# Hewlett Packard Enterprise Development LP

SiteScope v11.30

## Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1

Prepared for:

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

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

Prepared by:

**Corsec Security, Inc.**

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

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

# Table of Contents

# Table of Figures



# List of Tables

# 1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the HP SiteScope v11.30, and will hereafter be referred to as the TOE throughout this document. The TOE is a software-only, agentless application monitoring solution designed to ensure the availability and optimal performance of a distributed IT infrastructure.

## 1.1 Purpose

This ST is divided into nine sections, as follows:

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

## 1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

**Table 1 ST and TOE References**

| | |
|---|---|
| **ST Title** | Hewlett Packard Enterprise Development LP SiteScope v11.30 Security Target |
| **ST Version** | Version 1 |
| **ST Author** | Corsec Security, Inc. |
| **ST Publication Date** | 8/7/2015 |
| **TOE Reference** | HP SiteScope v11.30 [Build# 521] |
| **FIPS 140-2 Status** | Level 1, RSA[1] BSAFE Crypto-J JSAFE and JCE[2] Software Module, Software Version 6.1, Certificate No. 2057 |

[1] RSA – Ron Rivest, Adi Shamir, and Leonard Adleman
[2] JCE – Java Cryptography Extension

# 1.3 Product Overview

HP SiteScope is an industry-leading software solution for agentless monitoring. It is easy to install, configure, and use, which provides quick time to value for SiteScope users. SiteScope is designed to ensure the availability and optimal performance of distributed IT infrastructure (physical, virtual and cloud), including servers, operating systems, network devices and services, virtualization software, and applications. SiteScope continuously monitors over 100 different types of IT components through a web-based architecture that is lightweight, highly customizable, and does not require the installation of agent software on production systems. SiteScope empowers its users to automate application monitoring for today's dynamic cloud environments via APIs, Operation Orchestration flows, and HP Cloud Service Automation.

Remote applications and infrastructures are monitored by SiteScope using "Monitors" in accordance with several industry standard and monitored application proprietary protocols, including rlogin, SSH[3], WMI[4], HTTPS[5], TLS[6] and NetBIOS. SiteScope Monitors are responsible for collecting key performance metrics and providing reports on various infrastructure components. Monitors can be individually configured to automatically test performance and availability of systems and services in the network environment.

Monitor types include:

- Application Monitors – Used for monitoring third-party applications. Examples include: Apache, Broadvision, CheckPoint, Cisco Works, ColdFusion, Microsoft (Exchange/IIS[7]/ASP[8].NET), F5, WebSphere, Oracle, SAP[9], WebLogic, WebSphere, and several others.

- Database Monitors – Used to monitor database applications, including IBM[10] DB2, Oracle DB[11], Microsoft SQL[12] Server, and Sybase.

- Generic Monitors – Generic monitors include XML[13], Directory, File, Log File, JMX[14], Web Service, Custom WMI[15], Custom DB, Custom Java, etc.

- Integration Monitors – Used to capture and forward data from 3rd party management systems to HP BSM[16].

- Media Monitors – Used to monitor applications which stream media files, for example Microsoft Windows Media, Real Media, Microsoft Lync, etc.

- Network Monitors – Used to monitor network health and availability by monitoring networking protocols and network activities such as SNMP, DNS[17], FTP[18], Port, Ping, Mail, Bandwidth, Dialup, etc.

[3] SSH – Secure Shell
[4] WML – Wireless Markup Language
[5] HTTPS – Hypertext Transfer Protocol Secure
[6] TLS – Transport Layer Security
[7] IIS – Internet Information Services
[8] ASP – Active Server Pages
[9] SAP – Systems, Applications and Products in Data Processing
[10] IBM – International Business Machines
[11] DB – Database
[12] SQL – Structured Query Language
[13] XML – eXtensible Markup Language
[14] JMX – Java Management Extensions
[15] WMI – Windows Management Instrumentation
[16] BSM – Business Service Management
[17] DNS – Domain Name System
[18] FTP – File Transfer Protocol

- Server Monitors – A combination of Monitors including CPU[19], Disk, Memory, Microsoft Windows Performance Counter, Service, UNIX Resources, and Web Server Monitors.

- Web Transaction Monitors – Used to monitor web-based application such as WebScript, Link Check, URL[20], URL Content, URL List, URL Sequence, etc.

- Virtualization and Cloud Monitors – Used to monitor virtualized environments and cloud infrastructure. Examples include Vmware, Solaris Zones, Microsoft Hyper-V, Amazon Web Service, KVM, Citrix, etc.

Monitors collect performance and availability information about the monitored systems by checking the status of server components, critical application processes, log files, network devices, etc. They also collect data based on selected metrics and returns a status of "Good", "Warning", or "Error" with respect to the configured threshold. Monitors may be organized according to Groups, which are containers for monitoring assets. Groups may also contain sub-groups.

In addition to the monitoring feature, SiteScope also provides alerting and reporting capabilities, along with a real-time at-a-glance snapshot of all the monitored assets via dashboards. Whenever a problem occurs within the monitored IT infrastructure and applications, SiteScope can be configured to automatically send an alert to an administrator. Trending and analytical reports may also be generated periodically to analyze the performance and availability of the monitored assets over time.

To help deploy Monitors with similar monitoring configuration criteria across the enterprise, SiteScope provides a simple, out-of-the-box deployment using pre-defined solution templates, all of which are customizable to fit the needs of an organization. SiteScope also provides alert templates that can be used to communicate and record event information in a variety of media.

SiteScope provides SOAP[21]-based Web Services (WS) Client APIs[22] that can be used to gather the information on the TOE without needing to go through the predefined interfaces. These APIs are provided to help in large dynamic environments to simplify working with SiteScope templates, groups, monitors, alerts, remote servers, server health, search and filter tags, and configuration.

# 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, TOE environment, and TOE minimum requirements, and providing a deployment configuration.

The TOE is a software-only, agentless application monitoring solution designed to ensure the availability and optimal performance of a distributed IT infrastructure. Monitors are individually configured to automatically test performance and availability of systems and services in the network environment. Monitoring of the environment is performed through the collection and review of events captured as audit and data logs. Audit and data logs contain the date/time of the event, type of event, subject identity (if applicable), and the event outcome (success or failure). These events are viewable and can be sorted by log type, log file name, log size, and modification date. Alerts can be set to notify an Administrator of a security violation. When a security violation occurs, one or more alert actions are initiated.

[19] CPU – Central Processing Unit
[20] URL – Uniform Resource Locator
[21] SOAP – Simple Object Access Protocol
[22] API – Application Programming Interface

User identification and authentication is required before TOE functionality is available. User crednetials can be stored in a local database or in an external LDAP[23] server. Users can be authenticated through username/password or through PKI[24]with an X.509 certificate. All password information is obscured throughout the login process

The TOE includes all of the functionality and features described in section 1.3 above and section 1.5 below, except for the features and functionality listed below in section 1.5.3.

Table 2 and Table 3 identify any major non-TOE hardware and software that is required by the TOE including the TOE minimum requirements. Table 4 lists the 3rd party software requirements for the client workstation in the TOE environment. For additional information on system requirements refer to the HP SiteScope Deployment Guide. The TOE can be managed locally or remotely over the network from a client workstation via SiteScope UI[25] over HTTPS or using the SiteScope WS Client APIs over SSL[26] v3.1 (TLS v1.0, 1.1, 1.2). Figure 1 shows a typical deployment configuration of the TOE.

The failover functionality provided by the TOE is not part of the tested claims and is not included in this evaluation.

Following acronyms are present in the Figure 1 below that have not been mentioned earlier:

- NA – Network Automation
- CSA – Cloud Service Automation
- SA – Server Automation
- OO – Operations Orchestration
- SMTP – Simple Mail Transfer Protocol
- SNMP – Simple Network Management Protocol
- JVM – Java Virtual Machine

[23] LDAP – Lightweight Directory Access Protocol
[24] PKI – Public Key Infrastructure
[25] UI – User Interface
[26] SSL – Secure Socket Layer

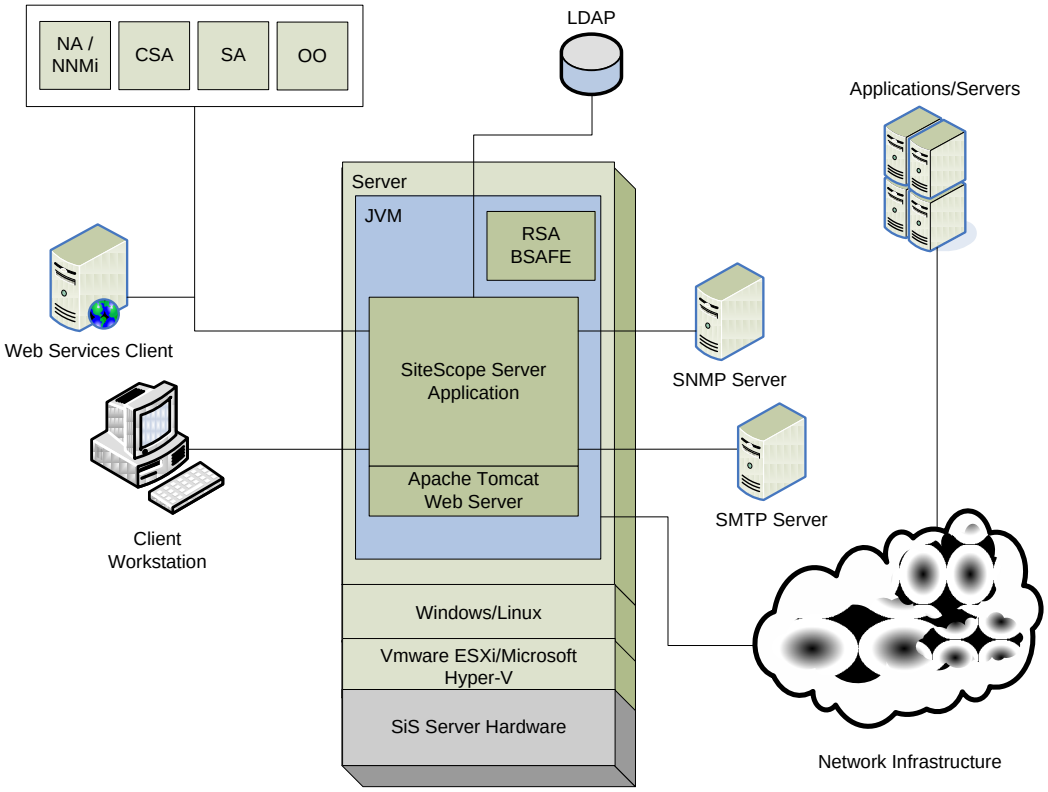


**Figure 1 Typical Deployment Configuration of the TOE**

## 1.4.1 TOE Environment

The TOE is installed on a server system running a Windows Operating System (OS). The OS is installed directly above the SiteScope Server Hardware. In the evaluated configuration, the Windows Server 2008 R2 SP1 Enterprise Edition 64-bit OS is running directly on the SiteScope Server Hardware (see section 1.5.1). The TOE relies on the underlying OS in the TOE environment on which the TOE is installed for providing reliable timestamps to the TOE. The TOE requires JRE version 7 to be present in the TOE environment on the SiteScope server to provide the JVM on which the TOE will execute.

The TOE is configured to use an external LDAP authentication service. When configured and enabled, as required for the evaluated configuration, the TOE environment requires an external LDAP server, which stores authentication information such as usernames, and passwords. The TOE supports multiple authentication methods, including username/password and PKI using X.509 certificates. The TOE relies on the client workstation for the PKI certificate extraction and verification.

Table 2 specifies the minimum server system hardware requirements for the proper operation of the TOE. For additional information on system requirements refer to the HP SiteScope Deployment Guide.

**Table 2 Server System Minimum Hardware Requirements**

| Name | Description |
|---|---|
| Computer/Processor | 1 core / 2000 MHz[27] minimum |
| Memory | 2 GB[28] minimum |

[27] MHz – Mega-Hertz
[28] GB – GigaByte

| Name | Description |
|---|---|
| | 8 GB to 16 GB is common for a highly loaded environment |
| Free Hard Disk Space | 10 GB |
| Network Card | 1 physical gigabit Network Interface Card minimum |

Table 3 specifies the list of software required for the TOE to operate. In the evaluated configuration, the TOE was tested with Microsoft Windows Server 2008 SP1 64-bit. For additional information on system requirements refer to the HP SiteScope Deployment Guide.

**Table 3 Server System Tested Operating Systems**

| OS Name | Version |
|---|---|
| Windows OS Variants | Microsoft Windows Server 2008 R2 SP1 Standard/Enterprise/Datacenter Edition (64-bit) |

Table 4 lists the 3rd party software requirements for the client workstation in the TOE environment. For additional information on system requirements refer to the HP SiteScope Deployment Guide.

**Table 4 Client Workstation Software Requirements**

| OS Name | Version |
|---|---|
| Supported Browsers (SiteScope UI) | Microsoft Internet Explorer 7, 8, 9 |
| | Microsoft Internet Explorer 10 (Alert, Monitor, and Server-Centric Reports are supported in compatibility mode only) |
| | Mozilla Firefox 24.0 |
| Supported Browsers (Multi-View) | Chrome 15 or later (recommended) |
| | Firefox 10 or later (recommended) |
| | Safari 5.1 or later (recommended) |
| | Microsoft Internet Explorer 8, 9, 10 |
| Java Plug-in (required to open SiteScope UI) | Java SE Runtime Environment (JRE) 7 |

# 1.5 TOE Description

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

## 1.5.1 Physical Scope

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

The TOE is a software-only solution for the monitoring of servers, operating systems, network devices, and services that runs on Windows and Linux Operating Systems. Multiple versions of each supported OS are listed in Table 3 and the minimum server system hardware requirements are listed in Table 2.

In the evaluated configuration, the TOE is installed on a Microsoft Windows Server 2008 R2 SP2 OS running on a server meeting the minimum requirements as specified in Table 2. With the installation of the supported OS, the TOE must have access to the network that is intended to be monitored. An Apache Tomcat Web Server v7.0.50 is used to host and provide access to the TOE. RSA BSAFE v6.1 is used to provide cryptographic functions within the TOE.

The client workstation that is used to manage the TOE must meet the minimum requirements listed in the 'Client Workstation Requirements' section of Table 2. The client workstation must also have a network connection (intranet or Internet) to the SiteScope Server application. The red-colored dotted line shown in Figure 2 below depicts the TOE boundary.

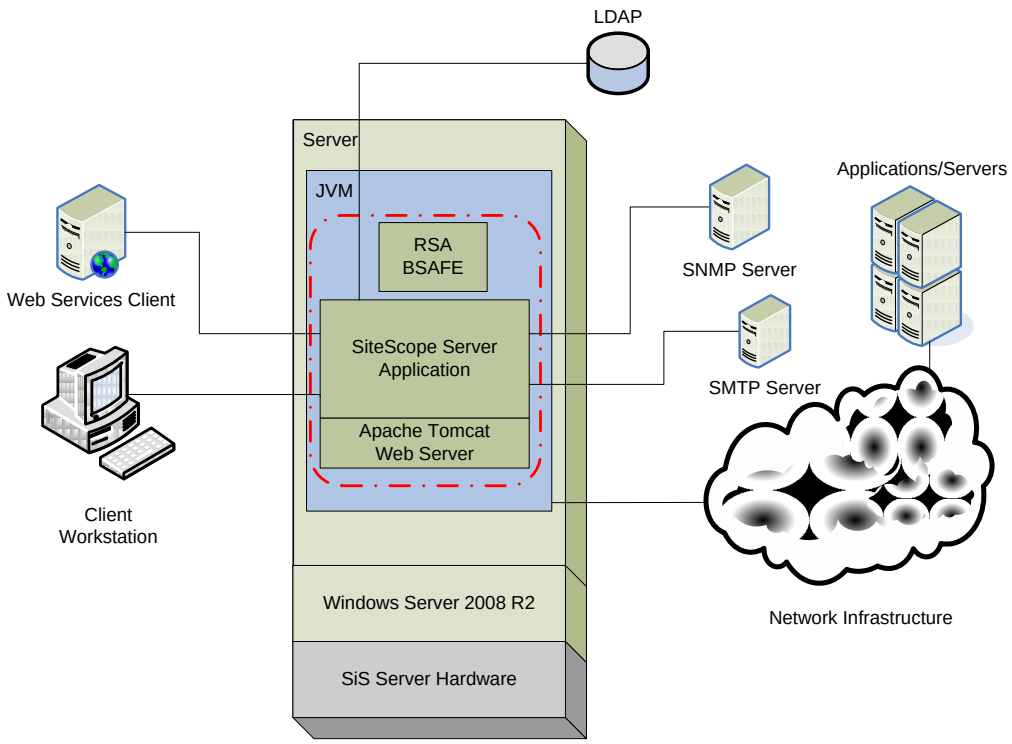


**Figure 2 Physical TOE Boundary**

#### 1.5.1.1 TOE Software

The TOE is a software-only solution for the monitoring of servers, operating systems, network devices, and services consisting of the components illustrated in Figure 2 and listed below:

- HP SiteScope (v11.30) software
- Apache Tomcat Web Server 7.0.50
- RSA BSAFE Crypto-J v6.1

#### 1.5.1.2 Guidance Documentation

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

- HP SiteScope – Deployment Guide, Release Date May, 2015
- HP SiteScope – Configuring the Integration with HP Diagnostics, Release Date March 2015
- HP SiteScope – Monitor Reference, Release Date June 2015
- HP SiteScope – Using SiteScope, Release Date May, 2015

## 1.5.2 Logical Scope

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

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Trusted Path/Channels

### 1.5.2.1 Security Audit

The TOE generates audit records for all auditable events, and the start-up and shutdown of the audit functions. A list of specific auditable events is provided in Table 12. Once an administrator configurable limit reaches maximum amount of records to store, the oldest log file will be overwritten.

The Administrator, or a TOE user that has been granted the "View log preferences" permissions, will be the only TOE users allowed to view audit logs. While viewing the log files, the user will be able to filter the audit logs based on type as well as sort the order of audit log files in ascending or descending manner. The TOE does not allow anyone to delete or modify audit records. These log files are presented in a suitable manner for easy interpretation. The Administrator, or a user that has been granted the "Alert" permissions, will be able to manage the audit triggers to help indicate a potential security violation. These triggers can be setup to send different alerts, when a violation is detected, depending on the configuration.

### 1.5.2.2 Cryptographic Support

The Cryptographic Support TSF provides cryptographic functions to secure sessions between client workstation to SiteScope, SiteScope to external IT product, and SiteScope to monitored assets (data-in-motion). TLS is used to secure these communications sessions. Other cryptographic functions provided by the TOE include encryption of persistent storage (data-at-rest). HP utilizes the FIPS 140-2 validated RSA BSAFE Crypto-J JSAFE and JCE Software Module, Software Version 6.1 library for all cryptographic implementations in the TOE.

### 1.5.2.3 User Data Protection

The TOE provides complete access control on all the Monitors within a group. The TOE enforces the Group Access Control SFP[29] on users accessing Monitors within a group. All operations among a TOE user and the Monitors within a group/s are covered by the Group access control policy. The TOE will not allow any access to any Monitors until the SiteScope user account is verified to have access assigned to a particular group. This ensures that all operations between any subject controlled by the TOE, and any object controlled by the TOE, are covered by the Group access control policy.

### 1.5.2.4 Identification and Authentication

All TOE users are required to successfully identify and authenticate with the TOE prior to any actions on the TOE. The user name, user type, allowed group, and password attributes are stored locally in the TOE and are maintained for each individual user. In the case when an external LDAP server is configured, all the user credentials are stored externally on the LDAP server. The TOE supports multiple authentication mechanisms: local password-based, external password-based authentication via LDAP, and PKI certificate-based authentication using public-private key pairs. When TOE users authenticate using the SiteScope UI, characters entered during password entry are replaced by dots to obscure the text.

[29] SFP – Security Function Policy

#### 1.5.2.5 Security Management

The TOE supports the roles of Administrator, Power User, Regular User, and Integration Viewer. The Administrator role may View or Change anything within the TOE. The Regular User role by default is only allowed to View groups, and its own user preferences. The Power User role has the same access as a Regular User plus access to manage user accounts. The Integration Viewer role has view-only permissions. The management of TSF data is broken down by role and what operations that can be performed for a given role. The TOE offers a User Management Preferences page where only privileged users may configure and manage user accounts.

The TOE provides complete access control on all the Monitors within a group. The TOE enforces Group access control SFP on a TOE user accessing Monitors within a group. All operations among a TOE user and the Monitors within the group/s are covered by the Group access control policy. Only Administrator and Power User have the ability to manage and specify alternate initial values for the security attributes of the SFP. The TSF enforces permissive default values for security attributes that enforce the SFPs.

#### 1.5.2.6 Protection of the TSF

The TOE protects exported TSF data to a configured external LDAP server from unauthorized disclosure during transmission using TLS. This keeps data from being disclosed or modified while it is being transmitted.

#### 1.5.2.7 Trusted Path/Channels

The TOE provides a communication path between itself and remote users. This path is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification and disclosure. The remote user will be allowed to initiate communication with the TOE over the HTTPS connection and will be required to only use this path for all remote actions taken within the TOE.

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

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

- Silent URL-based login
- Single sign-on through SiteMinder
- Integration with other HP products that are not monitored assets
- Failover functionality
- Monitored assets over all protocols except SSH/SFTP, LDAPS, SMTP over TLS, or HTTPS

# 2 Conformance Claims

This section and Table 5 provide the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

**Table 5 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 CEM[30] as of TBD 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) |

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

# 3 Security Problem

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

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

## 3.1 Threats to Security

This section identifies the threats to the IT[31] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

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

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[32] and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 6 below lists the applicable threats.

**Table 6 Threats**

| Name | Description |
|---|---|
| T.NOAUDIT | An attacker may perform security relevant operations on the TOE without being held accountable for them. |
| T.TRANSMIT | A user or process may be able to bypass the TOE's security mechanisms and gain access to the data while the data is in transit. |
| T.UNAUTH | An unauthorized person may gain access to the TOE and compromise its security functions by changing its configuration. |
| T.UNDETECT | A TOE resource may be compromised as a result of an authorized administrator of the TOE not having the ability to notice potential security violations. Therefore, limiting their ability to identify and take action against a possible security breach. |

[31] IT – Information Technology
[32] TSF – TOE Security Functionality

# 3.2 Organizational Security Policies

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

# 3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 7 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 7 Assumptions**

| Name | Description |
|---|---|
| A.ATTRIBUTES | The TOE environment will be able to maintain user security attributes when the TOE is configured to use external authentication. |
| A.INSTALL | The TOE is installed on the appropriate, dedicated hardware and operating system. |
| A.LOCATE | The TOE is located within a controlled access facility. |
| A.MANAGE | There are one or more competent individuals assigned to manage the TOE and the security of the information it contains. |
| A.NETCON | The TOE environment provides the network connectivity required to allow the TOE to perform its intended functions. |
| A.NOEVIL | The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance. |
| A.PROTECT | The TOE software will be protected from unauthorized modification. |
| A.TIMESTAMP | The TOE environment provides the TOE with the necessary reliable timestamps. |

# 4 Security Objectives

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

## 4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 8 below.

**Table 8 Security Objectives for the TOE**

| Name | Description |
|---|---|
| O.ADMIN | The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control. |
| O.ALERT | The TOE will provide the capability to monitor and send alerts upon the detection of a potential security violation based on the rules configured. |
| O.ATTRIBUTES | The TOE will be capable of maintaining user security attributes. |
| O.AUDIT | The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification and loss of the audit trail, and provide the authorized administrators with the ability to review and sort the audit trail. |
| O.AUTHENTICATE | The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data. |
| O.CRYPTO | The TOE must provide the means of protecting cryptographic operations and secure management of cryptographic keys using cryptography that conforms to standards specified in FIPS PUB 140-2. |
| O.SECURE | The TOE shall securely transfer data with other trusted IT entities and remote users. |

## 4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

### 4.2.1 IT Security Objectives

Table 9 below lists the IT security objectives that are to be satisfied by the environment.

**Table 9 IT Security Objectives**

| Name | Description |
|---|---|
| OE.ATTRIBUTES | The IT environment must be able to maintain user security attributes when the TOE is configured to use external authentication. |
| OE.MONITOR | The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function. |
| OE.PLATFORM | The TOE hardware and OS must support all required TOE functions. |
| OE.SECURE_COMM | The TOE Environment must provide a mechanism to provide a secure and authorized user access to the TOE environment for protecting the TOE and TOE data from modification. |
| OE.TIME | The underlying Operating System must provide reliable timestamps to the TOE. |

### 4.2.2 Non-IT Security Objectives

Table 10 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 10 Non-IT Security Objectives**

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

# 5 Extended Components

There are no extended SFRs and extended SARs for this TOE.

# 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_ARP.1 | Security alarms | | ✓ | | |
| FAU_GEN.1 (a) | Audit data generation – Audit Logs | ✓ | ✓ | | ✓ |
| FAU_GEN.1 (b) | Audit data generation – Data logs | ✓ | ✓ | | ✓ |
| FAU_GEN.2 | User identity association | | | | |
| FAU_SAA.1 | Potential violation analysis | | ✓ | | |
| FAU_SAR.1 | Audit review | | ✓ | | |
| FAU_SAR.3 | Selectable audit review | | ✓ | | |
| FAU_STG.1 | Protected audit trail storage | ✓ | | | |
| FAU_STG.4 | Prevention of audit data loss | | ✓ | ✓ | |
| FCS_CKM.1 | Cryptographic key generation | | ✓ | | |
| FCS_CKM.4 | Cryptographic key destruction | | ✓ | | |
| FCS_COP.1 | Cryptographic operation | | ✓ | | |
| FDP_ACC.2 | Complete access control | | ✓ | | |

| Name | Description | S | A | R | I |
|---|---|---|---|---|---|
| FDP_ACF.1 | Security attribute based access control | | ✓ | | |
| FIA_ATD.1 | User attribute definition | | ✓ | | |
| FIA_UAU.2 | User authentication before any action | | | | |
| FIA_UAU.5 | Multiple authentication mechanisms | | ✓ | | |
| FIA_UAU.7 | Protected authentication feedback | | ✓ | | |
| FIA_UID.2 | User identification before any action | | | | |
| FMT_MOF.1 | Management of security functions behavior | ✓ | ✓ | | |
| FMT_MSA.1 | Management of security attributes | ✓ | ✓ | | |
| FMT_MSA.3 | Static attribute initialization | ✓ | ✓ | | |
| FMT_MTD.1 | Management of TSF data | ✓ | ✓ | | |
| FMT_SMF.1 | Specification of management functions | | ✓ | | |
| FMT_SMR.1 | Security roles | | ✓ | | |
| FPT_ITC.1 | Inter-TSF confidentiality during transmission | | | | |
| FTP_TRP.1 | Trusted path | ✓ | ✓ | | |

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

## 6.2.1 Class FAU: Security Audit

**FAU_ARP.1 Security alarms**
**Hierarchical to: No other components.**
**Dependencies: FAU_SAA.1 Potential violation analysis**
***FAU_ARP.1.1***

The TSF shall take [*one or more of the following alerting actions to notify the administrator*

- *Disable or Enable Monitor alerts*
- *Email alerts*
- *Event console alerts*
- *Log Event alerts*
- *Post alerts*
- *Script alerts*
- *SNMP Trap alerts*
- *Sound alerts*

upon detection of a potential security violation.

**FAU_GEN.1 (a) Audit Data Generation – Audit Logs**
**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) [*other specifically defined auditable events – see Table 12 below* ].

***FAU_GEN.1.2***

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

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

**Table 12 Auditable Events**

| Event Type | Auditable Event |
|---|---|
| Authentication | Login<br>Logout |
| Certificate Management | Create<br>Delete |
| Downtime | Add<br>Delete<br>Update |
| Email/SNMP/Common Events Mapping (instance)<br>Schedule Preferences<br>User Management<br>Preferences<br>Credential Preferences<br>Search/Filter Tags | Create<br>Delete<br>Update |
| External files | Import |

| Event Type | Auditable Event |
|---|---|
| General Preferences<br>Infrastructure Preferences<br>Log Preferences<br>Email/SNMP/Common Events Mapping (default) | Update |
| Health Logging | Enable<br>Disable |
| Licensing | Import<br>Remove |
| Alert | Copy/Cut/Paste<br>Create<br>Delete<br>Enable/Disable<br>Global Search and Replace<br>Update |
| Alert Action | Copy<br>Create<br>Delete<br>Global Search and Replace<br>Update |
| Group | Copy to template<br>Copy/Cut/Paste<br>Create<br>Delete<br>Global Search and Replace<br>Manual run of all child monitors<br>Update |
| Health Logging | Enable<br>Disable |
| Licensing | Import<br>Remove |
| Monitor | Copy/Copy to Template<br>Create<br>Delete<br>Enable/Disable<br>Global Search and Replace<br>Manual run<br>Move (Cut/Paste)<br>Update |
| Monitor Acknowledgment | Add<br>Delete<br>Edit |
| Remote Server | Copy/Cut/Paste<br>Create<br>Delete<br>Update |
| Report Monitor | Copy |

| Event Type | Auditable Event |
|---|---|
| | Create<br>Delete<br>Global Search and Replace<br>Update |
| Template | Copy/Cut/Paste<br>Create<br>Delete<br>Deploy<br>Import<br>Publish changes<br>Update contained entities |
| Template Container<br>Template Variable Template | Copy/Cut/Paste<br>Create<br>Delete<br>Update |

**FAU_GEN.1 (b) Audit Data Generation – Data Log Files**
**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:

d) Start-up and shutdown of the audit functions;
e) All auditable events, for the [not specified] level of audit; and
f) [*Monitor statistics and SiteScope server health and statistics*].

***FAU_GEN.1.2***

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

c) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
d) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*Category, stateString, and ID Sample number*].

**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_SAA.1 Potential violation analysis**
**Hierarchical to: No other components.**
**Dependencies: FAU_GEN.1 Audit data generation**
***FAU_SAA.1.1***

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

***FAU_SAA.1.2.***

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

a) Accumulation or combination of [*administrator configured alert trigger conditions*] known to indicate a potential security violation;

b) [*none*].

**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 [*administrator and other users that are explicitly given "view log preferences" permissions by administrator*] with the capability to read [*all of audit information*] 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.

**FAU_SAR.3 Selectable audit review**
**Hierarchical to: No other components.**
**Dependencies: FAU_SAR.1 Audit review**
***FAU_SAR.3.1***
The TSF shall provide the ability to apply [*filtering and sorting*] of audit data based on [
- *Log type*
- *Log file name*
- *Log size*
- *Modification date*[33]]

**FAU_STG.1 Protected audit trail storage**
**Hierarchical to: No other components.**
**Dependencies: FAU_GEN.1 Audit data generation**
***FAU_STG.1.1***
The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.
***FAU_STG.1.2***
The TSF shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

**FAU_STG.4 Prevention of audit data loss**
**Hierarchical to: FAU_STG.3 Action in case of possible audit data loss**
**Dependencies: FAU_STG.1 Protected audit trail storage**
***FAU_STG.4.1***
The TSF shall [overwrite the oldest stored audit records] and [*no other actions*] if the audit trail is full.

[33] The log files cannot be modified by Users, but do track when the last time the system modified the log files.

## 6.2.2 Class FCS: Cryptographic Support

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

***FCS_CKM.1.1***

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*SP[34] 800-90A HMAC[35]_DRBG[36]*] and specified cryptographic key sizes [*cryptographic key sizes – see Table 13*] that meet the following: [*list of standards – see Table 13*].

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

***FCS_CKM.4.1***

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

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

***FCS_COP.1.1***

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

**Table 13 Cryptographic Operations**

| Cryptographic Operations | Cryptographic Algorithm | Key Size (bits) | Standards (Certificate #) |
|---|---|---|---|
| Symmetric Encryption and Decryption | Triple DES[37] (ECB[38], CBC[39], CFB[40], OFB[41]) | 168 | FIPS 46-3 (Certificate # 1408) |

[34] SP – Special Publication
[35] HMAC – Hash-based Message Authentication Code
[36] DRBG – Deterministic Random Bit Generator
[37] DES – Data Encryption Standard
[38] ECB – Electronic Code Book
[39] CBC – Cipher Block Chaining
[40] CFB – Cipher Feedback
[41] OFB – Output Feedback

| Cryptographic Operations | Cryptographic Algorithm | Key Size (bits) | Standards (Certificate #) |
|---|---|---|---|
| | AES in ECB, CBC, CFB, OFB | 128, 192, 256 | CAVP (cert #2249)<br><br>FIPS PUB 197, "Advanced Encryption Standard (AES)" NIST SP800-38A |
| Message Digest | SHA[42]-224, SHA-256, SHA-384, SHA-512 | N/A[43] | FIPS 180-3 (Certificate # 1938) |
| Message Authentication | HMAC-SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 | 160, 224, 256, 384, 512 | FIPS 198 (Certificate #1378) |
| Signature Generation and Verification | RSA X9.31, PKCS[44] #1 V1.5, RSA SSA[45]-PSS[46] | 2048, 3072 | ANSI[47] X9.31 (Certificate #1154) |
| Key generation | RSA X9.31, PKCS #1 V1.5, RSA SSA-PSS | 2048, 3072, 4096 | ANSI[48] X9.31 (Certificate #1154) |
| Random number generation | SP 800-90A HMAC-based | N/A | CAVP (cert #273)<br><br>NIST SP 800-90A, 'Recommendation for Random Number Generation Using Deterministic Random Bit Generators" |

[42] SHA – Secure Hash Algorithm
[43] N/A – Not Applicable
[44] PKCS – Public-Key Cryptography Standards
[45] SSA – Signature Scheme with Appendix
[46] PSS – Probabilistic Signature Scheme
[47] ANSI – American National Standards Institute
[48] ANSI – American National Standards Institute

### 6.2.3 Class FDP: User Data Protection

**FDP_ACC.2 Complete access control**
**Hierarchical to: FDP_ACC.1 Subset access control**
**Dependencies: FDP_ACF.1 Security attribute based access control**

***FDP_ACC.2.1***
The TSF shall enforce the [*Group access control SFP*] on [*Subjects: TOE users, and Objects: Monitors within a group*] and all operations among subjects and objects covered by the SFP.

***FDP_ACC.2.2***
The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

**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 [*Group access control SFP*] to objects based on the following: [*Subjects: TOE users; Objects: Monitors within a group; Security Attributes: access to a group*].

***FDP_ACF.1.2***
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*the Subject should have allowed access to the group and hence all the Monitors within that group]*

***FDP_ACF.1.3***
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

***FDP_ACF.1.4***
The TSF shall explicitly deny access of subjects to objects based on the [*none*].

### 6.2.4 Class FIA: Identification and Authentication

**FIA_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: [

- *User name*
- *User type*
- *Allowed Groups*
- *Password]*

**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 authentication*[49]*, PKI using 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 [

- *Password-based authentication is performed according to the verification of stored identity and credential information*
- *PKI (X.509) certificate-based authentication uses public-private key pairs for authentication*].

**FIA_UAU.7 Protected authentication feedback**
**Hierarchical to: No other components.**
**Dependencies: FIA_UAU.1 Timing of authentication**
***FIA_UAU.7.1***

The TSF shall provide only [*obscured feedback]* to the user while the authentication is in progress.

**FIA_UID.2 User identification before any action**
**Hierarchical to: FIA_UID.1 Timing of identification**
**Dependencies: No dependencies**
***FIA_UID.2.1***

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

[49] The remote Active Directory server provides password-based authentication via LDAP.

## 6.2.5 Class FMT: Security Management

**FMT_MOF.1 Management of security functions behaviour**
**Hierarchical to: No other components.**
**Dependencies: FMT_SMF.1 Specification of management functions**
**FMT_SMR.1 Security roles**

***FMT_MOF.1.1***
The TSF shall restrict the ability to [determine the behavior of, modify the behavior of, disable, enable the functions [*security functions as specified in* Table 14] to [*the roles listed in* Table 14].

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

***FMT_MSA.1.1***
The TSF shall enforce the [*Group access control SFP*] to restrict the ability to [modify] the security attributes [*access to an allowed group*] to *[Administrator and Power User*].

**FMT_MSA.3 Static attribute initialisation**
**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 [*Group access control SFP*] to provide [permissive] default values for security attributes that are used to enforce the SFP.

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

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

***FMT_MTD.1.1***
The TSF shall restrict the ability to [[*operations as listed in Table 14*]] the [*TSF data as specified in* Table 14] to [*the roles listed in* Table 14].

**Table 14 Management of TSF Data**

| TSF Data | Operation | Authorized Role |
|---|---|---|
| Groups | View, Edit, Refresh, Disable, Enable | Administrator; Power User and Regular User with "Groups" permission |
| | Refresh, View | Integration Viewer |
| Monitors | View, Edit, Delete, Refresh, Acknowledge, Disable, Enable | Administrator; Power User and Regular User with "Monitors" permission |
| | Refresh, View | Integration Viewer |

| TSF Data | Operation | Authorized Role |
|---|---|---|
| Alerts | View, Edit, Delete, Test, Disable alerts indefinitely, Disable alerts temporarily, Enable alerts | Administrator;<br>Power User and Regular User with "Alerts" permission |
| Reports | Generate, Edit | Administrator;<br>Power User and Regular User with "Reports" permission |
| Remote Servers | View, Edit, Test | Administrator;<br>Power User and Regular User with "Remote Servers" permission |
| Preferences<br>• General<br>• Infrastructure<br>• Integration<br>• Log<br>• Email, Pager and SNMP (Test also)<br>• Event Mappings<br>• Schedule<br>• Credential<br>• Certificate Management<br>• Tags<br>• Template<br>• Dashboard<br>• HTTP<br>• Event Console | View, Edit | Administrator;<br>Power User and Regular User with respective "Preferences" permissions |
| User Management Preferences | View, Edit | Administrator;<br>Power User |
| Server Statistics | View | Administrator;<br>Power User and Regular User with respective "Other" permission |
| Tools | Use | Administrator;<br>Power User and Regular User with respective "Other" permission |
| SiteScope Log Grabber run results | Download | Administrator;<br>Power User and Regular User with respective "Other" permission |

**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: [*as specified in FMT_MTD.1*].

**FMT_SMR.1 Security roles**
**Hierarchical to: No other components.**
**Dependencies: FIA_UID.1 Timing of identification**
***FMT_SMR.1.1***

The TSF shall maintain the roles [

- *Administrator*[50]
- *Power User*
- *Regular User*
- *Integration Viewer*]

***FMT_SMR.1.2***

The TSF shall be able to associate users with roles.

[50] TOE provides a single Administrator by default, which is a role based account and cannot be associated with a user. The Administrator account cannot be deleted or disabled.

### 6.2.6 Class FPT: Protection of the TSF

**FPT_ITC.1 Inter-TSF confidentiality during transmission**
**Hierarchical to: No other components.**
**Dependencies: No dependencies**
***FPT_ITC.1.1***

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

### 6.2.7 Class FTP: Trusted Path/Channels

**FTP_TRP.1 Trusted path**
**Hierarchical to: No other components.**
**Dependencies: No dependencies**
***FTP_TRP.1.1***
The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].
***FTP_TRP.1.2***
The TSF shall permit [remote users] to initiate communication via the trusted path.
***FTP_TRP.1.3***
The TSF shall require the use of the trusted path for [*all remote actions*].

# 6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2, augmented with ALC_FLR.2. Table 15 summarizes the requirements.

**Table 15 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_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 Security Specification

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

## 7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 16 lists the security functionality and their associated SFRs.

**Table 16 Mapping of TOE Security Functionality to Security Functional Requirements**

| TOE Security Functionality | SFR ID | Description |
|---|---|---|
| Security Audit | FAU_ARP.1 | Security alarms |
| | FAU_GEN.1 (a) | Audit data generation – Audit Logs |
| | FAU_GEN.1 (b) | Audit data generation – Data Logs |
| | FAU_GEN.2 | User identity association |
| | FAU_SAA.1 | Potential violation analysis |
| | FAU_SAR.1 | Audit review |
| | FAU_SAR.3 | Selectable audit review |
| | FAU_STG.1 | Protected audit trail storage |
| | FAU_STG.4 | Prevention of audit data loss |
| Cryptographic Support | FCS_CKM.1 | Cryptographic key generation |
| | FCS_CKM.4 | Cryptographic key destruction |
| | FCS_COP.1 | Cryptographic operation |
| User Data Protection | FDP_ACC.2 | Complete access control |
| | FDP_ACF.1 | Security attribute based access control |
| Identification and Authentication | FIA_ATD.1 | User attribute definition |
| | FIA_UAU.2 | User authentication before any action |
| | FIA_UAU.5 | Multiple authentication mechanisms |
| | FIA_UAU.7 | Protected authentication feedback |
| | FIA_UID.2 | User identification before any action |
| Security Management | FMT_MOF.1 | Management of security functions behavior |

| TOE Security Functionality | SFR ID | Description |
|---|---|---|
| | FMT_MSA.1 | Management of security attributes |
| | FMT_MSA.3 | Static attribute initialization |
| | FMT_MTD.1 | Management of TSF data |
| | FMT_SMF.1 | Specification of management functions |
| | FMT_SMR.1 | Security roles |
| Protection of TOE Security Functions | FPT_ITC.1 | Inter-TSF confidentiality during transmission |
| Trusted Path/Channels | FTP_TRP.1 | Trusted path |

### 7.1.1 Security Audit

The TOE generates audit records for all auditable events and the start-up and shutdown of the audit functions. A list of specific auditable events is provided in Table 12. Each audit record includes the fields specified in Table 17. For audit events resulting from actions of identified users, the TSF records the identity of the user that caused the event. TOE relies on the underlying OS for time stamps.

To view log files, the user must be an Administrator of the TOE, or a user that has been granted the "View log preferences" permissions. The TOE does not allow deletion of audit logs; locally stored log files are kept in use by the TOE to avoid unauthorized deletion. This also prevents unauthorized modifications to the audit trail. The TOE provides all audit log files in a manner that is suitable for easy interpretation. While viewing the log files within the "Server Statistics" context, the user will be able to filter the log files based on the type of the log files. The user will also be able to sort the order of log files in an ascending or descending manner based on the log file name, log size, or modification date. An authorized user with appropriate permissions can configure the total number of logs that can be stored within a log file and also specify maximum size of logs. The TOE will overwrite the oldest log file once it reaches its maximum record amount.

The TOE monitors all configured assets and events and based upon configuration triggers an alert to indicate a potential security violation. An Administrator, or a user granted alert permissions, may create or modify different alert triggers within the TOE. The TOE sends one or more alerts of the following types as configured to indicate a potential security violation:

- Disable or Enable Monitor alerts: These alerts can turn off and turn on the triggering of alerts for monitors.
- Email alerts: These alerts send event notifications from SiteScope to a designated email address.
- Event console alerts: These alerts send event notifications from SiteScope to an event console.
- Log Event alerts: These alerts can be used to extend the types of events that are logged to a Windows Application Event Log.
- Post alerts: These alerts use the Common Gateway Interface (CGI) protocol to forward POST data to a CGI enabled program.
- Script alerts: These alerts can automatically initiate recovery scripts.
- SNMP Trap alerts: These alerts forward event data from any type of SiteScope monitor to an SNMP enabled host or management system.
- Sound alerts: These alerts play a sound or audio file on the machine on which SiteScope is running when an alert is generated.

The TOE audit records contain the following information:

**Table 17 Audit Record Contents**

| Field | Content |
|---|---|
| Date | Date (yyyy-mm-dd) when the event occurred. |
| Time | Time (hh:mm:ss) when the event occurred. |
| User | User Identifier |
| Operation Performed | Information about the audit event and the outcome of the operation (when applicable). |

The TOE also records audit records for monitor statistics including data from each monitor run and SiteScope server health and statistics. These audit records contain the category, stateString, and ID Sample number for each event. The date and time of each event, the type of event, subject identity (if applicable) and the outcome of the event are also recorded.

**TOE Security Functional Requirements Satisfied:** FAU_ARP.1, FAU_GEN.1 (a), FAU_GEN.1(b), FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, and FAU_STG.4.

## 7.1.2 Cryptographic Support

The TOE utilizes a FIPS 140-2 Validated cryptographic module, which uses FIPS-Approved cryptographic algorithms to support cryptographic functionality such as encryption, decryption, and hashing. The TOE generates cryptographic keys to be used with encryption, decryption, keyed hash, and signature operations. AES, Triple-DES, RSA, and HMAC can be used by the TOE when performing the TLS protocol. Configuration files and credentials for both TOE users and external connections are stored on the local file system encrypted with 3-key Triple DES. All AES, Triple-DES, RSA, and HMAC keys are generated with the FIPS-Approved SP800-90A HMAC_DRBG.

Each of the cryptographic algorithms supported by the TOE have been tested and validated by the CAVP and have been awarded a certificate number. Table 13, provided in Section 6.2.2, lists each algorithm used by the TOE, their usage, and their associated algorithm certificate.

The TOE's cryptographic module is responsible for destroying keying material generated within the TOE boundary. The cryptographic module uses FIPS-Approved zeroization methods in order to destroy keys and other critical parameters generated by the TOE at the appropriate time.

TLS is used to secure sessions between client workstation to SiteScope and SiteScope to external IT product such as LDAP server. SiteScope to monitored assets (data-in-motion) communication is protected over SSH/SFTP, LDAPS, SMTP over TLS, or HTTPS.

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

## 7.1.3 User Data Protection

The TOE provides complete access control on all the Monitors within a group. Monitors are placed into groups when they are created. Group assignments can be done using a default group or a manually specified group. Once the Monitor is associated with a group, the TOE enforces the Group access control SFP on a TOE user accessing Monitors within a group. All operations among a TOE user and the Monitors within the group(s) are covered by the Group access control policy. The TOE will not allow any access to any Monitors until the SiteScope user account is verified to have access assigned to a particular group. This ensures that all operations between any subject controlled by the TOE, and any object controlled by the TOE, are covered by the Group access control policy.

**TOE Security Functional Requirements Satisfied:** FDP_ACC.2 and FDP_ACF.1.

### 7.1.4 Identification and Authentication

The identification and authentication functionality establishes and verifies a claimed user's identity. The TOE identification and authentication functionality enforces TOE users to successfully identify and authenticate to the TOE to access its functionality. Users must be successfully identified and authenticated prior to performing any TSF-mediated actions on the TOE. A password change request can be made before a TOE user is identified and authenticated to the TOE; however, the password change is not performed until after successful identification and authentication. The password change request functionality requires the following information to be input: User name; Password; and New password. This information must be accurate for an existing account before a password change is successful.

The TOE maintains the following security attributes belonging to individual users:

- User name
- User type
- Allowed Groups
- Password

For administrative sessions over the SiteScope UI, the TOE provides protected authentication feedback. On entry, passwords are not displayed in clear-text but rather the SiteScope UI displays dots to obscure the text.

The TOE will authenticate users with the following methods: password-based authentication (local or remote via LDAP) or certificate-based authentication. If the user is authenticating using the password-based method, the authentication is performed according to the stored identity and credential information. The TOE can perform authentication locally, or can leverage an external LDAP service for authentication, which is provided by the TOE environment. A user or a web service client can authenticate to the TOE using certificates. If a user is authenticating using the certificate-based method, the authentication uses public-private key pair authentication stored locally. The PKI authentication method and password-based authentication methods are mutually exclusive in the TOE, meaning enabling one method disables the other. .

**TOE Security Functional Requirements Satisfied:** FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UAU.7, and FIA_UID.2.

### 7.1.5 Security Management

The TOE supports the following roles for the management of the TOE:

- Administrator
- Power User
- Regular User
- Integration Viewer

By default, the TOE provides one Administrator account and one Integration Viewer account. The Administrator role may View or Change anything within the TOE. The Regular User role by default is allowed to View groups and the ability to manage its own user preferences. The Power User role has the same access as a Regular User plus access to manage user accounts. The Integration Viewer role has view-only permissions. The Administrator and Power User roles are allowed to manage user accounts by Creating, Editing, Deleting, and Viewing them as needed but with the two following restrictions:

- An Administrator account is created by default, during the TOE setup, and cannot be deleted or disabled by any role. Administrator is a role based account and cannot be associated with a user.
- A Power User account may not delete itself but may create other Power User accounts.

The Regular User role by default is only allowed to View groups, and its own user preferences. An account created with a Regular User role may be granted more access by the Power User or Administrator that creates it. The Integration Viewer role has the same permissions as a Regular User plus access to Refresh groups and monitors, and View permissions to all objects.

The TOE user accounts are managed from the User Management Preferences page. The User Management Preferences are available only to users accessing the TOE directly. From the User Management Preferences page, the TOE allows privileged users to associate accounts with the above stated roles. The management of TSF data is breakdown by role and what operations that can be performed, as shown in Table 14. Administrator and Power User can also create additional custom "user roles" and assign permissions to that role. Restricting the access by assigning roles allows the TOE to better manage the security of the TSF data.

The TOE provides complete access control on all the Monitors within a group. The TOE enforces Group access control SFP on a TOE user accessing Monitors within a group. All operations between a TOE user and the Monitors within the group/s are covered by the Group access control policy. Only Administrator and Power User have the ability to manage and specify alternate initial values for the security attributes of the SFP. The TSF enforces permissive default values for security attributes that enforce the SFPs.

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

### 7.1.6 Protection of the TSF

The TOE protects all data transmitted from itself to a configured external LDAP server from unauthorized disclosure during transmission using TLS. The TOE also protects all data communication between itself to monitored assets (data-in-motion) using SSH/SFTP, LDAPS, SMTP over TLS, or HTTPS. This keeps data from being disclosed or modified while it is being transmitted. For a list of each monitor and the protocol/technology it uses, refer to Chapter 3: Monitor Permissions and Credentials in the HP SiteScope Monitor Reference.

**TOE Security Functional Requirements Satisfied:** FPT_ITC.1.

### 7.1.7 Trusted Path/Channels

A remote user that will access the TOE will use an Internet browser to connect to the TOE over HTTPS using TLS. This connection protects the data being communicated from disclosure or modification, and assures end point identification. The remote user will be allowed to initiate communication with the TOE over the HTTPS connection and will be required to only use this path for all remote actions taken within the TOE.

**TOE Security Functional Requirements Satisfied:** FTP_TRP.1.

# 8 Rationale

## 8.1 Conformance Claims Rationale

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

## 8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

### 8.2.1 Security Objectives Rationale Relating to Threats

Table 18 below provides a mapping of the objects to the threats they counter.

**Table 18 Threats: Objectives Mapping**

| Threats | Objectives | Rationale |
|---|---|---|
| T.NOAUDIT<br>An attacker may perform security relevant operations on the TOE without being held accountable for them. | O.AUDIT<br>The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification and loss of the audit trail, and provide the authorized administrators with the ability to review and sort the audit trail. | O.AUDIT mitigates this threat by ensuring that security relevant events of the TOE are preserved. |
| | O.AUTHENTICATE<br>The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data. | O.AUTHENTICATE mitigates this threat by ensuring that a user or administrator is properly identified, thereby allowing the TSF to record the user's identity for any logs created as a result of the user's or administrator's actions. |
| T.TRANSMIT<br>A user or process may be able to bypass the TOE's security mechanisms and gain access to the data while the data is in transit. | O.CRYPTO<br>The TOE must provide the means of protecting cryptographic operations and secure management of cryptographic keys using cryptography that conforms to standards specified in FIPS PUB 140-2. | O.CRYPTO mitigates this threat by ensuring that the cryptographic keys are managed securely conforming to the FIPS PUB 140-2 standards. |
| | O.SECURE<br>The TOE shall securely transfer data with other trusted IT entities | O.SECURE mitigates this threat by providing trusted mechanisms to protect the TOE data that is |

| Threats | Objectives | Rationale |
|---|---|---|
| | and remote users. | transferred between trusted IT entities and remote users. |
| T.UNAUTH<br>An unauthorized person may gain access to the TOE and compromise its security functions by changing its configuration. | O.ADMIN<br>The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control. | O.ADMIN mitigates this threat by restricting the access to TOE security data to those users with access to the management functions of the TOE. |
| | O.ATTRIBUTES<br>The TOE will be capable of maintaining user security attributes. | O.ATTRIBUTES mitigates this threat by allowing only users with valid credentials to access the TOE. |
| | O.AUDIT<br>The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification and loss of the audit trail, and provide the authorized administrators with the ability to review and sort the audit trail. | O.AUDIT mitigates this threat by auditing all unauthorized attempts to access the TOE. |
| | O.AUTHENTICATE<br>The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data. | O.AUTHENTICATE mitigates this threat by ensuring that users are identified and authenticated prior to gaining access to TOE's administrative functions and data. |
| T.UNDETECT<br>A TOE resource may be compromised as a result of an authorized administrator of the TOE not having the ability to notice potential security violations. Therefore, limiting their ability to identify and take action against a possible security breach. | O.ALERT<br>The TOE will provide the capability to monitor and send alerts upon the detection of a potential security violation based on the rules configured. | O.ALERT mitigates this threat by ensuring that the TOE will provide alerts while monitoring for potential security violations. |

Every Threat is mapped to one or more Objectives in the Table 18 above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

### 8.2.2 Security Objectives Rationale Relating to Policies

There are no OSPs for this ST.

### 8.2.3 Security Objectives Rationale Relating to Assumptions

Table 19 below gives a mapping of assumptions and the environmental objectives that uphold them.

**Table 19 Assumptions: Objectives Mapping**

| Assumptions | Objectives | Rationale |
|---|---|---|
| A.ATTRIBUTES<br>The TOE environment will be able to maintain user security attributes when the TOE is configured to use external authentication. | OE.ATTRIBUTES<br>The IT environment must be able to maintain user security attributes when the TOE is configured to use external authentication. | OE.ATTRIBUTES upholds this assumption by ensuring that the TOE user security attributes are securely maintained by the external IT environment when the TOE is configured to use external authentication. |
| A.INSTALL<br>The TOE is installed on the appropriate, dedicated hardware and operating system. | OE.PLATFORM<br>The TOE hardware and OS must support all required TOE functions. | OE.PLATFORM upholds this assumption by ensuring that the TOE hardware meets minimum requirements and the OS supports all the TOE functions. |
| A.LOCATE<br>The TOE is located within a controlled access facility. | OE.PHYSICAL<br>Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. | OE.PHYSICAL upholds this assumption by ensuring that the TOE environment provides protection against physical attacks. |
| A.MANAGE<br>There are one or more competent individuals assigned to manage the TOE and the security of the information it contains. | OE.TRUSTED_ADMIN<br>Those responsible for operating the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains; however, they are capable of error. | OE.TRUSTED_ADMIN upholds this assumption by ensuring that those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use. |
| A.NETCON<br>The TOE environment provides the network connectivity required to allow the TOE to perform its intended functions. | OE.MONITOR<br>The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function. | OE.MONITOR upholds this assumption by ensuring that the TOE environment provides the appropriate network connectivity required for performance with a proper implementation of the TOE. |
| A.NOEVIL<br>The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance. | OE.TRUSTED_ADMIN<br>Those responsible for operating the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains; however, they are capable of error. | OE.TRUSTED_ADMIN upholds this assumption by ensuring that all administrators assigned to manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all administrator guidance. |
| A.PROTECT | OE.SECURE_COMM | OE.SECURE_COMM upholds this |

| Assumptions | Objectives | Rationale |
|---|---|---|
| The TOE software will be protected from unauthorized modification. | The TOE Environment must provide a mechanism to provide a secure and authorized user access to the TOE environment for protecting the TOE and TOE data from modification. | assumption by ensuring that the TOE environment provides a secure and authorized access to its users for protect the data from external interference or tampering. |
| A.TIMESTAMP<br>The TOE environment provides the TOE with the necessary reliable timestamps. | OE.TIME<br>The underlying Operating System must provide reliable timestamps to the TOE. | OE.TIME upholds this assumption by ensuring that the operating system where the TOE is installed will provide reliable time stamps for the TOE. |

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

# 8.3 Rationale for Extended Security Functional Requirements

There are no extended functional requirements defined for this TOE.

# 8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended functional requirements defined for this TOE.

# 8.5 Security Requirements Rationale

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

## 8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 20 below shows a mapping of the objectives and the SFRs that support them.

**Table 20 Objectives: SFRs Mapping**

| Objective | Requirements Addressing the Objective | Rationale |
|---|---|---|
| O.ADMIN<br>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 | FMT_MOF.1<br>Management of security functions behavior | The requirement meets this objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges. |
| | FMT_MSA.1 | The requirement meets this |

| Objective | Requirements Addressing the Objective | Rationale |
|---|---|---|
| those TOE users, may exercise such control. | Management of security attributes | objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only privileged users may manage the security behavior of the TOE. |
| | FMT_MSA.3<br>Static attribute initialization | The requirement meets this objective by restricting the ability to specify alternate values to security attributes only to authorized users. |
| | FMT_MTD.1<br>Management of TSF data | The requirement meets this objective by ensuring that the TOE restricts access to TSF data based on the user's role. |
| | FMT_SMF.1<br>Specification of management functions | The requirement meets this objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF. |
| | FMT_SMR.1<br>Security roles | The requirement meets this objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data. |
| O.ALERT<br>The TOE will provide the capability to monitor and send alerts upon the detection of a potential security violation based on the rules configured. | FAU_ARP.1<br>Security alarms | The requirement meets this objective by ensuring that the TOE generates alerts upon detection of a potential security violation. |
| | FAU_SAA.1<br>Potential violation analysis | The Administrator configures alert triggers for monitoring audited events that the TOE enforces. The requirement meets this objective by ensuring that the TOE is able to apply a set of rules for monitoring the audited events to indicate a potential violation of the enforcement of the SFRs. |
| | FDP_ACC.2<br>Complete access control | The requirement meets this objective by ensuring that access control is enforced on all monitoring operations among subjects and objects covered by the SFP. |
| | FDP_ACF.1<br>Security attribute based access | The requirement meets this objective by ensuring that the |

| Objective | Requirements Addressing the Objective | Rationale |
|---|---|---|
| | control | TOE enforces the access control based on permissions and credentials. |
| O.ATTRIBUTES<br>The TOE will be capable of maintaining user security attributes. | FIA_ATD.1<br>User attribute definition | The requirement meets this objective by ensuring that the TOE maintains a defined list of security attributes belonging to individual users. These may only be changed by authorized users. |
| | FMT_MTD.1<br>Management of TSF data | The requirement meets this objective by ensuring that only authorized users are allowed access to TSF data by their assigned rights. |
| | FMT_SMR.1<br>Security roles | The requirement meets this objective by ensuring that the TOE manages the defined user roles. The TOE does this by ensuring that only authorized users have access to TSF data. |
| O.AUDIT<br>The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification and loss of the audit trail, and provide the authorized administrators with the ability to review and sort the audit trail. | FAU_GEN.1 (a)<br>Audit data generation – Audit Logs | The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event. |
| | FAU_GEN.1 (b)<br>Audit data generation – Data Logs | The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event. |
| | FAU_GEN.2<br>User identity association | The requirement meets this objective by ensuring that the TOE associates auditable events with the identity of the user that caused the event. |
| | FAU_SAR.1<br>Audit review | The requirement meets this objective by ensuring that the TOE provides the ability to review logs with records being presented in a suitable manner for interpretation. |
| | FAU_SAR.3<br>Selectable audit review | The requirement meets this objective by ensuring that the TOE has the ability to apply ordering to the audit data. |
| | FAU_STG.1 | The requirement meets this |

| Objective | Requirements Addressing the Objective | Rationale |
|---|---|---|
| | Protected audit trail storage | objective by ensuring that the TOE protects the audit data from unauthorized deletion and modification. |
| | FAU_STG.4<br>Prevention of audit data loss | If the audit facilities become full, the TOE ensures that only the oldest records are overwritten. This requirement meets this objective by mitigating the risk of loss of audit trail data. |
| O.AUTHENTICATE<br>The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data. | FIA_UAU.2<br>User authentication before any action | The requirement meets this objective by ensuring that the TOE requires each user to be successfully authenticated before allowing any TOE administrative actions on behalf of that user. |
| | FIA_UAU.5<br>Multiple authentication mechanisms | The requirement meets this objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authenticated users are allowed access to TOE functions. |
| | FIA_UAU.7<br>Protected authentication feedback | The requirement meets this objective by ensuring that the password of a user is obscured by dots while the user authenticates. |
| | FIA_UID.2<br>User identification before any action | The requirement meets this objective by ensuring that the TOE requires each user to be successfully identified before allowing any TOE administrative actions on behalf of that user. |
| | FMT_MOF.1<br>Management of security functions behavior | The requirement meets this objective by ensuring that the TOE authenticates users prior to allowing access to administrative functions to ensure that only those trusted users may manage the security behavior of the TOE. |
| O.CRYPTO<br>The TOE must provide the means of protecting cryptographic operations and secure management of cryptographic keys using cryptography that conforms to standards specified in FIPS PUB | FCS_CKM.1<br>Cryptographic key generation | The requirement meets this objective by ensuring that the TOE generates cryptographic keys in accordance with FIPS PUB 140-2 approved techniques. |
| | FCS_CKM.4<br>Cryptographic key destruction | The requirement meets this objective by ensuring that the |

| Objective | Requirements Addressing the Objective | Rationale |
|---|---|---|
| 140-2. | | cryptographic keys are destroyed according to FIPS PUB 140-2 zeroization requirements. |
| | FCS_COP.1<br>Cryptographic operation | This requirement meets this objective by ensuring that the cryptographic operations are performed according to the FIPS PUB 140-2 approved algorithms and key sizes. |
| O.SECURE<br>The TOE shall securely transfer data with other trusted IT entities and remote users. | FPT_ITC.1<br>Inter-TSF confidentiality during transmission | The requirement meets this objective by ensuring that the TOE provides a trusted communication path which provides for the protection of the data from disclosure when in transit. |
| | FTP_TRP.1<br>Trusted path | The requirement meets this objective by ensuring that the TOE provides a trusted communication path which provides for the protection of the data from disclosure and modification while exchanged between remote users and TOE. |

## 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 21 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 21 Functional Requirements Dependencies**

| SFR ID | Dependencies | Dependency Met | Rationale |
|---|---|---|---|
| FAU_ARP.1 | FAU_SAA.1 | ✓ | |

| SFR ID | Dependencies | Dependency Met | Rationale |
|---|---|---|---|
| FAU_GEN.1 (a) | FPT_STM.1 | | The TOE environment i.e., the underlying Operating System provides reliable timestamps to the TOE. |
| FAU_GEN.1 (b) | FPT_STM.1 | | The TOE environment i.e., the underlying Operating System provides reliable timestamps to the TOE. |
| FAU_GEN.2 | FAU_GEN.1 | ✓ | |
| | FIA_UID.1 | ✓ | |
| FAU_SAA.1 | FAU_GEN.1 | ✓ | |
| FAU_SAR.1 | FAU_GEN.1 | ✓ | |
| FAU_SAR.3 | FAU_SAR.1 | ✓ | |
| FAU_STG.1 | FAU_GEN.1 | ✓ | |
| FAU_STG.4 | FAU_STG.1 | ✓ | |
| FCS_CKM.1 | FCS_COP.1 | ✓ | |
| | FCS_CKM.4 | ✓ | |
| FCS_CKM.4 | FCS_CKM.1 | ✓ | |
| FCS_COP.1 | FCS_CKM.4 | ✓ | |
| | FCS_CKM.1 | ✓ | |
| FDP_ACC.2 | FDP_ACF.1 | ✓ | |
| FDP_ACF.1 | FDP_ACC.1 | ✓ | Although FDP_ACC.1 is not included, FDP_ACC.2, which is hierarchical to FDP_ACC.1, is included. This satisfies the dependency. |
| | FMT_MSA.3 | ✓ | |
| FIA_ATD.1 | No dependencies | | |
| FIA_UAU.2 | FIA_UID.1 | ✓ | Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies the dependency. |
| FIA_UAU.5 | No dependencies | | |
| FIA_UAU.7 | FIA_UAU.1 | ✓ | |

| SFR ID | Dependencies | Dependency Met | Rationale |
|---|---|---|---|
| FIA_UID.2 | No dependencies | | |
| FMT_MOF.1 | FMT_SMF.1 | ✓ | |
| | FMT_SMR.1 | ✓ | |
| FMT_MSA.1 | FDP_ACC.1 | ✓ | Although FDP_ACC.1 is not included, FDP_ACC.2, which is hierarchical to FDP_ACC.1, is included. This satisfies the dependency. |
| | FMT_SMR.1 | ✓ | |
| | FMT_SMF.1 | ✓ | |
| FMT_MSA.3 | FMT_SMR.1 | ✓ | |
| | FMT_MSA.1 | ✓ | |
| FMT_MTD.1 | FMT_SMR.1 | ✓ | |
| | FMT_SMF.1 | ✓ | |
| FMT_SMF.1 | No dependencies | | |
| FMT_SMR.1 | FIA_UID.1 | ✓ | |
| FPT_ITC.1 | No dependencies | | |
| FTP_TRP.1 | No dependencies | | |

# 9 Acronyms

Table 22 in this section defines the acronyms used throughout this document.

**Table 22 Acronyms**

| Acronym | Definition |
|---|---|
| **ANSI** | American National Standards Institute |
| **API** | Application Programming Interface |
| **ASP** | Active Server Pages |
| **AWS** | Amazon Web Services |
| **BSM** | Business Service Management |
| **CBC** | Cipher Block Chaining |
| **CC** | Common Criteria |
| **CEM** | Common Methodology for Information Technology Security Evaluation |
| **CFB** | Cipher Feedback |
| **CGI** | Common Gateway Interface |
| **CM** | Configuration Management |
| **CPU** | Central Processing Unit |
| **CSA** | Cloud Service Automation |
| **DB** | Database |
| **DES** | Data Encryption Standard |
| **DNS** | Domain Name System |
| **DRBG** | Deterministic Random Bit Generator |
| **EAL** | Evaluation Assurance Level |
| **EC** | Elliptic Curve |
| **ECB** | Electronic Code Book |
| **FTP** | File Transfer Protocol |
| **GB** | GigaByte |
| **HMAC** | Hash-based Message Authentication Code |
| **HTML** | HyperText Markup Language |
| **HTTPS** | Hypertext Transfer Protocol Secure |
| **IBM** | International Business Machines |
| **ICMP** | Internet Control Message Protocol |
| **IIS** | Internet Information Services |
| **IPMI** | Intelligent Platform Management Interface |

| Acronym | Definition |
|---|---|
| **IT** | Information Technology |
| **JCE** | Java Cryptography Extension |
| **JDBC** | Java Database Connectivity |
| **JMX** | Java Management Extensions |
| **JRE** | Java Runtime Environment |
| **JVM** | Java Virtual Machine |
| **LDAP** | Lightweight Directory Access Protocol |
| **MHz** | Mega-Hertz |
| **N/A** | Not Applicable |
| **NA** | Network Automation |
| **NetBIOS** | Network Basic Input Output System |
| **NOC** | Network Operations Center |
| **OFB** | Output Feedback |
| **OM** | Operations Manager |
| **OO** | Operations Orchestration |
| **OS** | Operating System |
| **OSP** | Organizational Security Policy |
| **PKCS** | Public-Key Cryptography Standards |
| **PKI** | Public Key Infrastructure |
| **PP** | Protection Profile |
| **PSS** | Probabilistic Signature Scheme |
| **PUB** | Publication |
| **RSA** | Ron Rivest, Adi Shamir, and Leonard Adleman |
| **SA** | Server Automation |
| **SAM** | System Availability Management |
| **SAP** | Systems, Applications and Products in Data Processing |
| **SAR** | Security Assurance Requirement |
| **SFP** | Security Function Policy |
| **SFR** | Security Functional Requirement |
| **SFTP** | Secure File Transfer Protocol |
| **SHA** | Secure Hash Algorithm |
| **SNMP** | Simple Network Management Protocol |
| **SP** | Special Publication |

| Acronym | Definition |
|---|---|
| **SQL** | Structured Query Language |
| **SSA** | Signature Scheme with Appendix |
| **SSH** | Secure Shell |
| **SSL** | Secure Socket Layer |
| **ST** | Security Target |
| **TCO** | Total Cost of Ownership |
| **TCP** | Transmission Control Protocol |
| **TLS** | Transport Layer Security |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functionality |
| **UI** | User Interface |
| **URL** | Uniform Resource Locator |
| **WAR** | Web Application Archive |
| **WMI** | Windows Management Instrumentation |
| **WML** | Wireless Markup Language |
| **XML** | eXtensible Markup Language |

Prepared by:
**Corsec Security, Inc.**


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

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