Hewlett Packard Enterprise Development LP

HPE Operations Bridge Premium v2016.05 including HPE Operations Manager i v10.11, HPE Operations Agent v12.01, and HPE Operations Bridge Reporter v10.01

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.2

Prepared for:

Hewlett Packard Enterprise

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

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

Prepared by:

Corsec

Corsec Security, Inc.

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

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

Table of Contents

1. Introduction 5
1.1 Purpose 5
1.2 Security Target and TOE References 6
1.3 Product Overview 6
1.3.1 HPE Operations Bridge Premium Overview 6
1.4 TOE Overview 7
1.4.1 HPE OMi 10.11 7
1.4.2 HPE OA 12.01 8
1.4.3 HPE OBR v10.01 9
1.4.4 Brief Description of the Components of the TOE 10
1.4.5 TOE Environment 10
1.4.6 Product Physical/Logical Features and Functionality not included in the TOE 15
1.5 TOE Description 15
1.5.1 Physical Scope 16
1.5.2 Logical Scope 17
2. Conformance Claims 20
3. Security Problem 21
3.1 Threats to Security 21
3.2 Organizational Security Policies 22
3.3 Assumptions 22
4. Security Objectives 23
4.1 Security Objectives for the TOE 23
4.2 Security Objectives for the Operational Environment 23
4.2.1 IT Security Objectives 23
4.2.2 Non-IT Security Objectives 24
5. Extended Components 25
5.1 Extended TOE Security Functional Components 25
5.1.1 Class FDC: Data Collection and Analysis 25
5.2 Extended TOE Security Assurance Components 29
6. Security Requirements 30
6.1 Conventions 30
6.2 Security Functional Requirements 30
6.2.1 Class FAU: Security Audit 32
6.2.2 Class FCO: Communication 33
6.2.3 Class FCS: Cryptographic Support 34
6.2.4 Class FDP: User Data Protection 36
6.2.5 Class FIA: Identification and Authentication 39
6.2.6 Class FMT: Security Management 40
6.2.7 Class FPT: Protection of the TSF 42
6.2.8 Class FRU: Resource Utilization 43
6.2.9 Class FTA: TOE Access 44
6.2.10 Class FTP: Trusted Path/Channels 45
6.2.11 Class FDC: Data Collection and Analysis 46

6.3 Security Assurance Requirements 48
7. TOE Summary Specification 49
7.1 TOE Security Functionality 49
7.1.1 Security Audit 50
7.1.2 Communication 53
7.1.3 Cryptographic Support 53
7.1.4 User Data Protection 54
7.1.5 Identification and Authentication 54
7.1.6 Security Management 54
7.1.7 Protection of the TSF 55
7.1.8 Resource Utilization 56
7.1.9 TOE Access 56
7.1.10 Trusted Path/Channels 56
7.1.11 Data Collection and Analysis 56
8. Rationale 58
8.1 Conformance Claims Rationale 58
8.2 Security Objectives Rationale 58
8.2.1 Security Objectives Rationale Relating to Threats 58
8.2.2 Security Objectives Rationale Relating to Policies 59
8.2.3 Security Objectives Rationale Relating to Assumptions 59
8.3 Rationale for Extended Security Functional Requirements 61
8.4 Security Requirements Rationale 61
8.4.1 Rationale for Security Functional Requirements of the TOE Objectives 61
8.4.2 Security Assurance Requirements Rationale 64
8.4.3 Dependency Rationale 64
9. Acronyms 67

List of Figures

Figure 1 – Deployment Configuration of the TOE 11
Figure 2 – FDC: Data Collection and Analysis Class Decomposition 26
Figure 3 – System analysis family decomposition 26
Figure 4 – System scan family decomposition 27
Figure 5 – Scanned data storage family decomposition 28

List of Tables

Table 1 – ST and TOE References 6
Table 2 – Minimum System Requirements 13
Table 3 – TOE Guidance Documents 16
Table 4 – CC and PP Conformance 20
Table 5 – Threats 21
Table 6 – Assumptions 22
Table 7 – Security Objectives for the TOE 23
Table 8 – IT Security Objectives 24
Table 9 – Non-IT Security Objectives 24
Table 10 – Extended TOE Security Functional Requirements 25
Table 11 – TOE Security Functional Requirements 30
Table 12 – RSA BSAFE® Crypto-J JSAFE and JCE Software Module 6.2.1 Cryptographic Operations 34
Table 13 – OpenSSL FIPS Object Module 2.0.12 Cryptographic Operations 35
Table 14 – Resource Permissions 36
Table 15 – Assurance Requirements 48
Table 16 – Mapping of TOE Security Functionality to Security Functional Requirements 49
Table 17 – Audit Log Contexts 50
Table 18 – User/Group Management Configuration Changes 51
Table 19 – Operations Management Event Changes 51
Table 20 – Operations Management Configuration Changes 52
Table 21 – Threats: Objectives Mapping 58
Table 22 – Assumptions: Objectives Mapping 59
Table 23 – Objectives: SFRs Mapping 61
Table 24 – Functional Requirements Dependencies 65
Table 25 – Acronyms 67

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is HPE Operations Bridge Premium v2016.05 including HPE Operations Manager i v10.11 Build 016.001.63210 Hotfix QCCR8D53202_1011, HPE Operations Agent v12.01 Build 020, and HPE Operations Bridge Reporter v10.01 Build 953.00001 and will hereafter be referred to as the TOE throughout this document. The TOE is software-only and provides event monitoring, correlation, analysis, reporting, and automation services across an Information Technology (IT) environment.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile (PP), and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- 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 Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms 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 HPE Operations Bridge Premium v2016.05 including HPE Operations Manager i v10.11, HPE Operations Agent v12.01, and HPE Operations Bridge Reporter v10.01 Security Target
ST Version	Version 1.2
ST Author	Corsec Security, Inc.
ST Publication Date	11/15/2017
TOE Reference	HPE Operations Bridge Premium v2016.05 including: • HPE Operations Manager i v10.11 Build 016.001.63210 Hotfix: QCCR8D53202_1011 • HPE Operations Agent (OA) v12.01 Build 020 • HPE Operations Bridge Reporter v10.01 Build 953.00001
FIPS[1] 140-2 Status	• Level 1, RSA BSAFE® Crypto-J JSAFE and JCE[2] Software Module, Software Version 6.2.1, Certificate No. 2469 • Level 1, OpenSSL FIPS Object Module, Software Version 2.0.12, Certificate No. 1747

1.3 Product Overview

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

1.3.1 HPE Operations Bridge Premium Overview

HPE Operations Bridge Premium, also referred to as "HPE OpsBridge", is an IT event correlation and management software product. The HPE OpsBridge software includes the following components:

- HPE Operations Manager i (OMi)
- HPE Operations Agent (OA)
- HPE Operations Bridge Reporter (OBR)

The HPE OA is responsible for collecting event data from monitored systems. HPE OMi is responsible for receiving the event data and performing event data processing, automation and correlation. HPE OBR is a cross domain performance reporting tool.

All infrastructure events from various IT management systems are funneled into HPE OpsBridge via the HPE OA, where they are correlated via HPE OMi based on the relationships between Configuration Items (CIs) and analyzed to determine the root cause of a service condition. The HPE OpsBridge software allows events from monitored systems to be automatically prioritized via HPE OMi based on business rules associated with Key Performance

[1] FIPS – Federal Information Processing Standards
[2] JCE – Java Cryptography Extension

Indicators (KPIs) and Health Indicators (HIs) assigned to CIs within the IT topology. HPE OpsBridge also allows automatic workflows and actions to be triggered upon the detection of a service condition.

HPE OpsBridge provides the capability to forward events from monitored systems to other HPE products including Service Manager (SM), Service Anywhere (SAW), or corresponding third party trouble ticket systems where tickets are created from the forwarded events. Events from monitored systems can also be received from various applications including Business Service Management (BSM), AppPulse, Operations Manager (OM)[3], Network Node Manager i (NNMi), SiteScope (SiS), Nagios, and Microsoft System Center Operations Manager (SCOM). HPE OpsBridge can integrate with Operations Orchestration (OO) to trigger the launch of a work-flow in the context of an event. Additionally, HPE OpsBridge can integrate with HPE CMS[4]/UCMDB[5] to synchronize the topological data between HPE OpsBridge and CMS.

HPE OpsBridge utilizes FIPS 140-2 cryptographic modules and the SP[6] 800-90A HMAC[7] DRBG[8] to generate keys for all cryptographic operations.

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 and describing the TOE.

The TOE is an IT event correlation and management software suite that includes the following HPE OpsBridge components:

- HPE OMi Software
- HPE OA Software
- HPE OBR Software

1.4.1 HPE OMi 10.11

HPE OMi is the central component of the HPE OpsBridge product. HPE OMi receives events and topology information from HPE OA and processes, correlates, and analyzes events to identify service conditions. HPE OMi provides the following security features:

- Generates audit records for security relevant events (which can only be reviewed by authorized users)
- Provides automatic failover services to ensure the secure state and continued operations of the TOE
- Distributes certificates to HP OAs for the secure transmission of configuration and event data
- Enforces TOE user access control and provides a login banner warning against unauthorised use of the TOE
- Provides cryptographic support to protect event data from disclosure or modification when transferred internally between TOE components

[3] Operations Manager is a legacy systems monitoring product, not to be confused with OMi.
[4] CMS – Configuration Management System
[5] UCMDB – Universal Configuration Management Database System
[6] SP – Special Publication
[7] HMAC – Hash Message Authentication Code
[8] DRBG – Deterministic Random Bit Generator

- Provides cryptographic support to secure trusted paths and channels between itself and user workstations and external servers

The two primary components of HPE OMi include the HPE OMi Gateway (GW) Server and the HPE OMi Data Processing (DP) Server.

1.4.1.1 Gateway Server

The HPE OMi GW server is the front end component that provides the HPE OMi Web UI[9], OMi CLI[10] , JMX[11] Console, and various CLI tools used to perform the HPE OMi GW server's security management services. The HPE OMi Web UI security management services include:

- Audit configuration
- User management and access control
- Authentication setup
- Event collection and analysis
- Run-Time Service Model (RTSM)[12] administration.
- Automatic failover configuration

Additionally, the HPE OMi GW server provides web services APIs[13] for integrations with external systems. The web services APIs and HPE OMi Web UI are served by the Hewlett Packard Application Server (HPAS) and the included web server is Apache 2.4.

1.4.1.2 Data Processing Server

The HPE OMi DP server is the back-end component that interacts with an external Oracle or Microsoft SQL[14] database server for event storage. The HPE OMi DP server includes the event pipeline which relates incoming events with CIs, correlates events, automates actions, and stores events in the database. The HPE OMi DP server provides the OMi DP CLI for security management tasks. The OMi DP CLI includes the following tools:

- ovcm tool (to manage certificates)
- opr-archive-events tool (to delete closed events from the database)
- opr-agt tool (to manage and configure HP OA)
- opr-node tool (to manage nodes in the RTSM)

The HPE OMi DP server uses the HPAS and maintains a certificate server that issues certificates used for authentication and signing event/configuration payloads. Additionally, the DP server provides automatic failover services via a High-Availability Controller (HAC) and backup DP server.

1.4.2 HPE OA 12.01

HPE OA is responsible for collecting event data from monitored systems and consists of the Operations Monitoring Component and the Performance Collection Component. The Operations Monitoring Component builds up the

[9] UI – User Interface
[10] CLI – Command Line Interface
[11] JMX – Java Management Extensions
[12] RTSM is a self-contained instance of the HP Universal Configuration Management Database (UCMDB) product.
[13] API – Application Programming Interface
[14] SQL – Structured Query Language

monitoring and messaging capabilities of HPE OA and the Performance Collection Component provides the data collection and storage functionality. These components provide security management CLI tools that aid in the enforcement of the data collection and analysis functionality of the TOE. The HPE OA also utilizes cryptographic support to ensure that event data is protected when transmitted between TOE components.

The Operations Monitoring Component includes the following sub-components:

- Monitor Agent
- Action Agent
- Message Agent
- Trap Interceptor
- WMI[15] Interceptor
- Message Interceptor
- Logfile Encapsulator
- Event Correlation Agent
- Embedded Performance Component

The Performance Collection Component includes the following sub-components:

- Scope Collector
- Measurement Interface Daemon
- Transaction Tracking Daemon
- Embedded Performance Component

1.4.3 HPE OBR v10.01

HPE OBR processes event and topology information from HPE OMi and the HPE OA and displays them in reports. HPE OBR is a historical infrastructure reporting tool that displays high level cross-domain reports and detailed domain level reports. Domains include the server, network and application environments from which HPE OBR collects data. Cross-domain reports display data from related domains to give a broad picture of the health and performance of an IT infrastructure. HPE OBR reports can be used to analyze patterns in the IT environment, forecast IT resource performance based on historical data, and perform a custom analysis of the data using report filters.

HPE OBR reports are available in content packs. Content packs contain the rules that define how the performance metrics will be collected, transformed, and aggregated in the reports. A typical content pack defines the metrics for a specific domain along with the necessary rules for analysis required in that domain.

HPE OBR provides cryptographic support to ensure that event data is protected from disclosure or modification when transmitted between TOE components and to secure trusted path and channels between itself and user workstations and external servers.

HPE OBR provides the web-based HPE OBR Admin console and OBR CLI for configuration and management of the platform and installed content packs. The HPE OBR Admin console provides security management tasks, enforces authentication mechanisms, and presents a login banner warning against unauthorised use of the TOE.

[15] WMI – Windows Management Instrumentation

The OBR CLI utilizes the following tools and services for security management tasks:

- Create Vertica Database Tool
- Configure Poller Tool
- OBR Full Restore Tool
- OBR Backup Tool
- License Manager Tool
- Dimension Manager Tool
- Downtime Utility Tool
- Admin Server Client Auth Tool

1.4.4 Brief Description of the Components of the TOE

The HPE Operations Bridge Premium v2016.05 media kit includes the following components:

- HPE OMi v10.11 Build 016.001.63210 Hotfix: QCCR8D53202_1011
- HPE OBR v10.01 Build 953.00001
- HPE OA v12.01 Build 020

The software media kits differ depending on the operating system on which the TOE components are installed. Also, the same media kit is available in the following languages:

- Russian
- Simplified Chinese
- Korean
- Japanese
- French
- Spanish
- German
- English

1.4.5 TOE Environment

The evaluated configuration includes the HPE Operations Bridge Premium v2016.05 media kit (English) with both the Windows and Linux versions of the HPE OMi and HPE OA media kit zip files and the Linux version of the HPE OBR media kit. The TOE includes two instances of the HPE OMi GW server, four instances of the HPE OMi DP servers, and two instances of the HPE OAs. The TOE also includes one HPE OBR Server and one HPE OBR Remote Collector (installed from the HPE OBR software binary).

Figure 1 depicts the detailed deployment diagram for the TOE components in the evaluated configuration. The following are previously undefined acronyms that appear within the diagram:

- AD – Active Directory
- HTTPS – Hypertext Transfer Protocol Secure
- JDBC – Java Database Connectivity
- JMS – Java Message Service
- LDAP – Lightweight Directory Access Protocol

- LDAP/S – Lightweight Directory Access Protocol over Secure Sockets Layer (SSL)
- NTP – Network Time Protocol
- OS – Operating System
- RHEL – Red Hat Enterprise Linux

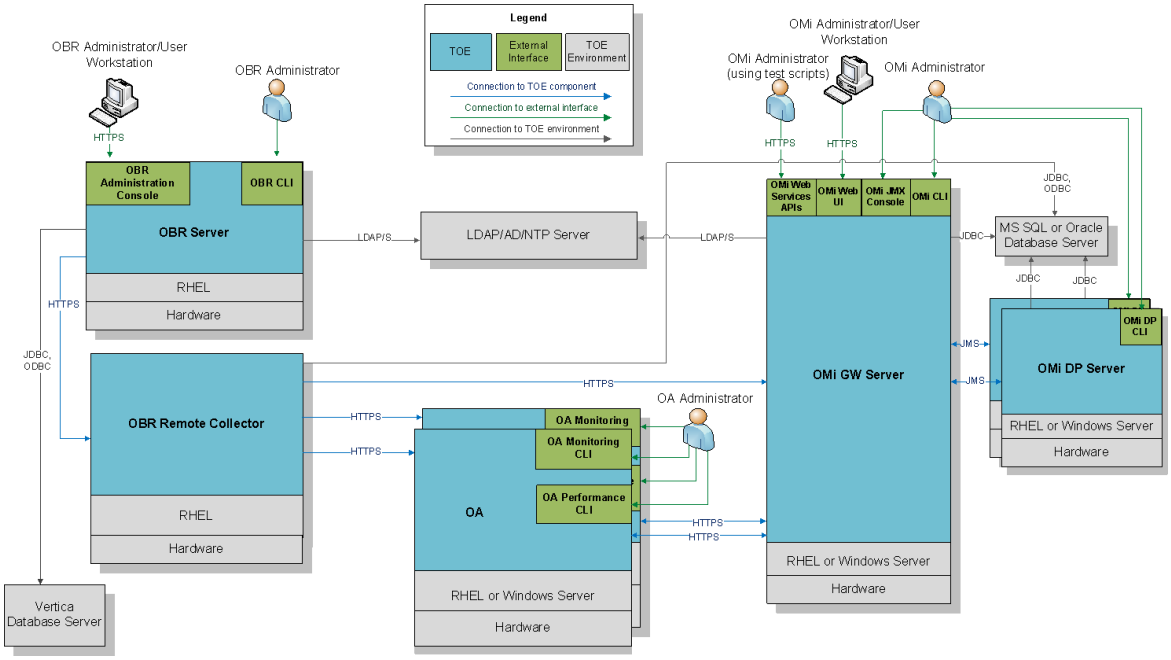

Figure 1 – Deployment Configuration of the TOE

1.4.5.1 Non-TOE Hardware/Software/Firmware Requirements

The TOE requires the following non-TOE hardware and software to be properly configured and available in the operational environment for its essential operation:

- LDAP or AD server
- NTP server
- Certificate authority (used to issue user certificates)

Though this hardware and software is necessary for the TOE's operation, it is not part of the TOE. Table 2 specifies the minimum system requirements for the proper operation of the TOE.

Table 2 – Minimum System Requirements

TOE Component	Hardware Requirements	OS Requirements	DB[16] Requirements	Browser Requirements	Other Requirements
HPE OMi	• 4 CPU[17] (64 bit) • Minimum Memory: ○ Small (up to 2,000 nodes) – 8GB[18] for DP server, 4GB for GW server ○ Medium (up to 5,000 nodes) – 12GB for DP server, 6GB for GW server ○ Large (more than 5,000 nodes) – 26GB for DP server, 10GB for GW server	• RHEL 6.7 • Microsoft Windows Server 2012 R2	• Microsoft SQL Server 2014 or Oracle DB 12c (Enterprise or Developer editions) • Small Deployment: 2 CPU cores, 2 GB RAM[19] • Medium Deployment: 2 CPU cores, 2 GB RAM • Large Deployment: 4 CPU cores, 4 GB RAM	• Mozilla Firefox 38 ESR (for RHEL) • Internet Explorer 11 (for Windows) • Browser requires JRE[20] 1.7.0_67 or greater, or 1.8.0_25 or greater.	• Adobe Flash Player 14 or later for Windows • Flash Player 11.2 or later for RHEL
HPE OA	• Minimum Memory: 2 GB or more • Processor: 1-2 CPU • Disk Space: 4 GB of free disk space; 500 MB[21] free disk space for temporary files	• Microsoft Windows Server 2012 R2	• N/A	• N/A	• N/A

[16] DB – Database
[17] CPU – Central Processing Unit
[18] GB – Gigabyte
[19] RAM – Random-Access Memory
[20] JRE – Java Runtime Environment
[21] MB – Megabytes

TOE Component	Hardware Requirements	OS Requirements	DB[16] Requirements	Browser Requirements	Other Requirements
HPE OBR Server	Small Deployment: • 8 CPU (64 bit) cores • 16 GB RAM • Diskspace: 400 GB for DB and 100 GB for software Medium Deployment (1): • 12 CPU (64 bit) cores • 24 GB RAM • Diskspace: 800 GB for DB and 200 GB for software Medium Deployment (2): • 16 CPU (64 bit) cores • 48 GB RAM • Diskspace: 1.6 TB[22] for DB and 400 GB for software Large Deployment: • 24 CPU (64 bit) cores • 64 GB RAM • Diskspace: 4.5 TB for DB and 0.5 TB for software	• RHEL 6.7	• External Vertica Database: 8 CPU; 16 GB RAM; Diskspace: 350 GB, RHEL 6.7	• Mozilla Firefox 38 ESR or Internet Explorer 11 browser • ActiveX & JavaScript controls must be enabled on browser • Browser requires JRE 1.7 or JRE 1.8	• N/A
HPE OBR Remote Collector	• 4 CPU (64 bit) cores • 8 GB RAM • Diskspace: 300 GB	• RHEL 6.7	• N/A	• N/A	• N/A

[22] TB – Terabyte

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

The HPE Operations Bridge Premium v2016.05 provides other security features that are out of the scope of the TOE. These features are not included in the TOE and will not be evaluated, and therefore there is no assurance level associated with them. The features not included in the TOE are the following:

- HPE Service Health Analyzer
- Local authentication
- SAP BO[23] Server
  - Including SAP BO BI Launchpad and SAP BO Central Management Console (except for initial configuration tasks)
- Content Development Environment (CLI and UI)
- The following HPE OMi API calls:
  - SendEvent
  - SubmitEvent
- The following HPE OMi CLI tools:
  - ConfigExchangeSiS Tool
  - BBC Trust Server Tool
  - opr-sis-file-manager Tool
  - opr-close-events Tool
  - opr-import-events Tool
  - Content Pack Auto Upload Tool
  - Content Pack Manager Tool
- The OA Java API
- The OMi JMX Console except for the hac-backup MBean service (required for HA configuration)
- The following HPE OBR CLI tools/services:
  - Enable NNMi Integration Tool
  - NNMi Remote Mount Tool
  - setenv, CreateCPFolders, createManifest Template Tool
- Lightweight Single Sign-On (LW-SSO)
- User Engagement
- OpenSSL 1.0.2j – The product contains a FIPS-capable OpenSSL 1.0.2j library which is linked with the OpenSSL FIPS Object Module 2.0.12. The non-FIPS functionality provided by OpenSSL 1.0.2j is not the cryptographic functionality evaluated in Class FCS: Cryptographic Support and there is no such assurance provided for the non-FIPS cryptographic functionality.

1.5 TOE Description

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

[23] BO – BusinessObjects

1.5.1 Physical Scope

The software-only TOE is a distributed system composed of the HPE OMi, OA, and OBR software. The HPE OMi software includes the GW and DP server components and the Management packs. The HPE OBR software includes the OBR Server, OBR Remote Collector, and Content packs.
The TOE is packaged along with the electronic documentation as an ISO[24]-9660 image for HPE OBR, and as multiple .zip files for HPE OMi. The HPE OA software binary is available as part of the HPE OMi package and as a separate ISO image.

The TOE guidance documents are also available on the HPE Software Support website (https://softwaresupport.HPE.com/) for registered customers to download.

The following guides in Table 3 are available in PDF[25] format and are required reading and part of the TOE:

Table 3 – TOE Guidance Documents

HPE Operations Manager i; Software Version: 10.11; OMi Administration Guide; Document Release Date: 25 May 2016; Software Release Date: May 2016
HPE Operations Manager i; Software Version: 10.11; OMi User Guide; Document Release Date: 25 May 2016; Software Release Date: May 2016
HPE Operations Manager i; Software Version: 10.11; OMi Extensibility Guide; Document Release Date: 25 May 2016; Software Release Date: May 2016
HPE Operations Manager i; Software Version: 10.11; OMi FIPS Configuration Guide; Document Release Date: 25 May 2016; Software Release Date: May 2016
HPE Operations Manager i; Software Version: 10.11; OMi Database Guide; Document Release Date: 25 May 2016; Software Release Date: May 2016
HPE Operations Manager i; Software Version: 10.11; RTSM Administration Guide; Document Release Date: May 2016; Software Release Date: May 2016
HPE Operations Agent; Software Version: 12.01; Reference Guide; Document Release Date: May 2016; Software Release Date: May 2016
HPE Operations Agent and Infrastructure SPIs; Software Version: 12.01; Installation Guide; Document Release Date: May 2016; Software Release Date: May 2016
HPE Operations Agent; Software Version: 12.01; User Guide; Document Release Date: May 2016; Software Release Date: May 2016
HPE Operations Bridge Reporter; Software Version: 10.01; Administration Guide; Document Release Date: June 2016; Software Release Date: June 2016
HPE Operations Bridge Reporter; Software Version: 10.01; Configuration Guide; Document Release Date: June 2016; Software Release Date: June 2016
HPE Operations Bridge Reporter; Software Version: 10.01; Release Notes; Document Release Date: May 2017; Software Release Date: June 2016

[24] ISO – International Organization for Standardization
[25] PDF – Portable Document Format

Hewlett Packard Enterprise Development LP; HPE Operations Bridge Premium v2016.05 including HPE Operations Manager i v10.11, HPE Operations Agent v12.01, and HPE Operations Bridge Reporter v10.01; Security Target; Evaluation Assurance Level (EAL): EAL2+ v1.2 (This document)
Hewlett Packard Enterprise Development LP; HPE Operations Bridge Premium v2016.05 including HPE Operations Manager i v10.11, HPE Operations Agent v12.01, and HPE Operations Bridge Reporter v10.01; Guidance Documentation Supplement Document; Evaluation Assurance Level (EAL): EAL2+ v1.1

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
- Communication
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF[26]
- Resource Utilization
- TOE Access
- Trusted Path/Channels
- Data Collection and Analysis

1.5.2.1 Security Audit

The Security Audit functionality provides the capability to generate audit data for HPE OMi security relevant events and records the identity of the subject responsible for initiating the event. TOE users[27] or administrators[28] with sufficient audit log permissions have access to view the audit logs. The TOE prevents any unauthorised deletion and modification of the audit logs.

1.5.2.2 Communication

The Communication functionality ensures that HPE OMi servers distribute certificates to HPE OAs for the secure transmission of configuration and event data. Signatures are applied to configuration payloads sent between the HPE OMi GW server and HPE OAs.

1.5.2.3 Cryptographic Support

The Cryptographic Support functionality utilizes the FIPS-validated RSA BSAFE® Crypto-J Module (software version 6.2.1, cert #2469) for Java based components of HPE OMi and the OpenSSL FIPS Object Module (software version

[26] TSF – TOE Security Functions
[27] "TOE users" refers to users with no administrative privileges.
[28] "Administrators" refers to users with administrative privileges.

2.0.12, cert #1747) for C++ based components of HPE OMi. These FIPS-validated modules are used by the HPE OMi TOE component to perform all cryptographic functions.

HPE OBR also utilizes the FIPS-validated RSA BSAFE® Crypto-J Module (software version 6.2.1, cert #2469) and the OpenSSL FIPS Object Module (software version 2.0.12, cert #1747). The TOE destroys all keys according to the FIPS 140-2 standard (by overwriting with zeroes).

1.5.2.4 User Data Protection

The User Data Protection functionality enforces the Resource Access Control SFP[29] for controlling the access of HPE OMi users to resources. The Resource Access Control SFP is also enforced when exporting event data from HPE OMi servers to targeted systems.

1.5.2.5 Identification and Authentication

The Identification and Authentication functionality requires TOE users and administrators to be identified and authenticated before gaining access to any TOE functionality. The TOE utilizes LDAP and X.509 certificate-based remote authentication.

1.5.2.6 Security Management

The Security Management functionality provides the capability for administrators with authorized roles to manage the security functionality, TSF data, and attributes provided by the TOE. HPE OMi provides the Super-Admin role and custom roles.

1.5.2.7 Protection of the TSF

The Protection of the TSF functionality ensures that the TOE maintains a secure state in the event of an HPE OMi DP server failure. The TOE also ensures that event data is protected from disclosure or modification when transferred internally between TOE components.

1.5.2.8 Resource Utilization

The Resource Utilization functionality provides the capability for the TOE to perform automatic failover procedures to ensure that all capabilities of the TOE are still operational in the event of an HPE OMi DP server failure.

1.5.2.9 TOE Access

The TOE Access functionality ensures that an advisory TOE access banner is displayed on the HPE OMi Web UI and HPE and OBR Admin console warning the TOE user or administrator against unauthorised access.

1.5.2.10 Trusted Path/Channels

The Trusted Path/Channels functionality provides Inter-TSF trusted channels for LDAP authentication via LDAP/S connections, HPE OMi external database communications via JDBC over TLS, and HPE OBR external database communications via JDBC over TLS. This functionality also provides a trusted path for HTTPS connections from TOE user or administrator workstations to the HPE OMi Web UI and HPE OBR Admin console interface.

1.5.2.11 Data Collection and Analysis

The Data Collection and Analysis functionality provides the capability for the TOE to monitor systems and gather event data. After the event data is gathered, the TOE performs an analysis of the event data to discover potential

[29] SFP – Security Function Policy

security violations. Event data is stored in an embedded or external database and the TOE does not allow deletion or modification of event data by unauthorised TOE users.

2. Conformance Claims

This section and Table 4 provide the identification for any CC, PP, and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.

Table 4 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 4, September 2012; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 11/15/2017 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ Augmented with Flaw Reporting Procedures (ALC_FLR.2)

3. Security Problem

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

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

3.1 Threats to Security

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

- TOE users: Authorized users who may misuse the TOE.
- Attacker who is not a TOE user: entities that have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources for attempting to tamper with the TOE, and have no physical access to the TOE.
- Operational conditions that cause the operation of the TOE to be interrupted as a result of hardware failures (e.g. power supplies, storage media, etc.) or software failures, where the source of the threat is non-human.

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4.1. Table 5 below lists the applicable threats.

Table 5 – Threats

Name	Description
T.DATA_AVAILABILITY	TOE data or capabilities may become unavailable due to DP server failures caused by an attacker who is not a TOE user (e.g. performing a denial of service attack), or an operational condition (power failures, etc.).
T.ADMIN_ERROR	A TOE user may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.AUDIT_COMPROMISE	An attacker who is not a TOE user may view audit records cause audit records to be lost or modified, or prevent future records from being recorded, thus masking an attacker who is not a TOE user's actions.
T.BAD_STATE	An attacker who is not a TOE user may exploit vulnerabilities in monitored IT entities that reach an insecure state without the network administrators becoming aware.
T.DATA_COMPROMISE	An attacker who is not a TOE user may read, modify, delay, or destroy security critical TOE configuration data stored on the TOE or being transmitted between physically separated parts of the TOE.
T.UNAUTHORISED_ACCESS	A TOE user may gain unauthorised access (view, modify, delete) to user data through possible misuse.

3.2 Organizational Security Policies

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

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 6 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 – Assumptions

Name	Description
A. AUTH	The TOE environment will provide the identification and authentication repository of users attempting to manage and use the TOE.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains. Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner.
A.LOCATE	The TOE, and all components of the TOE environment, including the authentication servers and database servers are located within a controlled access facility and appropriately located within the network to perform their functions. The devices with which the TOE communicates for exporting events are also located within a controlled access facility. Administrative and user workstations are located within a separate controlled access facility.
A.OS_ACCESS	The TOE environment is in a secure state and provides a sufficient level of protection to itself and the TOE components.
A.PROTECT	The TOE software will be protected from unauthorised modification.
A.NOEVIL	The administrators and users of the TOE are non-hostile, appropriately trained, and follow all guidance.
A.SECURE_COM	The TOE environment provides the necessary network infrastructure required for its operation and ensures the TOE is secured and protected from interference or tampering by using a firewall to prevent access from non-trusted entities. Additionally, the TOE environment provides a sufficient level of protection to secure communications between the TOE and network-attached devices within the secure access facility.
A.TIMESTAMP	The TOE environment provides the TOE with the necessary reliable timestamps.
A.ADMIN_PROTECT	The workstations in the TOE environment used to access the TOE are free of malicious software.

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 7 below.

Table 7 – Security Objectives for the TOE

Name	Description
O.BANNER	The TOE will provide a mechanism that warns against unauthorised use of the TOE.
O.FAIL_SECURE	The TOE will preserve a secure state and ensure that all capabilities of the TOE are still operational in the event of a DP server failure.
O.MONITOR	The TOE must be able to monitor machines on the network to ensure that they exist in a secure state and alert administrators if a system enters an insecure state. The TOE will also analyze and securely store the scanned and collected data.
O.PROTECT	The TOE will provide confidentiality and integrity services using FIPS 140-2 algorithms to protect TOE communication channels and user data. The TOE will also provide confidentiality of stored keys and keys used for cryptographic services performed by the TOE.
O.ACCESS	The TOE will ensure that TOE users and administrators gain only authorized access to it and to resources that it controls.
O.AUDIT	The TOE will provide the capability to detect security relevant events and create records of those events in the audit trail. The TOE will also ensure that the audit records remain available in the event of a failure and are protected from unauthorised modification and deletion.
O.AUDIT_REVIEW	The TOE will provide the capability for only authorized TOE users to view audit information.
O.USER_AUTHEN	The TOE will uniquely identify and authenticate TOE users and administrators prior to allowing access to TOE functions and data.
O.TOE_ADMIN	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE. The TOE will also provide the functions necessary to support the administrators operating the TOE and protections for logged-in administrators.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

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

Table 8 – IT Security Objectives

Name	Description
OE.TIMESTAMP	The TOE environment must provide reliable timestamps to the TOE.
OE.NET_CON	The TOE environment must be implemented such that the TOE is appropriately located within and connected to the network to perform its intended function.
OE.AUTH	The TOE environment must provide the authentication and identification repository of users attempting to use the TOE.
OE.OS_ACCESS	The operating system upon which the TOE is installed provides a sufficient level of protection for itself and the TOE software it contains.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference and tampering.
OE.SECURE_COM	The TOE environment must provide mechanisms to secure communications between TOE components and other devices to which the TOE is attached (including routers, switches, cabling, connectors, and firewalls) and must be properly implemented such that the TOE is secured and protected from interference or tampering. Firewalls must be configured to restrict all external access from outside the internal network where the TOE is accessible.
OE.ADMIN_PROTECT	The administrative and user workstations must be protected from any external interference and tampering by having all security updates and anti-malware software installed.

4.2.2 Non-IT Security Objectives

Table 9 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 9 – Non-IT Security Objectives

Name	Description
OE.MANAGE	The TOE environment will provide competent, non-hostile administrators and users of the TOE who are appropriately trained and follow all administrator and user guidance. Administrators of the TOE will ensure the system is used securely.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

5. Extended Components

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

5.1 Extended TOE Security Functional Components

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

Table 10 – Extended TOE Security Functional Requirements

Name	Description
FDC_SCN.1	System scan
FDC_ANA.1	System analysis
FDC_STG.1	Scanned data storage

5.1.1 Class FDC: Data Collection and Analysis

Data Collection and Analysis functions involve:

- Monitoring systems to obtain data,
- Storing the collected data,
- Performing analysis on collected data and presenting analytical results and reports to administrators in a format that allows them to take appropriate actions.

The FDC: Data Collection and Analysis class was modeled after the CC FAU: Security Audit class. The extended family and related components for FDC_ANA: System Analysis were modeled after the CC family and related components for FAU_SAA: Security Audit Analysis. The extended family FDC_SCN: System Scan was modeled after the CC family FAU_GEN: Security Audit Data Generation. The extended family FDC_STG: Scanned Data Storage was modeled after the CC family FAU_STG: Security Audit Event Storage.

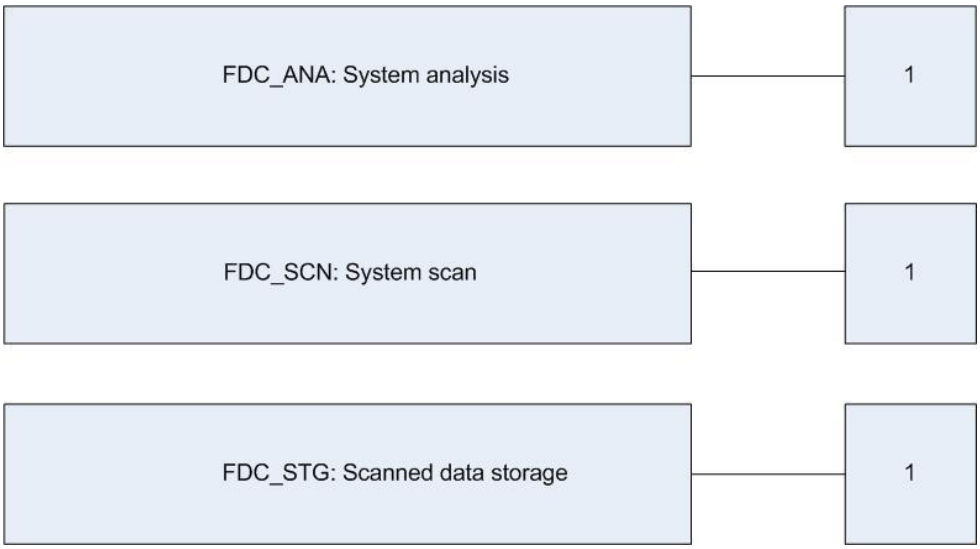

Figure 2 – FDC: Data Collection and Analysis Class Decomposition

5.1.1.1 FDC_ANA: System analysis

Family Behavior

This family defines the requirements for the use of analysis procedures that allow administrators to react to potential security violations found during collected data analysis.

Component Leveling

Figure 3 – System analysis family decomposition

FDC_ANA.1: System Analysis provides the capability to analyze collected data and present the results to administrators in a way that easily allows the administrators to respond to potential security violations found during the analysis.

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

- Maintenance (deletion, modification, addition) of the analysis rules or the set of systems the rules are applied to.

Audit: FDC_ANA.1 System Analysis

- There are no auditable events foreseen.

FDC_ANA.1 System analysis

Hierarchical to: **No other components.**

Dependencies: **FDC_SCN.1 System scan**

FDC_ANA.1.1

The TSF shall be able to apply a set of rules in analyzing collected event data and based upon these rules indicate potential security violations:

a) Calculate a status for correlated and processed event data

FDC_ANA.1.2

The TSF shall enforce the following set of rules for monitoring scanned event data: Accumulation or combination of [assignment: *subset of defined collected data*] known to indicate a potential security violation; [assignment: *any other rules*].

FDC_ANA.1.3

The TSF shall be able to indicate a possible security violation to [assignment: *list of TOE users or administrators with permission to review analytical results*] and allow [assignment: *list of TOE users or administrators with permission to modify user and security configurations*] to address security violations that are discovered.

5.1.1.2 FDC_SCN: System scan

Family Behavior

This family defines the requirements for monitoring systems to collect event data.

Component Leveling

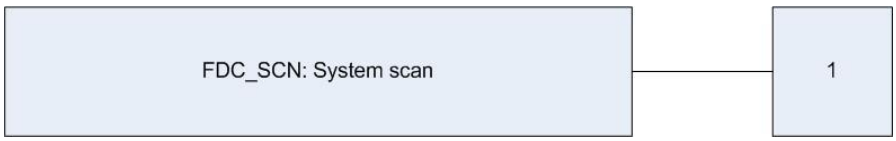

Figure 4 – System scan family decomposition

FDC_SCN.1 System Scan defines the monitoring function and specifies which machines will be monitored.

Management: FDC_SCN.1

- There are no management activities foreseen.

Audit: FDC_SCN.1

- There are no auditable events foreseen.

FDC_SCN.1 System scan

Hierarchical to: **No other components.**

Dependencies: **No dependencies**

FDC_SCN.1.1

The system shall be able to monitor and collect the following information from the targeted IT system resource(s):

- Event data from monitored processes, files, metrics, and systems
- System health information from monitored systems
- Event topology information from monitored systems

FDC_SCN.1.2

The TSF shall record within the event database at least the following information:

- Date and time of event occurrence
- Host system where the event occurred
- Application that caused the event
- Event severity
- Administrator responsible for solving the problem that caused the event (if assigned)

5.1.1.3 FDC_STG: Scanned data storage

Family Behavior

This family defines the requirements for protecting stored event data.

Component Leveling

Figure 5 – Scanned data storage family decomposition

FDC_STG.1 Scanned Data Storage defines how the TSF protects stored monitor data from unauthorised modification or deletion.

Management: FDC_STG.1

- There are no management activities foreseen.

Audit: FDC_STG.1

- There are no auditable events foreseen.

FDC_STG.1 Scanned data storage

Hierarchical to: **No other components.**
Dependencies: **FDC_SCN.1 System scan**

FDC_STG.1.1

The TSF shall protect the stored collected data from unauthorised deletion.

FDC_STG.1.2

The TSF shall be able to prevent unauthorised modifications to the stored collected data.

FDC_STG.1.3

The TSF shall ensure the storage of scanned data in the event of a [*assignment: storage failure*] by performing the following actions: [*assignment: list of actions used to ensure data is not lost in the event of a storage failure*].

FDC_STG.1.4

The TSF shall indicate a failure to store collected data by performing the following actions: [assignment: *list of actions that are used to notify administrators of a storage failure*].

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this ST.

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.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

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

Table 11 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	*Audit data generation*	✓	✓		
FAU_SAR.1	*Audit review*		✓		
FAU_STG.2	*Guarantees of audit data availability*	✓	✓	✓	
FCO_NRO.1	*Selective proof of origin*	✓	✓		
FCS_CKM.1	*Cryptographic key generation*		✓		
FCS_CKM.4	*Cryptographic key destruction*		✓		
FCS_COP.1	*Cryptographic operation*		✓		
FDP_ACC.1	*Subset access control*		✓		
FDP_ACF.1	*Security attribute based access control*		✓		
FDP_ETC.1	*Export of user data without security attributes*		✓		

Name	Description	S	A	R	I
FIA_UAU.2	*User authentication before any action*				
FIA_UAU.5	*Multiple authentication mechanisms*		✓		
FIA_UID.2	*User identification before any action*				
FMT_MOF.1	*Management of security functions behaviour*	✓	✓		
FMT_MSA.1	*Management of security attributes*	✓	✓		
FMT_MSA.3	*Static attribute initialisation*	✓	✓		
FMT_SMF.1	*Specification of management functions*		✓		
FMT_SMR.1	*Security roles*		✓		
FPT_FLS.1	*Failure with preservation of secure state*		✓		
FPT_ITT.1	*Basic internal TSF data transfer protection*	✓			
FRU_FLT.1	*Degraded fault tolerance*		✓		
FTA_TAB.1	*Default TOE access banners*				
FTP_ITC.1	*Trusted channel*	✓	✓		
FTP_TRP.1	*Trusted path*	✓	✓		
FDC_ANA.1	*System analysis*		✓		
FDC_SCN.1	*System scan*				
FDC_STG.1	*Scanned data storage*		✓		

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

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

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

FAU_GEN.1.1

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

a. Start-up and shutdown of the audit functions;
b. All auditable events, for the [not specified] level of audit; and
c. [
   - *HPE OMi user and administrator logins*
   - *HPE OMi user and group management actions*
   - *HPE OMi configuration changes*
   - *HPE OMi changes to events (configurable)*
   - *HPE OMi failed authentication attempts*

   ].

FAU_GEN.1.2

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

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

Application Note: The outcome (success or failure) of HPE OMi user and group management actions and HPE OMi changes to events (configurable) is implied and not explicitly stated in the audit records

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 [*TOE users and administrators with sufficient Setup and Maintenance (Audit Log) permissions*] with the capability to read [*all 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_STG.2 Guarantees of audit data availability

Hierarchical to: FAU_STG.1 Protected audit trail storage
Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.2.1

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

FAU_STG.2.2

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

FAU_STG.2.3

The TSF shall ensure that [*HPE OMi*] stored audit records will be maintained when the following conditions occur: [**Server** failure].

6.2.2 Class FCO: Communication

FCO_NRO.1 Selective proof of origin

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FCO_NRO.1.1

The TSF shall be able to generate evidence of origin for transmitted [*HPE OA policies*] at the request of the [recipient].

FCO_NRO.1.2

The TSF shall be able to relate the [*public key, certificate*] of the originator of the information, and the [*SHA[30]-2 digest]* of the information to which the evidence applies.

FCO_NRO.1.3

The TSF shall provide a capability to verify the evidence of origin of information to [recipient] given [*validity of the certificate*].

[30] SHA – Secure Hash Algorithm

6.2.3 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 [*key generation using a deterministic random number generator*] and specified cryptographic key sizes [*128- and 256-bit; 112-bit; 2048-bit*] that meet the following: [*none*].

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 standard 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.1.1a

The TSF shall perform [*list of cryptographic operations in Table 12 and Table 13*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms listed in Table 12 and Table 13*] and cryptographic key sizes [*key sizes listed in Table 12 and Table 13*] that meet the following: [*none*].

Table 12 – RSA BSAFE® Crypto-J JSAFE and JCE Software Module 6.2.1 Cryptographic Operations

Algorithm	Cert #
Symmetric Key Algorithms	
AES CBC, GCM modes for 128- and 256-bit key sizes	#3263
Triple-DES CBC, for keying option one (three different keys)	#1852
Digital Signature Algorithms	
RSA X9.31, PKCS#1 V.1.5, RSASSA-PSS Signature generation; Signature verification –2048-bit	#1663
ECDSA Signature generation for all NSA Suite B P, K, and B Curves, Signature Verification for all P, K, and B curves.	#619
Key Generation Algorithms	

Algorithm	Cert #
HMAC DRBG (HMAC-SHA-256)	#722
Hashing Functions	
SHA-1, SHA-256, SHA-384	#2701
MAC Functions	
HMAC with SHA-1, SHA-256, SHA-384	#2062

Table 13 – OpenSSL FIPS Object Module 2.0.12 Cryptographic Operations

Algorithm	Cert #
Symmetric Key Algorithms	
AES CBC, GCM modes for 256-bit key sizes	#2484
Digital Signature Algorithms	
RSA X9.31, PKCS#1 V.1.5, RSASSA-PSS Signature generation; Signature verification –2048-bit	#1273
ECDSA Signature generation for all NSA Suite B P, and K Curves, Signature Verification for all B, P, and K Curves.	#413
Key Generation Algorithms	
CTR DRBG (AES-256)	#342
Hashing Functions	
SHA-1, SHA-256, SHA-384	#2102
MAC Functions	
HMAC with SHA-1, SHA-256, SHA-384	#1526

6.2.4 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1

The TSF shall enforce the [*Resource Access Control SFP*] on [

Subjects:

- *HPE OMi TOE users*

Objects:

- *HPE OMi Web UI resource – Workspaces*
- *HPE OMi Web UI resource – Event Processing*
- *HPE OMi Web UI resource – Monitoring*
- *HPE OMi Web UI resource – Operations Console*
- *HPE OMi Web UI resource – Service Health*

Permissions by category displayed in Table 14 below:

Table 14 – Resource Permissions

TOE Component	Resource	Subset	Permissions
HPE OMi	*Web UI (Workspaces)*	*Predefined Pages*	*All, None*
		User Components	*Change, Delete, View, Add, All, None*
		User Pages	*Locked, Change, Delete, View, All, None*
HPE OMi	*Web UI (Event Processing)*	*Automation*	*All, Add, None*[31]
		Correlation	*All, None*
HPE OMi	*Web UI (Monitoring)*	*Assignments & Tuning* *Automatic Assignment Rules* *Deployment Jobs* *Management Templates & Aspects* *Policy Templates*	*All, None*
HPE OMi	*Web UI (Operations Console)*	*Custom Actions (Execution)* *Run Book Execution* *Tools (Execution)*	*Execute, All, None*
		Custom Actions (Administration) *Monitoring Dashboards* *Monitoring Dashboards (Administration)* *External Instructions* *Performance Graph Mappings* *ROI Dashboard*	*All, None*

[31] The "Event Submission" sub-category of the Event Processing/Automation Web UI resource can only be assigned the "Add" or "None" permissions. The remaining sub-categories can be assigned "All" or "None" permissions.

TOE Component	Resource	Subset	Permissions
		Tools (Administration) *View Mappings* *Design Graphs*	
		Events	*Change Properties* [32] *, Life Cycle Operations*[33]*, Launch Actions*[34]*, View, All, None*
		Event Browser	*Clear View Filter, Share Filters, None*
		Run Book Mappings	*Change, Delete, View, Add, All, None*
HPE OMi	*Web UI (Service Health)*	*Alerts*	*Change, None*
		Downtime Management	*View, All, None*
		Repositories	*Reset, None*

].

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 [*Resource Access Control SFP*] to objects based on the following: [
Subject Attributes:

- *HPE OMi user role/permissions*

Object Attributes:

- *Resource permissions for the following:*
  - *HPE OMi Web UI – Workspaces*
  - *HPE OMi Web UI – Event Processing*
  - *HPE OMi Web UI – Monitoring*
  - *HPE OMi Web UI – Operations Console*
  - *HPE OMi Web UI – Service Health*

].

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 TOE user or administrator is granted access to perform an operation on a resource based on the associated role/permissions within the TOE. Otherwise, access is denied and the operation is unavailable to the user*].

FDP_ACF.1.3

[32] "Change Properties" includes "Priority", "Solution", "Title", "Custom Attributes", "Description", "Severity", "Event Relations", and "Annotations".

[33] "Life Cycle Operations" includes "Assign To", "Close" "Close Transferred", "Transfer Control", "Work On/Resolve", and "Reopen" permissions.

[34] "Launch Actions" includes "Operation Action" and "Automatic Action" permissions.

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

FDP_ACF.1.4

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

FDP_ETC.1 Export of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ETC.1.1

The TSF shall enforce the [*Resource Access Control SFP*] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2

The TSF shall export the user data without the user data's associated security attributes.

6.2.5 Class FIA: Identification and Authentication

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.

Application Note: This SFR applies to the HPE OMi Web UI and HPE OBR Admin console.

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.
Dependencies: No dependencies

FIA_UAU.5.1

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

FIA_UAU.5.2

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

- *verification of stored credential information for LDAP authentication*
- *verification of stored X.509 certificates for certificate-based authentication*

].

Application Note: This SFR applies to the HPE OMi Web UI and HPE OBR Admin console.

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.

Application Note: This SFR applies to the HPE OMi Web UI and HPE OBR Admin console.

6.2.6 Class FMT: Security Management

FMT_MOF.1 Management of security functions behavior

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 [modify the behavior of] the functions [

- *Audit configuration*
- *Authentication management*
- *Event lifecycle management*
- *User management*
- *Automatic Failover configuration*
- *Reports and content pack configuration*

to [*authorized users with sufficient permissions or the Super-Admin role*].

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1

The TSF shall enforce the [*Resource Access Control SFP*] to restrict the ability to [modify, delete, [*add*]] the security attributes [*role, permissions*] to [*authorized users with sufficient permissions or Super-Admins*].

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

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

FMT_MSA.3.1

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

FMT_MSA.3.2

The TSF shall allow the [*authorized users with sufficient permissions or Super-Admins*] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No Dependencies

FMT_SMF.1.1

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

- *Manage the Resource Access Control SFP*
- *Configure event monitoring settings*
- *Manage audit configuration data*
- *Manage users and roles*

- *Manage authentication data*
- *Configure automatic failover settings*
- *Configure event automation and correlation settings*
- *OBR Management and configuration tasks*
- *Node/OA Management and configuration tasks*
- *Configure reports, content packs, packages, and management packs*

]

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 [

HPE OMi

- *Super-Admin role*
- *Custom roles*

].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.7 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [*DP server failure*].

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_ITT.1.1

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

6.2.8 Class FRU: Resource Utilization

FRU_FLT.1 Degraded fault tolerance

Hierarchical to: No other components.

Dependencies: FPT_FLS.1 Failure with preservation of secure state

FRU_FLT.1.1

The TSF shall ensure the operation of [*all TOE capabilities*] when the following failures occur: [*DP server failure*].

6.2.9 Class FTA: TOE Access

FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_TAB.1.1

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

6.2.10 Class FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_ITC.1.1

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

FTP_ITC.1.2

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

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [

- *LDAP authentication (LDAP/S)*
- *HPE OMi connections to the external databases (JDBC over TLS[35])*
- *HPE OBR connections to the external databases (JDBC over TLS)*

].

Application Note: Functions listed in FTP_ITC.1.3 are all initiated by the TOE.

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 [[*HTTPS connections to the HPE OMi Web UI, HPE OBR Admin console*]].

[35] TLS – Transport Layer Security

6.2.11 Class FDC: Data Collection and Analysis

FDC_ANA.1 System analysis

Hierarchical to: **No other components.**
Dependencies: **FDC_SCN.1 System scan**

FDC_ANA.1.1

The TSF shall be able to apply a set of rules in analyzing collected event data and based upon these rules indicate potential security violations:

b) Calculate a status for correlated and processed event data

FDC_ANA.1.2

The TSF shall enforce the following set of rules for monitoring scanned event data: Accumulation or combination of [*event data*] known to indicate a potential security violation; [*Suppress duplicated events; correlate events by analyzing relationships between CIs; trigger notifications; forward events; execute automated administrator-defined actions*].

FDC_ANA.1.3

The TSF shall be able to indicate a possible security violation to [*authorized TOE users with sufficient "Service Health" and "Operations Console" permissions*] and allow [*authorized administrators*] to address security violations that are discovered.

FDC_SCN.1 System scan

Hierarchical to: **No other components.**
Dependencies: **No dependencies**

FDC_SCN.1.1

The system shall be able to monitor and collect the following information from the targeted IT system resource(s):

- Event data from monitored processes, files, metrics, and systems
- System health information from monitored systems
- Event topology information from monitored systems

FDC_SCN.1.2

The TSF shall record within the event database at least the following information:

- Date and time of event occurrence
- Host system where the event occurred
- Application that caused the event
- Event severity
- Administrator responsible for solving the problem that caused the event (if assigned)

FDC_STG.1 Scanned data storage

Hierarchical to: **No other components.**
Dependencies: **FDC_SCN.1 System scan**

FDC_STG.1.1

The TSF shall protect the stored collected data from unauthorised deletion.

FDC_STG.1.2

The TSF shall be able to prevent unauthorised modifications to the stored collected data.

FDC_STG.1.3

The TSF shall ensure the storage of scanned data in the event of a [*database outage*] by performing the following actions: [

- *Buffer events until server is reachable again*
- *When server is reachable, send events in correct order*
- *When events are received on server, store events in a persistent queue*
- *Remove events from queue only after events are stored in database*

].

FDC_STG.1.4

The TSF shall indicate a failure to store collected data by performing the following actions: [*Create event that notifies an authorized TOE user or administrator that there is a problem if no keep alive messages are received by the HPE OMi server from the HPE* OA*. If the HPE OMi server does not allow the creation of an event for notification, an authorized TOE user or administrator will be notified by email*].

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 these 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_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7. TOE Summary Specification

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

7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 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_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_STG.2	Guarantees of audit data availability
Communication	FCO_NRO.1	Selective proof of origin
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_ETC.1	Export of user data without security attributes
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITT.1	Basic internal TSF data transfer protection
Resource Utilization	FRU_FLT.1	Degraded fault tolerance
TOE Access	FTA_TAB.1	Default TOE access banners
Trusted path/channels	FTP_ITC.1	Trusted channel
	FTP_TRP.1	Trusted path

TOE Security Functionality	SFR ID	Description
Data Collection and Analysis	FDC_ANA.1	System analysis
	FDC_SCN.1	System scan
	FDC_STG.1	Scanned data storage

7.1.1 Security Audit

The following sections describe the HPE OMi audit functionality.

7.1.1.1 HPE OMi Security Audit

HPE OMi records audits for successful and failed TOE user login attempts, user and group management actions, configuration changes, and changes to events (configurable). These audit logs include the modification date, TOE user, actions, and additional information fields. Although the TOE does not audit the startup and shutdown of the audit function, it does audit the startup and shutdown of the TOE, thereby indicating when the audit function is started and stopped as well.

The log viewer is available from the HPE OMi Web UI and is restricted to authorized roles based on permission. HPE OMi prevents unauthorised deletion/modification of the audit trail. The TOE contains the following HPE OMi audit log contexts in Table 17 below:

Table 17 – Audit Log Contexts

Audit Log Context	Description
CI Status Alert Administration	Displays actions related to creating alert schemes for a CI status alert.
Downtime/Event Scheduling	Displays actions related to creating and modifying downtime and scheduled events.
Infrastructure Settings	Displays actions related to modifying infrastructure settings. The result of each action is denoted as SUCCESS or FAILURE.
Login	Displays actions related to users' logins and logouts. The result of each action is denoted as SUCCESS or FAILURE.
Notification Template Administration	Displays actions related to modifying open ticket information, ticket settings, closed tickets, ticket templates, and subscription information: notification types (locations or general messages), and recipients.
Operations Management	Displays actions related to Operations Management, such as the creating and modifying of content packs, event rules, and notifications. This audit log can be configured to log the following changes: • Configuration – This is selected by default and ensures that only configuration changes are written to the audit log. • All – This setting ensures both event and configuration changes are written to the audit log.
Recipient Administration	Displays actions related to modifying information and general notifications.
Service Health	Displays actions related to the Service Health application.
Service Health Administration	Displays actions related to configurations made in Service Health Administration.
Startup/Shutdown	Displays actions related to startups and shutdowns of OMi host systems.

Audit Log Context	Description
User/Group Management	Displays actions related to adding, modifying, and deleting TOE users, TOE user groups, and roles. Additionally, it displays the assignments of permissions to roles and the assignments of roles to TOE users and TOE user groups.
View Manager	Displays actions related to KPIs such as adding a KPI, editing a KPI, and deleting a KPI. Additionally, it displays actions related to changing the Save KPI data over time for this CI option.

Table 18 below describes the configuration changes and actions written to the User/Group Management audit log:

Table 18 – User/Group Management Configuration Changes

Configuration Change	Action
Assigning Permissions to Roles	Create, edit, and delete
Role	Create, edit, and delete
TOE user	Create, edit, and delete
TOE user Group	Create, edit, and delete

The Operations Management audit log contains configuration and event changes. Table 19 below contains the type of event changes that are written to the Operations Management audit log:

Table 19 – Operations Management Event Changes

Event Change	Action
Action	Launch
Custom attributes	Create, edit, and delete
Annotations	Create, edit, and delete
Assign event to TOE user or group	Change
Event title	Edit
Forwarding actions	Launch
Lifecycle state of event	Change
opr-archive-events.bat, opr-close-events.bat	Launch
Priority of event	Change
Automatic or operator action	Rerun
Severity of event	Change
Tool	Launch

Table 20 below contains the type of configuration changes that are written to the Operations Management audit log:

Table 20 – Operations Management Configuration Changes

Configuration Change	Action
CI Resolver Mapping	Create, edit, and delete
Connected Server	Create, edit, and delete
Content Packs	Create, edit, delete, import, and export
Custom Action Configurations	Create, edit, and delete
Downtime Configuration	Create, edit, and delete
EPI[36] Configuration	Create, edit, and delete
Event Assignment Rules	Create, edit, and delete
Event Forwarding	web service-triggered actions using the console API
Filters	Create, edit, and delete
Forwarding Rules	Create, edit, and delete
Indicator Mapping Rules	Create, edit, and delete
Monitoring Automation: Aspect Versions	Create and delete
Monitoring Automation: Assignments	Create, delete, and change. Changes include disabling and enabling assignments, and changing parameter values.
Monitoring Automation: Automatic Assignments	Create and delete
Monitoring Automation: Configuration Folders	Create, delete, and change deployment
Monitoring Automation: Deployment Packages	Create and delete
Monitoring Automation: Instrumentations	Create, delete, and change
Monitoring Automation: Jobs	Create, delete, and change
Monitoring Automation: Management Template Versions	Create and delete
Monitoring Automation: Node Groups	Create, delete, and change Changes including adding a node to and removing a node from a node group
Monitoring Automation: Node Filters	Create, delete, and change
Monitoring Automation: Nodes	Create, delete, and change

[36] EPI – Event Processing Interface

Configuration Change	Action
Monitoring Automation: Template Groups	Create, delete, and change Changes include adding a template to or removing a template from a template group.

In addition, audit configuration changes (change, enable, and disable), are written to the Infrastructure Settings audit log.

The audit logs use the Apache log4j logging utility. Audit logs are stored in the external database, and the TOE does not provide delete/modify operations in the UI.

Audit logs are retained for an administrator-defined period between 90 and 350 days. If a value is not set, the logs are retained indefinitely.

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

7.1.2 Communication

HPE OMi maintains an internal PKI[37] which distributes certificates to HPE OAs for secure transmission of configuration and event data. Signatures are applied to configuration payloads sent to HPE OAs from HPE OMi using the HPE OMi server's private key.

TOE Security Functional Requirements Satisfied: FCO_NRO.1.

7.1.3 Cryptographic Support

HPE OMi utilizes the FIPS 140-2 validated RSA BSAFE® Crypto-J JSAFE and JCE Software Module (software version 6.2.1) and the OpenSSL FIPS Object Module (software version 2.0.12) libraries for performing all cryptographic operations. All HPE OMi cryptographic operations (including HTTPS/TLS support, TLS encrypted JDBC, internal X.509 PKI infrastructure, AES encryption of third-party credentials, agent configuration payload signatures, key generation/derivation, password hashing, and other cryptography related functions) are used according to the RSA BSAFE® Crypto-J Module or OpenSSL FIPS Object Module "FIPS-Mode" configuration as dictated by their respective Security Policies. HPE OMi uses SHA-2 algorithms for cryptographic signatures and supports TLS 1.2 cipher suites.

HPE OBR also uses the FIPS 140-2 validated RSA BSAFE® Crypto-J JSAFE and JCE Software Module (software version 6.2.1) and the OpenSSL FIPS Object Module (software version 2.0.12) for the HPE OBR cryptographic operations. All of the modules utilized by the TOE destroy all keys by overwriting them with zeros.

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

[37] PKI – Public Key Infrastructure

7.1.4 User Data Protection

The TOE enforces the Resource Access Control SFP on subjects (HPE OMi TOE users) accessing objects (HPE OMi Web UI resources). The HPE OMi Web UI resources include the Workspaces, Event Processing, Monitoring, Operations Console, and Service Health areas of the HPE OMi Web UI. The Resource Access Control SFP allows TOE users to gain access to the HPE OMi Web UI resources only if the TOE user has the correct permissions (determined by their role) for the resource. Access control parameters differ according to the resource area of the HPE OMi Web UI. These access control parameters are listed in Table 14.

Integrations with 3rd party products allow the exportation of events to other systems. The exportation of events to other systems is under the enforcement of the Resource Access Control SFP and is only allowed if the TOE user has the correct permissions (determined by their role) for the HPE OMi Web UI's "Operations Console – Events" resource.

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

7.1.5 Identification and Authentication

The HPE OMi Web UI and HPE OBR Admin console provide the Identification and Authentication functionality of the TOE. These user interfaces use certificate-based authentication and LDAP authentication to authenticate credentials passed by TOE users. Besides being used for authentication, LDAP is also used to synchronize HPE OMi users and groups with users and groups configured on the external LDAP server.

Prior to authenticating via the HPE OMi Web UI or HPE OBR Admin console, TOE users and administrators are not given access to any TOE functionality. TOE users and administrators must pass valid credentials to the TOE for authentication to be successful.

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

7.1.6 Security Management

HPE OMi provides the Super-Admin role and custom roles. A default administrative account named "admin" with Super-Admin privileges is provided after initial configuration of the TOE. The Super-Admin role includes full access permissions for TOE management functions. Custom roles are created by authorized administrators based on a set of granular permissions and are mapped to a TOE user or group. By default, TOE users have no access to the TOE until they are assigned to a role with permissions by an authorized role.

HPE OMi allows authorized roles with sufficient management permissions to perform the following administrative functions:

- Manage the Resource Access Control SFP
- Configure event monitoring settings
- Manage audit configuration data
- Manage users and roles
- Manage authentication data
- Configure automatic failover settings

- Configure event automation and correlation settings
- OBR Management and configuration tasks
- Node/OA Management and configuration tasks
- Configure reports, content packs, packages, and management packs

The OBR management and configuration tasks include performing restoration, updates, configuring pollers, creating databases, adding licenses, managing dimensions, and processing downtime information. The node/OA management and configuration tasks include managing the monitoring components, policies, notifications, and related certificates.

Only authorized Super-Admin roles or users with sufficient permissions can modify the behavior of audit configuration, authentication management, event lifecycle management, user management, reports and content pack configuration, or automatic failover configuration. Additionally, Super-Admin roles or users with sufficient permissions can modify, delete, add, or change the default of the security attributes required by the Resource Access Control SFP.

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

7.1.7 Protection of the TSF

The TOE utilizes cryptographic services to secure communications between distributed components of the TOE. These secure communications prevent unauthorised disclosure and modification of TSF data. The TOE uses:

- HTTPS for communication between HPE OMi GW server and HPE OAs
- JMS for communication between the HPE OMi GW server and HPE OMi DP server
- HTTPS for communication between HPE OBR Remote Collector and the HPE OMi RTSM (of the HPE OMi GW server)
- HTTPS for communication between HPE OBR Remote Collector and the HPE OAs
- HTTPS for communication between HPE OBR Remote Collector and the HPE OBR server

HPE OAs communicate with the HPE OMi GW server via the GW communication broker. This HTTPS connection is secured by the FIPS 140-2 validated OpenSSL library (referred to in section 7.1.3). The FIPS 140-2 validated RSA BSAFE® Crypto-J library (referred to in section 7.1.3) is used to secure communications between the HPE OMi GW server and HPE OMi DP server.

The TOE also maintains a secure state of operation by continuing to offer all of its functionality in the event of an HPE OMi DP server failure. The TOE utilizes a backup HPE OMi DP server and automatic failover procedures. The TOE communicates heartbeat information through the DB to the redundant backup server. The HPE OMi DP server HAC regularly checks a table in the DB for updates to determine whether a failover is required. In the event of an HPE OMi DP server failure, the HAC performs automatic failover and moves the services to the backup server. The server retrieves the current configuration from the management database and continues to provide the services as the new active HPE OMi DP server.

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

7.1.8 Resource Utilization

The TOE ensures that all capabilities of the TOE are still operational in the event of an HPE OMi DP server failure. Refer to section 7.1.7 for more information on how the HPE OMi DP server HA[38] procedures help to ensure a minimal impact on performance in the event of an HPE OMi DP server failure.

TOE Security Functional Requirements Satisfied: FRU_FLT.1.

7.1.9 TOE Access

The TOE provides a login banner containing an advisory and consent message regarding unauthorised use of the TOE on the HPE OMi Web UI and HPE OBR Admin console.

TOE Security Functional Requirements Satisfied: FTA_TAB.1.

7.1.10 Trusted Path/Channels

The TOE provides trusted channels between itself and external LDAP or AD servers and external databases that support secure communications. The TOE uses:

- LDAP/S for communication with LDAP or AD servers
- JDBC over TLS for HPE OMi connections to the HPE OMi external database
- JDBC over TLS for HPE OBR connections to the HPE OBR external database
- JDBC over TLS for HPE OBR connections to the HPE OMi external database

The TOE also provides a trusted path using HTTPS connections between TOE user and administrator workstations and the HPE OMi Web UI and HPE OBR Admin console. These protocols all rely on the FIPS 140-2 validated providers referred to in 7.1.3 for their cryptographic algorithms.

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

7.1.11 Data Collection and Analysis

HPE OAs are capable of generating event data from monitored processes, log files, performance metrics, system health information, topology information, and systems. Events have various attributes associated with them including:

- ID
- Severity
- Lifecycle State
- Business Priority
- Assigned TOE user/Group
- Category
- Related CIs

[38] HA – High Availability

- Event type
- Duplicate count
- Timestamps
- Source information

The date and time of event occurrence, host system (node) where the event occurred, application that caused the event, event severity, and the administrator responsible for solving the problem that caused the event (if assigned) are all recorded in the event database. When event data is collected, it is correlated and processed by HPE OMi and a status is calculated. Root cause analysis is performed to identify the source of related events, event duplicates and event storms (multiple events from the same source within a short time frame) are detected, and selected events are suppressed. Events can be used to trigger notifications (email, SMS[39], etc.) or automated administrator-defined actions. Event notifications are restricted to assigned TOE users or groups based the TOE user or group permissions (associated with the TOE user or group's role). Additionally, HPE OMi supports various integrations allowing events to be forwarded to other HPE products or third party help-desk ticketing systems.

HPE OMi regularly checks the health of the connected HPE OAs. The HPE OAs regularly send keep alive messages to HPE OMi. If HPE OMi receives no keep alive messages from an HPE OA for a certain interval, a corresponding event within the HPE OMi will be created that notifies an authorized administrator that there is a problem with the HPE OA. If HPE OMi is not reachable, the HPE OA buffers events until the server is reachable again and then sends them in the correct order. A maximum amount of time/number of events that shall be buffered can be configured by an administrator. When the events are received on the server they are stored in a persistent queue. HPE OMi reads the events from the queue and stores them in the database. Events are removed from the queue only after the events are stored. HPE OMi also includes integrated self-monitoring. If there is a problem detected on HPE OMi which does not allow the creation of an event for notification, HPE OMi sends an e-mail to notify an authorized administrator.

TOE Security Functional Requirements Satisfied: FDC_ANA.1, FDC_SCN.1, FDC_STG.1.

[39] SMS – Short Message Service

8. Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 extended 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 21 below provides a mapping of the objectives to the threats they counter.

Table 21 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.DATA_AVAILABILITY TOE data or capabilities may become unavailable due to DP server failures caused by an attacker who is not a TOE user (e.g. performing a denial of service attack), or an operational condition (power failures, etc.).	O.FAIL_SECURE The TOE will preserve a secure state and ensure that all capabilities of the TOE are still operational in the event of a DP server failure.	O.FAIL_SECURE counters this threat by ensuring that the TOE preserves a secure state and maintains all TOE capabilities in the event of a DP server failure.
	O.MONITOR The TOE must be able to monitor machines on the network to ensure that they exist in a secure state and alert administrators if a system enters an insecure state. The TOE will also analyze and securely store the scanned and collected data.	O.MONITOR counters this threat by ensuring that scanned events will be stored in the event of a database outage by buffering the events and storing them in a queue until the database is available again.
T.ADMIN_ERROR A TOE user may incorrectly install or configure the TOE resulting in ineffective security mechanisms.	O.TOE_ADMIN The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE. The TOE will also provide the functions necessary to support the administrators operating the TOE and protections for logged-in administrators.	O.TOE_ADMIN counters this threat by ensuring that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
T.AUDIT_COMPROMISE An attacker who is not a TOE user may view audit records, cause audit records to be lost or modified, or prevent future records from being recorded, thus masking an attacker who is not a TOE user's actions.	O.AUDIT The TOE will provide the capability to detect security relevant events and create records of those events in the audit trail. The TOE will also ensure that the audit records remain available in the event of a failure and are protected from unauthorised modification and deletion.	O.AUDIT counters this threat by ensuring that unauthorised attempts to access the TOE are recorded.
	O.AUDIT_REVIEW	O.AUDIT_REVIEW counters this threat by ensuring that only authorized TOE users are allowed to view the audit logs.

Threats	Objectives	Rationale
	The TOE will provide the capability for only authorized TOE users to view audit information.	
T.BAD_STATE An attacker who is not a TOE user may exploit vulnerabilities in monitored IT entities that reach an insecure state without the network administrators becoming aware.	O.MONITOR The TOE must be able to monitor machines on the network to ensure that they exist in a secure state and alert administrators if a system enters an insecure state. The TOE will also analyze and securely store the scanned and collected data.	O.MONITOR counters this threat by ensuring that systems on the network are monitored by the TOE and that the TOE alerts TOE users when a security violation occurs.
T.DATA_COMPROMISE An attacker who is not a TOE user may read, modify, delay, or destroy security critical TOE configuration data stored on the TOE or being transmitted between physically separated parts of the TOE.	O.PROTECT The TOE will provide confidentiality and integrity services using FIPS 140-2 algorithms to protect TOE communication channels and user data. The TOE will also provide confidentiality of stored keys and keys used for cryptographic services performed by the TOE.	O.PROTECT counters this threat by providing encryption services available to authorized TOE users, administrators, and TOE user or administrator applications.
T.UNAUTHORISED _ACCESS A TOE user may gain unauthorised access (view, modify, delete) to user data through possible misuse.	O.BANNER The TOE will provide a mechanism that warns against unauthorised use of the TOE.	O.BANNER counters this threat by ensuring that the TOE warns against unauthorised use by using an advisory warning message banner.
	O.ACCESS The TOE will ensure that TOE users and administrators gain only authorized access to it and to resources that it controls.	O.ACCESS counters this threat by ensuring that TOE users and administrators gain only authorized access to it and to resources that it controls.
	O.USER_AUTHEN The TOE will uniquely identify and authenticate TOE users and administrators prior to allowing access to TOE functions and data.	O.USER_AUTHEN counters this threat by ensuring that administrators and TOE users are authenticated and identified before being allowed access to the TOE.

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

8.2.2 Security Objectives Rationale Relating to Policies

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

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 22 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 22 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.ADMIN_PROTECT The workstations in the TOE environment used to access the TOE are free of malicious software.	OE.ADMIN_PROTECT The administrative and user workstations must be protected from any external interference and tampering by having all security updates and anti-malware software installed.	OE.ADMIN_PROTECT upholds this assumption by ensuring that the administrative and user workstations are protected from external interference and tampering.

Assumptions	Objectives	Rationale
A.AUTH The TOE environment will provide the identification and authentication repository of users attempting to manage and use the TOE.	OE.AUTH The TOE environment must provide the authentication and identification repository of users attempting to use the TOE.	OE.AUTH satisfies this assumption by ensuring that the TOE environment provides the authentication and identification repository of users attempting to use the TOE.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains. Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner.	OE.MANAGE The TOE environment will provide competent, non-hostile administrators and users of the TOE who are appropriately trained and follow all administrator and user guidance. Administrators of the TOE will ensure the system is used securely.	OE.MANAGE satisfies 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 unauthorised use.
A.LOCATE The TOE, and all components of the TOE environment, including the authentication servers and database servers are located within a controlled access facility and appropriately located within the network to perform their functions. The devices with which the TOE communicates for exporting events are also located within a controlled access facility. Administrative and user workstations are located within a separate controlled access facility.	OE.NET_CON The TOE environment must be implemented such that the TOE is appropriately located within and connected to the network to perform its intended function.	OE.NET_CON satisfies this assumption by ensuring that the TOE is appropriately located within and connected to the network to perform its intended function.
	OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	OE.PHYSICAL satisfies the assumption that the TOE environment provides physical security commensurate with the value of the TOE and the data it contains.
A.OS_ACCESS The TOE environment is in a secure state and provides a sufficient level of protection to itself and the TOE components.	OE.OS_ACCESS The operating system upon which the TOE is installed provides a sufficient level of protection for itself and the TOE software it contains.	OE.OS_ACCESS upholds this assumption by ensuring that the OS where the TOE is installed provides enough protection for itself and the TOE to prevent tampering in a physically secure environment.
A.PROTECT The TOE software will be protected from unauthorised modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference and tampering.	OE.PROTECT satisfies the assumption that the TOE environment provides protection from unauthorised modification.
A.NOEVIL The administrators and users of the TOE are non-hostile, appropriately trained, and follow all guidance.	OE.MANAGE The TOE environment will provide competent, non-hostile administrators and users of the TOE who are appropriately trained and follow all administrator and user guidance. Administrators of the TOE will ensure the system is used securely.	OE.MANAGE satisfies this assumption by ensuring that those responsible for the TOE will provide competent, non-hostile individuals to perform management of the security of the environment.
A.SECURE_COM The TOE environment provides the necessary network infrastructure required for its operation and ensures the TOE is secured and protected from interference or tampering by using a firewall to prevent access from non-	OE.SECURE_COM The TOE environment must provide mechanisms to secure communications between TOE components and other devices to which the TOE is attached (including routers, switches, cabling, connectors, and firewalls) and must be properly implemented such that	OE.SECURE_COM satisfies this assumption by ensuring that the TOE environment provides the appropriate connectivity and mechanisms to secure communications between the TOE and other devices, and to allow the TOE to perform its functions in a secure manner.

Assumptions	Objectives	Rationale
trusted entities. Additionally, the TOE environment provides a sufficient level of protection to secure communications between the TOE and network-attached devices within the secure access facility.	the TOE is secured and protected from interference or tampering. Firewalls must be configured to restrict all external access from outside the internal network where the TOE is accessible.	
A.TIMESTAMP The TOE environment provides the TOE with the necessary reliable timestamps.	OE.TIMESTAMP The TOE environment must provide reliable timestamps to the TOE.	OE.TIMESTAMP satisfies this assumption by ensuring that the operating system where the TOE is installed will provide reliable timestamps 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

A class of FDC requirements was created to specifically address the data collected and analyzed by the HPE OpsBridge devices. The audit class of the CC (FAU) was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of HPE OpsBridge products and provide requirements about collecting, analyzing, storing, and reviewing the event and topology data. FDC_SCN.1 has no dependencies since the stated requirements embody all the necessary security functions. FDC_ANA.1 and FDC_STG.1 are dependent on FDC_SCN.1 since they apply to scan data that must first be collected by the TOE. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

8.4 Security Requirements Rationale

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

8.4.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 23 below shows a mapping of the objectives and the SFRs that support them.

Table 23 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.PROTECT The TOE will provide confidentiality and integrity services using FIPS 140-2 algorithms to protect TOE communication channels and user data. The TOE will also provide confidentiality of stored keys and keys used for	FCO_NRO.1 Selective proof of origin	The requirement meets the objective by ensuring that FIPS 140-2 cryptographic operations are used when generating evidence of origin to help protect transmitted user data.
	FCS_CKM.1 Cryptographic key generation	The requirement meets the objective by ensuring that the TOE can generate cryptographic keys for use during cryptographic operations.

Objective	Requirements Addressing the Objective	Rationale
cryptographic services performed by the TOE.	FCS_CKM.4 Cryptographic key destruction	The requirement meets the objective by ensuring that the TOE destroys cryptographic keys when no longer in use.
	FCS_COP.1 Cryptographic operation	The requirement meets the objective by ensuring that the TOE provides confidentiality and integrity services for the TOE by providing FIPS 140-2 validated algorithms.
O.FAIL_SECURE The TOE will preserve a secure state and ensure that all capabilities of the TOE are still operational in the event of a DP server failure.	FPT_FLS.1 Failure with preservation of secure state	The requirement meets the objective by ensuring that the TOE preserves a secure state in the event of a DP server failure.
O.PROTECT The TOE will provide confidentiality and integrity services using FIPS 140-2 algorithms to protect TOE communication channels and user data. The TOE will also provide confidentiality of stored keys and keys used for cryptographic services performed by the TOE.	FPT_ITT.1 Basic internal TSF data transfer protection	The requirement meets the objective by providing FIPS 140-2 cryptographic operations to ensure that TSF data is protected from disclosure or modification when transmitted between separate parts of the TOE or
O.FAIL_SECURE The TOE will preserve a secure state and ensure that all capabilities of the TOE are still operational in the event of a DP server failure.	FRU_FLT.1 Degraded fault tolerance	The requirement meets the objective by ensuring that all TOE capabilities are operational in the event of a DP server failure.
O.BANNER The TOE will provide a mechanism that warns against unauthorised use of the TOE.	FTA_TAB.1 Default TOE access banners	The requirement meets the objective by ensuring that users are presented with an advisory warning message regarding unauthorised use of the TOE.
O.PROTECT The TOE will provide confidentiality and integrity services using FIPS 140-2 algorithms to protect TOE communication channels and user data. The TOE will also provide confidentiality of stored keys and keys used for cryptographic services performed by the TOE.	FTP_ITC.1 Trusted channel	The requirement meets the objective by utilizing FIPS 140-2 cryptographic operations for the trusted channels used by the TOE.
	FTP_TRP.1 Trusted path	The requirement meets the objective by utilizing FIPS 140-2 cryptographic operations for the trusted paths used by the TOE.
O.MONITOR The TOE must be able to monitor machines on the network to ensure that they exist in a secure state and alert administrators if a system enters an insecure state. The TOE will also analyze and securely store the scanned and collected data.	FDC_ANA.1 System analysis	The requirement meets the objective by ensuring the TOE analyzes the collected data.
	FDC_SCN.1 System scan	The requirement meets the objective by providing authorized TOE users and administrators with the capability to read the collected system data.
	FDC_STG.1 Scanned data storage	The requirement meets the objective by ensuring that the TOE securely stores information from the managed machines.

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE will ensure that TOE users and administrators gain only authorized access to it and to resources that it controls.	FDP_ACC.1 Subset access control	The requirement meets the objective by enforcing the Resource Access Control SFP on all subjects and all named objects and all operations among them. The Resource Access Control SFP specifies the access rules between all subjects and all named objects controlled by the TOE. While authorized TOE users and administrators are trusted to some extent, this requirement ensures only authorized access is allowed to named objects.
	FDP_ACF.1 Security attribute based access control	The requirement meets the objective by specifying the Resource Access Control SFP rules that will be enforced by the TSF and determines if an operation among subjects and named objects is allowed. Furthermore, it specifies the rules to explicitly authorize or deny access to a named object based upon security attributes.
	FDP_ETC.1 Export of user data without security attributes	The requirement meets the objective by ensuring that the Resource Access Control SFP enforces access control parameters during the exportation of events and configuration data to targeted systems.
O.AUDIT The TOE will provide the capability to detect security relevant events and create records of those events in the audit trail. The TOE will also ensure that the audit records remain available in the event of a failure and are protected from unauthorised modification and deletion.	FAU_GEN.1 Audit data generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_STG.2 Guarantees of audit data availability	The requirement meets the objective by ensuring that audit logs remain available are protected from unauthorised modification and deletion.
O.AUDIT_REVIEW The TOE will provide the capability for only authorized TOE users to view audit information.	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review logs.
O.USER_AUTHEN The TOE will uniquely identify and authenticate TOE users and administrators prior to allowing access to TOE functions and data.	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that every TOE user or administrator is authenticated before the TOE performs any TSF-mediated actions on behalf of that TOE user or administrator.
	FIA_UAU.5 Multiple authentication mechanisms	The requirement meets the objective by providing multiple authentication mechanisms to support TOE user or administrator authentication.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that every TOE user or administrator is identified before the TOE performs any TSF-mediated actions on behalf of that TOE user or administrator.

Objective	Requirements Addressing the Objective	Rationale
O.TOE_ADMIN The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE. The TOE will also provide the functions necessary to support the administrators operating the TOE and protections for logged-in administrators.	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that only authorized roles with sufficient permissions are able to disable, enable, or modify the behavior of TOE security functions.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by restricting the ability to manage security attributes for the TOE to authorized roles with sufficient permissions.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring that the TOE provides restrictive default values for security attributes, and specifies alternative initial values to override the default values when an object or information is created.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates TOE users and administrators with roles to provide access to TSF management functions and data.

8.4.2 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.

8.4.3 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 24 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 24 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	FPT_STM.1 is not included because time stamps are provided by the environment. An environmental objective states that the TOE will receive reliable timestamps.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG.2	FAU_GEN.1	✓	
FCO_NRO.1	FIA_UID.1	✓	
FCS_CKM.1	FCS_CKM.4	✓	
	FCS_COP.1	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FMT_MSA.3	✓	
	FDP_ACC.1	✓	
FDP_ETC.1	FDP_ACC.1	✓	
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 this dependency.
FIA_UAU.5	No dependencies	N/A	
FIA_UID.2	No dependencies	N/A	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1	FMT_SMR.1	✓	
	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FMT_SMF.1	No dependencies	N/A	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_FLS.1	No dependencies	N/A	
FPT_ITT.1	No dependencies	N/A	

SFR ID	Dependencies	Dependency Met	Rationale
FRU_FLT.1	FPT_FLS.1	✓	
FTA_TAB.1	No dependencies	N/A	
FTP_ITC.1	No dependencies	N/A	
FTP_TRP.1	No dependencies	N/A	
FDC_ANA.1	FDC_SCN.1	✓	
FDC_SCN.1	No dependencies	N/A	
FDC_STG.1	FDC_SCN.1	✓	

9. Acronyms

Table 25 defines the acronyms used throughout this document.

Table 25 – Acronyms

Acronym	Definition
AD	Active Directory
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
BI	Business Intelligence
BO	BusinessObjects
BSM	Business Service Management
CBC	Cipher Block Chaining
CC	Common Criteria
CCM	Counter with CBC- MAC
CFB	Cipher Feedback
CI	Configuration Item
CLI	Command Line Interface
CM	Configuration Management
CMAC	Cipher-Based MAC
CMS	Configuration Management System
CPU	Central Processing Unit
CTR	Counter Mode
DB	Database
DES	Data Encryption Standard
DP	Data Processing
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
EC	Elliptic Curve
ECB	Electronic Codebook
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm

Acronym	Definition
EPI	Event Processing Interface
ETL	Extraction, Transformation, Loading
FIPS	Federal Information Processing Standards
GB	Gigabyte
GCM	Galois Counter Mode
GW	Gateway
HA	High Availability
HAC	High-Availability Controller
HI	Health Indicator
HMAC	Hash Message Authentication Code
HPE	Hewlett Packard Enterprise Development LP
HPAS	Hewlett Packard Application Server
HTML	Hypertext Markup Language
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
ISO	International Organization for Standardization
IT	Information Technology
JCE	Java Cryptography Extension
JDBC	Java Database Connectivity
JMS	Java Message Service
JMX	Java Management Extensions
JRE	Java Runtime Environment
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
LDAP/S	Lightweight Directory Access Protocol over Secure Sockets Layer
LW-SSO	Lightweight Single Sign-On
MAC	Message Authentication Code
MB	Megabytes
NIST	National Institute of Standards and Technology
NNMi	Network Node Manager i
NSA	National Security Agency
NTP	Network Time Protocol
OBR	Operations Bridge Reporter

Acronym	Definition
OFB	Output Feedback
OM	Operations Manager
OMi	Operations Manager i
OO	Operations Orchestration
OS	Operating System
PDAPI	Pervasive Distribution And Payment Interface
PDF	Portable Document Format
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PP	Protection Profile
PRNG	Pseudo Random Number Generator
PSS	Probabilistic Signature Scheme
QA	Quality Assurance
RAM	Random-Access Memory
RHEL	Red Hat Enterprise Linux
RNG	Random Number Generator
RTSM	Run-Time Service Model
SAR	Security Assurance Requirement
SAW	Service Anywhere
SCOM	Microsoft System Center Operations Manager
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SiS	SiteScope
SM	Service Manager
SMS	Short Message Service
SP	Special Publication
SQL	Structured Query Language
SSL	Secure Sockets Layer
ST	Security Target
TB	Terabyte
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions

Acronym	Definition
UCMDB	Universal Configuration Management Database System
UI	User Interface
WMI	Windows Management Instrumentation
XEX	XOR-Encrypt-XOR
XOR	Exclusive Or

Prepared by:

Corsec Security, Inc.

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

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