Hewlett Packard Enterprise Development LP

HP Service Manager v9.41 Patch 3

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.4

Prepared for:

Hewlett Packard Enterprise

Hewlett Packard Enterprise Development LP
3000 Hanover Street
Palo Alto, CA 94304
United States of America

Email: info@hpe.com
www.hpe.com

Prepared by:

Corsec

Corsec Security, Inc.

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

Email: info@corsec.com
www.corsec.com

Table of Contents

List of Figures

List of Tables

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the Hewlett Packard Enterprise Development LP (HPE) HP Service Manager (HP SM) and will be referred to as the TOE throughout this document. The TOE is a comprehensive ITSM[1] software suite that enables service level management for IT[2] organizations. HP SM is built on the Information Technology Infrastructure Library (ITIL) framework, which provides best practices for governing ITSM.

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 (PP), and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.

[1] ITSM – Information Technology Service Management
[2] IT – Information Technology

- Security Objectives (Section 0) – 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 Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target and TOE References

Table 1 below provides the ST and TOE references.

Table 1 – ST and TOE References

ST Title	Hewlett Packard Enterprise Development LP HP Service Manager Security Target
ST Version	Version 1.4
ST Author	Corsec Security, Inc.
ST Publication Date	2/17/2016
TOE Reference	HP Service Manager v9.41 Patch 3 build #3016

1.3 Product Overview

The HP Service Manager Enterprise Suite, also called "HP SM", is a comprehensive ITSM software suite that enables service level management for IT organizations. HP SM is built on the Information Technology Infrastructure Library (ITIL) framework, which provides best practices for governing ITSM. HP SM can be thought of as a fully-featured, "on-premises", consolidated service desk that connects people, processes, and technology to effectively implement and manage IT services across an enterprise.

The primary entry point into HP SM is through a service request entered online by a user[3] or by a service desk agent. The service request could be a complaint, compliment, or problem. It could also be a request for administration, product changes, information, or items from the Service Catalog. The request is either resolved and closed or escalated for further consideration. When a request is escalated, it is considered an "incident[4]", and appropriate personnel are alerted to take action. Out-of-Box (OOB) workflows control the movement of a service request through the HP SM system, and these workflows can be customized.

The HP SM product provides the lifecycle management of IT services and is comprised of the modules listed in Table 2.

Table 2 – HP Service Manager Modules

Module	Description
Service Desk	The Service Desk module manages all IT-related service requests, resolving interactions on first contact or escalating them for further handling. Service requests may be entered via the "Self-Service" portal or through direct communications with service desk operators. Service Desk interacts with Incident Management, Change Management, and Request Management modules for the handling of different types of service requests.
Incident Management	The Incident Management module manages the tracking of various types of incidents. The reporting and incident tracking allow SLAs[5] to be met by enabling operators to quickly restore service operations to normal and minimize impacts to business operations.

[3] A "user" refers to any TOE user and is synonymous with "operator"
[4] An incident is any event that disrupts, or could disrupt, a service.
[5] SLA – Service Level Agreement

Module	Description
Problem Management	The Problem Management module identifies root causes for one or more incidents, implements workarounds, identifies known issues, and provides permanent resolutions to minimize incidents and prevent the recurrence of common problems. Automatic alerts and notifications can be generated when a problem is recorded or changes status.
Employee Self-Service	The Employee Self-Service module enables any user to connect with HP SM to request a service, provide information, or track previous requests. Self-Service users can also be granted capabilities for the approval of change requests.
Change Management	The Change Management module is used to track infrastructure changes and changes to service assets and configuration items (CIs) in the IT infrastructure. This process creates a history log for each item that is maintained for the CI's lifecycle.
Knowledge Management (KM)	The KM module organizes documentation by categories, groups, and types, and provides views that allow granular definition of access to end users.
Service Request Catalogs (SRC)	The SRCs contain comprehensive lists of enterprise products and services available to internal and external customers, depending on business roles. Users can submit service requests that follow planning and approval workflows which are then routed through the appropriate HP SM module(s).
Service Level Management	The Service Level Management module provides a set of monitoring tools to ensure compliance with SLAs. Service Level Targets are set which include configuration items (CI) availability metrics and service desk response times.
Request Fulfillment	The Request Fulfillment module manages common user requests for products and services. The requests usually affect only the person making the request, or a subordinate group of employees.
Survey	The Survey module implements email surveys that can be sent to users manually from a record or according to a schedule.
Calendar	The Calendar module is a built-in HP SM widget that can display time periods and associated business records in a graphical calendar UI[6].
Reporting	The Reporting module provides reports and dashboards, organizing data into various chart types and displaying dashboard reports that present relationships between various categories of data.
Time Period Management	The Time Period Management module manages time period definitions to enable end users to see how their activities will be affected during different time periods.
Configuration Management	The Configuration Management module identifies, defines, and tracks organizational assets by creating and managing records for those items.
Process Designer	The Process Designer module provides a graphical interface to develop workflows that can be used to control the flow of a single record throughout its lifecycle. The Process Designer enables an implementer to graphically create or update a workflow without being an expert in RAD[7] programming.
Collaboration	The Collaboration module is a text-based chat application and is only available to web clients.
Case Exchange	The Case Exchange module is an integration that enables automated data exchange between the Incident Manager module and HP Service Anywhere or other third party products.

[6] UI – User Interface

[7] RAD – Rapid Application Development software

1.4 TOE Overview

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

The TOE is software-only and is delivered by HPE as part of a Professional Services engagement. The installation is performed by HPE.

1.4.1 Brief Description of the Components of the TOE

The following components are included in the TOE evaluation:

- SM Server (2 instances) with the included SM Load Balancer running on the first instance, and the following HP SM modules:
  - Service Desk
  - Incident Management
  - Problem Management
  - Employee Self-Service
  - Knowledge Management
  - Change Management
  - Request Fulfillment
  - Service Level Management
  - Survey
  - Calendar
  - Reporting
  - Collaboration
  - Case Exchange
- Windows Client
- Web Server (deployed as a WAR[8] file)
- Mobility Server (deployed as a WAR file)
- SRC Server (deployed as a WAR file)

Users access the TOE via the Windows Client interface, the Web Client interface, the Mobility Client interface, and the SRC Client interface. All of the above are web-based interfaces with the exception of the Windows Client interface.

- The Windows Client interface is the primary administrative interface to the TOE. The Windows Client is a Java-based thick client application that runs on a Windows host. The Windows Client allows a System Administrator[9] to manage the TOE via a GUI[10]. Additionally, an administrator[11] can access HP SM modules

[8] WAR – Web Application Archive
[9] The term System Administrator refers to an operator with the user role “system administrator”. The system administrator user role provides full system administration privileges.
[10] GUI – Graphical User Interface
[11] An administrator includes both System Administrators and any operator with sufficient privileges for the management and administration of a module.

from the Windows Client. The underlying RSA BSAFE Crypto-J Module v6.2 secures communications between the Windows Client and the SM Server.

- The Web Client interface is web-based, and is hosted on the Web Server. The Web Client interface is supported by web browsers running on Windows hosts and is the primary interface for End Users[12]. An End User can create, view, and update service requests from this interface with a standard Employee Self-Service (ESS) view. Service Desk technicians, managers, and administrators use the Power User view for additional functionality.

- The Mobility Client interface is web-based, and is hosted on the Mobility Server. The Mobility Client interface is an entry point to Service Desk and provides a simplified Service Desk interface for users to perform the following tasks:
  1. Search the knowledge base
  2. Submit a self-service request
  3. View opened and closed tickets
  4. View, approve, or deny pending approval requests

- The SRC Client interface is web-based, and is hosted on the SRC Server. The SRC Client interface is supported by web browsers running on a Windows host and provides access to the Service Request Catalog module. From the ESS view, an End User can create, view, and update service requests and access the Service Request Catalog from this interface.

Communications to the SM Server originating from the Windows Client, Web Server, Mobility Server, and SRC Server, are load-balanced. Before an HTTPS/TLS v1.2 session is established, HTTP traffic is first passed by the SM Server Load Balancer to the SM Server. The SM Load Balancer software is installed on one instance of the SM Server.

After a HTTPS/TLS v1.2 session is established, the Windows Client, Web Server, Mobility Server, and SRC Server communicate directly with the SM Server. The RSA BSAFE Crypto-J Module v6.2 provides secure TLS v1.2 communications between the Windows Client, Web Server, Mobility Server, SRC Server and the SM Server.

The SM Server is the core component of the TOE and contains all the HP SM modules and business logic of the system, as well as the runtime environment (RTE). The Apache Tomcat 6 Server, embedded in the SM Server, hosts web services APIs[13] for internal communication and third-party integrations.

Figure 1 below shows the details of the deployment configuration of the TOE. The following undefined acronyms appear in the diagram:

- AD – Active Directory
- JRE – Java Runtime Environment
- LDAP – Lightweight Directory Access Protocol
- OCI – Oracle Call Interface
- ODBC – Oracle Data Base Connection

[12] An End User interacts with an application module and, if permissions allow, create, update, and view application records.
[13] API – Application Programming Interface

- OS – Operating System
- RHEL – Red Hat Enterprise Linux
- SQL – Structured Query Language

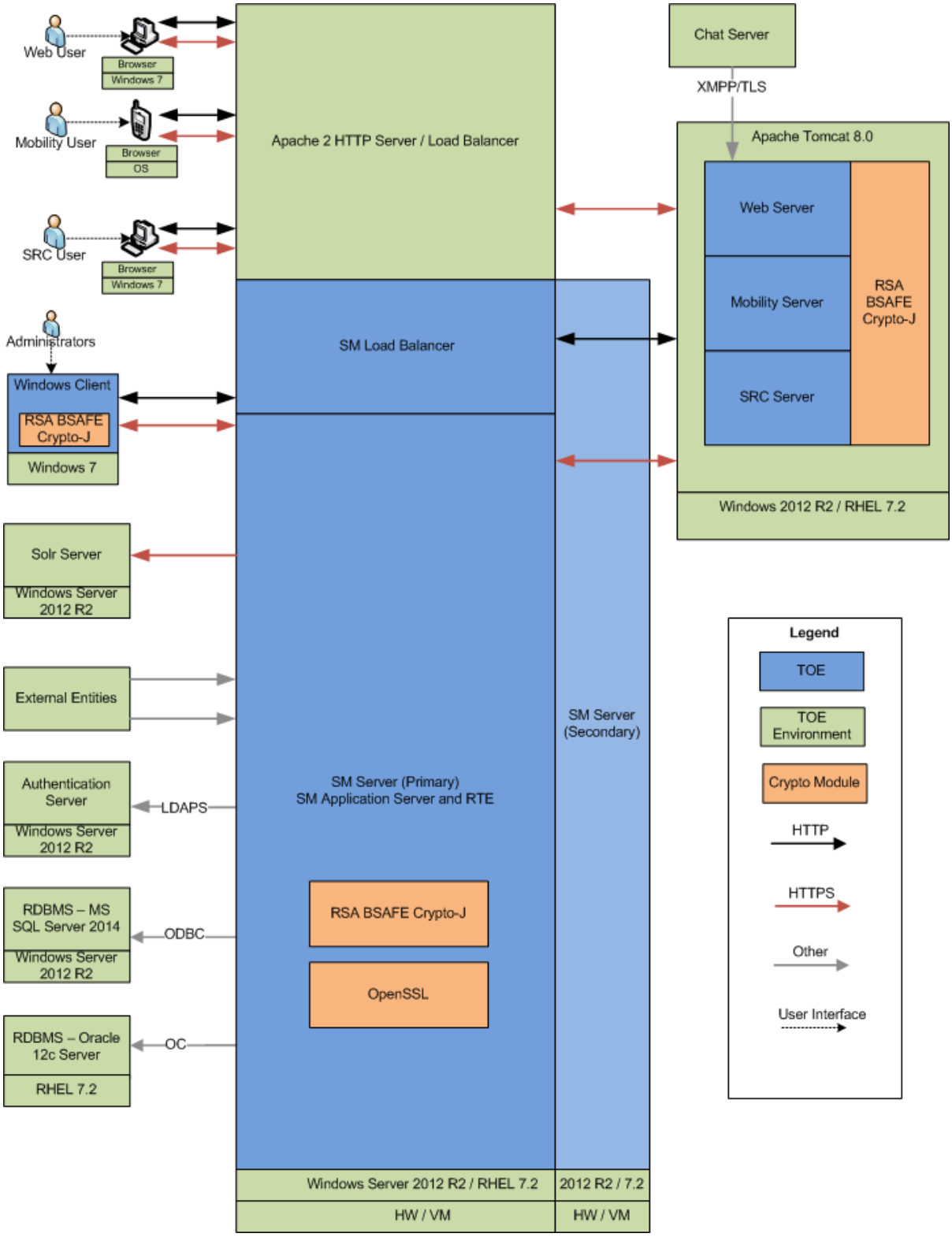

Figure 1 – Deployment Configuration of the TOE

1.4.2 TOE Environment

The TOE is intended to be deployed in a secure data center that protects physical access to the TOE. The SM Server, Web Client, Mobility Client, and SRC Client were tested in two configurations: Microsoft Windows Server 2012 R2 with Microsoft SQL Server 2014, and Red Hat Enterprise Linux (RHEL) 7.2 with Oracle Database 12c as depicted in Figure 1 above.

Table 3 specifies the minimum system requirements for the proper operation of the TOE.

Table 3 – TOE Minimum Requirements

Component	Software
TOE	
SM Server and SM Load Balancer	Windows Server 2012 R2
	Red Hat Enterprise Linux 7.2
Windows Client	Windows 7 64-bit
Web Server	Apache Tomcat 8.0
	JRE 8
Mobility Server	Apache Tomcat 8.0
	JRE 8
SRC Server	Apache Tomcat 8.0
	JRE 8
Non-TOE	
Database Servers	Oracle Database 12c
	Microsoft SQL Server 2014
Authentication Server	Microsoft Windows Active Directory Domain Services and Certificate Services
Knowledge Management	Apache Solr
Collaboration (Chat Server)	Ignite Realtime Openfire
Browser	Google Chrome 55 (uses mobile device emulation for Mobility Clients) running on Windows

The TOE relies on hardware and software that is not part of the TOE for its essential operation. The following software is required for the essential operation of the TOE and is not included in the TOE boundary:

- Platform (Microsoft Windows 2012 R2 or Red Hat Enterprise Linux 7.2)
- RDBMS[14] (Microsoft SQL[15] Server 2014 or Oracle Database 12c)
- Apache Tomcat 8.0

[14] RDBMS – Relational Database Management System
[15] SQL – Structured Query Language

- Apache HTTP Server 2.4
- Oracle Java Runtime Environment 8 (JRE)
- LDAPv3[16] / Microsoft Active Directory Domain Services
- Microsoft Active Directory Certificate Services
- Apache Solr (to support the Knowledge Management module)
- Ignite Realtime Openfire Chat Server (to support the Collaboration module)
- Google Chrome web browser
- Adobe Flash 10.3 or later

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

The TOE is to be installed on a customer-provided platform configured according to the software requirements listed in Table 3 above. For the evaluation, the TOE is to be installed on Windows Server R2 2012 OS with Microsoft SQL Server 2014 or Red Hat Linux 7.2 OS with Oracle 12c database.

1.5.1.1 TOE Software

The TOE installation is performed by HPE Professional Services using the ITSM Deployment Manager product. The software components deployed include the following:

- one instance of SM Server and SM Load Balancer on each primary SM Server in the Windows and RHEL environments
- one instance of SM Server (without the SM Load Balancer) on each secondary SM Server in the Windows and RHEL environments
- the following HP SM components:
    - Windows Client (Windows only)
    - Web Server (Windows or Linux)
    - Mobility Server (Windows or Linux)
    - SRC Server (Windows or Linux)

The TOE is deployed in the following configurations:

- Platform 1 – Windows Server 2012 R2
    - Configuration 1 – Local and LDAP authentication
    - Configuration 2 – X.509 authentication (excluding Mobility)
    - Configuration 3 – TSO authentication
- Platform 2 – RHEL Server 7.2
    - Configuration 1 – Local and LDAP authentication
    - Configuration 2 – X.509 authentication (excluding Mobility)
    - Configuration 3 – TSO authentication

[16] LDAP – Lightweight Directory Access Protocol

1.5.1.2 Non-TOE Software

The following non-TOE software provided by HPE is also required for TOE operation (in addition to the components specified in section 1.4.2 above:

- Knowledge Management Server (Apache Solr) as necessary to support the KM functionality.
- Chat Server (OpenFire Ignite Realtime) used to support the Collaboration module

1.5.1.3 Guidance Documentation

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

PDF files:

- *HP Service Manager; Software Version: 9.41 for the supported Windows® and UNIX® operating systems; Collaboration Guide; Document Release Date: September 2015*
- *HP Service Manager; Software Version: 9.41 for the supported Windows® and UNIX® operating systems; Mobile Applications User Guide; Document Release Date: September 2015*
- *HP Service Manager; Software Version: 9.41 for the supported Windows® and UNIX® operating systems; Processes and Best Practices Guide (Codeless Mode); Document Release Date: September 2015*
- *HP Service Manager; Software Version: 9.41 for the supported Windows® and UNIX® operating systems; Solr Search Engine Guide; Document Release Date: September 2015*
- *HP Service Manager; Software Version: 9.41 for the supported Windows® and UNIX® operating systems; Web Services Guide (Codeless Mode); Document Release Date: September 2015*
- *HP Service Manager; Software Version: 9.41 for the supported Windows® and UNIX® operating systems; Service Manager 9.41 Patch 3 Release Notes; Document Release Date: April 2016*
- *HP Service Manager; Software Version: 9.3x and 9.4x; Security Guide; Document Release Date: April 9, 2015*
- *HP Service Manager 9.41 Patch 3; Guidance Supplement; Document Version: 1.2; February 8, 2017*

HTML (.zip) files:

- *HP Service Manager 9.41 Help Center (Codeless Mode); Document Release Date: September 2015 (sm9.41_help_codeless.zip)*

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security functions/features which are further described in Sections 6 and 7 of this ST.

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functions (TSF)
- Resource Utilization
- Trusted Path/Channels
- TOE Access

1.5.3 Security Audit

The Security Audit functionality provides the capability to generate audit records for security relevant events, including the identity of the subject responsible for initiating the event. SM also records field level changes of SM database records in an audit log. Audit review from the Web Client interface is available to Administrators and users who have sufficient privileges.

1.5.4 Cryptographic Support

The Cryptographic Support functionality utilizes two FIPS-validated cryptographic libraries: RSA BSAFE®v6.2 Crypto-J Module for Java based TOE components and OpenSSL FIPS Object Module v2.0.11 for C++ based TOE components. Cryptographic operations are provided to secure communications, using TLS v1.2, among various physically separated TOE components and some trusted IT systems in the TOE environment.

1.5.5 User Data Protection

The User Data Protection functionality enforces the HP Service Manager Access Control SFP[17]. The TOE enforces role-based access control. Access control is enforced on SM records and database tables through a combination of user role, security group, kmprofile, and folder.

1.5.6 Identification and Authentication

The Identification and Authentication functionality requires users and administrators to identify and authenticate before gaining access to any TOE functionality. The TOE supports multiple authentication mechanisms: local password-based authentication, LDAP authentication, X.509 certificate-based remote authentication, and Trusted Sign-on (TSO) methods of authentication.

1.5.7 Security Management

The Security Management functionality provides the capability for administrators to manage the security functionality, TSF data, and security attributes provided by the TOE. The TOE provides the System Administrator role for TOE security management.

1.5.8 Protection of the TSF

The Protection of the TSF functionality ensures that the TOE maintains a secure state in the event of an SM Server failure. The TOE also ensures that data is protected from disclosure or modification when transferred internally between TOE components. Internal TSF data transfer protection is provided by HTTPS between the SM Server and:

- the Windows Client,
- the Web Server,
- the Mobility Server, and

[17] SFP – Security Function Policy

- the SRC Server.

1.5.9 Resource Utilization

The Resource Utilization functionality provides the capability for the TOE to perform automatic failover procedures to ensure that all capabilities of the TOE are still operational in the event of a SM Server failure. The SM Load Balancer software performs this function.

1.5.10 Trusted Path/Channels

The TOE provides trusted channels using TLS for communications between the SM Server and:

- the LDAP authentication server
- the Apache Solr server

The TOE provides trusted channels using TLS for communications between external clients connecting to the SM Server SOAP/REST APIs.

1.5.11 TOE Access

The TOE Access functionality ensures that HP SM user sessions are terminated by the TSF after the 30-minute default period of inactivity or a System Administrator-configured time interval of TOE user inactivity.

1.5.12 Service Level Management

The TOE performs analysis based on thresholds set for Service Level Targets (SLTs) for Service Level Agreements and internal Operational Level Agreements (OLAs). SLTs are defined for response, availability and escalations. Alerts are triggered as a function of time remaining until the SLT expires.

1.6 Excluded Functionality

The following features and functionality are excluded from the scope of the evaluation:

- Use of the command line interface.
- Use of the TOE in non-FIPS mode
- Human user access to REST and SOAP APIs
- Failover/load balancing for REST and SOAP APIs
- Access to the Mobility Client from mobile devices. Google Chrome Mobile Device Emulation mode was used in the evaluated configuration to simulate mobile device access.
- Mobility Client in the X.509 authentication configuration
- X.509 authentication for the Windows Client, REST and SOAP APIs
- The use of CAC or PIV cards for X.509 authentication
- TOE account lockout under TSO and X.509 configuration
- Session timeout for TSO and X.509 authentication
- TSO authentication for the REST and SOAP APIs
- LW-SSO authentication

- "Classic mode" of operation
- Custom user roles
- All Windows Client views except HP Service Manager
- All Web Client views except ESS and Power User
- All Mobility Client views except Power User

2. Conformance Claims

This section and Table 4 provide the identification for any CC, PP, and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 4 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 4, September 2012; CC Part 2 conformant CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the Common Evaluation Methodology (CEM) as of 2/17/2016 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with Flaw Remediation (ALC_FLR.2)

3. Security Problem

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

- Known and presumed threats countered by either the TOE or by the security environment
- 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: TOE System Administrators 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 (including those with module administration privileges) 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[18] and user data saved on or transitioning through the TOE and the hosts on the protected network. Both the confidentiality and integrity of the data must be protected. Removal, diminution and mitigation of the threats are through the objectives identified in Section 0 Security Objectives. Table 5 below lists the applicable threats.

Table 5 – Threats

Name	Description
T.AUDIT_COMPROMISE	An attacker who is not a TOE user may breach confidentiality by viewing audit records. The attacker may modify or delete audit records, or prevent future records from being recorded, thus masking the actions of an attacker who is not a TOE user.
T.DATA_COMPROMISE	An attacker who is not a TOE user may read, modify, delay, or destroy TOE configuration or user data stored on the TOE or being transmitted over the IT network.
T.DATA_UNAVAILABLE	TOE or IT Environment data or capabilities may become unavailable due to server failure.
T. MASQUERADE	An attacker or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.UNAUTHORIZED	A TOE user may gain unauthorized user access to user data, or to TOE security functions and data.
T. TAMPERING	A TOE user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.

[18] TSF – TOE Security Functionality

3.2 Organizational Security Policies

There are no Organizational Security Policies defined for this Security Target.

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 6 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 6 – Assumptions

Name	Description
A.AUTHENTICATE	The TOE environment will provide an authentication server for the identification and authentication of users and devices attempting to access the TOE. The authentication server will support Windows domain and certificate authentication.
A.INSTALL	The TOE, and supporting third party applications, will be installed on the appropriate dedicated operating system.
A.LOCATE	The TOE will be located within a controlled access facility and appropriately located within a secure internal network to perform its functions.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. Administrators of the TOE are assumed to be appropriately trained to undertake configuration and management of the TOE in a secure and trusted manner.
A.NOEVIL	The authorized administrators who manage the TOE and database administrators who manage the TOE environmental components will be non-hostile, appropriately trained, and follow all guidance.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.TIMESTAMP	The IT environment will provide the TOE with reliable timestamps.
A.FIPS	Cryptographic functionality will be provided by FIPS 140-2 validated crypto modules. Only FIPS 140-2 approved cryptographic algorithms and services will be used and the TOE will be configured to operate in "FIPS-mode" only.
A.PASSWORDS	All account names, passwords or public key certificates used by external applications to communicate with the TOE via its APIs will be appropriately safeguarded and not shared with any user.

4. Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 0). 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 7 below.

Table 7 – Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE must enforce an access control policy in order to prevent unauthorized users from gaining access to it and the resources that it controls.
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.ALERT	The TOE must alert appropriate users when a service level security policy violation occurs.
O.AUDIT	The TOE must provide the capability to detect security relevant events and generate audit records of those events. The TOE will provide the capability for only authorized TOE users to access the audit information.
O.AUTHENTICATE	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.
O.AVAILABILITY	The TOE shall preserve the availability of IT functions and data.
O.FAIL_SECURE	The TOE must preserve a secure state and SM Server capabilities in the event of a server failure.
O.FIPS	The TOE must implement FIPS 140-2 validated cryptographic modules and approved algorithms for the TOE to perform cryptographic functions.
O.PROTECT	The TOE must ensure the integrity of user, audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
O.SESSION	The TOE must terminate a user session after an administrator-configured period of inactivity.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 8 below lists the IT security objectives that are to be satisfied by the environment.

Table 8 – IT Security Objectives

Name	Description
OE.AUTHENTICATOR	The TOE environment will provide an authentication server for the identification and authentication of individuals and devices attempting to access the TOE.
OE.NET_CON	The TOE environment must be implemented such that the TOE is appropriately located within and connected to the network to perform its intended function.
OE.PLATFORM	The TOE hardware and operating system must support all required TOE functions.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference and tampering.
OE.SECURE_COMM	The TOE environment must support or provide secure communications between the TOE and external users or servers to protect the confidentiality and integrity of TSF and User data. FIPS 140-2 approved cryptographic algorithms and services must be used to provide the TLSv1.2 communications where possible. All external servers should be configured to provide secure communication when communicating with the TOE. Where possible, a VPN should be used to protect access to the TOE over untrusted networks.
OE.TIMESTAMP	The TOE environment must provide reliable timestamps to the TOE.
OE.EXTERNAL_SERVERS	The LDAP and RDBMS server used by the TOE should be secured appropriately using best practices to ensure that TOE user accounts and TOE data is appropriately protected. TOE service accounts are used only for the purpose of facilitating communication with these servers and their privileges should be limited only to the functions necessary for TOE operation.

4.2.2 Non-IT Security Objectives

Table 9 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 9 – Non-IT Security Objectives

Name	Description
NOE.MANAGE	Sites deploying the TOE must provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system and its environment are used securely.
NOE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.

5. Extended Components

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

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 10 identifies all extended SFRs implemented by the TOE.

Table 10 – Extended TOE Security Functional Requirements

Name	Description
EXT_SLM_AAE	Alert and Escalation
EXT_SLM_STA	Service Target Analysis

5.1.1 Class SLM: Service Level Management Function

Service Level Management functions involve the analysis Service Level Targets (SLTs) and the escalation and alerting of any potential availability violations. The analysis is based on thresholds set for Service Level Targets (SLTs) for Service Level Agreements and internal Operational Level Agreements (OLAs). SLTs are defined for response and availability and escalations and alerts are triggered as a function of time remaining until the SLT expires. The EXT_SLM: Service Level Management class was modeled after the CC FAU: Security audit class. The extended family EXT_SLM_STA: Service target analysis and related components were modeled after the CC family FAU_SAA: Security audit analysis. The extended family EXT_SLM_AAE: Alert and notification and related components were modeled after the CC family FAU_ARP.

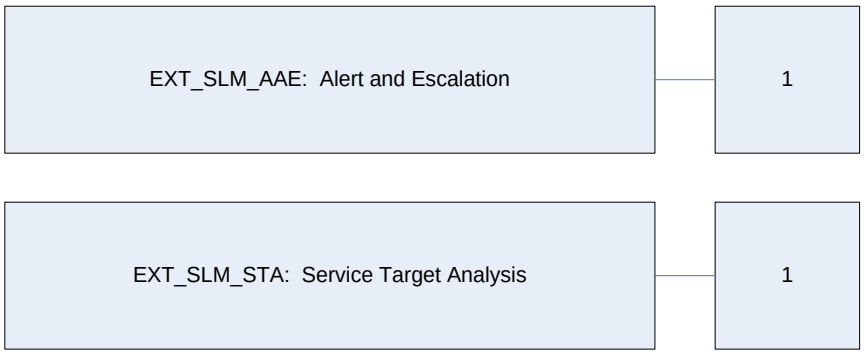

Figure 2 – EXT_SLM: Service Level Management Function Class Decomposition

5.1.1.1 Alert and Escalation (EXT_SLM_AAE)

Family Behavior

This family defines requirements for the response to be taken in case of a detected, potential or actual SLT violations that may lead to a loss of the availability of services managed by the TOE.

Component Leveling

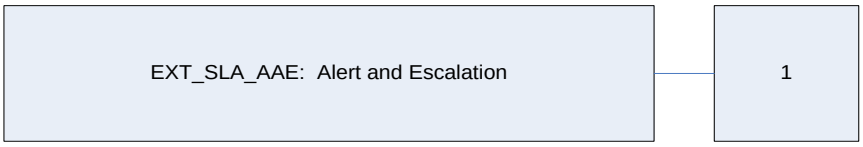

Figure 3 – EXT_SLM_AAE Family Decomposition

EXT_SLM_AAE.1 Alert and Escalation, specifies that the TSF will take actions when a SLT is violated or has the potential to be violated.

Management: EXT_SLM_AAE.1
The following actions could be considered for the management functions in FMT:
Threshold Settings (add, modify, delete), and alerting and escalation functions (add, modify, delete).

Audit: EXT_SLM_AAE.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
Minimal: event, users notified, means of notification

EXT_SLM_AAE.1 Alert and Escalation
Hierarchical to: No other components.
Dependencies: None
EXT_SLM_AAE.1
The TSF shall generate an alert or escalation, and notify specified users, when SLT thresholds are violated.

5.1.1.2 Service Target Analysis (EXT_SLM_STA)

Family Behavior

This family defines requirements for automated means that apply escalation and alert criteria to for possible or actual security violations involving availability of services managed by the TOE. The actions to be taken based on the detection can be specified using the Service level management EXT_SLM_AAE: Alert and Escalation family.

Component Leveling

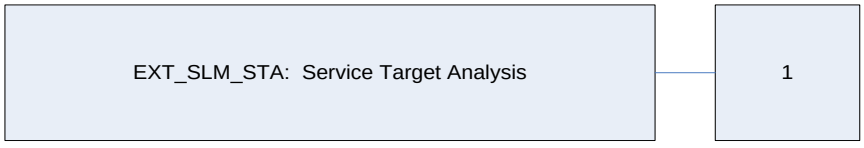

Figure 4 – EXT_SLM_STA Family Decomposition

EXT_SLM_STA.1 Service Target Analysis, specifies that the TOE will perform analysis of SLTs. The TSF shall be able to detect the occurrence of potential or actual violations of SLTs and generate an event that identifies the potential loss of the availability of services managed by the TOE.

Management: EXT_SLM_STA.1
The following actions could be considered for the management functions in FMT:

- Configuration of SLT threshold settings.

Audit: EXT_SLM_STA.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Generated events

EXT_SLM_STA.1 Service Target Analysis
Hierarchical to: No other components.
Dependencies: None

EXT_SLM_STA.1 .1

The TSF shall be able to detect the occurrence of a SLT threshold violation. If a violation is identified, the TSF shall generate an event that identifies a potential loss of the availability of services managed by the TOE.

EXT_SLM_STA.1 .2

The TSF shall be able to enforce analysis of SLTs and conditions under which SLT violations affect service availability.

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 11 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 11 – TOE Security Functional Requirements

Name	*Description*	*S*	*A*	*R*	*I*
FAU_GEN.1	*Audit data generation*	✓	✓		
FAU_GEN.2	*User identity association*				
FAU_SAR.1	*Audit Review*		✓		
FIA_AFL.1	*Authentication failure handling*	✓	✓		
FIA_ATD.1	*User attribute definition*		✓		
FIA_UAU.2	*User authentication before any action*				
FIA_UAU.5	*Multiple authentication mechanisms*		✓		
FIA_UID.2	*User identification before any action*				
FCS_COP.1	*Cryptographic operation*		✓		
FDP_ACC.1	*Subset access control*		✓		
FDP_ACF.1	*Security attribute based control*		✓		
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_FLS.1	*Failure with preservation of secure state*		✓		
FPT_ITT.1	*Basic internal TSF data transfer protection*	✓			
FRU_FLT.1	*Degraded fault tolerance*		✓		
FTA_SSL.3	*TSF-initiated termination*	✓	✓		
FTP_ITC.1(a)	*Inter-TSF trusted channel (TSF)*		✓		✓
FTP_ITC.1(b)	*Inter-TSF trusted channel (Trusted IT product)*		✓		✓
EXT_SLM_AAE.1	*Alert and Escalation*				
EXT_SLM_STA.1	*Service Target Analysis*				

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

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1

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

a. Start-up and shutdown of the audit functions;
b. All auditable events, for the [*not specified*] level of audit; and
c. [

Syslog events:

- *user and administrator login and logout*
- *failed login authentication attempts*

Audit Log events:

- *modification to any specified SM Server database field*

].

FAU_GEN.1.2

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

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST,

[

Captured in the Syslog: Event, Start Time, Stop Time, User Name, Terminal Name, Current Status
Captured in the Audit Log: Modified field name, old version of the data, new version of the data, current date and time, user ID

].

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 [*the System Administrator*] with the capability to read [*all system logs and Audit Log data]* from the audit records.

FAU_SAR.1.2

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

Application Note*:* All audit data can be reviewed by an authorized user as described above with the exception of audit startup and shutdown events, which are recorded in the `sm.log` file. The `sm.log` file is written to the primary and secondary HP SM Servers and accessed via OS interfaces. The Syslog and Audit logs are accessed from the Windows Client and Web Client.

6.2.2 Class FCS: Cryptographic Support

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 [*the operations listed in Table 12 – RSA BSAFE Crypto-J Cryptographic Services and Table 13 – OpenSSL Cryptographic Services*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms listed in Table 12 and Table 13],* and cryptographic key sizes [*the cryptographic key sizes listed in Table 12 and Table 13*]. The operations, cryptographic algorithms, and cryptographic key sizes must correspond to [*the certificate numbers listed in Table 12 and Table 13*].

Table 12 – RSA BSAFE Crypto-J Cryptographic Services

Cryptographic Operation	Cryptographic Algorithm	Key / Digest Size	Standard	Certificate #
Asymmetric Cipher (Key Transport)	RSA	2048 bit, 3072 bit, 4096 bit	FIPS 186-2	Non-Approved Allowed in FIPS mode for key transport
Key Derivation	KDF[19] TLS12	256 bit, 384 bit, 512 bit	NIST SP 800-135rev1	471
Symmetric Cipher (Encryption / Decryption)	AES in CBC and GCM modes	128 bit, 256 bit	FIPS 197	3263
	Triple DES in CBC mode	Three 56 bit keys	NIST SP 800-67	1852
Message Digest (MD)	SHA[20]-1, SHA-2	160 bit, 256 bit, 384 bit, 512 bit	FIPS 180-4	2701
Message Authentication Code	HMAC[21] SHA	Depends on the SHA MD selected	FIPS 198-1	2062
Digital Signature	RSA X9.31, PKCS#1 V.1.5, RSASSA-PSS	2048 bit, 3072 bit	FIPS 186-2	1663
Random bit generation	HMAC DRBG	Must use approved Message Digest algorithm	SP 800-90A	722

Table 13 – OpenSSL Cryptographic Services

[19] KDF – Key Derivation Function
[20] SHA – Secure Hash Algorithm
[21] HMAC – Hash-based Message Authentication Code

Cryptographic Operation	Cryptographic Algorithm	Key / Digest Size	Standard	Cert #
Symmetric Cipher Encryption / Decryption	AES in CBC and GCM modes	128 bit, 256 bit	FIPS 197	2484
	Triple DES in CBC mode	Three 56 bit keys	NIST SP 800-67	1522
Message Digest – Hash Function	SHA-1, SHA-2	160 bit, 256 bit, 512 bit	FIPS 180-4	2102
Message Authentication Code	HMAC SHA	Depends on the SHA MD selected	FIPS 198-1	1526
Digital Signature	RSA X9.31, PKCS#1 V.1.5, RSASSA-PSS	2048 bit, 3072 bit, 4096 bit	FIPS 186-2	1273
Random bit generation	HMAC DRBG	Must use approved Message Digest algorithm	SP 800-90A	342

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 [*HP Service* Manager *Access Control SFP*] on

[

Subjects: TOE operators and TOE administrators

Objects: area, database tables, SM records

Operations:

SM functionality:

access

Database tables:

view, update (TOE operators)

view, new (add), update, delete (TOE administrators)

SM records:

view, new (add), update, and delete/close

].

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 [*HP Service* Manager *Access Control SFP*] to objects based on the following:

[

S*ubject Attributes:*

user role, security group, kmprofile, folder

Object Attributes:

SM functionality: Area

Database tables: Database name, table name

SM records: field name, security folder field, Mandant field

].

Application Note*:* The TOE grants access to users based on the security model based on a combination of attributes, which are explained below:

User Role – A user role is a container of security roles and capability words that grants/restricts access to interfaces that is assigned to an operator.

Security Group – Operators are assigned to security groups. Security groups are a component of the Mandanten security mechanism. Mandanten provides the capability to filter records and restrict queries. The Mandant field is associated with a security group and defines the field value(s) to apply filtering conditions to the records an operator may view. Restricting queries, also associated with a security group, further limit the data an operator can access when querying a Mandanten protected file.

Kmprofile – A Knowledge Management profile includes the specific access rights to KM documents. A kmprofile can be associated with an operator record or can be associated with a kmgroup that is associated with an operator record.

Folder – If folder entitlement is enabled, operators can access a folder if the folder is included in the operator record.

FDP_ACF.1.2

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

[

1. *If the operator is associated with a user role, security group, kmprofile, or folder that authorizes an operation, then the operation is allowed. Otherwise, the operation is denied.*
2. *If a folder is specified in the operator record, then the operator can only access records included their folder and are denied access to records which are not included in their folder.*
3. *If a security group is specified in the operator record and the security group contains a Mandant field value, then the operator can access only the records satisfying the "include" filtering conditions for the field value and are denied access to all other records.*

].

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*No additional rules*].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [*If a security group is specified in the operator record and the security group contains a Mandant field value, then the operator cannot view the SM records that satisfy the "exclude" filtering conditions for the field value*.]

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 to 2147483647]* unsuccessful authentication attempts occur related to [*attempted logins to the Windows Client, Web Client, Mobility Client, and SRC Client*].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [*lock the account until the System Administrator resets the lockout*].

Application Note – The "Attempts per login session" value is long type in C/C++, an integer value from 1 to 2147483647. If an out-of-bounds positive value is entered, the user login attempt is rejected. If an out-of-bounds negative value is entered, the user is locked out.

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*
- *password*
- *user role*
- *security group*
- *kmprofile*
- *folder*
- *failed login count*
- *allowed inactive time*
- *password expiration*
- *administrative lockout*

].

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.5 Multiple authentication mechanisms

Hierarchical to: No other components.
Dependencies: No dependencies

FIA_UAU.5.1

The TSF shall provide [*password-based and X.509 certificate-based authentication*] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the
[
following rules:

Only one of the authentication methods below can be configured at a given time. The first configuration supports password-based authentication. The second configuration supports TSO authentication, and the third configuration supports X.509 authentication. The authentication methods are described below.

1. *Password-based authentication.*

   a. *LDAP and Local*

   When the TOE is configured for LDAP and local authentication. If a user has a valid LDAP record, then LDAP authentication is attempted, otherwise local authentication is attempted. User-entered credentials are sent by the Web, Mobility, SRC, and Windows Clients over HTTPS to the SM Server. The SM Server sends the username to the LDAP server to verify a match.

   If the username corresponds to a valid domain user, the SM Server sends the user-entered password to the LDAP server. If the password sent by the SM Server matches the stored LDAP password, the user is authenticated and allowed access to the TOE.

   If the username does not correspond to a valid domain user, the SM Server checks to see that the username corresponds to a valid operator record. If the user has a valid operator record, the SM Server compares a hash of the user password to the value stored in the user's operator record. If they match, the user is authenticated and allowed access to the TOE.

2. *TSO*

   When the TOE is configured to use TSO, a user can login through Web, SRC, and Windows Client without entering their credentials, if they are already logged into the Windows domain, using Integrated Windows Authentication and the user's session information provided by the OS.

3. *X.509 certificate-based authentication:*

   The user presents an X.509 certificate. If the Web Client SM client successfully verifies that the *certificate is valid and the Distinguished Name of the user is recognized as a valid user in the LDAP directory, then the user is authenticated.*

X.509 authentication is not available from the Mobility Client and Windows Client. When X.509 is enabled, the Mobility Client must be installed on a separate server or removed from the installation. When TSO is enabled, local and LDAP authentication is used to authenticate a user from the Mobility Client using Basic

Authentication. When x.509 is enabled, local and LDAP authentication is used to authenticate a user from the Windows Client. Once authenticated the user can access the TOE.].

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 or
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1

The TSF shall enforce the [*HP Service Manager Access Control SFP*] to restrict the ability to [*change default, query, modify, delete*] the security attributes [*user role, security group, kmprofile, folder*] *to* [*System Administrators*].

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 [*HP Service Manager 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 [*no one*] to specify alternative initial values to override the default values when an object or information is created.

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 audit and alerts*
- *System administration and configuration*
- *Manage access control to tables and administrative functions*
- *Configuration and assignment of: user role, security group, kmprofile, folder*

].

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 [

- *System Administrator*
- *Change Management roles*
- *Incident Management roles*
- *Knowledge Management roles*
- *Problem Management roles*
- *Request Fulfillment roles*

- *Service Catalog roles*
- *Service Desk roles*
- *Self Service*

].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.6 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [*Failure of an SM Server instance*].

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 and modification*] when it is transmitted between separate parts of the TOE.

Application Note: All traffic handled by the SM Load Balancer is plaintext and does not contain user or TSF data.

6.2.7 Class FRU: Resource Utilization

FRU_FLT.1 Degraded fault tolerance

Hierarchical to: No other components.

Dependencies: FPT_FLS.1 Failure with preservation of secure state

FRU_FLT.1.1

The TSF shall ensure the operation of [*the SM Server capabilities (excluding REST and SOAP)*] when the following failures occur: [*failure of an SM Server instance*].

6.2.8 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_SSL.3.1

The TSF shall terminate an interactive session after a [*default of 30 minutes or a System Administrator configured interval of user inactivity*].

6.2.9 Class FTP: Trusted Path/Channels

FTP_ITC.1(a) Inter-TSF trusted channel (TSF)

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_ITC.1(a).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(a).2

The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1(a).3

The TSF shall initiate communication via the trusted channel for

[

- Communications with the LDAP server
- Communications with the Apache Solr server

].

FTP_ITC.1(b) Inter-TSF trusted channel (Trusted IT product)

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_ITC.1(b).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(b).2

The TSF shall permit [*the remote trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1(b).3

The TSF shall initiate communication via the trusted channel for

[

- Communications with SOAP/REST API clients

].

6.2.10 Class SLM: Service Level Management

EXT_SLM_AAE.1 Alert and Escalation
Hierarchical to: No other components.
Dependencies: None
EXT_SLM_AAE.1

The TSF shall generate an alert or escalation, and notify specified users, when SLT thresholds are violated.

EXT_SLM_STA.1 Service Target Analysis
Hierarchical to: No other components.
Dependencies: None
EXT_SLM_STA.1 .1

The TSF shall be able to detect the occurrence of a SLT threshold violation. If a violation is identified, the TSF shall generate an event that identifies a potential loss of the availability of services managed by the TOE.

EXT_SLM_STA.1 .2

The TSF shall be able to enforce analysis of SLTs and conditions under which SLT violations affect availability of services managed by the TOE.

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2+ augmented with ALC_FLR.2. Table 14 summarizes these requirements.

Table 14 – Assurance Requirements

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

7. TOE Summary 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 15 lists the security functionality and their associated SFRs.

Table 15 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit Review
Cryptographic Support	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based 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.5	Multiple authentication mechanisms
	FIA_UID.2	User identification before any action
Security Management	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 the TOE Security Functions (TSF)	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITT.1	Basic internal TSF data transfer protection
Resource Utilization	FRU_FLT.1	Degraded fault tolerance
TOE Access	FTA_SSL.3	TSF-initiated termination
Trusted Path/Channels	FTP_ITC.1(a)	Inter-TSF trusted channel (TSF)
	FTP_ITC.1(b)	Inter-TSF trusted channel (Trusted IT product)
Service Level Management	EXT_SLM_AAE.1	Alert and Escalation
	EXT_SLM_STA.1	Service Target Analysis

7.1.1 Security Audit

HP SM provides an auditing feature that records modifications to a customized selection of fields in the HP SM database. Field modifications are detected by comparing the fields in the original version of a record to the updated version. When a modification is detected, the SM Server generates an Audit record. See Table 16 below for the record contents.

The HP SM System log (Syslog) table captures user authentication attempts, including successful[22] and failed logins (see Table 16 below for the fields in the Syslog table). Startup and shutdown events, in addition to more detailed authentication logs are captured in the `sm.log` file. The Syslog table is stored in the database, where the `sm.log` file is stored in the filesystem.

System Administrators can view the System Log table, can specify the fields to be recorded in the Audit table, and can view the Audit table to see changes to database fields.

Table 16 – Audit Record Information

Audit Record Information	
Files / Tables	**Audit/Syslog Record Contents**
Audit Log (dB table)	Modified field name, old version of the data, new version of the data, current date and time, user ID
System Log (Syslog file)	Event, Start Time, Stop Time, User Name, Terminal Name, Current Status

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

7.1.2 Cryptographic Support

The TOE implements two FIPS-validated cryptographic modules:

- OpenSSL FIPS Object Module v2.0.11, certificate # 2398
- RSA BSAFE® Crypto-J v6.2, certificate # 2468

The SM Server and clients run in FIPS mode when the "fipsmode" parameter is set to "2" on the SM Server. The FIPS modules are completely contained within the TOE boundary.

All cryptographic support claims involve the use of FIPS-validated algorithms. The algorithms and certificate numbers are listed above in Table 12. The TOE implements TLS v1.2, which makes use of encryption and decryption, digital signature verification, hashing, and MAC functionality provided by the cryptographic libraries.

[22] Successful logins are recorded in the Syslog table with the details of the event. When the user logs out, the "Current Status" field is changed to "Logged out". Therefore, the records will display a status of "Logged on" only while a user session is active. For investigation purposes after a user has logged out, the `sm.log` file should be used to review successful logins.

The OpenSSL FIPS Object Module v2.0.11 is used to provide a secure TLS connection between the SM Server and the LDAP Server. The RSA BSAFE Crypto-J Module v6.2 is used to provide secure mutually authenticated TLS connections between the SM Server and the following components: Windows Client, Web Server, Mobility Server, SRC Server, and Solr Server. The processing of X.509 certificates is also handled by RSA BSAFE Crypto-J Module v6.2.

In addition, for local authentication, the SM Server calls the RSA BSAFE Crypto-J Module v6.2 for the SHA-512 algorithm to hash the password and then compares the newly hashed value to the hashed value stored in the RDBMS.

TOE Security Functional Requirements Satisfied: FCS_COP.1

7.1.3 User Data Protection

The TOE implements role-based access control. The SM Security Access Control SFP uses a combination of models: the Process Designer security model, Knowledge Management, and Mandanten and Folder Entitlement. The Process Designer security model uses a combination of security attributes in the operator record to control access to TOE data and functionality. SM provides out-of-box user roles for the SM modules. A user role is a combination of one or more security roles and capability words which restrict user interface access.

The Process Designer Security Model controls TOE access for the following modules:

- Service Desk
- Incident Management
- Change Management
- Problem Management
- Request Fulfillment
- Service Level Management
- Survey
- Knowledge Management (Administrative functions only)

The Knowledge Management document access control is based on Knowledge Management profiles (sets of rights). Documents are associated with categories, which map Knowledge Management groups to Knowledge Management profiles. To access a document, an operator must be associated with the Knowledge Management profile which grants rights to the document category. The Knowledge Management profile can be associated with an operator record or the operator can belong to a Knowledge Management group that is associated with the Knowledge Management profile.

Mandanten and Folder Entitlement are optional choices to restrict access to database files and their contents and applies to all modules, with special handling required for the Knowledge Management module. Mandanten filters what records operators see and additionally restricts what they can query. Operators who are members of a security group see only the records that meet the specific filtering criteria for the group. The feature can be used for segregating customer information or data within an organization. Folder Entitlement provides another layer of access control. If the feature is enabled, then a System Administrator must select the folders that each security role or KM profile can access.

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

7.1.4 Identification and Authentication

HP SM provides out-of-box login accounts with system administration privileges. These accounts include System.Admin and falcon, and they each have a default blank password. The System.Admin account is used for the initial connection to the SM Server. The falcon account is a service account. The System Administrator must disable the initial System.Admin account or change its password after creating other operator accounts and must assign a new password to the falcon account.

No actions are allowed before a user is authenticated. User attributes are stored in the operator record and include the mandatory fields of username and password and may also contain: user role, security groups, kmprofile, login and session information, lockout information, etc. The TOE enforces lockout after a specified number of failed authentication attempts, and accounts remain locked until reset by an administrator.

HP SM supports password-based mechanisms, local (password hashes are stored in the database) and LDAPv3, X.509 certificate authentication, and TSO. The authentication options are configured during installation by an HPE engineer and remain fixed while the TOE is in operation. Only one configuration is available for each installation. The three evaluated configurations are:

- Local and LDAPv3 (password-based)
- X.509
- TSO

With LDAP and local authentication, if a user has a valid LDAP record, then LDAP authentication is attempted, otherwise local authentication is attempted.

With TSO, HP SM clients can be configured to automatically log on using the same authentication information entered by users when logging onto the OS used to access the Windows Client, Web Client or SRC Client. With TSO enabled, users bypass the HP SM logon screen and directly enter HP SM. The SM Server grants access to clients only if the following conditions are met:

- The user's logon credentials match an existing operator record in SM or a valid LDAP source recognized by SM.
- A trusted authentication authority, such as the operating system, validates the user's logon credentials.
- The Windows Client, Web Client, or SRC Client, must present a signed TLS certificate.

When X.509 certificate authentication is used, a user must present a valid certificate in order to authenticate to the Web Server or SRC Server. User lookups are performed via LDAP.

TOE Security Functional Requirements Satisfied: FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UID.2

7.1.5 Security Management

The out-of-box System Administrator user role is grants administrative rights to all areas. The System Administrator user role is assigned to the out-of-box operators, System.Admin and falcon. Only users with the System Administrator user role can access or perform the behavior of the Security Management Functions listed in Table 17 below.

Table 17 – System Administrator Security Management Functions

Action	Security Management Functions
Set individual access restrictions in operator records.	
Assign:	operators to km profiles
	roles to operators
	Security Roles to operators for Process Designer enabled modules
	operators to assignment groups
	operators to security groups
	operators to user role descriptions
Create:	a login profile (can set a default password)
Modify:	field-level rights
Enable:	user session restrictions
Set access restrictions by tailoring the application layer.	
Create:	display screen or display options records
	document engine objects, states, and processes
	format control records
	menus
Set global access restrictions in the System Wide Company record.	
Enable:	account expiration times
	active integrations to external applications
	application time limits
	login restrictions
	password requirements
Set global access restrictions to application tables in Mandanten.	
Define:	security group access to database tables
Filter:	records visible to users by security groups
Limit:	access to records by adding security group restricting queries
Set global access restrictions in the initialization file.	
Define:	named users and restricting login to these named users only
Enable:	Transport Layer Socket (TLS) connections between the server and clients
	shared Mandanten file restrictions

System Administrators have full rights to manage the modules. User roles associated with module administration roles have module administration and configuration rights as follows:

- **View** – view administration and configuration settings
- **Update** – update the value of existing settings
- **Create** – create new configuration settings
- **Delete** – delete configuration settings
- **Expert –** provides module specific settings
- **Admin** – provides the ability to add, edit or delete administration settings and certain configuration settings

Module administrators, i.e., user roles associated with a module configuration area, are assigned Expert or Admin rights. Examples include: Change Manager, Incident Manager, Problem Manager, Request Administrator, Service Catalog Manager, and Service Desk Manager. Most roles have View access. The default access rights for View, Update, Create, Delete, Expert, or Admin vary depending on the out of the box roles. A system administrator can change the default access rights. Security management functions are permitted based on a combination of area (grouped by module below), areas, and rights for the following modules:

Table 18 – Security Management by Area

Module	Areas	Rights
Service Desk	Service Desk, Service Desk Configuration	View, New, Update, Delete/Close, Modify Template, Expert, Admin
Incident Management	Incident, Incident Tasks, Incident Management Configuration	View, New, Update, Delete/Close, Modify Template, Expert, Admin
Problem Management	Problem, Problem Management Configuration, Problem Tasks	View, New, Update, Delete/Close, Modify Template, Expert, Admin
Change Management	Change, Change Tasks, Change Management Configuration	View, New, Update, Delete/Close, Modify Template, Expert, Admin, Allowed Categories, Allowed Statuses
Request Fulfillment	Request, Request Tasks, Request Management Configuration	View, New, Update, Delete/Close, Modify Template, Expert, Admin, Allowed Categories, Allowed Statuses
Service Level Management	Service Level Management, Service Level Management Configuration	View, New, Update, Delete/Close, Modify Template, Expert, Admin
Knowledge Management	Knowledge, Knowledge Administration	View, New, Update, Delete/Close, Modify Template, Expert, Admin
Survey	Survey, Survey Configuration	View, New, Update, Delete/Close, Modify Template, Expert, Admin
Service Desk, Incident Management, Change Management, Problem Management Default Security Rights and Settings	Security	View, New, Update, Delete/Close, Modify Template, Expert, Admin
	Common Configuration	View, New, Update, Delete/Close, Modify Template, Expert, Admin
	Tailoring	View, New, Update, Delete/Close, Modify Template, Expert, Admin

The KMAdmin capability word added to an operator record grants Knowledge Management administration and configuration capabilities.

SOAP API and RESTful API capability words grant access to web services.

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

7.1.6 Protection of the TSF

The TOE utilizes the RSA BSAFE Crypto-J Module v6.2® cryptographic functionality to secure communications between TOE components. These secure communications prevent unauthorized disclosure and modification of TSF data. The TOE uses HTTPS for communications between:

- the Windows Client and the SM Server
- the Web Server and SM Server
- the Mobility Server and SM Server
- the SRC Server and SM Server

The Windows Client and Servers above mutually authenticate with the SM Server through the exchange and verification of their signed certificates.

The TOE provides secure failover using the SM Server Load Balancer which is installed on both instances of the SM Server. If a service degradation or interruption occurs with a single SM Server, the traffic is diverted to another available SM Server and the security of the TOE is maintained.

TOE Security Functional Requirements Satisfied: FPT_ITT.1, FPT_FLS.1

7.1.7 Resource Utilization

The TOE provides fault tolerance using the SM Server Load Balancer. If a service degradation or interruption occurs within a single SM Server, the traffic is diverted to another available SM Server.

TOE Security Functional Requirements Satisfied: FRU_FLT.1

7.1.8 TOE Access

User sessions are terminated by the TOE after a System Administrator-configured period of inactivity.

TOE Security Functional Requirements Satisfied: FTA_SSL.3

7.1.9 Trusted Channels

The OpenSSL FIPS Object Module v2.0.11 provides the cryptographic algorithms and services to establish TLS communications between the SM Server and the LDAP Server. The RSA BSAFE Crypto-J Module v6.2 provides the cryptographic algorithms and services to establish TLS communications between the SM Server and other applications via the SOAP/REST APIs, as well as communications with the Solr server.

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

7.1.10 Service Level Management

An alert is a system event that occurs when the event meets predefined criteria. The alert serves as a checkpoint, warning, or reminder to keep an activity on schedule. Criteria for the generation of alerts and escalations can be created by a System Administrator, or a module administrator with sufficient rights. Alerts and escalations can also be triggered through evaluation of Service Levels as defined in the Service Level Management module. Users are notified of alerts and escalations via Active Note.

Service Level Management functions involve the analysis of Service Level Targets (SLTs) and the escalation and alerting of any potential availability violations for services managed by the TOE. The analysis is based on thresholds set for Service Level Targets (SLTs) for Service Level Agreements and internal Operational Level Agreements (OLAs). SLTs are defined for response, availability and escalations. Alerts are triggered as a function of time remaining until the SLT expires. Five out of box thresholds are configured to trigger alerts when a SLA deadline approaches a pre-defined threshold. Administrators can change the out of box settings or create new ones based on business rules.

TOE Security Functional Requirements Satisfied: EXT_SLM_AAE.1, EXT_SLM_STA.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 Revision 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 objectives to the threats they counter.

Table 19 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.AUDIT_COMPROMISE An attacker who is not a TOE user may breach confidentiality by viewing audit records. The attacker may modify or delete audit records, or prevent future records from being recorded, thus masking the actions of an attacker who is not a TOE user.	O.AUDIT The TOE must provide the capability to detect security relevant events and generate audit records of those events. The TOE will provide the capability for only authorized TOE users to access the audit information.	The O.AUDIT objective counters this threat by ensuring that the TOE will detect security relevant events and generate audit records of those events and protect the audit records from unauthorized access.
T.DATA_COMPROMISE An attacker who is not a TOE user may read, modify, delay, or destroy TOE configuration or user data stored on the TOE or being transmitted over the IT network.	O.FIPS The TOE must implement FIPS 140-2 validated cryptographic modules and approved algorithms for the TOE to perform cryptographic functions.	The O.FIPS objective counters this threat by providing FIPS validated cryptography for the protection of TOE data.
	O.PROTECT The TOE must ensure the integrity of user, audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	The O.PROTECT objective counters this threat by providing mechanisms to protect the TOE data from unauthorized modifications and access to its functions and data.
	OE.SECURE_COMM The TOE environment must support or provide secure communications between the TOE and external users or servers to protect the confidentiality and integrity of TSF and User data. FIPS 140-2 approved cryptographic algorithms and services must be used to provide the TLSv1.2 communications where possible. All external servers should be	The OE.SECURE_COMM objective counters this threat by ensuring the integrity and confidentiality of transmitted data.

Threats	Objectives	Rationale
	configured to provide secure communication when communicating with the TOE. Where possible, a VPN should be used to protect access to the TOE over untrusted networks.	
T.DATA_UNAVAILABLE TOE or IT Environment data or capabilities may become unavailable due to server failure.	O.ALERT The TOE must alert appropriate users when a service level security policy violation occurs.	The O.ALERT objective counters this threat by alerting authorized users of conditions that if unresolved, would result in a loss of availability. The alert facilitates the proactive resolution of issues that would, if not recognized and resolved, result in a loss of availability.
	O.AVAILABILITY The TOE shall preserve the availability of IT functions and data.	The O.AVAILABILTY objective counters this threat by identifying conditions that threaten availability and generating security violation events.
	O.FAIL_SECURE The TOE must preserve a secure state and SM Server capabilities in the event of a server failure.	The O.FAIL_SECURE objective counters this threat by ensuring that the TOE preserves a secure state and maintains all TOE capabilities in the event of a SM Server failure.
	O.PROTECT The TOE must ensure the integrity of user, audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	The O.PROTECT objective counters this threat by providing mechanisms to protect the TOE against unauthorized modifications and access to its functions and data which could result in a loss of availability.
T. MASQUERADE An attacker or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.AUTHENTICATE The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.	The O.AUTHENTICATE objective counters this threat by ensuring that a user is successfully identified and authenticated before allowing any other TOE-mediated actions.
T.UNAUTHORIZED A TOE user may gain unauthorized user access to user data, or to TOE security functions and data.	O.ACCESS The TOE must enforce an access control policy in order to prevent unauthorized users from gaining access to it and the resources that it controls.	The O.ACCESS objective builds on the O.AUTHENTICATE objective and counters this threat by ensuring that the authenticated user's access is restricted to only the functions and data for which the user is authorized.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	The O.ADMIN objective counters this threat by providing administrators TOE security management tools for the configuration of user roles, security groups, kmprofiles, and folder assignments, in order to restrict access to only those users with the appropriate privileges.
	O.AUDIT The TOE must provide the capability to detect security relevant events and generate audit records of those events. The TOE will provide the capability for only authorized TOE users to access the audit information.	The O.AUDIT objective counters this threat by recording all unauthorized and failed access attempts.
	O.AUTHENTICATE	The O.AUTHENTICATE objective counters this threat by ensuring that a user is successfully

Threats	Objectives	Rationale
	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.	identified and authenticated before allowing any other TOE-mediated actions.
	O.SESSION The TOE must terminate a user session after an administrator-configured period of inactivity.	The O.SESSION objective counters this threat by terminating an inactive user session, preventing an attacker from hijacking the session.
	OE.AUTHENTICATOR The TOE environment will provide an authentication server for the identification and authentication of individuals and devices attempting to access the TOE.	The OE.AUTHENTICATOR objective counters this threat by ensuring that an authentication server in the TOE environment will provide identification and authorization of users attempting to access the TOE.
T. TAMPERING A TOE user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	The O.ADMIN objective counters this threat by ensuring that only authorized users may configure the TOE security mechanisms.
	O.AUDIT The TOE must provide the capability to detect security relevant events and generate audit records of those events. The TOE will provide the capability for only authorized TOE users to access the audit information.	The O.AUDIT objective counters this threat by ensuring that events that indicate attempts to tamper with the TOE are recorded.
	O.PROTECT The TOE must ensure the integrity of user, audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	The O.PROTECT objective counters this threat by providing mechanisms to protect the TOE data from unauthorized modifications.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference and tampering.	The OE.PROTECT objective ensures that the TOE is protected from external interference or tampering.
	OE.EXTERNAL_SERVERS The LDAP and RDBMS server used by the TOE should be secured appropriately using best practices to ensure that TOE user accounts and TOE data is appropriately protected. TOE service accounts are used only for the purpose of facilitating communication with these servers and their privileges should be limited only to the functions necessary for TOE operation.	The OE.EXTERNAL_SERVERS objective ensures that the external authentication and database servers used by the TOE are secured appropriately such that TOE accounts and data are protected.

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

8.2.2 Security Objectives Rationale Relating to Policies

There are no security objectives relating to policies.

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.AUTHENTICATE The TOE environment will provide an authentication server for the identification and authentication of users and devices attempting to access the TOE. The authentication server will support Windows domain and certificate authentication.	OE.AUTHENTICATOR The TOE environment will provide an authentication server for the identification and authentication of individuals and devices attempting to access the TOE.	The OE.AUTHENTICATOR objective supports this assumption by requiring the implementation of an authentication server in the TOE environment.
A.INSTALL The TOE, and supporting third party applications, will be installed on the appropriate dedicated operating system.	OE.PLATFORM The TOE hardware and operating system must support all required TOE functions.	The OE_PLATFORM objective supports this assumption by ensuring that the hardware, operating system, and third party applications, support the TOE functions.
A.LOCATE The TOE will be located within a controlled access facility and appropriately located within a secure internal network to perform its functions.	NOE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	The OE.PHYSICAL objective supports the assumption that the TOE environment provides physical security for the TOE and the data it contains.
	OE.NET_CON The TOE environment must be implemented such that the TOE is appropriately located within and connected to the network to perform its intended function.	The OE.NET_CON objective supports this assumption by ensuring that the TOE is appropriately located with and connected to the network to perform its intended function.
A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. Administrators of the TOE are assumed to be appropriately trained to undertake the configuration and management of the TOE in a secure and trusted manner.	NOE.MANAGE Sites deploying the TOE must provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system and its environment are used securely.	The OE.MANAGE objective supports this assumption by ensuring that competent administrators are trained and assigned to manage the TOE and the TSF.
A.NOEVIL The authorized administrators who manage the TOE and database administrators who manage the TOE environmental components will be non-hostile, appropriately trained, and follow all guidance.	NOE.MANAGE Sites deploying the TOE must provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system and its environment are used securely.	The OE.MANAGE objective supports this assumption by ensuring that competent and non-hostile, administrators will follow guidance provided for the TOE.

Assumptions	Objectives	Rationale
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference and tampering.	The OE.PROTECT objective satisfies this assumption by ensuring that the TOE environment provides protection from unauthorized modification.
	OE.EXTERNAL_SERVERS The LDAP and RDBMS server used by the TOE should be secured appropriately using best practices to ensure that TOE user accounts and TOE data is appropriately protected. TOE service accounts are used only for the purpose of facilitating communication with these servers and their privileges should be limited only to the functions necessary for TOE operation.	The OE.EXTERNAL_SERVERS objective satisfies this assumption by ensuring that the external servers used by the TOE are secured from unauthorized access, modification, or tampering.
A.TIMESTAMP The IT environment will provide the TOE with reliable timestamps.	OE.TIMESTAMP The TOE environment must provide reliable timestamps to the TOE.	The OE.TIMESTAMP objective supports this assumption by ensuring that the OS provides reliable timestamps to the TOE.
A.FIPS Cryptographic functionality will be provided by FIPS 140-2 validated crypto modules. Only FIPS 140-2 approved cryptographic algorithms and services will be used and the TOE will be configured to operate in "FIPS-mode" only.	OE.SECURE_COMM The TOE environment must support or provide TLSv1.2 communications between the TOE and external users or servers to protect the confidentiality and integrity of TSF and User data. FIPS 140-2 approved cryptographic algorithms and services must be used to provide the TLSv1.2 communications where possible. All external servers should be configured to use TLS when communicating with the TOE. Where possible, a VPN should be used to protect access to the TOE over untrusted networks.	The OE.SECURE_COMM objective supports this assumption by providing the required FIPS 140-2 validated crypto modules.
A.PASSWORDS All account names, passwords or public key certificates used by external applications to communicate with the TOE via its APIs will be appropriately safeguarded and not shared with any user.	NOE.MANAGE Sites deploying the TOE must provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system and its environment are used securely.	The NOE.MANAGE objective ensures that TOE administrators will take the necessary precautions to safeguard credentials used to access the TOE by external applications.

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

8.3 Rationale for Extended Security Functional Requirements

A class of EXT_SLM requirements was created to specifically address the monitoring and alerting of Service Level Agreement violations that would adversely affect the availability of IT functionality and data. The audit class of the CC (FAU) was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of monitoring, identifying, and alerting potential and actual Service Level Agreement violations which could impact the availability of IT functions and data. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no Extended TOE Security Assurance Requirements.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 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 TOE must enforce an access control policy in order to prevent unauthorized users from gaining access to it and the resources that it controls.	FIA_AFL.1 Authentication failure handling	The requirement supports the O.ACCESS objective by ensuring that a TOE user account is disabled after failed authentication attempts.
	FDP_ACC.1 Subset access control	The requirement supports the O.ACCESS objective by specifying the SM Access Control SFP rules on all subject and objects and all operations between them.
	FDP_ACF.1 Security attribute based control	The requirement supports the O.ACCESS objective by specifying the SM Access Control SFP rules that will be enforced by the TSF and determines if an operation between subjects and objects is allowed. Furthermore, it specifies the rules to explicitly authorize or deny access to a named object based on security attributes.
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 the O.ADMIN objective by restricting the ability to manage security attributes for the TOE to authorized roles with sufficient permissions.
	FMT_MSA.3 Static attribute initialization	The requirement meets the O.ADMIN objective by ensuring that the TOE provides restrictive default values for security attributes and specifies alternative initial values to override the default values when an object or information is created.
	FMT_SMF.1 Specification of management functions	The requirement meets the O.ADMIN objective by ensuring that the TOE includes

Objective	Requirements Addressing the Objective	Rationale
		administrative functions to facilitate the management of the TOE.
	FMT_SMR.1 Security roles	The requirement meets the O.ADMIN objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
O.ALERT The TOE must alert appropriate users when a service level security policy violation occurs.	EXT_SLM_AAE.1 Alert and Escalation	The requirement meets the O.ALERT objective through the generation of alerts, escalations, and notifications.
	EXT_SLM_STA.1 Service Target Analysis	The requirement supports the O.ALERT objective by providing the capability to analyze SLTs and record criteria for alert generation and escalation.
O.AUDIT The TOE must provide the capability to detect security relevant events and generate audit records of those events. The TOE will provide the capability for only authorized TOE users to access the audit information.	FAU_GEN.1 Audit data generation	The requirement supports the O.AUDIT objective by ensuring that the TOE maintains a record of security related events.
	FAU_GEN.2 User identity association	The requirement supports the O.AUDIT objective by associating the TOE user identity and action for each incident history record created.
	FAU_SAR.1 Audit Review	The requirement supports the O.ALERT objective by ensuring that the TOE provides the capability to review logs.
O.AUTHENTICATE The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.	FIA_ATD.1 User attribute definition	This requirement supports the O.AUTHENTICATE objective by requiring the TOE to store data related to login and role assignment.
	FIA_UAU.2 User authentication before any action	This requirement supports O.AUTHENTICATE by requiring the TOE to authenticate users and administrators prior to granting access to any TOE functionality.
	FIA_UAU.5 Multiple authentication mechanisms	The requirement supports the O.AUTHENTICATE objective by providing multiple authentication mechanisms to support TOE user or administrator authentication.
	FIA_UID.2 User identification before any action	The requirement supports the O.AUTHENTICATE objective by ensuring that a user is successfully identified before allowing any other TOE-mediated actions.
O.AVAILABILITY The TOE shall preserve the availability of IT functions and data.	EXT_SLM_AAE.1 Alert and Escalation	This requirement supports the O.AVAILABILITY objective by generating alerts, escalating incidents, and notifying specified individuals of security violations that could result in a loss of IT availability.
	EXT_SLM_STA.1 Service Target Analysis	This requirement supports the O.AVAILABILITY objective through rule-based analysis which generates security violation events for

Objective	Requirements Addressing the Objective	Rationale
		conditions that could lead to the loss of availability of IT functions.
O.FAIL_SECURE The TOE must preserve a secure state and SM Server capabilities in the event of a server failure.	FPT_FLS.1 Failure with preservation of secure state	The requirement supports the O.FAIL_SECURE objective by ensuring that in the event of an SM Server instance failure, another SM Server instance will ensure that the TOE maintains a secure state.
O.FIPS The TOE must implement FIPS 140-2 validated cryptographic modules and approved algorithms for the TOE to perform cryptographic functions. The cryptographic functions are available to authorized TOE users, administrators, and TOE applications.	FCS_COP.1 Cryptographic operation	The TOE supports the O.FIPS objective by ensuring that the TOE provides confidentiality and integrity services for the TOE by providing FIPS 140-2 validated algorithms.
O.PROTECT The TOE must ensure the integrity of user, audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	FCS_COP.1 Cryptographic operation	The requirement meets the O.PROTECT objective by ensuring that the TOE uses recommended standards for all cryptographic functionality implemented to secure communications with trusted remote IT systems.
	FPT_ITT.1 Basic internal TSF data transfer protection	The requirement meets the O.PROTECT objective by providing FIPS 140-2 cryptographic operations to ensure that TSF data is protected from disclosure or modification when transmitted between separate parts of the TOE.
	FTP_ITC.1(a) Inter-TSF trusted channel (TSF)	The requirement meets the O.PROTECT objective by protecting TSF data from modification and disclosure while it is transmitted between TOE and other trusted IT entities.
	FTP_ITC.1(b) (Trusted IT product)	The requirement meets the O.PROTECT objective by protecting TSF data from modification and disclosure while it is transmitted between TOE and other trusted IT entities.
O.SESSION The TOE must terminate a user session after an administrator-configured period of inactivity.	FTA_SSL.3 TSF-initiated termination	The requirement satisfies the O.SESSION objective by ensuring that a TOE user session is terminated after a period of TOE user inactivity.

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.1	FPT_STM.1		Timestamps for the TOE are provided by the OE_TIMESTAMP objective. This dependency is met.
FAU_GEN.2	FAU_GEN.1	✓	FAU_GEN.1 is claimed and meets this dependency.
	FIA_UID.1	✓	FIA_UID.2, which is hierarchical to FIA_UID.1, is claimed and meets this dependency.
FAU_SAR.1	FAU_GEN.1	✓	FAU_GEN.1 is claimed and meets this dependency.
FIA_AFL.1	FIA_UAU.1	✓	FIA_UAU.2, which is hierarchical to FIA_UAU.1, is claimed and meets this dependency.
FIA_ATD.1	No dependencies	N/A	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is included and is hierarchical to FIA_UID.1.
FIA_UAU.5	No dependencies	N/A	
FIA_UID.2	No dependencies	N/A	
FCS_COP.1	FCS_CKM.1	N/A	Not required per CCCS[23] Instruction #4.
	FCS_CKM.4	N/A	Not required per CCCS Instruction #4.
FDP_ACC.1	FDP_ACF.1	✓	FDP_ACF.1 is claimed and meets this dependency.
FDP_ACF.1	FMT_MSA.3	✓	FMT_MSA.3 is claimed and meets this dependency.
	FDP_ACC.1	✓	FDP_ACC.1 is claimed and meets this dependency.
FMT_MSA.1	FDP_SMF.1	✓	FMT_SMF.1 is claimed and meets this dependency.
	FDP_ACC.1	✓	FDP_ACC.1 is claimed and meets this dependency.
	FMT_SMR.1	✓	FMT_SMR.1 is claimed and meets this dependency.
FMT_MSA.3	FMT_SMR.1	✓	FMT_SMR.1 is claimed and meets this dependency.
	FMT_MSA.1	✓	FMT_MSA.1 is claimed and meets this dependency.

[23] CCCS – Canadian Common Criteria Scheme

FMT_SMF.1	No dependencies	N/A	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is claimed and meets this dependency.
FPT_FLS.1	No dependencies	N/A	
FPT_ITT.1	No dependencies	N/A	
FRU_FLT.1	FPT_FLS.1	✓	FPT_FLS.1 is claimed and meets this dependency.
FTA_SSL.3	No dependencies	N/A	
FTP_ITC.1(a)	No dependencies	N/A	
FTP_ITC.1(b)	No dependencies	N/A	
EXT_SLM_AAE.1	No dependencies	N/A	
EXT_SLM_STA.1	No dependencies	N/A	

9. Acronyms

Table 23 defines the acronyms used throughout this document.

Table 23 – Acronyms

Acronym	Definition
AD	Active Directory
AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher Block Chaining
CC	Common Criteria
CCM	Counter with CBC- MAC
CCS	Common Criteria Scheme
CI	Configuration Item
CLI	Command Line Interface
CTR	Counter Mode
DB	Database
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
ESS	Employee Self Service
FIPS	Federal Information Processing Standards
GA	General Availability
GB	Gigabyte
GCM	Galois Counter Mode
GUI	Graphical User Interface
HA	High Availability
HMAC	Hash Message Authentication Code
HP	Hewlett Packard Enterprise Development LP
HTML	Hypertext Markup Language
HTTPS	Hypertext Transfer Protocol Secure
IDOL	Intelligent Data Operating Layer
IIS	Internet Information Services
ISO	International Standards Organization
IT	Information Technology
ITIL	Information Technology Infrastructure Library

ITSM	Information Technology Security Management
JRE	Java Runtime Environment
KM	Knowledge Management
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
OS	Operating System
OSP	Organizational Security Policy
OWASP	Open Web Application Security Project
PID	Process Identification
PP	Protection Profile
RAM	Random-Access Memory
RHEL	Red Hat Enterprise Linux
RSA	Rivest, Shamir, Adelman
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
SM	Service Manager
SP	Special Publication
SPARC	Scalable Processor Architecture
SQL	Structured Query Language
SRC	Service Request Catalog
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
UI	User Interface
WAR	Web Application Archive

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