators*
- *Server Storage Managers*
- *Storage System Managers*
- *Storage Fabric Managers]*

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.6 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection
Hierarchical to: No other components.
Dependencies: No dependencies
FPT_ITT.1.1

The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

FPT_TST.1 TSF testing
Hierarchical to: No other components.
Dependencies: No dependencies
FPT_TST.1.1

The TSF shall run a suite of self tests [periodically during normal operation, at the request of the authorized user] to demonstrate the correct operation of [*SA Core and SA Agent*].

FPT_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of [*SA Core and SA Agent*].

FPT_TST.1.3

The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

6.2.7 Class FTA: TOE Access

FTA_SSL.1 TSF-initiated session locking
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL.1.1

The TSF shall lock an interactive session after [*Super Administrator configured time interval of user inactivity for the SA client only*] by:

a) clearing or overwriting display devices, making the current contents unreadable;
b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2

The TSF shall require the following events to occur prior to unlocking the session: [*successful re-authentication of the TOE user]*.

6.2.8 Class FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel
Hierarchical to: No other components.
Dependencies: No dependencies

FTP_ITC.1.1

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2

The TSF shall permit [the TSF and third-party applications running on external IT entities] to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [*remote authentication requests*].

FTP_TRP.1 Trusted path
Hierarchical to: No other components.
Dependencies: No dependencies

FTP_TRP.1.1

The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2

The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [*all remote actions*].

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 16 summarizes the requirements.

Table 16 Assurance Requirements

Assurance Requirements	
Class ASE: Security target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC: Life cycle support	ALC_CMC.2 Use of a CM[40] 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

[40] CM – Configuration Management

7 TOE Security 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 Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 17 lists the security functionality and their associated SFRs.

Table 17 Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID[41]	Description
Security Audit	FAU_GEN_EXT.1	Security Audit data generation – SA Core and SA Client
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
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	Subset access control
	FDP_ACF.1	Security attribute based access control
Identification and Authentication	FIA_AFL.1	Authentication Failure Handling
	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management	FMT_MTD.1	Management of TSF Data
	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
Protection of TOE Security Functions	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_TST.1	TSF Testing
TOE Access	FTA_SSL.1	TSF-initiated session locking
Trusted Path/Channels	FTP_ITC.1	Inter-TSF Trusted Channel

[41] ID - Identifier

TOE Security Functionality	SFR ID[41]	Description
	FTP_TRP.1	Trusted path

7.1.1 Security Audit

The TOE is capable of auditing a variety of events (actions performed by SA users), including startup of the TOE[42]. When an authorized user accesses or modifies a managed server, SA records the event in an audit log. The audit logs contain information about the following events:

- Startup of the TOE
- All login activities via any TOE interface
- Invalid login attempts

The audit logs consists of two sets of logs files:

- Startup logs
- SA client logs

Startup log files are stored in */var/log/opsware/startup*. Default settings of SA components are configured to "log-only" errors and warnings.

The SA client logs contain user logon information from the SA client and web GUI. The SA client logs are viewable through the Reports feature under User and Security Reports by using the User Login report. The username, IP address, time, and date are recorded for each login event. The IP address recorded when logging in from the web GUI will reflect the IP address of the SA Core server. The IP address recorded when logging in from the SA client will reflect that of the local workstation running the SA client.

The TSF provides only the authorized roles with the ability to view audit records in the User Login Reports. Audit records in the Startup Log must be viewed in the operating environment. The audit records are presented in a human-readable format on all TOE interfaces.

TOE relies on the underlying OS for time stamps.

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

7.1.2 Cryptographic Support

The FIPS-validated cryptographic modules provide all necessary cryptographic services in the TOE. SA utilizes the FIPS 140-2 validated OpenSSL FIPS Object Module, Software Version 2.0.5 and RSA Crypto-J Software Module, Software Version 6.1 libraries for performing cryptographic operations. The FIPS 140-2 certificates of the crypto modules used by the TOE are #1747 and #2057, respectively.

The TOE utilizes cryptographic services to employ TLS v1.0 communications between distributed components of the TOE:

- SA Core and SA Agent(s)
- SA Satellite and SA Agent(s)
- SA Client and SA Core
- SA Core and SA Satellite

[42] The TOE's startup starts the TOE's audit function.

The TOE also uses cryptography to implement the HTTPS protocol for providing communications via trusted path. HTTPS (via TLS v1.0) provides a trusted path for remote users accessing the GUI over a web browser.

SA Core components rely on both the OpenSSL and RSA Crypto-J libraries for cryptography. SA Agent and SA Satellite components rely on the OpenSSL library, and SA Client components rely on the RSA Crypto-J library for cryptography. The TOE's cryptographic modules destroy all ephemeral keying material generated within the TOE boundary. The cryptographic module uses FIPS-approved zeroization methods in order to destroy all ephemeral keys and other critical parameters generated by the TOE at the appropriate time.

Table 11, Table 12, Table 13, and Table 14 in section 6.2.2 lists the cryptographic operations, algorithms, key sizes, modes of operation, and algorithm certificates utilized by the product.

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

7.1.3 User Data Protection

The TOE provides user data protection by enforcing the SA Access Control SFP on the following objects:

- Resources
- Folders

The SA Access Control SFP limits each user's access based on role (see section 7.1.5), and object-level permissions, which grant authorizations to perform operations on objects. SA provides the following permissions needed to perform any action on managed servers:

7.1.3.1 Resource permissions

All managed servers are grouped by facility, by customer, and by device groups.

- Facilities are the managed servers associated with an SA facility. Every managed server belongs to one and only facility.
- Customers are the managed servers associated with a customer. Every managed server belongs to one and only one customer.
- Device Groups are the managed servers belonging to a device group. Every managed server can belong to one or more device groups.

Resource permissions specify access to facilities, customers, and device groups. An authorized user can set the following types of resource permissions to TOE users:

- Read: Users can view the resource only.
- Read & Write: Users can view, create, modify or delete the resource.
- No resource permissions are assigned: Users cannot view or modify the resource. The resource does not appear at all in the SA Client.

Resource permissions for a role determine if the users in the role can view or modify the managed servers. A role only has access to the servers in the facilities, customers, and device groups for which it has been granted resource permissions. Because every server belongs to one facility, one customer, and at least one device group, to have access to servers, a role must have permissions to at least one facility, at least one customer, and at least one device group.

7.1.3.2 Folder Permissions

Folder permissions control access to the contents of folders in the SA Library, such as software policies, patch policies, OS build plans, server scripts, and subfolders.

An authorized user can set the following types of folder permissions to TOE users:

- List contents of folder: This allows user to list and view the folder's properties.
- Read objects within folder: This allows user to view all attributes of the folder's contents, open object browsers on folder's contents, and use folder's contents in actions. Setting this permission automatically adds the list contents of folder permission.
- Write objects within folder: This allows user to view, use, create, and modify the folder's contents. Setting this permission automatically adds the list contents of folder and the read objects within folder permissions.
- Execute objects within folder: This allows user to run the scripts contained in the folder and view the names of the folder's contents. This permission allows users to run scripts, but not to read or write them. Setting this permission automatically adds the list contents of folder permission.
- Edit folder permissions: Modify the permissions or add customers to the folder. Setting this permission enables users to delegate the permissions management of a folder (and its contents) to another role.

TOE Security Functional Requirements Satisfied: FDP_ACC.1 and FDP_ACF.1.

7.1.4 Identification and Authentication

The TOE identification and authentication functionality enforces TOE users to successfully identify and authenticate to the TOE prior to performing any TSF-mediated actions on the TOE.

The TOE maintains the following security attributes belonging to individual users for enforcement of identification and authentication functionality:

- User name
- Role
- Password
- Account lockout status

The TOE automatically suspends user accounts when the allowed number of unsuccessful login attempts is met. The suspended user account can be manually re-activated by an authorized user. The Account lockout status is listed as either "Active" or "Suspended" for each user account.

Once successfully authenticated, the user will inherit the security attributes that were previously defined by the Super Administrator for that user. The TOE provides password-based user authentication mechanism. This authentication is performed based on matching submitted credentials with stored user identity and password information. During password entry, the TOE provides protected feedback in the form of bullets ('*') over the SA Client and GUI over web browser.

TOE Security Functional Requirements Satisfied: FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UAU.7, and FIA_UID.2.

7.1.5 Security Management

The TOE provides management facilities to TOE users. The TOE implements RBAC, which selectively grants administrative permissions to roles as needed. RBAC provides varying levels of privileges that determine an authenticated user level of access within the TOE.

Management of TSF data is restricted to Super Administrators and any users that are explicitly given permissions by Super Administrator. The TOE ships with a single Super Administrator account with default credentials. A Super Administrator is a TOE user who can create users and roles, specify permissions for roles, and assign users to roles. A user can have one or many roles and will assume all capabilities of the combine roles. Super Administrators can modify the SA client's session timeout settings and the password policy parameters such as reset, expiration, retention, and login failure. Super Administrators can manage customers and facilities, and set folder permissions. Only a Super Administrator can manage other user accounts and change other account's passwords. All object security attributes contain restrictive default values, where a Super Administrator can modify, query, and change the default values to all object security attributes.

In addition to the Super Administrator role, HPE includes the predefined roles specified in Table 18. Table 18 also specifies the type of operations that the roles are authorized to perform on the objects associated with SA Access Control SFP (see section 7.1.3). All TOE users can manage their own passwords.

Table 18 Authorized Roles

Object	Operation	Authorized Role
SA Application	Full access to administer the SA application.	Opsware System Administrators
Devices	Read-only access to all resources.	Viewers
Reports	Full access to reports.	Reporters
Patch	Access to set patching policy.	Patch Policy Setters
	Access to install patches.	Patch Deployers
Software	Access to set software policy.	Software Policy Setters
	Access to install software.	Software Deployers
Compliance	Access to define compliance policies.	Compliance Policy Setters
	Access to execute compliance scans.	Compliance Auditors
	Access to remediate compliance failures.	Compliance Enforcers
VM	Access to add, edit, and remove virtualization services, manage lifecycle of VMs and VM Templates, and administer permissions for virtualization inventory.	Virtualization Administrators
	Access to create, delete, and register VMs.	Hypervisor Managers
	Access to start and stop VMs.	Virtual Machine Managers
	Access to create, modify, migrate, clone, and delete VMs as well as VM Template Deployer tasks.	VM Lifecycle Managers
	Access to create VMs from VM Templates, clone VMs, customize VM guest OS, start and stop VMs.	VM Template Deployers
	Access to create, modify, and delete VM templates as well as VM Lifecycle Manager tasks.	VM Template Managers
Shell	Full shell access to servers	Command Line Administrators
Storage	Full access to manage server storage.	Server Storage Managers
	Full access to manage storage systems.	Storage System Managers
	Full access to manage storage fabrics.	Storage Fabric Managers

TOE Security Functional Requirements Satisfied: FMT_MTD.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, and FMT_SMR.1.

7.1.6 Protection of the TSF

SA utilizes cryptographic services to secure communications between distributed components of the TOE. These secure communications prevent unauthorized disclosure, and modification of TSF data. The TOE employs TLS v1.0 communications for securing communications between the SA components:

- SA Core and SA Agent(s)
- SA Satellite and SA Agent(s)
- SA Client and SA Core
- SA Core and SA Satellite

The TOE provides health tests for monitoring SA Agents installed on managed servers, which include:

- AGT Test: The AGT Test tests if the SA core can communicate with the SA Agent running on the SA Managed Server.
- CRP Test: The CRP Test tests the encryption and security of the connection between the SA core and the SA Managed Server on which SA Agent is installed.
- CE Test: The CE Test tests if the SA Managed Server on which SA Agent is installed can retrieve commands health tests to be executed from the SA core.
- DAE Test: The DAE Test tests if the SA Managed Server on which SA Agent is installed can retrieve its stored device information from the SA core.
- SWR Test: The SWR Test tests if the SA Managed Server on which SA Agent is installed can retrieve software and patches from the SA core.
- MID Test: The MID Test Verifies that the if the SA Managed Server's on which SA Agent is installed machine ID is the same as the machine ID stored in the SA core.

These test works by testing communication and data exchange between the SA Core and SA Agent installed on each SA Managed Server. If any of these tests fail, the TOE provides an unexpected error to the user.

In addition, the TOE provides local and global health tests for monitoring the SA Core status and operation. The local health tests verify the availability of individual SA Core components and the conditions necessary for the components to operate. The global health tests checks an entire SA Core by performing the a suite of tests that:

- Checks the Multimaster state of the SA Core
- Verifies the versions of all of the components in the SA Core
- Verifies system clock synchronization across SA Core servers
- Validates the virtual memory and disk space on SA partitions thresholds
- Validates full functionality of all SA components
- Validates that the Model Repository [43] tablespace usage is within acceptable limits

The TOE runs these tests periodically, or an authorized user can invoke these tests on demand.

TOE Security Functional Requirements Satisfied: FPT_ITT.1, and FPT_TST.1.

7.1.7 TOE Access

The TOE mitigates unauthorized user access by automatically locking the current session over the SA client after a Super Administrator configured time interval of inactivity. Once the session is locked, the TSF will clear or overwrite TSF controlled display devices, ensuring the current contents are unreadable. Locking the session will disable any activity of the user's TSF controlled data access and all display devices other than unlocking the session. In order for an authorized user to regain access of a timed out

[43] Model Repository is the central repository of the TOE, where TOE configuration data and Managed Servers information is stored.

session, the user must successfully re-authenticate with the credentials of the user owning the locked out session.

TOE Security Functional Requirements Satisfied: FTA_SSL.1.

7.1.8 Trusted Path/Channels

The TOE provides a secure communication path between itself and remote users. The cryptographic functionality of the TOE provides the TOE with the ability to create trusted paths. The TOE provides a trusted path between the TOE's GUI and remote users. The GUI is used over a web browser via HTTPS (via TLS v1.0). The protocol and the cryptography implemented by the TOE provide adequate defense against unauthorized disclosure and provide for the detection of modification of TSF data while it is in transit.

Additionally, the TOE provides a trusted channel between the TOE and trusted IT products. Trusted IT products consist of an authentication server, and web services clients. The trusted channel to secure the communication between the TOE and the authentication server is established using TLS v1.0 to prevent unauthorized disclosure and detect modification of authentication data. Communications with web services clients are secured over HTTPS.

TOE Security Functional Requirements Satisfied: FTP_ITC.1, and FTP_TRP.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Release 4.

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 are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 19 below provides a mapping of the objects to the threats they counter.

Table 19 Threats: Objectives Mapping

Threats	Objectives	Rationale
T.ACCESS The TSF must control access of subjects to objects based on access control. The TSF must allow authorized users to specify which subjects are allowed to access a specific object. A threat agent might gain access to user data stored, processed, or transmitted by the TOE without being appropriately authorized according to the TOE security policy.	O.ACCESS The TSF must control access of subjects to objects based on access control. The TSF must allow authorized users to specify which subjects are allowed to access objects covered by access control SFP.	O.ACCESS mitigates this threat by ensuring that access to user data including TSF data stored with the TOE, have discretionary access control protection.
T.COMINT An unauthorized person may attempt to compromise the integrity of the data discovered and events produced by the TOE by bypassing a security mechanism.	OE.PROTECT The TOE environment must protect itself, the network on which the TOE is deployed, and the TOE from external interference or tampering.	OE.PROTECT mitigates this threat by enforcing that the TOE environment must protect the TOE from external interference or tampering.
	O.AUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	O.AUTH mitigates this threat by ensuring that users are identified and authenticated prior to gaining access to TOE data.
	O.CRYPTO The TOE must provide the means of protecting cryptographic operations and secure management of cryptographic keys using cryptography that conforms to standards specified in FIPS PUB 140-2.	O.CRYPTO mitigates this threat by providing cryptographic algorithms and procedures to protect cryptographic operations during the transfer of in-flight data.

Threats	Objectives	Rationale
	O.SECURE The TOE shall securely transfer data with other trusted IT entities and remote users.	O.SECURE mitigates this threat by ensuring that the TOE securely transfers data with other trusted IT entities and remote users.
T.FAILURE The failure of an SA Core component or SA Agent could go undetected or cause a breach of the TSF.	O.AUTO The TOE must provide the ability to automatically run the health tests for monitoring SA Core components and SA Agents both periodically and at the request of an authorized user.	O.AUTO mitigates this threat by ensuring that health tests are run to detect any failures of the SA Core components and SA Agents.
T.NOAUDIT An attacker may perform security relevant operations on the TOE without being held accountable for them.	O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review audit records.	O.AUDIT mitigates this threat by ensuring that security relevant events of the TOE are preserved.
	O.AUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	O.AUTH mitigates this threat by ensuring that a user or administrator is properly identified, thereby allowing the TSF to record the user's identity for any logs created as a result of the user's or administrator's actions.
T.TRANSMIT A user or process may be able to bypass the TOE's security mechanisms and gain access to the data while the data is in transit.	O.CRYPTO The TOE must provide the means of protecting cryptographic operations and secure management of cryptographic keys using cryptography that conforms to standards specified in FIPS PUB 140-2.	O.CRYPTO mitigates this threat by ensuring that the cryptographic keys are managed securely conforming to the FIPS PUB 140-2 standards.
	O.SECURE The TOE shall securely transfer data with other trusted IT entities and remote users.	O.SECURE mitigates this threat by providing trusted mechanisms to protect the TOE data that is transferred between trusted IT entities and remote users.
T.UNATTEND An unauthorized user could attempt to take over an unattended session and perform malicious activities.	O.SESSION The TOE will provide a mechanism that controls a user's logical access to the TOE.	O.SESSION mitigates this threat by ensuring that users may only have a maximum of a specified number of active sessions open at any given time, and are inactive after an inactivity period.
T.UNAUTH An unauthorized user may bypass	O.ADMIN The TOE must include a set of	O.ADMIN mitigates this threat by restricting the access to TOE

Threats	Objectives	Rationale
the TOE's identification, authentication, or authorization mechanisms in order to illicitly utilize the TOE's management functions, or TSF data.	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.	security data to those users with access to the management functions of the TOE.
	O.ATTRIB The TOE will be capable of maintaining user security attributes.	O.ATTRIB mitigates this threat by allowing only users with valid credentials to access the TOE.
	O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review audit records.	O.AUDIT mitigates this threat by auditing all unauthorized attempts to access the TOE.
	O.AUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	O.AUTH mitigates this threat by ensuring that users are identified and authenticated prior to gaining access to TOE's administrative functions and data.

Every Threat is mapped to one or more Objectives in the Table 19 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 OSPs for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 20 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 20 Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate, dedicated hardware and operating system.	OE.PLATFORM The hardware and OS from the operating environment that host the TOE must support all required TOE functions.	OE.PLATFORM upholds this assumption by ensuring that the TOE hardware meets minimum requirements, and the OS supports all the TOE functions.
A.LOCATE The TOE is located within a controlled access facility.	NOE.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are	OE.PHYSICAL upholds this assumption by ensuring that the TOE environment provides protection against physical attacks.

Assumptions	Objectives	Rationale
	protected from physical attack that might compromise IT security objectives.	
A.NETCON The TOE environment provides the network connectivity required to allow the TOE to perform its intended functions.	OE.MONITOR The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.	OE.MONITOR upholds this assumption by ensuring that the TOE environment provides the appropriate network connectivity required for performance with a proper implementation of the TOE.
A.NOEVIL The users who manage the TOE and the security of the information it contains are non-hostile, appropriately trained, and follow all guidance.	NOE.NOEVIL Those responsible for operating the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.	NOE.NOEVIL upholds this assumption by ensuring that all administrators assigned to manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all administrator guidance.
A.PROTECT The TOE software is protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself, the network on which the TOE is deployed, and the TOE from external interference or tampering.	OE.PROTECT upholds this assumption by ensuring that the TOE environment provides a secure and authorized access to its users for protect the data from external interference or tampering.
A.TIMESTAMP The TOE environment provides the TOE with the necessary reliable timestamps.	OE.TIME The underlying Operating System must provide reliable timestamps to the TOE.	OE.TIME upholds this assumption by ensuring that the operating system where the TOE is installed will provide reliable time stamps for the TOE.
A.DEDICATED Those responsible for installing the TOE will ensure that the SA Core server is only used for the SA Core and have no other purpose. In addition, the users responsible for installing the TOE will protect the SA Core installation log.	OE.DEDICATED The hardware and OS from the operating environment that host the SA Core server must be used to only support the SA Core server's functionality.	OE.DEDICATED upholds this assumption by ensuring that dedicated hardware and OS are used to support the SA Core server and are only used for the SA Core server's functionality.
	NOE.NOEVIL Those responsible for operating the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.	NOE.NOEVIL upholds this assumption by ensuring that the administrators assigned to manage the TOE are capable of managing the security of the SA Core installation log and the information it contains.

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

There are no extended functional requirements defined for this TOE.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended functional requirements defined for this TOE.

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 21 below shows a mapping of the objectives and the SFRs that support them.

Table 21 Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TSF must control access of subjects to objects based on access control. The TSF must allow authorized users to specify which subjects are allowed to access objects covered by access control SFP.	FDP_ACC.1 Subset access control	The requirement meets this objective by ensuring that access control is enforced on all monitoring operations among subjects and objects covered by the SFP.
	FDP_ACF.1 Security attribute based access control	The requirement meets this objective by ensuring that the TOE enforces the access control based on permissions and credentials.
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	FMT_MSA.1 Management of security attributes	The requirement meets this objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only privileged users may manage the security behavior of the TOE.
	FMT_MSA.3 Static attribute initialization	The requirement meets this objective by restricting the ability to specify alternate values to security attributes only to authorized users.
	FMT_MTD.1 Management of TSF Data	The requirement meets this objective by ensuring that the TOE restricts administrative

Objective	Requirements Addressing the Objective	Rationale
		functions to only those users with the appropriate privileges.
	FMT_SMF.1 Specification of management functions	The requirement meets this objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets this objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
	FPT_TST.1 TSF Testing	The requirement meets this objective by ensuring that the TOE provides the ability to invoke health tests to authorized users.
O.ATTRIB The TOE will be capable of maintaining user security attributes.	FIA_ATD.1 User attribute definition	The requirement meets this objective by ensuring that the TOE maintains a defined list of security attributes belonging to individual users. These may only be changed by authorized users.
	FMT_SMR.1 Security roles	The requirement meets this objective by ensuring that the TOE manages the defined user roles. The TOE does this by ensuring that only authorized users have access to TSF data.
O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review audit records.	FAU_GEN_EXT.1 Security Audit data generation – SA Core and SA Client	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_GEN.2 User identity association	The requirement meets this objective by ensuring that the TOE associates auditable events with the identity of the user that caused the event.
	FAU_SAR.1 Audit review	The requirement meets this objective by ensuring that the TOE provides the ability to review logs with records being presented in a suitable manner for interpretation.
O.AUTH The TOE must be able to identify and authenticate users prior to	FIA_AFL.1 Authentication Failure Handling	The requirement meets this objective by ensuring that the TOE provides a mechanism to

Objective	Requirements Addressing the Objective	Rationale
allowing access to TOE administrative functions and data.		identify and react to unsuccessful authentication attempts.
	FIA_UAU.2 User authentication before any action	The requirement meets this objective by ensuring that the TOE requires each user to be successfully authenticated before allowing any TOE administrative actions on behalf of that user.
	FIA_UAU.7 Protected authentication feedback	The requirement meets this objective by ensuring that the password of a user is obscured by dots while the user authenticates.
	FIA_UID.2 User identification before any action	The requirement meets this objective by ensuring that the TOE requires each user to be successfully identified before allowing any TOE administrative actions on behalf of that user.
O.AUTO The TOE must provide the ability to automatically run the health tests for monitoring SA Core components and SA Agents both periodically and at the request of an authorized user.	FPT_TST.1 TSF Testing	The requirement meets this objective by ensuring that the TOE provides health tests (both periodically and at the request of an authorized user) that check for the failure of SA Core components or SA Agents.
O.CRYPTO The TOE must provide the means of protecting cryptographic operations and secure management of cryptographic keys using cryptography that conforms to standards specified in FIPS PUB 140-2.	FCS_CKM.1 Cryptographic key generation	The requirement meets this objective by ensuring that the TOE generates cryptographic keys in accordance with FIPS PUB 140-2 approved techniques.
	FCS_CKM.4 Cryptographic key destruction	The requirement meets this objective by ensuring that the cryptographic keys are destroyed according to FIPS PUB 140-2 zeroization requirements.
	FCS_COP.1 Cryptographic operation	This requirement meets this objective by ensuring that the cryptographic operations are performed according to the FIPS PUB 140-2 approved algorithms and key sizes.
O.SECURE The TOE shall securely transfer data with other trusted IT entities and remote users.	FPT_ITT.1 Basic internal TSF data transfer protection	The requirement meets this objective by ensuring that the TOE provides a trusted communication path, which provides for the protection of the data from disclosure when in

Objective	Requirements Addressing the Objective	Rationale
		transit.
	FTP_ITC.1 Inter-TSF Trusted Channel	The requirement meets this objective by ensuring that the TOE provides a trusted communication channel which provides for the protection of the data from disclosure and modification while exchanged between another trusted IT product and TOE.
	FTP_TRP.1 Trusted path	The requirement meets this objective by ensuring that the TOE provides a trusted communication path which provides for the protection of the data from disclosure and modification while exchanged between remote users and TOE.
O.SESSION The TOE will provide a mechanism that controls a user's logical access to the TOE.	FTA_SSL.1 TSF-initiated session locking	The requirement meets this objective by ensuring that TSF locks a user session after an inactivity period.

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. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System 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

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 22 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 22 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN_EXT.1	FPT_STM.1		Although FPT_STM.1 is not included, the underlying OS, which is

SFR ID	Dependencies	Dependency Met	Rationale
			in the TOE environment, provides reliable timestamps to the TOE.
FAU_GEN.2	FAU_GEN.1	✓	Although FAU_GEN.1 is not included, FAU_GEN_EXT.1, which is an extended version of it, is included. This satisfies the dependency.
	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FAU_SAR.1	FAU_GEN.1	✓	Although FAU_GEN.1 is not included, FAU_GEN_EXT.1, which is an extended version of it, is included. This satisfies the dependency.
FCS_CKM.1	FCS_COP.1	✓	
	FCS_CKM.4	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FMT_MSA.3	✓	
	FDP_ACC.1	✓	
FIA_AFL.1	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2, which is hierarchical to FIA_UAU.1 is included. This satisfies this dependency.
FIA_ATD.1	No dependencies		
FIA_UAU.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.

SFR ID	Dependencies	Dependency Met	Rationale
FIA_UAU.7	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2, which is hierarchical to FIA_UAU.1 is included. This satisfies this dependency.
FIA_UID.1	No dependencies		
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1	FDP_ACC.1	✓	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FMT_SMF.1	No dependencies		
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_ITT.1	No dependencies		
FPT_TST.1	No dependencies		
FTA_SSL.1	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2, which is hierarchical to FIA_UAU.1 is included. This satisfies this dependency.
FTP_ITC.1	No dependencies		
FTP_TRP.1	No dependencies		

9 Acronyms

Table 23 in this section defines the acronyms used throughout this document.

Table 23 Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CCM	Counter with CBC-MAC
CEM	Common Methodology for Information Technology Security Evaluation
CFB	Cipher Feedback
CLI	Command Line Interface
CM	Configuration Management
CMAC	Cipher-Based Message Authentication Code
CTR	Counter Mode
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
ECB	Electronic Codebook
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
IP	Internet Protocol
IT	Information Technology
JCE	Java Cryptography Extension
JVM	Java Virtual Machine
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
NIST	National Institute of Standards and Technology

Acronym	Definition
OCSP	Online Certificate Status Protocol
OFB	Output Feedback
OGFS	Global File System
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
PUB	Publication
RBAC	Role Based Access Control
RHEL	Red Hat Enterprise Linux
RMI	Remote Method Invocation
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
SA	Server Automation
SAR	Security Assurance Requirement
SAV	Server Automation Visualizer
SCM	Security Compliance Manager
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SP	Special Publication
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
VM	Virtual Machine
XEX	XOR-Encrypt-XOR
XOR	Exclusive OR
XTS	XEX-based Tweaked-codebook mode with ciphertext Stealing

Prepared by:
Corsec Security, Inc.

13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

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