Hewlett Packard Enterprise Development LP

Asset Manager v9.50 with Connect-It v9.60

Security Target

Evaluation Assurance Level (EAL): EAL2+

Document Version: 1.4

Prepared for:

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

Prepared by:

Corsec Security, Inc.
13291 Park Center Road., Suite 460
Herndon, VA 20171
United States of America

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the HP[1] Asset Manager v9.50 with Connect-It v9.60, and will hereafter be referred to as the TOE or AM[2] throughout this document. The TOE is a system that provides an organized way to manage the life cycle of IT[3] infrastructure from procurement to end-of-life. AM facilitates enterprise management of physical objects, including computers, machines, tools, consumables, office supplies, and intangible objects (software installations)[4] and the events (such as procurement, work orders, tax, maintenance contracts, leases, license agreements, and warranties) associated with the lifecycle of the items in the system.

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.

[1] HP – Hewlett Packard
[2] AM – Asset Manager
[3] IT – Information Technology
[4] Collectively referred to as portfolios.

- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 ST and TOE References

ST Title	Hewlett Packard Enterprise Development L.P. Asset Manager v9.50 with Connect-It v9.60 Security Target
ST Version	Version 1.4
ST Author	Corsec Security, Inc.
ST Publication Date	2015-12-23
TOE Reference	HP Asset Manager v9.50 with Connect-It v9.60 build #12154 (AM) and 010 (CIT)
FIPS[5] 140-2 Status	Level 1, Validated crypto modules OpenSSL 2.0 cert # 1747 RSA[6] BSAFE Crypto-J v6.1cert# 2058

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation and provides the introduction to the parts of the overall product offering that are specifically being evaluated.

AM provides organizations with visibility into their current IT hardware and software inventories, as well as non-IT assets[7] such as office supplies, machines, and tools. AM provides insights into the current status of assets, such as contracts, licensing obligations, and when software is over-deployed for an environment. Assets are organized within AM into portfolio items, which contain a list of assets, information relevant to who is responsible for the assets, and where the assets are located geographically. Connect-It is embedded in AM to assist in importing asset data from external discovery tools. Connect-It not only feeds various types of data into AM, but also pushes

[5] FIPS – Federal Information Processing Standard
[6] RSA – Rivest, Shamir, Adelman
[7] Asset – any item (such as computers, software installations, office supplies, or machines-tools) that is entered into the Asset Manager system.

asset data to external service management, configuration management, cloud services, and other corporate systems.

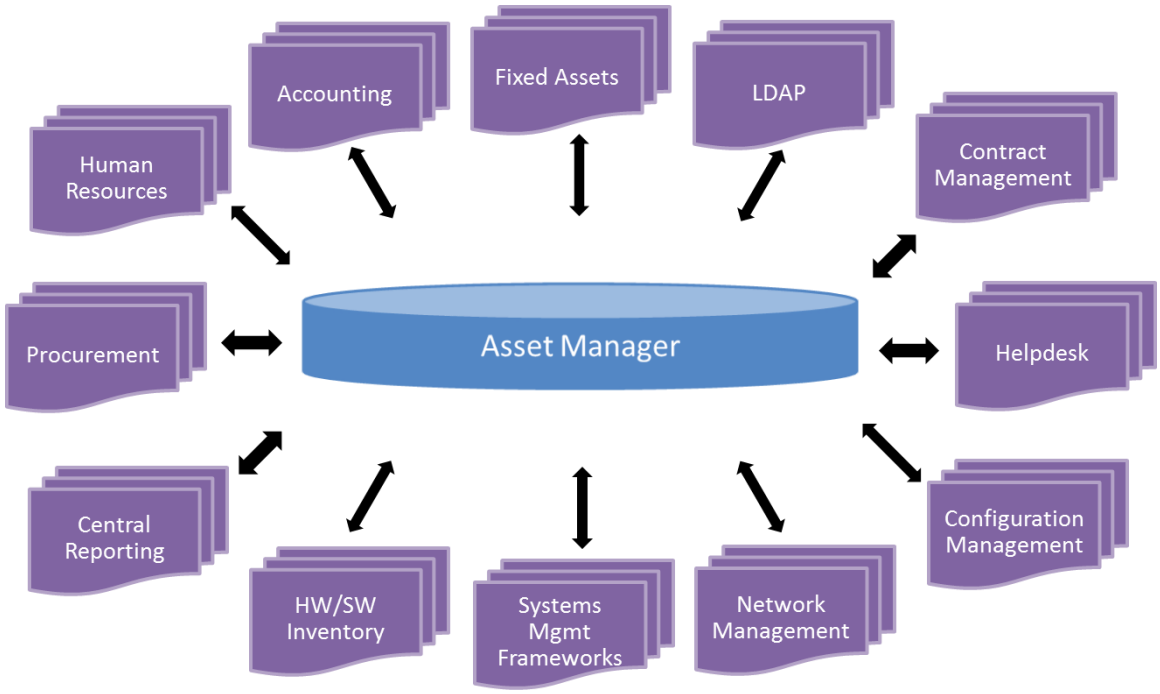

Figure 1 Asset Manager Integration

In typical customer environment, the TOE integrates with various IT tools, including directory services (such as Active Directory), financial systems (such as SAP or Oracle Financials), procurement tools, enterprise reporting systems, CMDB, Human Resources and other corporate systems. As such, HP Asset Manager implementations within customer environments contain or have direct access to sensitive information, including organizational structure, billing codes, financial and other restricted information, requiring tight access controls to the system.

The information stored and maintained in HP Asset Manager will include information, including location of assets – which in many government and military applications is consider sensitive. The data stored in this tool, if compromised can be used to create effective cyber attacks or extrapolate other information, such as location of government or military employees, troop deployments, etc. Supplier and financial information stored in the tool will allow unauthorized users gain insight into buying practices and access into budgets and purchasing systems.

Assets can be entered into AM either as portfolio items or as an individual asset[8]. Portfolio items can include any resource that has been entered into the AM system. Assets are those portfolio items that contain additional information about the resource, such as:

- what contracts are associated with the asset
- what work orders are associated with the asset
- what projects the asset is assigned to
- any purchase requests for the asset
- any purchase orders for the asset
- any receiving slips for the asset

Portfolios are made up of the portfolio items and assets distributed throughout the IT and non-IT infrastructure. These items can be classified individually or as collections. Portfolio items contain:

- A description of the portfolio item
- The user and manager who were issued the item
- The geographic location of the item
- The cost center liable for the item

Both assets and portfolio items, which are maintained in separate tables by AM, contain the information in the bulleted lists above as fields within their respective tables.

Portfolio items can be tracked individually, collectively (by batch), and via undifferentiated management. Individual and batch items are tracked in the Assets table. Undifferentiated batches are not tracked. Individualized management is used to track portfolio items of substantial value. For example, a server can be tracked individually with regards to its exact location, supervisor, price, depreciation type, etc. All of this information is tracked uniquely to the particular asset. Collective management (by batch) is used to track identical portfolio items of lesser value. In this case, the Assets table holds information that helps keep track of the entire batch rather than the unique instances of each item in the batch. The benefit of using a batch method is that tracking information (such as acquisition price) is not duplicated across multiple items. Undifferentiated management (by untracked batch) is used for items of little value, or consumables (such as pencils and ink cartridges).

AM portfolio management uses a system of tables to structure and organize portfolios and related information. Each table is linked to the portfolio items or assets tables and contains fields representing relevant information to the resources in the system. This information includes such

[8] Due to the duplicate usage of asset to mean resources entered into the AM system, and also the physical manifestation of those items in the real world, the more generic usage of “asset” will be referred to as “resource” throughout the remainder of this document. Any further reference to an asset will refer to an asset entered into the AM system.

fields as license expiration, the person the resource was issued to, the cost center of the resource, etc.

After resources have been added to AM, the system provides services that can be used to gather insights about the data being tracked. These services include:

- Measuring total cost of ownership
- Aligning business services to their supporting assets and contracts
- Avoiding potential penalties by using license management automation
- Enabling fixed asset and invoice reconciliation
- Directly tying IT cost to business unit consumption
- Optimized allocation of IT assets for greatest Return On Investment (ROI)
- Complete asset and project expense audit tracking

The following software components compose and are collectively referred to as the AM system:

- **Asset Portfolio**: The Asset Portfolio component is the heart of AM implementation. It defines and manages the relationships among assets, contracts, and costs, providing consistent and accurate inventory information.
- **Procurement**: The Procurement component automates and streamlines the entire request lifecycle. It verifies each request against corporate approval standards by validating against a catalog of approved assets, and monitors existing stocks and budgets so that requests are filled through available inventory.
- **Contracts**: The Contracts component simplifies, automates, and improves the business processes related to contract management. It tracks contract terms and conditions and sends automatic notifications of important dates, such as contract expirations.
- **Financials**: The Financials component captures, monitors, and manages all costs associated with an asset, from acquisition through retirement.
- **Software Asset Management**: The Software Asset Management component provides a simple, standardized and proactive way to manage software license compliance. Using a central repository of existing contracts, the Software Asset Management component associates software purchase invoices with each software license agreement.

AM can also utilize separate automated discovery and inventory tools, such as HP Universal Discovery and Universal Configuration Management Database. These tools automatically discover portfolio items and assets on the IT infrastructure (such as computers, servers, software, license information etc.) and add them to the AM database. The following applications can be added to AM to enhance the functionality provided by the total solution:

- **Federation**: Federation offers the ability to integrate and share data across IT processes. Through its integrated processes, data can be pulled from multiple sources, integrated, and shared with the end user at the presentation layer.
- **Connect-It**: Connect-It is an application that creates tests and administers integration scenarios between AM and a wide variety of other external applications. Connect-It leverages industry-standard protocols and connects with third-party information systems, including HP, BMC, CA[9], and IBM[10] products, to import data into AM.
- **Web Services**: Web Services provides interoperability between software applications running on disparate platforms. It uses Simple Object Access Protocol (SOAP) technology to establish a standard messaging framework.

AM and Connect-It provide the majority of their functionality via a pair of graphical interfaces. These interfaces are available through a client installed on a Windows system. In addition, the AM interface can be accessed via a web-based version through Internet Explorer or Firefox running Java 1.6 or 1.7. This interface can interoperate with Department of Defense Common Access Cards (CAC) and Personal Identity Verification (PIV) authentication mechanisms using the X.509 certificates within these cards, when properly configured. The interfaces offer a series of menus, toolbars, buttons, and form elements. Additionally, users have access to graphical dashboards, tables, and graphs that allow users to visualize the data managed by AM and set up integration tasks for Connect-It. All access to this functionality is controlled by a role-based access control policy. The Windows client is accessed through the Windows operating system. An Application Programming Interface (API) version of the AM interfaces is also available.

Command Line Interface (CLI) utilities for both AM and Connect-It are also available on the client system. These are used primarily for maintenance and database access purposes. These utilities include the Asset Manager Export Tool, Asset Manager Import Tool, Asset Manager Automated Process Manager, and Asset Manager Application Designer. These tools have a graphical and CLI implementation. The tools are used to import and export data from the Asset Manager database, set up automated tasks for the Asset Manager system, and design applications that can perform repetitive tasks on the Asset Manager system. The AM CLI tools are accessed via the Access Manager Graphical User Interface (GUI). The Connect-IT CLI tools are accessed through the Connect-It GUI.

AM includes a set of FIPS-validated cryptographic libraries, OpenSSL (modified to correct the Heartbleed vulnerability) runs on the client machine and RSA BSAFE Crypto-J operates on the AM servers. The RSA BSAFE Crypto-J library provides an SP800-90 compliant HMAC-DRBG for key generation. AM uses the cryptographic functionality provided by these libraries to protect

[9] CA – Computer Associates

[10] IBM – International Business Machines

communications between the client and server components, to protect stored passwords, and to protect connections to external LDAP[11] servers, if present.

1.4 TOE Overview

The TOE Overview provides a detailed listing of the components and functionality included in the TOE. It also describes the environment and documentation required for proper use of the TOE.

1.4.1 TOE Components

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-only TOE and provides an organized way to manage the life cycle of IT infrastructure from procurement to end-of-life. AM facilitates enterprise management of physical objects and the events associated with the life cycle of these objects. CIT is integrated with AM to assist in importing data to the AM database.

The TOE is deployed on three platforms. The platforms are part of the TOE environment, but the TOE components on each platform are described below:

- Client
  - AM Client provides user interface and CLI utilities for AM.
  - Connect-It Client provides user interface and CLI utilities for Connect-It and all Connect-It functionality.
  - OpenSSL FIPS module provides secure communications for the Client
- AM Front End Server
  - AM Web Tier provides web-based access for non-client users.
  - Apache Tomcat server hosts the web interfaces.
  - BSAFE Crypto-J FIPS module provides secure communications for Front End Server.
- AM Back End Server
  - AM API provides access to database and accepts connections from AM Front End and external components.
  - Apache Tomcat server hosts the web interfaces.
  - BSAFE Crypto-J FIPS module provides secure communications for Back End Server.
  - AM Server Components includes Asset Portfolio, Procurement, Contracts, Financials, and Software Asset Management as described above.

[11] LDAP – Lightweight Directory Access Protocol

1.4.2 TOE Secure Functionality

These components work together to provide the security functionality of the product.

The BSAFE Crypto-J FIPS libraries and OpenSSL FIPS library provide the TOE with the capability to generate and destroy keys and perform cryptographic operations. These operations include secure communications between some TOE components, secure management on the AM web UI, and secure communications with a LDAP server. These libraries also perform start-up self tests to verify cryptographic functions prior to offering these functions.

The Connect-It client allows users to create and manage scenarios and connections to external discovery and inventory tools prior to identification and authentication. For all other functions, the TOE requires user to authenticate before granting access to functionality or data within the TOE. During authentication the TOE obscures user passwords with bullets. After authentication, the TOE implements role-based access controls for user attempting to access the various screens of the AM UI, the data stored in the AM database, and all connectors attempting to import data to or export data from the TOE. By default, users are given a set of guest permissions that can be modified by a user with Administrative rights permission. A user with Administrative rights permissions can configure user accounts to lock out users after a configurable number of failed login attempts.

The AM and Connect-It UIs are the primary management interfaces for the TOE. Users with Administrative rights permissions are granted full access to the functionality of these interfaces and all data in the database. Other users have access restricted according their role-based access control settings. Administrative rights permissions allow a user to manage license keys, databases, database objects, and user roles and permissions.

Data stored within the AM database can be analyzed to ensure that only authorized users have access to assets and that only authorized hardware and software is used by an asset.

Additionally, Section 1.5.3 lists any logical and functional components of the above components that are excluded from the evaluation. The TOE does not include any of the hardware components that compose the server and client systems.

Figure 2 shows the details of the deployment configuration of the TOE:

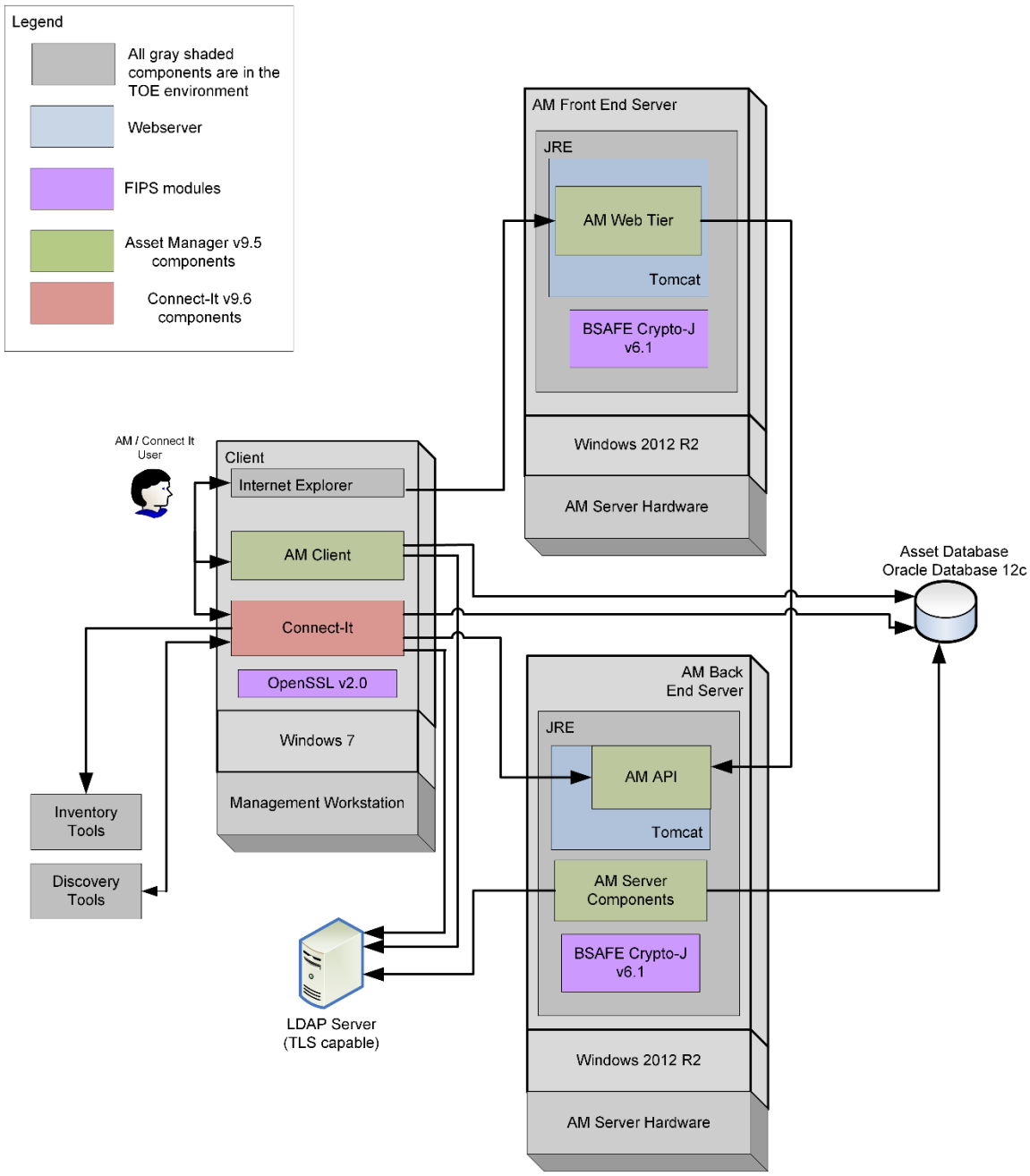

Figure 2 Deployment Configuration of the TOE

1.4.3 Non-TOE Hardware/Software/Firmware

AM runs on independent server hardware with an Intel Xeon or equivalent processor. The recommended server configuration includes 4 Gigabytes (GB) of free RAM[12] (with an additional 2 GB available for Automated Process Manager) and 4 GB of hard-disk space (and an additional 4 GB allocated for Automated Process Manager). For the operating environment, HP recommends one of:

- Microsoft Windows Server 2008 R2 or 2012 R2 (used in the evaluated configuration)
- Red Hat Enterprise Linux 5 or 6

Additionally, the recommended database management system for the server component includes one of:

- Microsoft Structured Query Language (SQL)
- Oracle Database 12c (used in the evaluated configuration)
- IBM DB2 9.7 or 10.1

For the client components, the recommended operating environments include Microsoft Windows 7 or 8. Additionally, clients should have Oracle Java Runtime Environment 1.7 or 1.8 and Internet Explorer 10 or later or Mozilla Firefox 29 or later.

The TOE requires a remote LDAP server capable of supporting Transport Layer Security (TLS) connections in the TOE environment. The LDAP server handles authentication for all credentials submitted by users attempting to login to the TOE.

As an optional component of the TOE Environment, the TOE can connect to an HP Universal Discovery or Universal Configuration Management Database in order to automatically discover assets on the network and propagate their information into the AM database. The Federation and Web Services applications are also optional components that can exist within the TOE environment if desired.

The TOE is placed in a secure facility along with the LDAP server and AM database. These components are connected on an internal network that is protected by a firewall any access from outside of the secure facility must use VPN access to the corporate network. Only the AM Web GUI is accessible from outside of this internal network.

1.5 TOE Description

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

[12] RAM – Random Access Memory

1.5.1 Physical Scope

Figure 3 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

The TOE is a resource tracking tool which runs on a Windows or Linux Operating System (OS) compliant to the minimum software and hardware requirements as listed in Section 1.5.3. The TOE is software only is delivered via the HP download site https://softwaresupport.hp.com/. The TOE is installed on a client and two server platforms as depicted in Figure 3 below. The essential physical components of the TOE in the evaluated configuration are

- Asset Manager v9.50 software
- Connect-It v9.60 software
- Server to host the Asset Manager software,

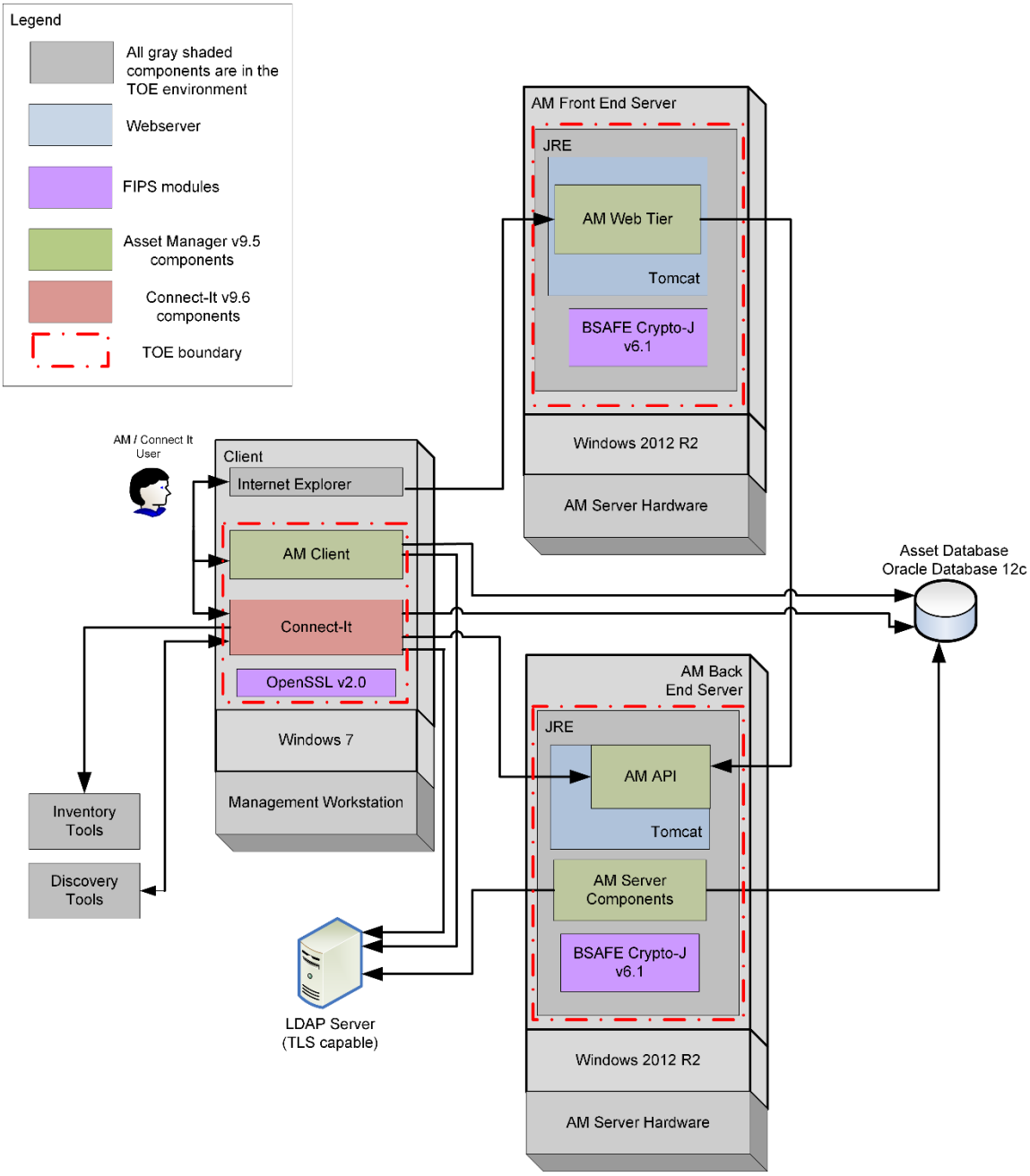

Figure 3 TOE Boundary

1.5.1.1 Guidance Documentation

The following guides are provided in PDF format and are required reading and part of the TOE:

- HP Asset Manager Software Version: 9.50 Installation and Upgrade
- HP Asset Manager Software Version: 9.50 Administration

- HP Asset Manager Software Version: 9.50 Concepts and Implementation
- HP Asset Manager Software Version: 9.50 Programmer Reference
- HP Asset Manager Software Version: 9.50 User Interface
- HP Asset Manager Software Version: 9.50 Release Notes
- HP Asset Manager Software Version: 9.50 Web Implementation
- HP Connect-It Software Version: 9.60 Quick Start
- HP Connect-It Software Version: 9.60 User Guide
- HP Connect-It Software Version: 9.60 Connector Guide
- HP Connect-It Software Version: 9.60 Asset Manager Database Integration Solution
- HP Connect-It Software Version: 9.60 Programmer's Reference
- HP Connect-It Software Version: 9.60 Release Notes

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:

- Cryptographic Support,
- User Data Protection,
- Identification and Authentication,
- Security Management,
- Protection of the TOE Security Functionality (TSF),
- Trusted Path/Channels
- Asset Management Analysis

1.5.2.1 Cryptographic Support

The TOE provides two FIPS 140-2 validated cryptographic libraries that provide cryptographic services for the TOE. All keys are generated according to FIPS standards for key generation and destroyed via FIPS-approved zeroization methods. Cryptographic operations are provided to secure communications among various physically-separated TOE components and trusted IT products in the TOE environment. Secure operations use TLS v1.1 or v1.2 in the evaluated configuration.

1.5.2.2 User Data Protection

The TOE implements role-based access controls on all users attempting to access the various screens of the AM UIs, the data stored in the AM database, and all connectors attempting to import data to or export data from the TOE. By default, all users with accounts on the TOE are given a set of guest permissions that can be modified by a user with Administrative rights permissions. Users with Administrative rights permissions can also give a different set of permissions to each user.

1.5.2.3 Identification and Authentication

The Connect-It client allows users to create and manage scenarios and connections to external discovery and inventory tools prior to identification and authentication. For all other functions, the TOE requires users to authenticate before granting access to functionality or data within the TOE. While authenticating, the TOE obscures user passwords by replacing the individual characters with bullets while the user is typing the password at the login prompt. The TOE supports the use of certificates or LDAP for authentication. User accounts can be configured to be locked out after a user with Administrative rights permissions-configurable number of failed login attempts.

1.5.2.4 Security Management

The TOE is managed primarily via the AM and Connect-It UIs. All user accounts have an "Administration Rights" permission which can be enabled by authorized users with Administrative rights permissions to grant full access to the functionality of these interfaces and all data in the database. Otherwise, access is constrained by a highly customizable role-based access control system. Management tasks available to users with Administrative rights permissions include management of license keys, databases, and user roles and permissions.

1.5.2.5 Protection of the TSF

The TOE provides a secure connection to a remote LDAP server that is used whenever credentials are passed to be evaluated. The TOE performs cryptographic self-tests during startup to test the proper function of the cryptographic modules. The TOE also performs conditional self-tests during the operation of the cryptographic module in order to ensure that critical functionality of the cryptographic module is working properly.

1.5.2.6 Trusted Path/Channels

The TOE provides a trusted path between users accessing the TOE via the AM web UI. This path uses TLS and its supported cryptographic functionality to secure all communications between the user workstation and the Tomcat server running on the server components of the TOE.

1.5.2.7 Asset Management Analysis

Once data is imported or input into AM, the data can be analyzed to ensure that only authorized users have access to assets and that authorized hardware and software is being used with an asset.

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

No Features/Functionality that are excluded from the evaluated configuration of the TOE.

2 Conformance Claims

This section and Table 2 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 2 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 Common Evaluation Methodology (CEM) as of 2014-07-02 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with Flaw Remediation (ALC_FLR.2)

3 Security Problem

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

- Known and presumed threats countered by either the TOE or by the security environment
- 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 basic skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE. An attacker may initiate a process within the TOE to act on its behalf. This process is assumed to have all attributes of the attacker.
- 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 no physical access to the TOE. TOE users only have access to the TOE remotely.

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 3 below lists the applicable threats.

Table 3 Threats

Name	Description
T.MASQUERADE	An attacker or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.TAMPERING	An attacker or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.

Name	Description
T.UNAUTH	An attacker or a TOE user may gain access to user or TSF data on the TOE, even though they are not authorized in accordance with the TOE security policy.
T.FALREC	Attackers may use the TOE to order or install unauthorized items on the network.
T.INTERCEPT	The TOE may communicate with remote IT entities and user workstations that lie outside of the organization's trusted network. An attacker may attempt to intercept these communications in order to read or modify critical TSF data.

3.2 Organizational Security Policies

There are no Organizational Security Policies defined for this evaluation.

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 4 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 4 Assumptions

Name	Description
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware and operating system.
A.NETCON	The TOE environment provides the network connectivity required to allow the TOE to perform its intended functions.
A.LOCATE	The TOE and external database are located within a controlled access facility.
A.PROTECT	The TOE software will be protected from unauthorized modification.

Name	Description
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The users with Administrative rights who manage the TOE and database administrators who manage the TOE environmental components are non-hostile, appropriately trained, and follow all guidance.

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 5 below.

Table 5 Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE must enforce an access control policy in order to prevent unauthorized users from gaining access to user data stored on the TOE.
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.AUTHENTICATE	The TOE must be 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 system data by protecting itself from unauthorized modifications and access to its functions and data.
O.ANALYZE	The TOE will analyze stored asset data to ensure purchasing and deployment policies are enforced.
O.ALERT	The TOE will alert appropriate administrators if a possible policy violation is found.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 6 below lists the IT security objectives that are to be satisfied by the environment.

Table 6 IT Security Objectives

Name	Description
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.PLATFORM	The TOE hardware and OS must support all required TOE functions.
OE.ACCESSIBILITY	The TOE is positioned on the network such that authorized users are able to access the TOEs functionality while unauthorized external users are blocked from accessing the TOE.

4.2.2 Non-IT Security Objectives

Table 7 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 7 Non-IT Security Objectives

Name	Description
OE.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 and its environment are used securely.
OE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.

5 Extended Components

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

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 8 identifies all extended SFRs implemented by the TOE

Table 8 Extended TOE Security Functional Requirements

Name	Description
AMA_SAD.1	Stored asset data
AMA_SAA.1	Stored asset analysis

5.1.1 Class AMA: Asset Management Analysis

Asset Management analysis involves monitoring stored asset data for inconsistencies with administrator configured policies. The AMA: Asset Management Analysis class was modeled after the CC FAU: Security Audit class. It differs from the FAU: Security Audit class in that the data covered by this class is user data, not audit data. The extended family and related components for AMA_SAD: Stored asset data was modeled after the CC family FAU_GEN: Security audit data generation. The extended families and related components for AMA_SAA: Stored asset analysis are modeled after the CC family FAU_SAA: security audit analysis.

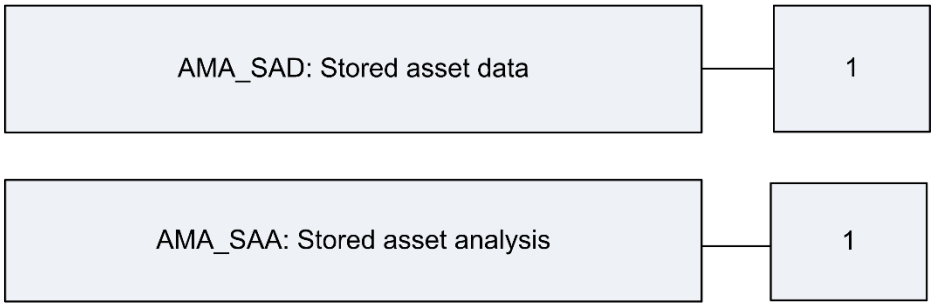

Figure 4 AMA: Asset Management Analysis Class Decomposition

5.1.1.1 Stored asset data (AMA_SAD)

Family Behaviour

This family defines the requirements for the information from each asset that is stored. This family enumerates the types of assets that the TSF shall store data for and identifies the minimum set of information that should be stored for each asset.

Component Leveling

Figure 5 AMA Stored asset data family decomposition

AMA_SAD.1 Stored asset data, defines the types of assets for which data is stored and specifies the minimum list of data stored for each asset.

Management: AMA_SAD.1

There are no management activities foreseen.

Audit: AMA_SAD.1

There are no auditable events foreseen.

AMA_SAD.1 Stored asset data

Hierarchical to: No other components.

Dependencies: No other components.

AMA_SAD.1.1

The TSF shall be able to store data for at least the following types of assets: [assignment: *types of assets stored and managed by the TOE*].

AMA_SAD.1.2

The TSF shall store at least the following information for each asset: [assignment: *data stored for an asset, data associated with an asset*].

5.1.1.2 Stored asset analysis (AMA_SAA)

Family Behaviour

This family defines the analysis the TOE performs on the stored asset data. This family describes the action taken if a potential policy violation is found in the data.

Component Leveling

Figure 6 AMA Stored asset analysis family decomposition

AMA_SAA.1 Stored asset analysis specifies that the TSF shall monitor the stored data according to configurable rules and alert the asset owner if a rule violation is detected.

Management: AMA_SAA.1

The following actions could be considered for the management functions in FMT:

a) Maintenance of the rules by adding, modifying, deletion of rules from the set of rules.

Audit: AMA_SAA.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Minimal: Enabling and disabling of any of the analysis mechanisms.

AMA_SAA.1 Stored asset analysis

Hierarchical to: No other components.

Dependencies: AMA_SAD.1.

AMA_SAA.1.1

The TSF shall be able to apply a configurable set of rules in monitoring the stored asset data and based upon these rules indicate unauthorized hardware, software, or users.

AMA_SAA.1.2

The TSF shall enforce the following rules for monitoring stored asset data: [assignment: *list of rules asset data is monitored for*].

5.2 Extended TOE Security Assurance Components

There are no extended SARs 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.
- 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*
FCS_CKM.1	*Cryptographic key generation*		✓		✓
FCS_CKM.4	*Cryptographic key destruction*		✓		
FCS_COP.1(a)	*Cryptographic operation (Server)*		✓		✓
FCS_COP.1(b)	*Cryptographic operation (Client)*		✓		✓
FDP_ACC.1	*Subset access control*		✓		

Name	Description	S	A	R	I
FDP_ACF.1	Security attribute based access control		✓		
FDP_ETC.2	Export of user data with security attributes		✓		
FDP_ITC.1	Import of user data without security attributes		✓		
FIA_AFL.1	Authentication failure handling	✓	✓		
FIA_UAU.1	Timing of authentication		✓		
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UAU.5	Multiple authentication mechanisms		✓		
FIA_UID.1	Timing of identification		✓		
FMT_MOF.1	Management of security functions behavior	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialization	✓	✓		
FMT_SMF.1	Specification of Management Functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_ITC.1	Inter-TSF confidentiality during transmission				
FPT_TST.1	TSF testing	✓	✓		
FTP_TRP.1	Trusted path	✓	✓		
AMA_SAA.1	Stored asset analysis		✓		
AMA_SAD.1	Stored asset data		✓		

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

Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
Dependencies: FCS_COP.1(a) Cryptographic operation (Front End and Back End Server)
FCS_COP.1(b) Cryptographic operation (AM Client)
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 [*key sizes listed in Table 10*] that meet the following: [*none*].

Table 10 List of Key Sizes that the TOE (Server) can Generate

Key Type	Key Sizes	Security Strength
AES[13] Key	128	128
Triple-DES[14] 3-Key	168	112

Table 11 List of Key Sizes that the TOE (client) can Generate

Key Type	Key Sizes	Security Strength
AES Key	128	128
Triple-DES 3-Key	168	112
Keyed Hash (HMAC)	SHA-1, SHA-2 (256)	N/A

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: 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(a) Cryptographic operation (Front End and Back End Server)
Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(a)

[13] AES – Advanced Encryption Standard
[14] DES – Digital Encryption Standard

The TSF shall perform [*the operations listed in Table 12 "Cryptographic Operation" column*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms listed in Table 12 "Cryptographic Algorithm" column*] and cryptographic key sizes [*the cryptographic key sizes listed in Table 12 "Key/Digest Size" column*] that meet the following: [*the standards listed in Table 12 "Standard (cert. #)" column*].

Table 12 Server-Provided Cryptographic Services

Cryptographic Operation	Cryptographic Algorithm	Cipher Modes	Key/Digest Size	Standard (cert. #)
Symmetric Cipher	AES	Cipher-Block Chaining (CBC)	128	FIPS 197 (cert. #2249)
	Triple-DES 3-Key	CBC	168	FIPS 46-3 (cert. #1408)
Message Digest	SHA	N/A	SHA-1 (160), SHA-2 (256)	FIPS 180-4 (cert. #1938)
Message Authentication Code	HMAC-SHA	N/A	SHA-1 (160), SHA-2 (256)	FIPS 198-1 (cert. #1378)
Signature	RSA	N/A	1024, 2048, 3072, 4096	FIPS 186-3 (cert. #1154)

FCS_COP.1(b) Cryptographic operation (AM Client)
Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(b)

The TSF shall perform [*the operations listed in Table 13 "Cryptographic Operation" column*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms listed in Table 13 "Cryptographic Algorithm" column*] and cryptographic key sizes [*the cryptographic key sizes listed in Table 13 "Key/Digest Size" column*] that meet the following: [*the standards listed in Table 13 "Standard (cert. #)" column*].

Table 13 Client-Provided Cryptographic Services

Cryptographic Operation	Cryptographic Algorithm	Cipher Modes	Key/Digest Size	Standard (cert. #)
Symmetric Cipher	AES	CBC	128	FIPS 197 (cert. #1884, 2116, 2234, 2342, 2394, 2484)
	Triple-DES 3-Key	CBC	168	FIPS 46-3 (cert. #1223, 1346, 1398, 1465, 1492, 1522)

Cryptographic Operation	Cryptographic Algorithm	Cipher Modes	Key/Digest Size	Standard (cert. #)
Message Digest	SHA	N/A	SHA-1 (160), SHA-2 (256)	FIPS 180-4 (cert. #1655, 1840, 1923, 2019, 2056, 2102)
Message Authentication Code	HMAC-SHA	N/A	SHA-1 (160), SHA-2 (256)	FIPS 198-1 (cert. #1126, 1288, 1363, 1451, 1485, 1526)
Signature	RSA	N/A	1024, 1536, 2048, 3072, 4096	FIPS 186-3 (cert. #960, 1086, 1145, 1205, 1273)

6.2.1 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 [*Database Access Control SFP*[15]] on [

Subjects:

- *User accounts:*
  - *Client connections*
  - *Data connector connections*

Objects (client connections):

- *Data objects*
  - *Databases*
  - *Tables*
  - *Fields*
  - *Screen*
  - *Wizard*

Operations:

- *Access:*
  - *Create data object*
  - *Modify data object*
  - *View data object*
  - *Delete data object*
  - *Import data object*
  - *Export data object*
  - *View GUI screen*
  - *Launch GUI wizard*

].

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 [*Database Access Control SFP*] to objects based on the following: [

Subjects:

- *User accounts:*

[15] SFP – Security Functionality Policy

- *Client connection attributes:*
  - *Client IP address*
  - *Username*
  - *Associated permissions (User Rights, Functional Rights, and Access Restrictions)*
- *Data connector connection attributes:*
  - *Data connector IP address*
  - *Username*
  - *Associated permissions (User Rights, Functional Rights, and Access Restrictions)*

Objects (client connections):

- *Data objects*
  - *Database attributes*
    - *Database name*
  - *Table attributes:*
    - *Table name*
    - *Database name*
  - *Field attributes:*
    - *Field name*
    - *Table name*
    - *Database name*
  - *Screen attributes:*
    - *Screen name*
  - *Wizard attributes:*
    - *Wizard name*

].

FDP_ACF.1.2

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

- *If a user's role has the appropriate Functional Rights to access the screen or wizard within the Asset Manager, then access is allowed,*
- *If a user's role has the appropriate User Rights to access the table, field, or link, then access is allowed,*
- *If a user's role is not restricted with an Access Restriction to read the field, then a read or export request is permitted,*
- *If a user's role has the appropriate Access Restriction to write to the field, then a write or import request is permitted,*
- *Otherwise, all access, read, and write requests are denied.*

].

FDP_ACF.1.3

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

- *If a user has the "Administration rights" permission enabled, then that user is granted full access to all objects and screens in the Asset Manager*
- *All users can view file locations, but not file content, when presented in error messages*].

FDP_ACF.1.4

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

FDP_ETC.2 Export of user data with security attributes
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FDP_ETC.2.1

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

FDP_ETC.2.2

The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3.

The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4

The TSF shall enforce the following rules when user data is exported from the TOE: [*no additional rules*].

FDP_ITC.1 Import of user data without security attributes
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation
FDP_ITC.1.1

The TSF shall enforce the [*Database Access Control SFP*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*no additional rules*].

6.2.2 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication
FIA_AFL.1.1

The TSF shall detect when [an administrator configurable positive integer within [*3 to 10*]] unsuccessful authentication attempts occur related to [*attempted logins via the Asset Manager UI, AM Web Tier interface, and AM API*].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*lock the account until an administrator manually unlocks it or 15 minutes have passed*].

FIA_UAU.1 Timing of authentication
Hierarchical to: No other components
Dependencies: FIA_UID.1 Timing of identification
FIA_UAU.1.1

The TSF shall allow [*creation, modification, deletion, and scheduling of Connect-It scenarios; creating and deleting connections to discovery and inventory tools; and creation or deletion of database connection*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

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: FIA_UID.1 Timing of identification
FIA_UAU.5.1

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

FIA_UAU.5.2

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

1. *Users accessing the AM Web Tier interface can use X.509 certificates if the TOE has been configured for two-way SSL authentication.*
2. *All other users, on all other interfaces must use LDAP with username and password for authentication.*
3. *All users use LDAP with username and password when two-way authentication is not configured*].

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 representing characters of the password*] to the user while the authentication is in progress.

FIA_UID.1 Timing of identification
Hierarchical to: No other components
Dependencies: No dependencies
FIA_UID.1.1

The TSF shall allow[*creation, modification, deletion, and scheduling of Connect-It scenarios; creating and deleting connections to discovery and inventory tools; and creation or deletion of database connection*] on behalf of the user to be performed before the user is identified.

FIA_UID.12

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

6.2.3 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 [*Asset Manager database behavior*] to [*users with the "Administration rights" permission enabled*].

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles
FMT_MSA.1.1

The TSF shall enforce the [*Database Access Control SFP*] to restrict the ability to [change_default, modify] the security attributes [*Functional Rights, Access Restrictions, User Rights*] to [*users with the "Administration rights" permission enabled*].

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 [*Database Access Control SFP*] to provide [[*administrator-defined "guest" role permissions*]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*users with the "Administration rights" permission enabled*] 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: [

- *Management of the Asset Manager Database*
- *Management of access types (read, write)*
- *Management of user and guest permissions*

].

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 [*custom profiles*[16] *defined by a user with the "Administration rights" permission enabled*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

[16] A profile is a construct that takes each database or database object access permission and access type and defines it for a narrow role (for example, the "Saint Louis Accountant" profile would have access to fields within an accounting table for the St. Louis office, Purchasing supervisor would have access to the purchase orders table, etc.)

6.2.4 Class FPT: Protection of the TSF

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

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

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

The TSF shall run a suite of self tests [during initial start-up, periodically during normal operation] to demonstrate the correct operation of [[*the FIPS-validated OpenSSL and RSA BSAFE cryptographic modules*]].

FPT_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of [[*the FIPS-validated OpenSSL and RSA BSAFE cryptographic modules*]].

FPT_TST.1.3

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

Application Note 1: The OpenSSL integrity check is performed voer the contents included within the cryptographic module boundary, which is defined as the internal binary regions of libeay32-10.dll. These can be identified by following the guidelines in the Object Code Tutorial v0.7 document, provided by the OpenSSL foundation.

Application Note 2: The RSA BSAFE integrity check is performed over the contents included within the cryptographic module boundary defined as jcm_fips.jar.

6.2.5 Class FTP: Trusted Path/Channels

FTP_TRP.1 Trusted path
Hierarchical to: No other components.
Dependencies: No dependencies
FTP_TRP.1.1

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

FTP_TRP.1.2

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

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [initial user authentication, [*administration of the TOE, user access to data stored on the TOE*]].

6.2.6 Class AMA: Asset Management Analysis

AMA_SAD.1 Stored asset data
Hierarchical to: No other components.
Dependencies: No other components.
AMA_SAD.1.1

The TSF shall be able to store data for at least the following types of assets: [

a) Servers;
b) Computers;
c) Software;].

AMA_SAD.1.2

The TSF shall store at least the following information for each asset: [

a) Stored data: asset name, location of asset, asset owner, asset licenses
b) Associated data: approved software, approved user].

AMA_SAA.1 Stored asset analysis
Hierarchical to: No other components.
Dependencies: AMA_SAD.1.
AMA_SAA.1.1

The TSF shall be able to apply a configurable set of rules in monitoring the stored asset data and based upon these rules indicate unauthorized hardware, software, or users.

AMA_SAA.1.2

The TSF shall enforce the following rules for monitoring stored asset data:[

a) An owner is assigned to key assets and the licenses of those assets;
b) An entitlement is granted for a department or user to use licenses of an asset;
c) A report is generated showing departments and users entitled to use asset licenses;
d) TSF sends a message to the owner when departments or users exceed concurrent usage limit for licenses of an asset;
e) TSF sends a message to the owner when hardware, software, or users not associated with or entitled to licenses of an asset are detected for an asset].

6.3 Security Assurance Requirements

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

Table 14 Assurance Requirements

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

7 TOE 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 security functionality implemented in the actual TOE. Hence, each implementation of the security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 15 lists the security functionality and their associated SFRs.

Table 15 Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(a)	Cryptographic operation (Server)
	FCS_COP.1(b)	Cryptographic operation (Client)
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_ETC.2	Export of user data with security attributes
	FDP_ITC.1	Import of user data without security attributes
	AMA_SAA.1	Stored asset analysis

TOE Security Functionality	SFR ID	Description
	AMA_SAD.1	Stored asset data
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_UAU.1	Timing of authentication
	FIA_UAU.7	Protected authentication feedback
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.1	Timing of identification
Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of TOE Security Functionality	FPT_ITC.1	Inter-TSF confidentiality during transmission
	FPT_TST.1	TSF testing
Trusted Path/Channels	FTP_TRP.1	Trusted path
Asset Management Analysis	AMA_SAA.1	Stored asset analysis
	AMA_SAD.1	Stored asset data

7.1.1 Cryptographic Support

The TOE contains two FIPS 140-2 validated cryptographic libraries:

- OpenSSL 2.0 modified to remove the Heartbleed vulnerability
- RSA BSAFE Crypto-J v6.1

The OpenSSL library resides in the AM client and provides TLS with AES and Triple-DES 3-Key encryption and decryption services for remote users accessing the TOE. The Crypto-J library resides in the Front End and Back End servers and provides TLS v1.1 or v1.2 with AES and Triple-DES 3-Key encryption and decryption services for these server components. The Crypto-J library is used when the servers connect to remote clients, secure remote-LDAP server connections, connections between each other, and SHA-256 hashing for passwords stored locally on the TOE. TLS also makes use of digital signatures, hashing, and MAC functionality provided by the cryptographic libraries.

The FIPS modules are completely contained within the TOE boundary and contain all instructions to generate and zeroize cryptographic keys. Keys are generated by a deterministic random bit generator for both client and server modules. Zeroization meets FIPS 140-2 requirements. All cryptographic operations performed by the modules use FIPS-validated algorithms. All algorithms and certificate numbers are listed above in Table 12 and Table 13.

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

7.1.2 User Data Protection

The TOE implements a role-based access control mechanism to determine which users can access data stored on the TOE. Users are required to have an entry in the Departments and Employees table in order to log into the system. By default, users with Administrative rights permissions-defined set of “guest” permissions are assigned to users logging into the TOE. User with Administrative rights permissions can modify a user’s role at any time in order to give different permissions to a user.

Access to database objects (databases, tables, fields, links, and indexes) requires that users have access to each object. A user can also be given Functional Rights, which allow the user to view and use the various pages within the Asset Manager UI.

The TOE uses User Rights to determine which tables, fields, and links a user is allowed to access. If a user doesn’t have the appropriate User Right for an object, then the user cannot access the data stored on the TOE in that object. The User Right does not determine the type of access allowed, only whether access is allowed to the object or not.

The type of access (if any) granted to a user is determined by the user’s Access Restrictions, which can be read, write, or none. Having read Access Restrictions allows a user to view data stored in a given field of the database from the Asset Manager UI. Having read Access Restrictions allows a user to view or export data stored in a given filed of the database from the Asset Manager web

UI. Having write Access Restrictions allows a user to write or import data to a given field of the database. If a user does not have read or write Access Restrictions then the user cannot view, modify, import, or export the data in a given field of the database.

Connect-It performs imports and exports of data via the AM API, so access rights are identical to those of AM. Data exported from the TOE is exported with security attributes. The tables and their associations are maintained when exported from the TOE.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_AFC.1, FDP_ETC.2, FDP_ITC.1.

7.1.3 Identification and Authentication

The TOE obscures all credentials when they are typed into the login screens of any of the user interfaces used to access the TOE by replacing the actual characters in the password with bullets. The TOE can use a secure connection to a remote trusted LDAP server to authenticate users accessing the user and management interfaces provided by the TOE. Authentication can also be performed with certificates when the AM Web Tier is configured to support two-way SSL authentication. The X.509 formatted certificate is loaded into the browser on the management workstation and used for authentication to the AM Web Tier. The X.509 certificate authentication requires the LDAP server for validating the username. The TOE user is granted access to the TOE if the X.509 certificate's UPN[17] or CN[18] match the username of an existing TOE account. Users are given a user with Administrative rights permissions-configurable number of attempts to successfully log into the Asset Manager UIs, browser interface, and API before the TOE automatically locks those accounts. The default number of attempts is 3. Accounts can be manually unlocked by a user with Administrative rights permissions or are automatically unlocked after 15 minutes.

The TOE allows users to connect to the external database through AM UI without authentication. All other actions on the AM interfaces require successful authenticated with their identity and password. The Connect-It interfaces are unauthenticated and allow:

- Creation, modification, and deletion of scenarios prior to authentication. These scenarios include usernames and passwords that are used to authenticate to the TOE when the scenario is run.
- Connections to external discovery and inventory tools to be established or deleted.

Stored passwords in scenarios and connectors are encrypted.

[17] UPN – User Principle Name

[18] CN – Common Name

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

7.1.4 Security Management

The TOE provides an Asset Manager UI and Connect-It UI that can be installed on a client workstation as standalone applications. The Asset Manager UI can also be accessed via a web browser and used as a web-based interface. These interfaces provide users with Administrative rights permissions and other users with the ability to view, edit, administer, and maintain the TOE database (user management and creation and deletion of databases).

The TOE limits access to administrative functions (functions other than reading or writing data in the database) to users who have the "Administration rights" permission enabled (there is a check box in each users profile that allows this setting to be toggled). All users are granted "guest" permissions by default upon creation of the user account. Users with the "Administration rights" permission enabled can control the permissions granted to the default guest role, and can also issue a new role to users as needed. These permissions should be restricted to basic permissions (log in, change own password, view own entry in user table) until a users with Administrative rights permissions grants the user additional privileges.

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

7.1.5 Protection of the TSF

The TOE protects passwords transmitted from the server components of the TOE to the remote trusted LDAP server. This channel uses TLS and a FIPS 140-2 validated RSA BSAFE Crypto-J library to initiate cryptographic connections between the TOE server and the LDAP server. Passwords transmitted over this connection are encrypted and decrypted via FIPS-approve AES or Triple-DES 3-Key algorithms.

Due to the inclusion of two FIPS 140-2 validated cryptographic modules, the TOE automatically checks the integrity of each module during the startup of the TOE software components. The OpenSSL module boundary, for integrity checking includes the internal binary regions of libeay32-10.dll, which are identified by the guidelines listed in the OpenSSL foundation's Object Code Tutorial v0.7. The RSA BSAFE integrity check is performed over the contents included within the cryptographic module boundary defined as jcm_fips.jar. Additionally, the TOE runs self-tests to check the correct operation of the algorithms provided by these modules at startup (power-on self-tests) and whenever a random number is generated or an asymmetric key is generated by one of the modules (conditional self-tests).

The power-on self-tests generally check the encryption function by encrypting a known plaintext and comparing it to a known ciphertext. The conditional self-test for DRBG checks to see if the

module has generated a random number that is different from the previously generated number. The conditional self-test for asymmetric key pairs encrypts a known plaintext with the newly generated key and then decrypts it with the other key in the pair to ensure that the two keys are compatible. If any errors occur during any of the self-tests, then the module displays an error message on the system console.

TOE Security Functional Requirements Satisfied: FPT_ITC.1, FPT_TST.1.

7.1.6 Trusted Path/Channels

The TOE implements a trusted path between users on the client system and the AM front end server and AM back end server. This path uses TLS and a FIPS 140-2 validated BSAFE Crypto-J library to initiate cryptographic connections between the client and the server. The trusted path is used by users and administrators accessing the TOE via a web browser.

TOE Security Functional Requirements Satisfied: FTP_TRP.1.

7.1.7 Asset Management Analysis

The TOE can store data on many types of assets. The key asset types that are analyzed for security violations are: servers, computers, software, and users. For each asset, the TOE stores the asset name, its licenses, and its physical location. An owner is assigned to each asset. This owner is responsible for managing and maintaining the asset, as well as granting entitlements to departments and users to use the licenses of that asset. Other assets (such as approved hardware and software) can be associated with the asset. Users with Administrative rights permissions can create workflows that periodically monitor the data stored for an asset, including license entitlement and usage. If an asset's concurrently used licenses exceed the license limit, the TSF will send a message to the asset owner. If unauthorized hardware, software, or license user is detected, the TSF will send a message to the asset owner. This allows the owner to ensure only approved hardware and software are being used and that only entitled users have access to the asset.

TOE Security Functional Requirements Satisfied: AMA_SAD.1 and AMA_SAA.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 3 and has extended Part 2 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 16 below provides a mapping of the objects to the threats they counter.

Table 16 Threats: Objectives Mapping

Threats	Objectives	Rationale
T.MASQUERADE An attacker or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	By ensuring that The TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data, O.AUTHENTICATE satisfies this threat.
T.TAMPERING An attacker 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.

Threats	Objectives	Rationale
	O.PROTECT The TOE must ensure the integrity of 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.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT ensures that the TOE is protected from external interference or tampering.
T.UNAUTH An attacker or a TOE user may gain access to user or TSF data on the TOE, even though they are not authorized in accordance with the TOE security policy.	O.ACCESS The TOE must enforce an access control policy in order to prevent unauthorized users from gaining access to user data stored on the TOE.	The objective O.ACCESS ensures that access control policies prevent unauthorized users from gaining access to user data stored on the TOE.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	The objective O.ADMIN ensures that access to TOE security data is limited to those users with access to the management functions of the TOE.
	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	The objective O.AUTHENTICATE ensures that users are identified and authenticated prior to gaining access to TOE security data.

Threats	Objectives	Rationale
T.INTERCEPT The TOE may communicate with remote IT entities and user workstations that lie outside of the organization's trusted network. An attacker may attempt to intercept these communications in order to read or modify critical TSF data.	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	The objective O.AUTHENTICATE ensures that the users of the TOE must be authenticated before they are granted access to any data stored on the TOE.
	O.PROTECT The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data.	The objective O.PROTECT ensures that the TOE ensures the integrity of TSF data by protecting itself from unauthorized modifications and access.
T.FALREC Attackers may use the TOE to order or install unauthorized items on the network.	O.ANALYZE The TOE will analyze stored asset data to ensure purchasing and deployment policies are enforced.	The objective O.ANALYZE ensures that stored data on items are analyzed according to defined policies.
	O.ALERT The TOE will alert appropriate administrators if a possible policy violation is found.	The objective O.ALERT ensures that a message or alert is sent when a policy violation is detected.

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 evaluation.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 17 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 17 Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate, dedicated hardware and operating system.	OE.PLATFORM The TOE hardware and OS must support all required TOE functions.	OE.PLATFORM ensures that the TOE hardware and OS supports the TOE functions.
	OE.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 and its environment are used securely.	Those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use. OE.MANAGE satisfies this assumption.
A.NETCON The TOE environment provides the network connectivity required to allow the TOE to perform its intended functions.	OE.ACCESSIBILITY The TOE is positioned on the network such that authorized users are able to access the TOEs functionality while unauthorized external users are blocked from accessing the TOE.	OE.ACCESSIBILITY satisfies the assumption that the TOE environment will provide the appropriate connectivity to allow the TOE to perform its function.
A.LOCATE The TOE and external database are located within a controlled access facility.	OE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	Physical security is provided within the TOE environment to provide appropriate protection to the network resources. OE.PHYSICAL satisfies this assumption.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	The TOE environment provides protection from external interference or tampering. OE.PROTECT satisfies this assumption.

Assumptions	Objectives	Rationale
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.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 and its environment are used securely.	OE.MANAGE satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.
A.NOEVIL The users with Administrative rights who manage the TOE and database administrators who manage the TOE environmental components are non-hostile, appropriately trained, and follow all guidance.	OE.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 and its environment are used securely.	OE.MANAGE satisfies the assumption that the users who manage the TOE and its environment are non-hostile, appropriately trained and follow all guidance.

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 AMA requirements was created to specifically address the analysis of the stored asset data. The CC FAU: Security Audit class was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of asset data monitoring and provide for requirements for alerting when violations are detected. These requirement's dependencies have been noted in 5.1.1. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended SARs defined for this evaluation.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 18 below shows a mapping of the objectives and the SFRs that support them.

Table 18 Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must enforce an access control policy in order to prevent unauthorized users from gaining access to user data stored on the TOE.	FDP_ACC.1 Subset access control	The requirement meets the objective by ensuring that access control is applied to all users before granting access to data stored on the TOE.
	FDP_ACF.1 Security attribute based access control	The requirement meets the objective by ensuring that the TOE enforces access control based on the implemented policy.
	FDP_ETC.2 Export of user data with security attributes	The requirement meets the objective by ensuring that any attempt to export data from the TOE must meet the requirements of the access control policy before the export is allowed.

Objective	Requirements Addressing the Objective	Rationale
	FDP_ITC.1 Import of user data without security attributes	The requirement meets the objective by ensuring that any attempt to import data to the TOE must meet the requirements of the access control policy before the import is allowed.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that only authorized administrators have the capability to modify the permissions for the access control policy.
	FMT_MSA.3 Static attribute initialization	The requirement meets the objective by ensuring that appropriate default values are granted for new user accounts and that only authorized administrators can modify the initial default permissions.
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.	FIA_AFL.1 Authentication failure handling	The requirement meets the objective by ensuring that security attributes, including authentication failure thresholds, may only be changed by authorized users.
	FMT_MOF.1 Management of security functions behavior	The requirement meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges.

Objective	Requirements Addressing the Objective	Rationale
	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.ALERT The TOE will alert appropriate administrators if a possible policy violation is found.	AMA_SAA.1 Stored asset analysis	The requirement meets the objective by messaging the asset owner if a potential violation is detected.
O.ANALYZE The TOE will analyze stored asset data to ensure purchasing and deployment policies are enforced.	AMA_SAA.1 Stored asset analysis	The requirement meets the objective by analyzing stored data to determine if unauthorized hardware, software, or users are associated with an asset.
	AMA_SAD.1 Stored asset data	The requirement supports the objective by ensuring the TOE stores the data necessary for analysis.

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_AFL.1 Authentication failure handling	In order to ensure that users are properly authenticated prior to access, the TOE enforces a lockout after a configurable number of unsuccessful authentication attempts. The requirement for authentication failure handling meets the objective by mitigating the risk of a brute force attack on a username and password.
	FIA_UAU.1 Timing of authentication	The requirement meets the objective by ensuring that users are authenticated before access to all TOE administrative functions except those specified is allowed.
	FIA_UAU.5 Multiple authentication mechanisms	The requirement meets the objective by providing different authentication mechanisms and by specifying when the TOE uses each mechanism.
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by obscuring a user's password while it is being typed into the login prompt for the user interfaces provided by the TOE. This prevents an adversary from reading the password as it is being entered by a user and logging in with their credentials.

Objective	Requirements Addressing the Objective	Rationale
	FIA_UID.1 Timing of identification	The requirement meets the objective by ensuring that the users are identified before access to all TOE administrative functions except those specified is allowed.
	FMT_MOF.1 Management of security functions behavior	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.
O.PROTECT The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data.	FCS_CKM.1 Cryptographic key generation	The requirement meets this objective by ensuring that cryptographic keys created for use by the TOE meet recommended standards for secure generation.
	FCS_CKM.4 Cryptographic key destruction	The requirement meets the objective by ensuring that cryptographic keys no longer in use by the TOE are destroyed via recommended standard key destruction methods.
	FCS_COP.1(a) Cryptographic operation (Server)	The requirement meets the objective by ensuring that the TOE uses recommended standards for all cryptographic functionality implemented to secure communications with trusted remote IT systems.

Objective	Requirements Addressing the Objective	Rationale
	FCS_COP.1(b) Cryptographic operation (Client)	The requirement meets the objective by ensuring that the TOE uses recommended standards for all cryptographic functionality implemented to secure communications with trusted remote IT systems.
	FIA_UAU.1 Timing of authentication	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 all TOE functions except those specified.
	FIA_UID.1 Timing of identification	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 all TOE functions except those specified.
	FPT_ITC.1 Inter-TSF confidentiality during transmission	The requirement meets the objective by ensuring that the TOE protects communications with remote trusted IT products when exporting data from the TOE.

Objective	Requirements Addressing the Objective	Rationale
	FPT_TST.1 TSF testing	The requirement meets the objective by testing the correct operation of the cryptographic functionality provided by the TOE.
	FTP_TRP.1 Trusted path	The requirement meets the objective by ensuring that communications initiated by a remote workstation to manage the TOE are protected from unauthorized disclosure or modification.

8.5.2 Security Assurance Requirements Rationale

EAL2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. The System is expected to be placed into a non-hostile position and protected by other products designed to address threats that correspond with the intended environment. At EAL2+, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 19 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 19 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FCS_CKM.1	FCS_COP.1(a)	✓	
	FCS_COP.1(b)	✓	
	FCS_CKM.4	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1(a)	FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FCS_COP.1(b)	FCS_CKM.4	✓	
	FCS_CKM.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_ETC.2	FDP_ACC.1	✓	
FDP_ITC.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FIA_AFL.1	FIA_UAU.1	✓	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UAU.7	FIA_UAU.1	✓	
FIA_UAU.5	FIA_UID.1	✓	
FIA_UID.1	None	Not applicable	

SFR ID	Dependencies	Dependency Met	Rationale
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	Not applicable	
FMT_SMR.1	FIA_UID.1	✓	
FPT_ITC.1	None	Not applicable	
FPT_TST.1	None	Not applicable	
FTP_TRP.1	None	Not applicable	
AMA_SAA.1	AMA_SAD.1	✓	
AMA_SAD.1	None	Not applicable	

9 Acronyms and Terms

This section and Table 20 define the acronyms and terms used throughout this document.

9.1 Acronyms

Table 20 Acronyms and Terms

Acronym	Definition
AD	Active Directory
AES	Advanced Encryption Standard
AM	Asset Manager
API	Application Programming Interface
CA	Computer Associates
CAC	Common Access Card
CBC	Cipher Block Chaining
CC	Common Criteria
CD/DVD	Compact Disk/Digital Versatile Disc
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CN	Common Name
DES	Digital Encryption Standard
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GB	Gigabyte
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
HP	Hewlett Packard
IBM	International Business Machines
ID	Identifier
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code

Acronym	Definition
OS	Operating System
PIV	Personal Identity Verification
PP	Protection Profile
RAM	Random Access Memory
ROI	Return On Investment
RSA	Rivest, Shamir, Adelman
SAR	Security Assurance Requirement
SFP	Security Functionality Policy
SFR	Security Functionality Requirement
SHA	Secure Hashing Algorithm
SOAP	Simple Object Access Protocol
SP	Special Publication
SQL	Structured Query Language
SSL	Secure Socket Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UI	User Interface
UPN	User Principal Name

9.2 Terminology

Asset – any item (such as computers, software installations, office supplies, or machines-tools) that is entered into the Asset Manager system.

Resource – Due to the duplicate usage of asset to mean resources entered into the Asset Manager system, and also the physical manifestation of those items in the real world, the more generic usage of “asset” will be referred to as “resource” throughout the remainder of this document. Any further reference to an asset will refer to an asset entered into the Asset Manager system.

Prepared by:

Corsec Security, Inc.

13291 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