Hewlett Packard Enterprise Development LP

Operations Orchestration v10.20

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.14

Prepared for:

Prepared by:

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

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

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy, Suite 220
Fairfax, VA 22033
United States of America

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the HP Operations Orchestration v10.20, and will hereafter be referred to as the TOE throughout this document. The TOE is a software-based IT[1] Process Automation (ITPA) and IT runbook[2] solution for creating and implementing structured and automated flows over enterprise network, storage, and server deployments.

1.1 Purpose

This ST is divided into nine sections, as follows:

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

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 ST and TOE References

ST Title	Hewlett Packard Enterprise Development LP Operations Orchestration v10.20 Security Target
ST Version	Version 0.14
ST Author	Corsec Security, Inc.
ST Publication Date	8/11/2015

[1] IT – Information Technology

[2] A runbook is a routine compilation of procedures and operations that the system administrator or operator carries out

ST Title	Hewlett Packard Enterprise Development LP Operations Orchestration v10.20 Security Target
TOE Reference	HP Operations Orchestration 10.20 • Operations Orchestration Central • Operations Orchestration Remote Action Services (RAS)
FIPS[3] 140-2 Status	Level 1, RSA[4] BSAFE® Crypto-J JSAFE and JCE[5] Software Module v6.1, Certificate No. 2057

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, TOE Overview (Section 1.4), will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

HP Operations Orchestration (OO) is an industry-leading software solution for ITPA and IT runbook automation. OO is a system designed for creating and executing actions in structured sequences (referred to as flows), which enable IT administrators to efficiently maintain, troubleshoot, repair, and provision IT resources. Using OO, organizations can automate the following tasks:

- Checking, diagnosing, and repairing networks, servers, services, software applications, and workstations.
- Checking clients, servers and virtual machines for needed software and updates, and if needed, automatically deploying the required software and updates.
- Performing repetitive tasks, such as checking the status of websites, both internal and external.

In many IT service-oriented organizations, manual or mismanaged IT processes may lead to several issues that result in poor quality of service, delayed time-to-market, and high operating costs. Below are examples of the issues that these organizations may face:

- Incidents – floods of alerts, unnecessary escalations
- Change and release management – manual errors, lack of audit trails
- Process management – need for complex processes, e.g. disaster recovery
- Virtualization – inconsistent provisioning and management of physical and virtual assets

HP OO enables network, server, or storage automation for tasks ranging from provisioning and change management to policy compliance and reporting. Runbook automation can be used for common and repeatable IT processes across all infrastructure tiers, IT groups, and systems. Automation does not have to occur within a single solution. OO automation can be integrated into application, server, network, and storage solutions across the data center. When implemented within business services, OO provides continuous control over each phase of the service life cycle; including monitoring and ticketing across the data center and client endpoints.

1.3.1 HP OO Product Specification

HP Operations Orchestration is comprised of two major components: OO Central and OO RAS. Two additional components are associated with HP Operations Orchestration; OO Studio and OO Content. These two components are not part of the TOE evaluation, but can be utilized for a more comprehensive experience with the TOE.

[3] FIPS – Federal Information Processing Standards
[4] RSA – Rivest, Shamir, Adleman
[5] JCE – Java Cryptography Extension

1.3.1.1 OO Studio

HP OO Studio is a Microsoft Windows desktop-based application, similar to an IDE[6], which is used to create flows. This enables the author to design, debug, and package flows. OO Studio provides automation via code capabilities, such as integration with SCM[7] systems, project separation, and multi-authoring.

The Studio Designer (integrated within OO Studio) is a graphical designer used to formulate flows out of various operations and sub-flows. The Debugger is used to test the flow designs, and reflects the behavior of the flow as it would be executed in the real world. Customer-authored flow content may be grouped into granular projects based on various project criteria. OO Studio also enables documentation generation for each flow or groups of flows, including information and graphical representations of each flow. Once a flow is created, the customer can export the flow to the OO Central component as a “Content Pack”. These content packs can be executed directly via the OO Central component or they can be imported to the Studio for use within another flow.

1.3.1.2 OO Central

HP OO Central is a pure Java web application and is the central component of the entire Operations Orchestration deployment. In addition to OO configuration, management, and administration, OO Central provides the runtime environment for flow execution, monitoring, and reporting. OO Central is administered through a web-based UI[8] as well as a set of REST[9]ful web service APIs. In order to maintain backward compatibility with older versions, OO Central is deployed with a Process Automation System (PAS), which provides a SOAP[10]-based web service.

An OO Central server deployment is comprised of four components; Manager, Reporter, Worker, and Orchestrator. Management of OO Central is provided by the Manager component which handles flow triggering, scheduling, content, and event management. The Reporter provides flow execution tracking and history. The Worker is a back-end engine that processes and manages flow execution, including step execution, state persistency, and end-user interaction.

Multiple OO Central deployments may be clustered by adding additional nodes behind a load balancer. OO Central deployments are stateless, therefore no additional clustering software, operating systems (OS), or shared file systems are required. OO Central is deployed on a Tomcat server and can be executed as a Windows service or UNIX daemon. OO Central can support the following OS’s: 64-bit editions of Microsoft Windows Server 2008 (including R2) and Server 2012, Red Hat Enterprise Linux (RHEL) 5.x/6.x, and Ubuntu 12.04.1. OO Central server also requires a connection to a database for persistent storage of Events, Content, RAS state, and configuration. OO Central is compatible with various RDBMS’s[11], as listed in Table 2. Please refer to the latest version of "HP Operations Orchestration: System Requirements” for the latest Operating Systems and Databases supported.

1.3.1.3 OO Remote Action Services (RAS)

OO RAS enables flow execution against entities in remote and/or disjoint networks and data centers. RAS interacts with OO Central via its exposed REST API web service and polls Central for operations to execute. All RAS to Central communication is unidirectional from the RAS server to the Central server. RAS is deployed in the same way as OO Central and supports the same OS’s.

The main component of OO RAS is the Worker, which handles the execution of flows. The Worker pulls tasks (executions) from OO Central and performs the steps within these executions. RAS communicates with Central via the REST API to retrieve the RAS configuration. The configuration information retrieved from Central includes the group that a RAS Worker belongs to. RAS Workers support a grouping

[6] IDE – Integrated Development Environment
[7] SCM – Software Configuration Management
[8] UI – User Interface
[9] REST – Representational State Transfer
[10] SOAP – Simple Object Access Protocol
[11] RDBMS – Relational Database Management System

mechanism which enables dynamic execution of flow steps amongst distributed RASes. Workers may belong to multiple groups simultaneously. In addition, multiple OO RASes may be deployed in a highly-available configuration by simply adding another RAS and pointing it to the main OO Central instance.

1.3.1.4 OO Content

OO Content refers collectively to the flows, integrations, operations, and process automation libraries in HP OO. HP OO provides over 5,000 out-of-the-box operations, flows, and integration adapters delivered as a set of granular content packs. These packs can be used to author complex flows and orchestrate various services. Additional custom content can be generated by OO users using wizards such as the Web Service Wizard or developed using the Java and .NET SDKs. HP OO offers content in the areas of cloud orchestration, security operations, disaster recovery, monitoring, service management, applications, and security products.

1.4 TOE Overview

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

The TOE is a software-based ITPA and IT runbook solution for creating and implementing structured and automated flows over enterprise network, storage, and server deployments. For this evaluation of HP Operations Orchestration v10.20, the ST will focus on the major software components which work together to create, deploy, implement, and manage enterprise-scale workflow capabilities. The components of the HP OO solution which provide the largest impact on the implementation, management, and monitoring of HP OO are considered for the TOE boundary. In addition to the OO components, the TOE boundary also includes the Java runtime components necessary for the secure and continuous operation of HP Operations Orchestration v10.20. The TOE is comprised of the following components:

- Software components:
  - Operations Orchestration Central – Central component of HP Operations Orchestration deployment
  - Operations Orchestration RAS – Flow execution external to the OO Central implementation
  - RSA BSAFE Crypto-J JSAFE and JCE Software Module v6.1 – FIPS 140-2 Certified cryptographic library (FIPS Cert # 2057)
  - Apache Tomcat Server (Tomcat) – Java-based web server and servlet container providing a “pure java” web server environment
- Hardware components:
  - No hardware components are included as part of the TOE evaluation

1.4.1 TOE Environment

HP Operations Orchestration components are installed on a 64-bit Windows Server 2012 R2 Operating System (OS). Users of OO can access OO Central with a supported web browser[12] listed in Table 2. Access to an external LDAP server and external SAML[13] 2.0 Identity Provider (IdP) is required by OO Central in order to provide access to externally authenticated TOE users.

The TOE does not support direct-connect access and requires TOE users to connect to it remotely. Connections to the TOE by a web browser are secured with an encrypted HTTPS[14] connection. The web browser should be installed on a General Purpose Computer (GPC) workstation that can provide an uninterrupted network connection.

[12] Windows Internet Explorer 10.0 was used for testing the TOE
[13] SAML – Security Assertion Markup Language
[14] HTTPS – Secure Hyper–Text Transmission Protocol

OO Central and OO RAS shall be installed on separate host devices running 64-bit Windows Server 2012 R2 Operating System. The Java Runtime Environment (JRE) is required to operate OO Central and OO RAS as it provides the operational components needed to run OO Central and OO RAS and the Java components that are packaged with them (Tomcat server and Crypto-J). The JRE component is included with the installation of Central and RAS.

A remote database is used by OO Central to store TOE configuration, RAS states, OO events, audit records, and local user information. The remote database should be installed on a hardware device running 64-bit Windows Server 2012 R2 Operating System. This OS supports RDBMS[15] connections from OO Central. The database host should be able to provide an uninterrupted network connection.

Table 2 defines the system requirements and supported platforms for installing and accessing HP OO. Please refer to the latest version of "HP Operations Orchestration: System Requirements" for the latest Operating Systems and Databases supported.

Table 2 TOE Requirements

Requirement	TOE	TOE Environment
HP Operations Orchestration v10.20 • Installation includes: ○ HP OO Central ○ HP OO RAS ○ Apache Tomcat Server ○ RSA Crypto-J Cryptographic Library	✓	
TOE Hardware Requirements (for all TOE components): • Quad Core Processor (2 GHz[16]) • 4 GB[17] RAM[18] • 5 GB HDD[19] • Network Adapter		✓
TOE Operating System: • Microsoft Windows 2012 Server R2 (64-bit)		✓
Database for storing TOE information: • Microsoft SQL Server 2012		✓
Database Hardware Requirements: • 1 Processor • 2 GB RAM • 2 GB HDD • Network Adapter		✓
Supported Browsers: • Microsoft Internet Explorer 9.x, 10.x • Mozilla Firefox (latest release) • Google Chrome (latest release) • Apple Safari (latest release)		✓

[15] RDBMS – Relational Database Management System
[16] GHz – Gigahertz
[17] GB – Gigabytes
[18] RAM – Random Access Memory
[19] HDD – Hard Disk Drive

Requirement	TOE	TOE Environment
Java Runtime Environment (Includes Java Database Connectivity API)		✓
Microsoft .NET Framework 4.5		✓
LDAP Directory		✓
SAML 2.0 Identity Provider		✓
DHC REST Client (Google Chrome Browser Extension)		✓

1.4.2 TOE Evaluated Configuration

Please refer to the list below for the evaluated configuration for the TOE:

- TOE Components
  - OO Central v10.20
  - OO RAS v10.20
  - RSA BSAFE Crypto-J JSAFE and JCE Software Module v6.1
  - Apache Tomcat Server v 7.0.47
- Environmental Components
  - Microsoft Windows 2012 Server R2 (64-bit)
    - For OO Central, OO RAS, SQL Server, LDAP Directory
  - Java Runtime Environment v1.70
  - Microsoft SQL (MS SQL) Server 2012
  - Microsoft Active Directory v6.1 (LDAP Directory)
  - SAML 2.0 Identity Provider

1.5 TOE Description

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

1.5.1 Physical Scope

in Section 1.4 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

The TOE is a software-only ITPA and IT runbook solution that runs on both Windows and Linux OS's. The Windows and Linux OS's can be installed on any server hardware that meets the hardware criteria listed in Table 2 above. Each of the other TOE components are standalone software components and may be in installed onto the same sever appliance or separate server appliances. The appliances hosting OO Central and OO RAS must have access to the same network in order for the components to communicate with one another.

As a software-only TOE, the TOE boundary does not include any of the hardware devices used to host the TOE software. Additionally, the TOE boundary does not include the external LDAP or RDBMS servers hosting authentication and content data. Components of the TOE, the TOE environment, and the TOE boundary are shown in Figure 1~~Figure 1~~ below.

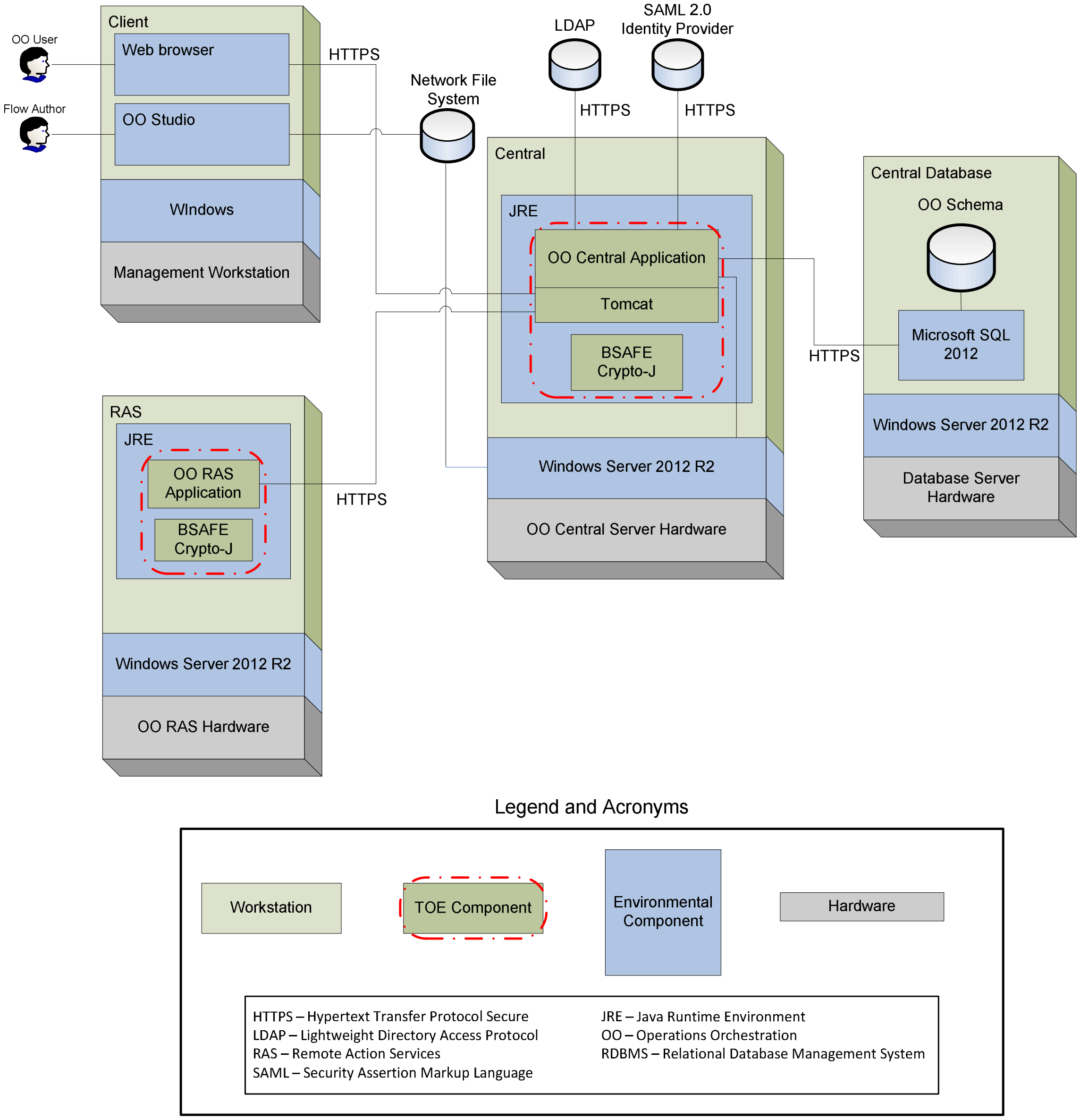

Figure 1 Operations Orchestration v10.20 TOE Boundary

1.5.1.1 Guidance Documentation

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

- HP Operations Orchestration: Installation Guide, Software Version 10.20, November, 2014
- HP Operations Orchestration: Administration Guide, Software Version 10.20, November, 2014
- HP Operations Orchestration: Concepts Guide, Software Version 10.20, November, 2014
- HP Operations Orchestration: Central User Guide, Software Version 10.20, November, 2014
- HP Operations Orchestration: Application Program Interface (API) Guide, Software Version 10.20, November, 2014
- HP Operations Orchestration: Operations Orchestration Shell User Guide, Software Version 10.20, November, 2014
- HP Operations Orchestration: Studio Authoring Guide, Software Version 10.20, November, 2014

- HP Operations Orchestration: Hardening Guide, Softare Version 10.20, November, 2014
- HP Operations Orchestration: System Requirements, Software Version 10.20, March, 2015
- HP Operations Orchestration: Architecture Guide, Software Version 10.20, November, 2014
- HP Operations Orchestration: Database Guide, Software Version 10.20, November, 2014

1.5.2 Logical Scope

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

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF[20]
- TOE Access
- Trusted Path/Channel

1.5.2.1 Security Audit

The Security Audit function provides the TOE with the functionality of generating audit records. Audit records are generated by OO Central and are stored in the external MS SQL database. Audit records are generated by the TOE when specific events within the TOE occur. Auditable events include login attempts, TOE configuration, user account management, and content pack/flow configuration and worker management. As a TOE user accesses, manages, and configures the TOE, their activities are tracked and tied to their identity. The full list of auditable events is provided in Table 14~~Table 14~~ in Section 7.1.1.

1.5.2.2 Cryptographic Support

The TOE utilizes a FIPS 140-2 Validated cryptographic module, which uses Approved cryptographic algorithms to support cryptographic functionality such as encryption, decryption, and hashing. The TOE generates cryptographic keys to be used with encryption, decryption, keyed hash, and signature operations. Each of the cryptographic algorithms supported by the TOE have been tested and validated by the CAVP[21]. The TOE uses FIPS-Approved zeroization methods in order to destroy all keys and other critical parameters generated by the TOE at the appropriate time.

1.5.2.3 User Data Protection

The TOE provides the User Data Protection security function to manage user and RAS access and interaction with content packs managed by OO Central. The TOE enforces this access via the Central Access Control Policy. Actions permitted by the TOE on content packs are enforced by the user and RAS attributes. Individual attributes will determine whether content packs can be viewed, edited, or deployed. Once a content pack is deployed, user and RAS attributes determine the ability to view and execute flows from the content packs. Workers must be assigned to a worker group while users must be mapped to a capable role.

1.5.2.4 Identification and Authentication

TOE users are required to authenticate and successfully identify themselves prior to accessing the services provided by OO Central. The TOE provides multiple authentication methods, allowing for a TOE user to authenticate using local or external authentication credentials. Local authentication is handled with the user

[20] TSF – TOE Security Functionality
[21] CAVP – Cryptographic Algorithm Validation Program

providing a username and password. External authentication is provided by LDAP and SAML 2.0. Once authenticated, the user will be associated with a role based on the credentials they provided or the LDAP user-group they are associated with. Plaintext feedback of authentication data is not provided. Once authenticated, a TOE user will only be able to see areas of the OO Central UI in which they have the ability to perform an operation.

1.5.2.5 Security Management

Management of the TOE is controlled through the use of RBAC. RBAC allows TOE administrators control which actions the users of the TOE are allowed to perform, based on their role. OO Central provides five default roles which can be assigned to TOE users. The default roles provided by OO Central are ADMINISTRATOR, END_USER, EVERYBODY, PROMOTER, and SYSTEM_ADMIN. Each role, either default or created, and their actions, are controlled by the permissions assigned to that role.

1.5.2.6 Protection of the TSF

Communications between OO RAS and the OO Central are secured with a TLS session. TSF data being transferred from OO Central to the OO RAS is protected from disclosure and modification using encryption and message authentication provided by the TLS protocol. OO Central and OO RAS both utilize the FIPS-validated cryptographic module to provide encryption and message authentication on the data being transferred over the TLS session.

1.5.2.7 TOE Access

OO Central displays an access banner to all TOE users attempting to access OO Central's Web UI from a web browser. The access banner cautions users on the authorized use of the TOE prior to allowing the user to log into OO Central. The access banner is configurable by a TOE administrator with "Manage Security Configuration" permissions.

OO Central enforces a thirty (30) minute inactivity period on all active HTTPS sessions. This includes connections to the TOE via the Web UI and via the REST interface. If a TOE user is inactive with Central (does not interact with the page content) for 30 minutes, the user will be forced to re-authenticate to the TOE.

1.5.2.8 Trusted Path/Channels

OO provides trusted channels for all data, and protects that data from disclosure or modification while in transit between TOE components and authorized IT entities. The TOE implements HTTPS for protection of remote web access to the management of the TOE via OO Central. The TOE uses FIPS validated cryptographic algorithms to implement the above cryptographic functions.

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

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

- HP OO Studio
- HP OO Content
- Process Automation System (PAS)
- HP OO Shell Utility
- Failover support
- JCE
- JRE

2 Conformance Claims

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

Table 3 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM[22] as of October 2, 2014 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ Augmented with Flaw Remediation ALC_FLR.2

[22] CEM – Common Evaluation Methodology

3 Security Problem

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

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

3.1 Threats to Security

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

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

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[23] and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 4 below lists the applicable threats.

Table 4 Threats

Name	Description
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.TAMPERING	A user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.
T.UNAUTH	A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.
T.DATA_COMPROMISE	An unauthorized user may read, modify, delay, or destroy security critical TOE data stored on the TOE or being transmitted between physically separated parts of the TOE.
T.ADMIN_ERROR	An administrator may incorrectly configure the TOE resulting in ineffective security mechanisms.
T.EXTERNAL_COMPROMISE	A malicious user or process may modify the audit data or LDAP data stored in the TOE environment

[23] TSF – TOE Security Functionality

3.2 Organizational Security Policies

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

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 5 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 5 Assumptions

Name	Description
A.INSTALL	The TOE is installed on the appropriate operating system and runtime environment
A.NETCON	The TOE environment provides the network connectivity required to allow the TOE to provide secure routing and switching functions.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
A.LOCATE	The TOE and its environmental components are located within a controlled access facility.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.APPLICATIONS	TOE users will use compatible applications in order access the TOE
A.ENVIRONMENT_ACCESS	The users who manage the TOE environment are authorized to access the TOE environment

4 Security Objectives

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

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 6 below.

Table 6 Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.
O.AUDIT	The TOE will provide the capability to detect security relevant events, record them to the audit trail, and identify the user which caused the event.
O.AUTHENTICATE	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.CRYPTO	The TOE will provide FIPS-Approved cryptographic algorithms and procedures to TOE users during operation of the TOE.
O.PROTECT	The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
O.PROTECT_COMM	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

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

Table 7 IT Security Objectives

Name	Description
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.

Name	Description
OE.ENVIRONMENT	The TOE environment must provide a compatible Windows or Linux Operating System for the installation of TOE components
OE.TRAFFIC	The TOE environment must be implemented such that the distributed TOE components are appropriately located within the same network.
OE.NETWORK	The TOE environment must provide a consistent network connection to the TOE.
OE.TRUSTED_ADMIN	Trusted TOE Administrators must follow and apply all administrator and configuration guidance.
OE.ACCESS	The TOE Environment must prevent unauthorized users from accessing data and resources

4.2.2 Non-IT Security Objectives

Table 8 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 8 Non-IT Security Objectives

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

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

There are no extended TOE security functional components defined for this evaluation.

5.2 Extended TOE Security Assurance Components

There are no extended TOE security assurance components defined for this evaluation.

6 Security Requirements

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

6.1 Conventions

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

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

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

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓	✓	
FAU_GEN.2	User Identity Association				
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
FDP_ACC.2	Complete access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FIA_ATD.1(a)	User attribute definition		✓	✓	✓
FIA_ATD.1(b)	User attribute definition		✓	✓	✓
FIA_UAU.2	User authentication before any action				
FIA_UAU.5	Multiple authentication mechanisms		✓		
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.2	User identification before any action				

Name	Description	S	A	R	I
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1(a)	Management of TSF data	✓	✓		✓
FMT_MTD.1(b)	Management of TSF data	✓	✓		✓
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_ITT.1	Basic internal TSF data transfer protection	✓			
FTA_TAB.1	Default TOE access banners				
FTA_SSL.3	TSF-initiated Termination		✓		
FTP_ITC.1	Inter-TSF trusted channel	✓	✓		
FTP_TRP.1	Trusted path	✓	✓		

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

6.2.1 Class FAU: Security Audit

FAU_GEN.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) [*The following auditable events:*

- *Audit Management*
- *Authentication-Authorization*
- *Central Lifecycle*
- *Content Configuration*
- *Content Deployment*
- *Runs*
- *System Configuration*
- *Topology Management*].

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, [*inputs received, outputs generated*].

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

FAU_GEN.2.1

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

6.2.2 Class FCS: Cryptographic Support

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

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Algorithms listed with the "Key generation" operation in the "Cryptographic Operation" column in Table 10*] and specified cryptographic key sizes [*Key sizes listed in the "Key Sizes" column in Table 10*] that meet the following: [*Standards listed in the "Standard" column in Table 10*].

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

FCS_CKM.4.1

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

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

FCS_COP.1.1

The TSF shall perform [*cryptographic operations listed in the "Cryptographic Operation" column of Table 10*] in accordance with a specified cryptographic algorithm [*cryptographic algorithm listed in the "Algorithm" column of Table 10*] and cryptographic key sizes [*key sizes listed in the "Key Sizes" column of Table 10*] that meet the following: [*standards listed in the "Standard" column of Table 10*.

Table 10 Cryptographic Algorithms

Algorithm	Key Sizes	Cryptographic Operation	Standard	Certificate Number
AES	128-, 192-, 256-bits	Encryption; Decryption	FIPS PUB[24] 197	2249
RSA	2048- and 3072-bits	Key generation; Signature generation; Signature verification	FIPS PUB 186-4; PKCS[25]#1 v1.5; PSS[26]	1154
DSA[27]	2048- and 3072-bits	Key generation; Signature generation; Signature verification	FIPS PUB 186-4	701

[24] PUB – Publication
[25] PKCS – Public Key Cryptography Standards
[26] PSS – Public Signature Scheme
[27] DSA – Digital Signature Algorithm

Algorithm	Key Sizes	Cryptographic Operation	Standard	Certificate Number
ECDSA[28]	2048- and 3072-bits	Key generation; Signature generation; Signature verification	FIPS PUB 186-4	357
HMAC[29]	160-, 224-, 256-, 384-, and 512-bit	Keyed Hash/Message Authentication	SP800-107rev1	1938
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	N/A	Hashing	FIPS PUB 180-4	1378
TLS 1.2 Key Derivation Function (KDF)	N/A	Symmetric Key Derivation	SP 800-135	39
SP800-90A HMAC_DRBG[30]	160-, 224-, 256-, 384-, and 512-bit output	Random number/key generation	SP800-90A	273

[28] ECDSA – Elliptic Curve Digital Signature Algorithm
[29] HMAC – Hash-based Message Authentication Code
[30] DRBG – Deterministic Random Bit Generator

6.2.3 Class FDP: User Data Protection

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

FDP_ACC.2.1

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

- *Subjects: Users accessing OO Central, OO RAS Workers accessing OO Central*
- *Objects: Content pack*
- *Operations: view, edit, execute, deploy*]

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2

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

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

FDP_ACF.1.1

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

- *Subject attributes (Users)*
  - *Username*
  - *Password*
  - *Role*
- *Subject attributes (Workers)*
  - *Worker ID*
  - *Worker group*
  - *Central Certificate*
- *Object attributes (Content pack)*
  - *Flows*
  - *Configuration*]

FDP_ACF.1.2

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

- *Users must be assigned to the correct role in order to view or deploy content packs*
- *Users must be assigned to the correct role in order to view, deploy, and/or execute the flows within a content pack*
- *Users must be assigned to the correct role in order to view and/or edit the content pack configuration*
- *Workers must present the correct Central certificate in order to access the flows*
- *Workers must be associated with a worker group in order to view and execute a flow*].

FDP_ACF.1.3

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

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules[

- *User's role*
- *Worker's Central certificate*].

6.2.4 Class FIA: Identification and Authentication

FIA_ATD.1(a) User attribute definition
Hierarchical to: No other components.
Dependencies: No dependencies
FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to ~~individual users~~ **locally created user**: [*Username, password, role*].

FIA_ATD.1(b) User attribute definition
Hierarchical to: No other components.
Dependencies: No dependencies
FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to ~~individual users~~ **remotely managed users**: [*role*].

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification
FIA_UAU.2.1

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

FIA_UAU.5 Multiple authentication mechanisms
Hierarchical to: No other components.
Dependencies: No dependencies
FIA_UAU.5.1

The TSF shall provide [

1. *Local authentication*
2. *LDAP Authentication*
3. *SAML Authentication*]

to support user authentication.

FIA_UAU.5.2

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

1. *Entry of the correct username and password combination by a TOE user authenticating with credentials stored by the TOE*
2. *Successful connection of the TOE to the LDAP server; Entry of the correct credentials stored on the LDAP server; LDAP user's user-group is mapped to a role created within the TOE.*
3. *The SAML assertion signature provided to the TOE has been verified; The user was authenticated by the SAML server; OO Central can match the user's LDAP user-group to a role defined on the TOE*].

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

The TSF shall provide only [*Bullets (●)*] to the user while the authentication is in progress.

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

FIA_UID.2.1

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

6.2.5 Class FMT: Security Management

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

FMT_MOF.1.1

The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of] the functions [*listed under the 'Security Functions' column of Table 11*] to [*the roles listed under the 'Roles' column of Table 11*].

Table 11 Management of OO Security Function Behavior by Role

Roles	Security Function
ADMINISTRATOR	View and manage schedules, content packs, content pack configuration items, flow permissions, system settings, topology, and security configuration
END_USER	No default security functions.
EVERYBODY	No default security functions.
PROMOTER	View and manage content packs, content pack configuration items, and flow permissions
SYSTEM_ADMIN	View and manage system settings, topology, and security configuration

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 [*Central Access Control Policy*] to restrict the ability to [change_default, query, modify, delete] the security attributes [*username, password, role, worker group*] to [*ADMINISTRATOR and SYSTEM_ADMIN*].

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

FMT_MSA.3.1

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

FMT_MSA.3.2

The TSF shall allow the [*ADMINISTRATOR and SYSTEM_ADMIN*] to specify alternative initial values to override the default values when an object or information is created.

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

FMT_MTD.1.1

The TSF shall restrict the ability to [change_default, query, modify, delete, clear] the [*username, password, role, worker group*] to [*ADMINISTRATOR and SYSTEM_ADMIN*].

FMT_MTD.1(b) Management of TSF data

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

FMT_MTD.1.1

The TSF shall restrict the ability to [query, *execute*] the [*flows, configuration items*] to [*ADMINISTRATOR and PROMOTER*].

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: [*Run Time Management, Content Management, System Management*].

FMT_SMR.1 Security roles

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

FMT_SMR.1.1

The TSF shall maintain the roles [*ADMINISTRATOR, END_USER, EVERYBODY, PROMOTER, SYSTEM_ADMIN, created roles*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.6 Class FPT: Protection of the TSF

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

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

6.2.7 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated Termination
Hierarchical to: No other components.
Dependencies: No dependencies
FTA_SSL.3.1

The TSF shall terminate an interactive session after a [*30 minute period of user inactivity*].

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.

6.2.8 Class FTP: Trusted Path/Channels

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

FTP_ITC.1.1

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

FTP_ITC.1.2

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

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [*Connections to an external LDAP server*].

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 [the TSF, remote users] to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [initial user authentication].

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 12 Assurance Requirements~~Table 12 Assurance Requirements~~ summarizes the requirements.

Table 12 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 Basic Flaw Remediation
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Functional Specification
	ADV_TDS.1 TOE Design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing
Class AVA: Vulnerability Assessment	AVA_VAN.2 Vulnerability Analysis

7 TOE Security Specification

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

7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 13~~Table 13~~ lists the security functionality and their associated SFRs.

Table 13 Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_ACC.2	Complete access control
	FDP_ACF.1	Security attribute based access control
Identification and Authentication	FIA_ATD.1(a)	User attribute definition
	FIA_ATD.1(b)	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1(a)	Management of TSF data
	FMT_MTD.1(b)	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles

TOE Security Functionality	SFR ID	Description
Protection of TOE Security Functions	FPT_ITT.1	Basic internal TSF data transfer protection
TOE Access	FTA_TAB.1	Default TOE access banners
	FTA_SSL.3	TSF-initiated Termination
Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

7.1.1 Security Audit

The Security Audit function provides the TOE with the functionality of generating audit records. Audit records are generated by OO Central and are stored in the external MS SQL database. Audit records are generated by the TOE when specific events within the TOE occur. Auditable events include authentication, authorization, content configuration, and system configuration. As a TOE user accesses, manages, and configures the TOE, their activities are tracked and tied to their identity. Table 14~~Table 14~~ lists all of the auditable event types that occur on the TOE.

Table 14 Auditable Events

Group	Type
Audit Management	Audit Configuration Change
Authentication-Authorization	AuthenticationFailure
	AuthorizationFailure (no Subject)
	Login Attempt
	Logout
	Authentication Configuration Update
	Role Create
	Role Update
	Role Delete
	Role Set Default
	LDAP Configuration Create
	LDAP Configuration Update
	LDAP Configurations Delete
	Internal User Create
	Internal User Update
	Internal Users Delete
	SAML Configuration Create
	SAML Configuration Update
	SSO Configuration Update
	Path Entitlement Update
	SAML Configuration Delete
Central Lifecycle	Central Startup (no subject)
	Central Shutdown (no subject)
Content Configuration	Group Alias Create
	Group Alias Update
	Group Aliases Delete
	System Account Create
	System Account Update

Group	Type
	System Accounts Delete
	ContentConfigurationItemCreate
	ContentConfigurationItemUpdate
	ContentConfigurationItemDelete
Content Deployment	DeploymentProcessCreate
	ContentUploadToDeploymentProcess
	ContentRemoveFromDeploymentProcess
	ContentForDeleteAddToDeploymentProcess
	DeploymentProcessStart
	Content Deployment
	Content Rollback
	Content Delete
Runs	Run Triggered (only manual runs)
	Run Status Change
	Schedule Create
	Schedule Edit
	Schedules Enable
	Schedules Disable
	Schedules Delete
System Configuration	System Configuration Create or Update
	System Configuration Delete
Topology Management	WorkerRegister
	Workers Delete
	Worker Update
	Workers Update
	Workers Assign-To-Group
	Workers Remove from group
	External URL Create or Update
	External URL delete

The audit list contains the columns and information listed in Table 15~~Table 15~~.

Table 15 Audit Record Contents

Field	Content
time	Date and time (ephoc timestamp) when the event occurred

Field	Content
type	The event type causing the audit record to be generated
group	The group from which the event type occurred (see "Group" column in Table 14~~Table 14~~)
subject	User Identifier
Outcome*	The event will be flagged as: "Success", "Failure", "System Error."
Inputs Received**	External inputs from the user that caused the event.
Outputs Generated**	Internal and external outputs which were generated by the event.

* Failed login attempts due to incorrect username/password are distinguished from failed login attempts due to system error.
** Excludes passwords, file contents, and trigger/schedule inputs.

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

7.1.2 Cryptographic Support

The TOE utilizes a FIPS 140-2 Validated cryptographic module, which uses FIPS-Approved cryptographic algorithms to support cryptographic functionality such as encryption, decryption, and hashing. The TOE generates cryptographic keys to be used with encryption, decryption, keyed hash, and signature operations. AES, RSA, and HMAC are all used by the TOE when performing the TLS protocol. AES is also used when encrypting system account passwords and Worker IDs. All AES, DSA, ECDSA, RSA, and HMAC keys are generated with the FIPS-Approved SP800-90A HMAC_DRBG.

Each of the cryptographic algorithms supported by the TOE have been tested and validated by the CAVP. Each algorithm has been awarded a certificate number. Table 10, provided in Section 6.2.2, lists each algorithm used by the TOE, their usage, and their associated algorithm certificate.

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

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

7.1.3 User Data Protection

The TOE provides the User Data Protection security function to manage user and RAS access and interaction with content packs managed by OO Central. The TOE enforces the Central Access Control Policy, which limits access to actions on content packs and their contents. Limitations are enforced by the user and RAS security attributes. Individual attributes will determine whether content packs can be viewed, edited, or deployed.

In order to access and manage content packs, users accessing the TOE must provide the correct username and password and must be mapped to the ADMINISTRATOR or PROMOTER role. Once logged in, users can deploy and manage content packs and their configuration settings. Users in these roles can also execute individual flows provided by the deployed content packs. Users which don't provide the correct username and password or are not mapped to the appropriate role will not have access to the content packs or their flows.

Workers connect to OO Central in order to obtain flows to perform. Workers are assigned to a worker group within OO Central. Content packs can specify which worker group(s) to use for execution, which will send its tasks only to those workers assigned to the worker group(s). Workers can only connect to OO Central if they possess a valid Central certificate. Workers will only be aware of the flows assigned to the worker groups on which the worker is assigned to.

TOE Security Functional Requirements Satisfied: FPD_ACC.2, FDP_ACF.1

7.1.4 Identification and Authentication

TOE users are required to authenticate prior to accessing the services provided by the TOE. Each user of the TOE is associated with role. The TOE provides multiple authentication methods, allowing for a TOE user to authenticate using local or external credentials. Local authentication is handled with the user providing a username and password. External authentication is provided by LDAP and SAML 2.0. Once the user has successfully authenticated with the external component, their external identity's user-group will be mapped to a role on the TOE.

When authenticating locally, the TOE user must provide the correct username and password combination created and stored within the TOE. LDAP authentication requires the TOE to be connected to an external LDAP server hosting LDAP credentials. A user will select the LDAP authentication option and proceed to provide the domain, username, and password of a user stored on the LDAP server. The user's LDAP user-group must be mapped to a role created within the TOE prior to allowing access to TOE functions. Passwords are obscured with bullets during input to the OO Central logon screen.

SAML 2.0 authentication works when OO Central has been associated with an external Identity Provider (IdP) and has sent its metadata onto the IdP. When a user attempts to access OO Central with SAML 2.0 enabled, their browser will be redirected to the IdP, where they must provide the username and password associated with the LDAP server. The IdP authenticates the user using the LDAP server and then sends a SAML authentication assertion packet back to the user's browser, which then passes the assertion onto OO Central. The security assertion contains the user's SAML security artifacts (username, LDAP user-group, and authentication success/failure result). If the results of authentication are successful, OO Central determines that the LDAP user-group is mapped to a role created within the TOE before allowing the user access to TOE functions.

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

7.1.5 Security Management

Management of the TOE is controlled through the use of RBAC. RBAC allows TOE administrators to control which actions the users of the TOE are allowed to perform, based on their role. OO Central provides five default roles which can be assigned to TOE users: ADMINISTRATOR, END_USER, EVERYBODY, PROMOTER, and SYSTEM_ADMIN. In addition, a TOE administrator can create new roles. Roles in OO Central are defined as a collection of permissions. Each role, either default or created, and their actions, are controlled by the permissions assigned to that role. Furthermore, the permissions assigned to each role will control which UI components and actions within OO Central are exposed to the user in that role. By default, when creating a new role or new user, the role or user will not have any permissions associated with them until the administrator assigns them. The list of permissions that can be assigned to each role, along with a description of the permission, is provided in Table 16 below.

Table 16 HP OO Central Permissions

Permission	Description
Run Management	
View Schedules	Permission to view flow schedules
Manage Schedules	Permission to create and modify flow schedules
Manage Others' Runs	Permission to modify flow runs that were triggered by other users
Remote Debugging	Permission to trigger the Studio Debugger via OO Central
Content	
View Content Packs	Permission to view content packs
Manage Content Packs	Permission to modify content packs, deploy content, and roll back a content pack deployment
View Configuration Items	Permission to view configuration items (i.e. group aliases, system accounts, system properties)
Manage Configuration Items	Permission to modify configuration items
Manage Flow Permissions	Permission to modify content permissions (for flows and folders)
System	
View System Settings	Permission to view the Monitoring and System Information reports
Manage System Settings	Permission to configure the log level using REST API
View Topology	Permission to view workers and worker groups
Manage Topology	Permission to enable/disable workers and configure worker groups
View Security Configuration	Permission to view the security configuration. This includes viewing internal users, LDAP authentication, and roles.
Manage Security Configuration	Permission to modify the security configuration. This includes configuring internal users, LDAP authentication, SAML authentication, and roles.
View Audit Events	Permission to view the audit records
Dashboard	
View Dashboard	Permission to view the dashboard workspace.

The default roles provided by OO Central are ADMINISTRATOR, END_USER, EVERYBODY, PROMOTER, and SYSTEM_ADMIN. Each default role has a set of permissions mapped to it, which determine whether the role can view, modify, execute, or remove TSF data. By default, a newly created user is given the EVERYBODY role, which has none of the permissions listed in Table 16. The list of default permissions mapped to each role is provided in Table 17 below.

Table 17 Mapping Permissions to Roles

Role	Default Permissions
ADMINISTRATOR	All permissions listed in Table 16
END_USER	No default permissions
EVERYBODY	No default permissions
PROMOTER	View Content Packs, Manage Content Packs, View Configuration Items, Manage Configuration Items, Manage Flow Permissions, View Dashboard
SYSTEM_ADMIN	View System Settings, Manage System Settings, View Topology, Manage Topology, View Security Configuration, Manage Security Configuration

TOE users with the "Manage Topology" permission are permitted to assign OO RAS workers to worker groups. Worker groups can be added by the TOE user with the "Manage Configuration Items" permission. When the TOE admin creates a new TOE user, the TOE provides restrictive default permission values for the new user. The admin will create a new username and password and will assign the new user to an existing role. Only the ADMINISTRATOR or SYSTEM_ADMIN roles can create new users and assign them to roles.

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

7.1.6 Protection of the TSF

Communications between OO RAS and the OO Central are secured with a TLS session. TLS sessions use AES for encryption in addition to RSA and HMAC for data integrity and authentication. TSF data being transferred from OO Central to the OO RAS is protected from disclosure using AES encryption and from modification using HMAC message authentication. OO Central and OO RAS both utilize the FIPS-validated cryptographic module to provide the AES and HMAC algorithms used during the TLS session.

TOE Security Functional Requirements Satisfied: FPT_ITT.1

7.1.7 TOE Access

OO Central displays an access banner to all TOE users attempting to access OO Central's Web UI from a web browser. The access banner cautions users on the correct use of the TOE prior to allowing the user to log into OO Central. The access banner is configurable by a TOE administrator with "Manage Security Configuration" permissions. The security banner is customizable up to 2,000 characters and will be displayed to all users accessing OO Central via their web browser.

OO Central enforces a thirty (30) minute inactivity period on active HTTPS sessions via the Web UI and REST interface. If a TOE user does not interact with Central's Web UI for 30 minutes, their next attempted interaction will not succeed and the user will be directed to the access banner and login page. If a TOE user does not interact with Central's REST interface for 30 minutes, their next attempted interaction will not success and the user will be asked for an authentication header. The user must re-authenticate via the Web UI or REST interface in order to interact with the TOE. There are two pages within the TOE that do not enforce the session time out: 1) the Dashboard Workspace and 2) flow execution drilldown (when viewing the execution details of a flow). These pages do not present any management functionality nor do they expose any security-related information. After navigating away from these pages to any other page, session termination will be active.

TOE Security Functional Requirements Satisfied: FTA_SSL.3, FTA_TAB.1.

7.1.8 Trusted Path/Channels

OO provides trusted channels for all data, and protects that data from disclosure or modification while in transit between TOE components and authorized IT entities, such as an external LDAP server. All communications between the TOE and the LDAP server are secured via HTTPS. The TOE also implements HTTPS for protection of remote web and REST access to the TOE. HTTPS prevents the data being transferred between an LDAP server or a remote web or REST client and the TOE from disclosure and modification. The TOE generates its own certificate which is then shared among the distributed components. The certificate helps to establish a secure session which will encrypt and hash the data entering and leaving the TOE. The TOE uses FIPS-Approved cryptographic algorithms to implement the cryptographic functionality.

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

8 Rationale

8.1 Conformance Claims Rationale

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

8.2 Security Objectives Rationale

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

8.2.1 Security Objectives Rationale Relating to Threats

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

Table 18 Threats: Objectives Mapping

Threats	Objectives	Rationale
T.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	O.AUTHENTICATE satisfies this threat by ensuring that The TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
	O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT satisfies this threat by placing access control policies on TOE data and by presenting a warning banner to users about unauthorized use of the TOE prior to logging in.
T.TAMPERING A user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN supports the mitigation of this threat by ensuring that only authorized users may configure the TOE security mechanisms.
	O.AUDIT The TOE will provide the capability to detect security relevant events, record them to the audit trail, and identify the user which caused the event.	O.AUDIT satisfies the threat by ensuring that security relevant events that may indicate attempts to tamper with the TOE are recorded.

Threats	Objectives	Rationale
	O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT mitigates this threat by providing mechanisms to protect the TOE data from unauthorized modification.
T.UNAUTH A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN ensures that access to TOE security data is limited to those users with access to the management functions of the TOE.
	O.AUDIT The TOE will provide the capability to detect security relevant events, record them to the audit trail, and identify the user which caused the event.	O.AUDIT ensures that unauthorized attempts to access the TOE are recorded.
	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	O.AUTHENTICATE ensures that users are identified and authenticated prior to gaining access to TOE security data.
	O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT prevents unauthorized access and modification to security data by enforcing an access control policy.
T.DATA_COMPROMISE An unauthorized user may read, modify, delay, or destroy security critical TOE data stored on the TOE or being transmitted between physically separated parts of the TOE.	O.CRYPTO The TOE will provide FIPS-Approved cryptographic algorithms and procedures to TOE users during operation of the TOE.	O.CRYPTO counters this threat by providing encryption services available to authorized users and/or user applications.
	O.PROTECT_COMM The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	O.PROTECT_COMM counters this threat by providing protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
T.ADMIN_ERROR An administrator may incorrectly configure the TOE resulting in ineffective security mechanisms.	OE.TRUSTED_ADMIN Trusted TOE Administrators must follow and apply all administrator and configuration guidance.	OE.TRUSTED_ADMIN counters this threat by ensuring that administrators follow all administrative guidance.

Threats	Objectives	Rationale
T.EXTERNAL_COMPROMISE A malicious user or process may modify the audit data or LDAP data stored in the TOE environment	OE.ACCESS The TOE Environment must prevent unauthorized users from accessing data and resources	OE.ACCESS prevents unauthorized access and modification to security data stored in the TOE environment

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

Every policy is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

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

Table 19 Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate operating system and runtime environment	OE.ENVIRONMENT The TOE environment must provide a compatible Windows or Linux Operating System for the installation of TOE components	OE.ENVIRONMENT satisfies the assumption by ensuring compatible operating systems and Java Runtime Environment is installed prior to the installation of the TOE
	OE.TRUSTED_ADMIN Trusted TOE Administrators must follow and apply all administrator and configuration guidance.	OE.TRUTED_ADMIN satisfies this assumption by ensuring TOE Administrators follow and apply all configuration guidance.
A.NETCON The TOE environment provides the network connectivity required to allow the TOE to provide secure routing and switching functions.	OE.TRAFFIC The TOE environment must be implemented such that the distributed TOE components are appropriately located within the same network.	OE.TRAFFIC satisfies the assumption by ensuring the distributed portions of the TOE are implemented within the same network.
	OE.NETWORK The TOE environment must provide a consistent network connection to the TOE.	OE.NETWORK satisfies the assumption by ensuring the TOE environment will provide the appropriate connectivity to allow the TOE to perform its function.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME satisfies the assumption that the environment provides reliable timestamps to the TOE.

Assumptions	Objectives	Rationale
A.LOCATE The TOE and its environmental components are located within a controlled access facility.	NOE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	NOE.PHYSICAL satisfies this assumption by ensuring physical security is provided within the TOE environment to provide appropriate protection to the network resources and to prevent manipulation of data across the network.
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	NOE.MANAGE satisfies the assumption that the users who manage the TOE are non-hostile, appropriately trained and follow all guidance.
A.APPLICATIONS TOE users will use compatible applications in order access the TOE	NOE.COMPATIBLE The TOE environment must provide compatible applications for TOE users.	NOE.COMPATIBLE satisfies the assumption by ensuring that compatible software applications are installed onto the TOE environment for use by TOE users.
A.ENVIRONMENT_ACCESS The users who manage the TOE environment are authorized to access the TOE environment	OE.ACCESS The TOE Environment must prevent unauthorized users from accessing data and resources	OE.ACCESS satisfies the assumption by ensuring that only authorized user are able to access the TOE environment

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 Security Requirements Rationale

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

8.3.1 Rationale for Security Functional Requirements of the TOE Objectives

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

Table 20 Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by restricting the ability to perform actions on security attributes to specific users.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by providing authorized users the ability to change default security attribute values.
	FMT_MTD.1(a) Management of TSF data	The requirement meets the objective by ensuring that the TOE restricts access to TSF data based on the user's role.
	FMT_MTD.1(b) Management of TSF data	The requirement meets the objective by ensuring that the TOE restricts access to TSF data based on the user's role.
	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 users with roles to provide access to TSF management functions and data.
O.AUDIT The TOE will provide the capability to detect security relevant events, record them to the audit trail, and identify the user which caused the event.	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_GEN.2 User Identity Association	The requirement meets this objective by ensuring that the TOE associates each auditable event with an identified TOE user which caused the event.

Objective	Requirements Addressing the Objective	Rationale
O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	FIA_ATD.1(a) User attribute definition	The requirement meets the objective by associating a username and password to each TOE user
	FIA_ATD.1(b) User attribute definition	The requirement meets the objective by associating a username and password to each TOE user
	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that users are authenticated before access to TOE administrative functions is allowed.
	FIA_UAU.5 Multiple authentication mechanisms	The requirement meets the objective by providing multiple means of authentication prior to accessing the TOE
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the users are identified before access to TOE administrative functions is allowed.
	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE authenticates users prior to allowing access to administrative functions to ensure that only those trusted users may manage the security behaviour of the TOE.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that the TOE authenticates users prior to allowing access to security attributes to ensure that only those trusted users may manage the security attributes.
	FMT_MTD.1(a) Management of TSF data	The requirement meets the objective by ensuring that only authorized users are allowed access to TSF data.
	FMT_MTD.1(b) Management of TSF data	The requirement meets the objective by ensuring that only authorized users are allowed access to TSF data.

Objective	Requirements Addressing the Objective	Rationale
O.CRYPTO The TOE will provide FIPS-Approved cryptographic algorithms and procedures to TOE users during operation of the TOE.	FCS_CKM.1 Cryptographic key generation	The requirement meets the objective by ensuring that the TOE can generate FIPS-Approved cryptographic keys for use during cryptographic operations.
	FCS_CKM.4 Cryptographic key destruction	The requirement meets the objective by ensuring that the TOE destroys cryptographic keys when no longer in use using FIPS-Approved methods
	FCS_COP.1 Cryptographic operation	The requirement meets the objective by ensuring that the TOE provides FIPS-Approved confidentiality and integrity services for the TOE.
O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	FDP_ACC.2 Complete access control	The requirement meets the objective by enforcing the Central Access Control Policy on all subjects and all named objects and all operations among them. The policy specifies the access rules between all subjects and all named objects controlled by the TOE. While authorized users 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 ensuring that the TOE enforces access control based on the Central Access Control Policy.
	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authenticated users are allowed access to TOE functions.
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by preventing password material from being obtained from an unauthorized person, thus protecting from unauthorized access.

Objective	Requirements Addressing the Objective	Rationale
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only identified users are allowed access to TOE functions.
	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only privileged users may manage the security behaviour of the TOE.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authorized users have access to security attributes.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by enforcing restrictive default values for security attributes, thus preventing unauthorized access or modification of TSF data
	FMT_MTD.1(a) Management of TSF data	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authorized users have access to TSF data.
	FMT_MTD.1(b) Management of TSF data	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authorized users have access to TSF data.
	FTA_SSL.3 TSF-initiated Termination	The requirement meets the objective by terminating inactive and unattended sessions and ensuring unauthorized users cannot access the session

Objective	Requirements Addressing the Objective	Rationale
	FTA_TAB.1 Default TOE access banners	The requirement meets the objective by presenting an advisory access banner to user prior to authentication. This prevents unauthorized use of the TOE.
O.PROTECT_COMM The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	FPT_ITT.1 Basic internal TSF data transfer protection	The requirement meets the objective by protecting data being transferred between TOE components from disclosure and modification.
	FTP_ITC.1 Inter-TSF trusted channel	The requirement meets the objective by providing a secure and trusted communications channel between all trusted IT products and the TOE.
	FTP_TRP.1 Trusted path	The requirement meets the objective by providing a secure communications path to all users accessing the TOE remotely.

8.3.2 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.

8.3.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 21 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 21 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_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_GEN.2	FAU_GEN.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.
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.2	FDP_ACF.1	✓	
FDP_ACF.1	FMT_MSA.3	✓	
	FDP_ACC.1	✓	
FIA_ATD.1(a)	No dependencies	✓	
FIA_ATD.1(b)	No dependencies	✓	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FIA_UAU.5	No dependencies	✓	
FIA_UAU.7	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2, which is hierarchical to FIA_UAU.1, is included. This satisfies this dependency
FIA_UID.2	No dependencies	✓	
FMT_MOF.1	FMT_SMR.1	✓	

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

9 Acronyms

This section and Table 22 define the acronyms and terms used throughout this document.

9.1 Acronyms

Table 22 Acronyms and Terms

Acronym	Definition
AES	Advanced Encryption System
API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
CSA	Cloud Service Automation
DB	Database
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards
GB	Gigabyte
GHz	Gigahertz
GPC	General Purpose Computer
HDD	Hard Drive Disk
HMAC	(keyed-) Hash Message Authentication Code
HTTPS	Secure Hyper-Text Transfer Protocol
ID	Identification
IDE	Integrated Development Environment
IT	Information Technology
ITPA	IT Process Automation
JCE	Java Cryptographic Engine
JRE	Java Runtime Environment
JSP	JavaServer Pages
JVM	Java Virtual Machine
LDAP	Lightweight Directory Access Protocol

Acronym	Definition
LTS	Long Term Support
NA	Network Automation
OO	Operations Orchestration
OS	Operating System
OSP	Organizational Security Policy
PAS	Process Automation System
PKCS	Public Key Cryptography Standards
PP	Protection Profile
PSS	Public Signature Scheme
PUB	Publication
RAM	Random Access Memory
RAS	Remote Action Server
RBAC	Role-Based Authentication Control
RDBMS	Relational Database Management System
REST	Representational State Transfer
RHEL	Red Hat Enterprise Linux
RSA	Rivest, Shamir, Adleman
RSS	Really Simple Syndication
SA	Server Automation
SAR	Security Assurance Requirement
SCM	Software Configuration Management
SDK	Software Configuration Management
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SS	SiteScope
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation

Acronym	Definition
TSF	TOE Security Functionality
TSP	TOE Security Policy
UI	User Interface

Prepared by:
Corsec Security, Inc.

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

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