Security Target

McAfee Data Loss Prevention Endpoint 10.0 and ePolicy Orchestrator 5.1.3

Document Version1.1

October 11, 2016

Prepared For:

Intel Corporation.

2821 Mission College Blvd.

Santa Clara, CA 95054

Prepared By:

Primasec Ltd

Le Domaine de Loustalviel

11420 Pech Luna, France

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Data Loss Prevention Endpoint 10.0 and ePolicy Orchestrator 5.1.3. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	Security Target: McAfee Data Loss Prevention Endpoint 10.0 and ePolicy Orchestrator 5.1.3
ST Revision	1.1
ST Publication Date	October 11, 2016
Author	Primasec Ltd

1.2 TOE Reference

TOE Reference	McAfee Data Loss Prevention Endpoint 10.0 and ePolicy Orchestrator 5.1.3
TOE Type	Data Loss Prevention

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by *italicized* text.
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by underlined text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FIA_UAU.1.1 (1) and FIA_UAU.1.1 (2) refer to separate instances of the FIA_UAU.1 security functional requirement component.

Outside the SFRs, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table describes the terms and acronyms used in this document:

TERM	DEFINITION
AD	Active Directory
CC	Common Criteria version 3.1 (ISO/IEC 15408)
DBMS	DataBase Management System
DLPe	Data Loss Prevention Endpoint
EAL	Evaluation Assurance Level
ECB	Electronic CodeBook
ePO	ePolicy Orchestrator
GUI	Graphical User Interface
I&A	Identification & Authentication
IP	Internet Protocol
IT	Information Technology
NTFS	New Technology File System
OS	Operating System
OSP	Organizational Security Policy
PDC	Primary Domain Controller
PP	Protection Profile

TERM	DEFINITION
RAM	Random Access Memory
RM	Rights Management
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Mail Protocol
SP	Service Pack
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
VGA	Video Graphics Array
XML	eXtensible Markup Language

Table 2 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

McAfee Data Loss Prevention Endpoint software protects enterprises from the risk associated with unauthorized transfer of data from within the organization to the outside. Data loss is defined as confidential or private information leaving the enterprise as a result of unauthorized communication, through channels such as applications, physical devices, or network protocols.

Seamless integration with McAfee ePolicy Orchestrator® (ePO™) eases DLPe Agent deployment, policy management, and reporting. ePO provides the user interface for the TOE via a GUI accessed from remote systems using web browsers. Custom reports can be fully automated, scheduled, or exported. ePO requires the user to identify and authenticate themselves before access is granted to any data or management functions. Audit log records are generated to record configuration changes made by ePO users. The audit log records may be reviewed via the GUI. Users can review the results of the DLP policy audits via ePO. Access to this information is controlled by per-user permissions.

The endpoint components (DLP Endpoint Agent and McAfee Agent as described below) integrate with the RSA BSAFE Crypto-C Micro Edition v4.0.1 to provide crypto services, while ePolicy Orchestrator integrates with OpenSSL v1.0.1m with FIPS module v2.0.8 for crypto services. The endpoint and server components must be installed in FIPS mode (as detailed in *Common Criteria Evaluated Configuration Guide for McAfee Data Loss Prevention Endpoint 10.0* and *User Guide McAfee ePolicy Orchestrator 5.1.0 Software FIPS Mode)* to ensure that cryptographic services used by the TOE are FIPS validated.

The following sections provide a summary of the specific TOE sub-components.

1.6.1 DLP Endpoint Agent

The DLPe Agents reside on enterprise computers, which are referred to as managed computers, and enforce the DLP policies and rules defined in the DLP Policy Manager. The agents monitor user activities

to record, control, and prevent unauthorized users from copying, printing, uploading to the internet (or Cloud repositories such as Dropbox) or transferring corporate confidential data outside of the corporate network via email, FTP or any other network protocols. The DLP Endpoint Agents also generate events that are recorded by the ePO Event Parser, and store to a network file server the original sensitive file (or email) that was copied or transferred in order for it to be used as an evidence for the event.

1.6.2 McAfee Agent

McAfee Agent is a vehicle of information and enforcement between the ePO server and each managed system. McAfee Agent deploys McAfee products, retrieves updates, runs client tasks, distributes policies, and forwards events from each managed system back to ePO. McAfee Agent uses a secure channel (using TLS v1.2) to transfer data from/to the ePO server.

1.6.3 ePolicy Orchestrator

ePolicy Orchestrator (ePO) provides a platform for centralized policy management and enforcement of DLPe on the managed systems. It uses the System Tree to organize managed systems into units for monitoring, assigning policies, scheduling tasks, and taking actions. The System Tree is a hierarchical structure that allows administrators to combine managed systems into groups. Policies can then be applied to groups of managed systems, rather than individually.

ePO allows administrators to manage the targeted systems from a single location through the combination of product policies and client tasks. Policies ensure that the DLPe features are configured correctly. Client tasks are the scheduled actions that run on the managed systems hosting the DLPe Agents. Client tasks are commonly used for product deployment, product functionality, upgrades, and updates.

Within the TOE configuration the ePO software is comprised of the following components:

1.6.3.1 ePO Server

The ePO server deploys DLPe agents to managed systems (via the McAfee agent) and controls DLPe agent updates, it creates DLPe policies and distributes them to the managed systems, and processes the events for all the managed systems. It includes the following subcomponents:

- **Policy Catalog**
  The ePO policy catalog stores the DLPe Policies and allows an ePO user to edit, delete, duplicate or create new DLP policies. The types of DLP policies are:
  - *DLP Policy* – contains rule sets and endpoint discovery scans;
  - *Client Configuration* – contains settings to control the DLPe agent on managed systems;
  The policy is the entity that is distributed to managed systems to enforce the DLP rules.
- **DLP Classifications**
  Defines the content classification options (e.g. PCI, PHI, HIPAA) and the classification criteria and the definitions used to configure them. It also sets up registered document repositories and user authorization for manual tagging.
- **DLP Policy Manager**
  Defines the data protection rules, device control rules, endpoint discovery rules, and the

definitions used to configure them. Multiple rules are grouped into a rule set, and multiple rule sets can be assigned to a DLP Policy.

- **DLP Incident Manager**
  Events resulting from policy violations, sent to the DLP Event Parser, are displayed in the DLP Incident Manager, a GUI accessed from the ePolicy Orchestrator Reporting console. All events can be filtered and sorted based on criteria such as protection rule types, severity, date, time, user, computer name, or policy version. Events can be labeled by the administrator for tracking purposes.
- **DLP Operational Events**
  Displays administrative events, such as deployments, policy updates and operational errors (such as DLPe agent could not copy evidence file to evidence share – no sufficient space)
- **Application server**
  This includes the Automatic Response[1] functionality, Registered Servers (see below), and the user interface.
- **Agent handler**
  Distributes network traffic generated by agent-to-server communications responsible for communicating policies, tasks, and properties.
- **Event parser**
  This parses events received from DLPe Agents and insert them into the ePO DBMS.
- **Registered servers** - used to register different server types in ePO (e.g. LDAP, SNMP, Ticketing servers, MS-RMS server).

1.6.3.2 Database

The database is the central storage component for all data created and used by ePO. The database can be housed on the ePO server, or on a separate server, depending on the specific needs of the organization. However, the evaluated configuration only supports the database housed on the same server as ePO.

1.6.3.3 Master Repository

The Master Repository is the central location for all McAfee updates and signatures, and it resides on the ePO server. The Master Repository retrieves user-specified updates and signatures from McAfee or from user-defined source sites.

1.7 TOE Description

McAfee Data Loss Prevention Endpoint is a content-based agent solution that inspects enterprise users' actions concerning sensitive content in their own work environment, their computers. It uses advanced discovery technology as well as predefined dictionaries, regular expressions and validation algorithms to identify this content, and incorporates plug and play and removable storage device management for additional layers of control.

[1] Automatic Responses functionality allows administrators to create rules for responding to events that are specific to the managed business environment, such as sending email notifications or SNMP traps, or creating issues for use with integrated third-party ticketing systems.

1.7.1 Physical Boundary

The TOE is a software TOE and includes:

1. The ePO application executing on a dedicated server with DLP Extension
2. The McAfee Agent application on each managed system to be audited
3. The DLP Endpoint Agent software on each managed system to be audited

Note specifically that the hardware, operating systems and third party support software (e.g. DBMS) on each of the systems are excluded from the TOE boundary.

In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	DLP ePO Extension 10.0.0.9 (with Full DLP license) DLP Endpoint Agent 10.0.0.1322 ePolicy Orchestrator 5.1.3.188 with Hotfix 1151890 McAfee Agent 5.0.2.132 with MA ePO Server extension[2] 5.0.2.118
IT Environment	Specified in the following: • Table 4 – ePO Server System Requirements • Table 5 – Supported Agent Platforms • Table 6 –Agent Platform Hardware Requirements

Table 3 – Evaluated Configuration for the TOE

The evaluated configuration consists of a single instance of the management system (with ePO and the DLP Incident Manager and DLP Policy Manager as provided by the DLP ePO Extension) and one or more instances of managed systems (with McAfee Agent and the DLP Endpoint Agent).

ePO supports authentication of user account credentials either by Windows or ePO itself (ePO by default). Both are supported in the evaluated configuration. User accounts (other than the password) are still required to be defined in ePO so that attributes and permissions can be associated with the account.

The following figure presents an example of an operational configuration. The shaded elements in the boxes at the top of the figure represent the TOE components.

[2] This extension is the McAfee Agent v5.0.2 ePO Policy and Reporting Extension (RTW)

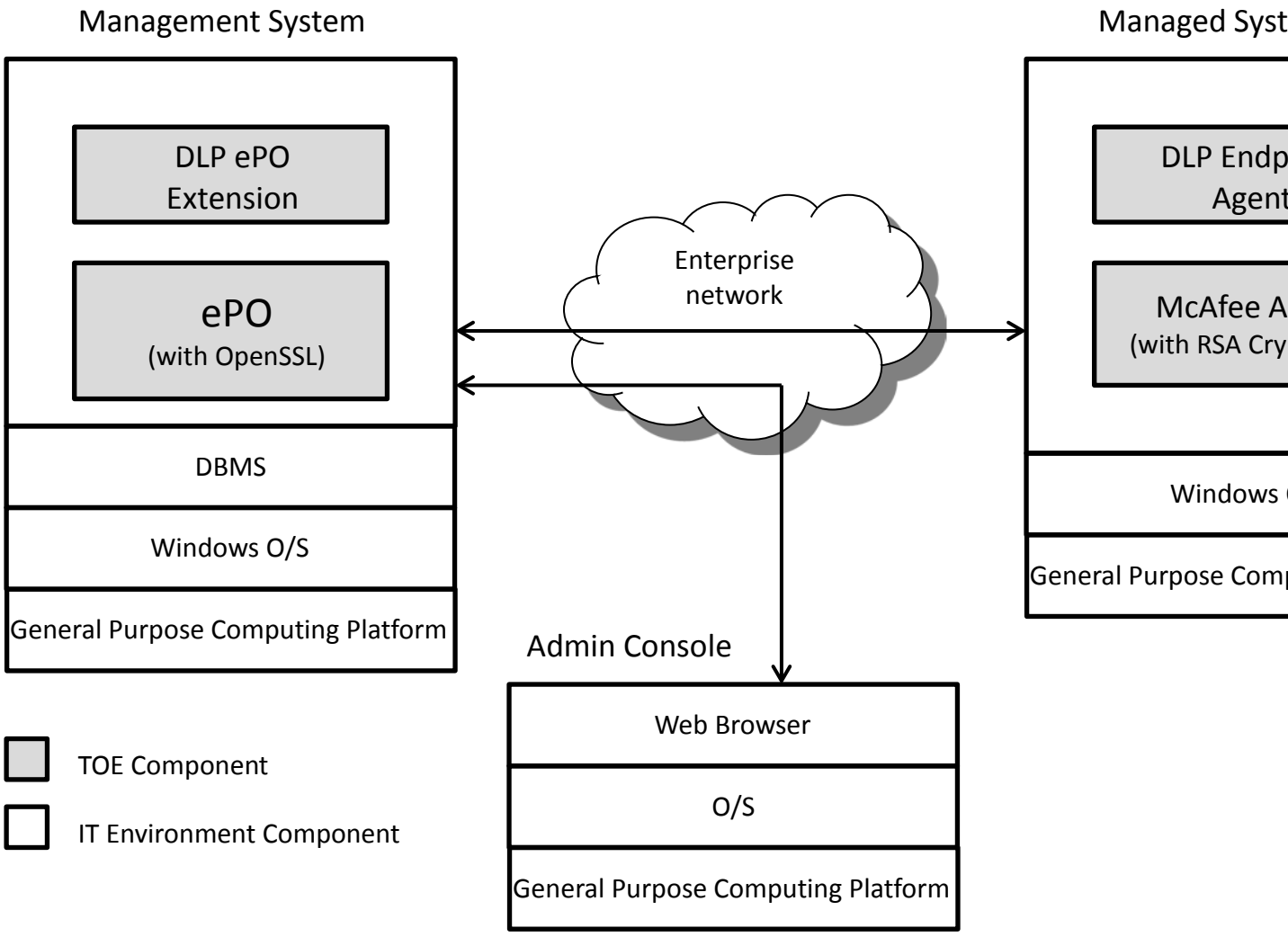

Figure 1 – TOE Boundary

The following specific configuration options apply to the evaluated configuration:

1. McAfee Agent wake-up calls are enabled.
2. Incoming connections to McAfee Agents are only accepted from the configured address of the ePO server.
3. The only repository supported is the ePO server.

1.7.2 Hardware and Software Supplied by the IT Environment

The TOE consists of a set of software applications. The hardware, operating systems and all third party support software (e.g., DBMS, Active Directory server) on the systems on which the TOE executes are excluded from the TOE boundary.

The platform on which the ePO and DLPe software are installed must be dedicated to functioning as the management system. The ePO server operates as a distribution system and management system for a client-server architecture offering components for the server part of the architecture (not the clients).

The TOE requires the following hardware and software configuration on this platform.

The ePO server system requirements are:

COMPONENT	MINIMUM REQUIREMENTS
Processor	64-bit Intel Pentium D or higher 2.66 GHz or higher
Memory	8 GB available RAM recommended minimum
Free Disk Space	80 GB — Recommended minimum
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	Windows Server 2008 R2
DBMS	Microsoft SQL Server 2008 R2
Network Card	Ethernet, 100Mb or higher
Disk Partition Formats	NTFS
Domain Controllers	The system must have a trust relationship with the Primary Domain Controller (PDC) on the network
Miscellaneous	Microsoft .NET Framework 2.0 or later Microsoft Visual C++ 2005 SP1 Redistributable Package Microsoft Visual C++ 2008 Redistributable Package (x86) MSXML 6.0

Table 4 – ePO Server System Requirements

The McAfee Agent and DLP Endpoint Agent execute on one or more systems whose policy settings are to be audited. The platforms within the scope of the evaluation for DLP endpoint agent are:

SUPPORTED OS FOR DLPE AGENT	PLATFORM
Windows 7	X64 platforms
Windows 10	X64 platforms
Windows 2008 R2 Server	X64 platforms
Windows 2012 R2 Server	X64 platforms

Table 5 – Supported Agent Platforms

The minimum hardware requirements for the agent platforms are specified in the following table:

COMPONENT	MINIMUM HARDWARE REQUIREMENTS
Processor speed	1 GHz or higher
Memory	1GB RAM
Free Disk Space	300MB, excluding log files
Network Card	Ethernet, 100Mb or higher

Table 6 –Agent Platform Hardware Requirements

The ePO management system is accessed from remote systems via a browser. The browser used to access the ePO management system in this evaluation was:

- Microsoft Internet Explorer 11.0.

The TOE relies on ePO or Windows to authenticate user credentials during the logon process. User accounts must be defined within ePO in order to associate permissions with the users.

1.7.3 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

TSF	DESCRIPTION
Policy Enforcement	The TOE enforces DLP policies on managed systems and audits end-user action against those policies. The TOE ensures end users aren't allowed to copy files as specified by an administrator through a data loss prevention policy. DLP incidents and operational events are stored in the database (the DBMS is in the IT Environment), and reports based upon completed policy audits may be retrieved via the GUI interface.
Identification & Authentication	On the ePO management system, the TOE requires users to identify and authenticate themselves before accessing the TOE software. User accounts must be defined within ePO, but authentication of the user credentials is performed either by ePO or by Windows. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with their user account that define the functionality the user is allowed to perform. On all managed systems, I&A for local login to the operating system (i.e., via a local console) is performed by the local OS (IT Environment).
Management	The TOE's Management Security Function provides support functionality that enables users to configure and manage TOE components. Management of the TOE may be performed via the GUI. Management privileges are defined per-user.
Audit	The TOE's Audit Security Function provides auditing of management actions performed by administrators. Authorized users may review the audit records via ePO.
System Information Import	The TOE may be configured to import information about systems to be managed from Active Directory (LDAP servers) or domain controllers. This functionality ensures that all the defined systems in the enterprise network are known to the TOE and may be configured to be managed.
TSF Data Protection	The TOE provides TLS v1.1 protection of all communication between the McAfee Agent and ePO, using the crypto services provided by RSA BSAFE Crypto-C Micro Edition v4.0.1 and OpenSSL v1.0.1m library with FIPS module v2.0.8 respectively.

Table 7 –Logical Boundary Descriptions

1.7.4 TOE Guidance

The following guidance documentation is provided as part of the TOE:

- *Product Guide: McAfee Data Loss Prevention Endpoint 10.0.0*
- *Installation Guide McAfee ePolicy Orchestrator 5.1.0 Software*
- *Product Guide for McAfee ePolicy Orchestrator 5.1.0 Software*
- *Product Guide McAfee Agent 5.0.0*[3]

[3] The Product Guide for McAfee Agent 5.0.0 is equally relevant to McAfee Agent 5.0.2

- *Common Criteria Evaluated Configuration Guide for McAfee Data Loss Prevention Endpoint 10.0.0*

1.7.5 Features not part of the evaluated TOE

ePO includes the following features that are not part of the evaluated TOE:

- **Distributed Repositories** - placed throughout a managed environment to provide managed systems access to receive signatures, product updates, and product installations with minimal bandwidth impact.
- **Remote Agent Handlers** - servers installed in various network locations to help manage McAfee Agent communication, load balancing, and product updates.

In addition to the platforms given in Table 4, ePO can also be installed on the following operating system platforms that have not been tested during the evaluation:

- Windows Server 2008 SP2 or later
- Windows Server 2012

Additional supported browsers for access to the ePO management interface that have not been tested during the evaluation are:

- Internet Explorer 8.0 and later
- Firefox 10.0 and later
- Chrome 17 and later
- Safari 6.0 and later

In addition to the platforms given in Tables 5 and 6, the DLPe Agent can also be installed on the following operating system platforms that have not been tested during the evaluation:

- Windows 7 SP1 all editions (32-bit)
- Windows 8 all editions (32-bit and 64-bit)
- Windows Server 2008 SP2 or later 32-bit
- Windows Server 2008 SP2 or later 64-bit
- Windows Server 2012
- Apple OS X Lion 10.7.5 or later
- Apple OS X Mountain Lion 10.8.0 or later
- Apple OS X Mavericks 10.9.0

1.8 Rationale for Non-bypassability and Separation of the TOE

The responsibility for non-bypassability and non-interference is split between the TOE and the IT Environment. TOE components are software only products and therefore the non-bypassability and non-interference claims are dependent upon hardware and OS mechanisms. The TOE runs on top of the IT Environment supplied operating systems.

The TOE ensures that the security policy is applied and succeeds before further processing is permitted whenever a security relevant interface is invoked: the interfaces are well defined and ensure that the access restrictions are enforced. Non-security relevant interfaces do not interact with the security functionality of the TOE. The TOE depends upon OS mechanisms to protect TSF data such that it can only be accessed via the TOE. The system on which the ePO and DLP extension TOE components execute is dedicated to that purpose.

The TOE is implemented with well-defined interfaces that can be categorized as security relevant or non-security relevant. The TOE is implemented such that non-security relevant interfaces have no means of impacting the security functionality of the TOE. Unauthenticated users may not perform any actions within the TOE. The TOE tracks multiple users by sessions and ensures the access privileges of each are enforced.

The server hardware provides virtual memory and process separation, which the server OS utilizes to ensure that other (non-TOE) processes may not interfere with the TOE; all interactions are limited to the defined TOE interfaces. The OS and DBMS restrict access to TOE data in the database to prevent interference with the TOE via that mechanism.

The TOE consists of distributed components. Communication between the components is protected by TLS, as enforced by the McAfee Agent on the endpoint and ePO on the management system, to protect the information exchanged from disclosure or modification.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 4 (September 2012) Part 2 conformant and Part 3 conformant at Evaluation Assurance Level 2 and augmented by ALC_FLR.2 – Flaw Reporting Procedures.

2.2 Protection Profile Conformance Claim

The TOE does not claim conformance to a Protection Profile.

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organizational security policy statements or rules with which the TOE must comply.
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential data loss to go undetected.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the system's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data
T.SENSITIVE_DATA	An unauthorized user may transmit or transfer sensitive data from managed systems.

Table 8 – Threats

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The following Organizational Security Policies apply to the TOE:

POLICY	DESCRIPTION
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.DETECT	Static configuration information that might be indicative of the potential for a future data loss or the occurrence of a past data loss of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.IMPORT	The TOE shall be able to import data about managed systems from LDAP servers and NT Domains.
P.INTEGRITY	Data collected and produced by the TOE shall be protected from modification while in transit.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized access and disruptions of TOE data and functions.

Table 9 – Organizational Security Policies

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the IT Systems the TOE monitors.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.LOCATE	The processing resources of the TOE server will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

Table 10 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ACCESS	The TOE must allow authorized users to access only authorized TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions on the management system.
O.AUDIT_PROTECT	The TOE must provide the capability to protect audit information generated by the TOE.
O.AUDIT_REVIEW	The TOE must provide the capability for authorized administrators to review audit information generated by the TOE.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDENTIFY	The TOE must be able to identify users prior to allowing access to TOE functions and data on the management system.
O.IMPORT	The TOE must provide mechanisms to import system data from Active Directory (LDAP servers) and Domain Controllers.
O.INTEGRITY	The TOE must ensure the integrity of all System data.
O.SENSITIVE_DATA	The TOE must take specified actions upon the access, transmission, printing, or copying of sensitive files or data from managed systems.
O.PROTECT_DATA	The TOE must ensure the integrity of audit and system data by protecting it from unauthorized modifications and access during transfer.

Table 11 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.INTEROP	The TOE must be interoperable with the managed systems it monitors
OE.PERSON	Personnel working as authorized administrators must be carefully selected and trained for proper operation of the System.
OE.DATABASE	Those responsible for the TOE must ensure that access to the database via mechanisms outside the TOE boundary (e.g., DBMS) is restricted to authorized users only.

OBJECTIVE	DESCRIPTION
OE.IDAUTH	The IT Environment must be able to identify and authenticate users prior to them gaining access to TOE functionality on the managed system. It must also be able to authenticate user credentials on the management system when requested by the TOE.
OE.PROTECT	The IT environment must protect itself and the TOE from external interference or tampering.
OE.SD_PROTECTION	The IT Environment must provide the capability to protect system data via mechanisms outside the TOE.
OE.STORAGE	The IT Environment must store TOE data in the database and retrieve it when directed by the TOE.
OE.TIME	The IT Environment must provide reliable timestamps to the TOE

Table 12 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies (if applicable). The following table provides a high level mapping of coverage for each threat, assumption, and policy:

OBJECTIVE / THREAT / ASSUMPTION	O.EADMIN	O.ACCESS	O.IDENTIFY	O.INTEGRITY	OE.INSTALL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTEROP	O.AUDITS	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.IMPORT	O.SENSITIVE_DATA	OE.TIME	OE.PROTECT	OE.SD_PROTECTION	OE.IDAUTH	OE.DATABASE	O.PROTECT_DATA	OE.STORAGE
A.ACCESS									✓												
A.ASCOPE									✓												
A.DATABASE																			✓		
A.DYNMIC								✓	✓												
A.LOCATE						✓															
A.MANAGE								✓													
A.NOEVIL					✓	✓	✓														
A.PROTCT						✓															
P.ACCACT			✓							✓		✓						✓			
P.ACCESS		✓	✓														✓	✓	✓		
P.DETECT										✓					✓						
P.IMPORT													✓								
P.INTEGRITY				✓							✓									✓	✓
P.MANAGE	✓	✓	✓		✓		✓	✓										✓			
P.PROTCT						✓										✓				✓	✓
T.COMDIS		✓	✓													✓		✓			
T.COMINT		✓	✓	✓												✓		✓			
T.IMPCON	✓	✓	✓		✓													✓			
T.LOSSOF		✓	✓	✓														✓			
T.NOHALT		✓	✓															✓			
T.PRIVIL		✓	✓															✓			

OBJECTIVE / THREAT / ASSUMPTION	O.EADMIN	O.ACCESS	O.IDENTIFY	O.INTEGRITY	OE.INSTALL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTEROP	O.AUDITS	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.IMPORT	O.SENSITIVE_DATA	OE.TIME	OE.PROTECT	OE.SD_PROTECTION	OE.IDAUTH	OE.DATABASE	O.PROTECT_DATA	OE.STORAGE
T.SENSITIVE_ DATA														✓							

Table 13 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

The following table provides detailed evidence of coverage for each threat, policy, and assumption:

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions. The OE.INTEROP objective ensures the TOE has the needed access.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors. The OE.INTEROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users. The OE.DATABASE objective ensures that access to any mechanisms outside the TOE boundary that may be used to access the database is configured by the administrators such that only authorized users may utilize the mechanisms.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors. The OE.INTEROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will managed appropriately.
A.LOCATE	The processing resources of the TOE server will be located within controlled access facilities, which will prevent unauthorized physical access. The OE.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The OE.INSTALL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. The OE.PHYCAL provides for the physical protection of the TOE hardware and software.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE. The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDENTIFY objective supports this objective by ensuring each user is uniquely identified. The OE.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The O.AUDIT_REVIEW objective provides the ability for administrators to review the audit records generated by the TOE so that accountability for administrator actions can be determined.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes. The O.IDENTIFY objective provides for identification of users prior to any TOE function accesses via the ePO web interface. The OE.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDENTIFY and OE.IDAUTH objectives by only permitting authorized users to access TOE functions. The OE.SD_PROTECTION and OE.DATABASE objectives address this policy for mechanisms outside the TOE via IT Environment protections of the system data trail and the database used to hold TOE data. The O.ACCESS objective addresses this policy for mechanisms inside the TOE via TOE protections of the system data trail and the database used to hold TOE data.
P.DETECT	Static configuration information that might be indicative of the potential for a future data loss or the occurrence of a past data loss of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected. The O.AUDITS objectives address this policy by requiring collection of audit and policy audit data. The OE.TIME objective supports this policy by providing a time stamp for insertion into the system data records.
P.IMPORT	The TOE shall be able to import data about managed systems from LDAP servers and NT Domains. The O.IMPORT objective addresses this policy by requiring the TOE to provide functionality to import data about managed systems from LDAP servers and NT Domains.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
P.INTEGRITY	Data collected and produced by the TOE shall be protected from modification. This policy relates to data collected and produced by the TOE. It does not relate to user managed data on the endpoint workstation. The O.INTEGRITY objective ensures the protection of System data from modification. The O.AUDIT_PROTECT objective ensures the integrity of audit records generated by the TOE while stored in the database, using TOE access control mechanisms. The O.PROTECT_DATA objective helps to address this policy by requiring the TOE to provide cryptographic functionality and protocols to protect the data during transit. The OE.STORAGE objective requires the IT Environment to provide storage and retrieval mechanisms for System data for use by the TOE.
P.MANAGE	The TOE shall only be managed by authorized users. The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTALL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDENTIFY objective provides for identification of users prior to any TOE function accesses. The OE.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. This data aspects of this policy relate to data collected and produced by the TOE. They do not relate to user data on the endpoint workstation. Hence the objectives addressing this policy will apply TSF data as controlled by the management system (ePO). The OE.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports the TOE protection from the IT Environment and the O.PROTECT_DATA objective helps to address this policy by requiring the TOE to provide cryptographic functionality and protocols to protect the data during transit. The OE.STORAGE objective requires the IT Environment to provide storage and retrieval mechanisms for System data for use by the TOE.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism. This threat relates to data collected and produced by the TOE. It does not relate to user data stored on the endpoint workstation. The O.PROTECT_DATA objective helps to counter this threat by requiring the TOE to provide cryptographic functionality and protocols to protect the data during transit. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE data. The OE.PROTECT objective supports the TOE protection from the IT Environment.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism. This threat relates to data collected and produced by the TOE. It does not relate to user data on the endpoint workstation. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE data. The O.INTEGRITY objective ensures no System data will be modified. The OE.PROTECT objective supports the TOE protection from the IT Environment The O.PROTECT_DATA objective helps to counter this threat by requiring the TOE to provide cryptographic functionality and protocols to protect the data during transit.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential data loss to go undetected. The OE.INSTALL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE data. The O.INTEGRITY objective ensures no System data will be deleted.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.SENSITVE_DATA	An unauthorized user may transmit or transfer sensitive data from managed systems. The O.SENSITIVE_DATA objective requires the TOE to take specified actions upon the access, transmission, printing, or copying of sensitive files or data.

Table 14 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

This Security Target does not include any extended components.

6 Security Requirements

The security requirements that are levied on the TOE are specified in this section of the ST.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and those that were explicitly stated, all of which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_SAR.3	Selectable Audit Review
	FAU_STG.1	Protected Audit Trail Storage
Information Flow Control	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UID.2	User Identification before any action
	FIA_UAU.2	User authentication before any action
	FIA_USB.1	User-Subject Binding
Security Management	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Cryptographic Support	FCS_CKM.1(1-4)	Cryptographic Key Generation
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1	Cryptographic Operation
Protection of the TSF	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
	FPT_TDC.1	Inter-TSF Basic TSF Data Consistency

Table 15 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) *The events identified in* Table 16 – Audit Events and Details

FAU_GEN.1.2 The TSF shall record within each audit record at last the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the information detailed in* Table 16 – Audit Events and Details*.*

Application Note: The auditable events for the (not specified) level of auditing are included in the following table:

COMPONENT	EVENT	DETAILS
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to the TOE and System data	Object IDs, Requested access
FAU_SAR.1	Reading of information from the audit records.	User identity
FAU_SAR.2	Reading of information from the audit records. Note: Unsuccessful attempts to read information from the audit records do not occur because the TOE does not present that capability to users that are not authorized to read the audit records.	User identity
FDP_IFF.1	All requests for information flow that violate a DLP rule.	The presumed addresses of the source and destination subject and the object.
FIA_ATD.1	All changes to TSF data (including passwords) result in an audit record being generated. Note that passwords are not configured, so no audit records for rejection of a tested secret will be generated.	
FIA_UID.2	All use of the user identification mechanism	User identity, location
FIA_UAU.2	All use of the user authentication mechanism	User identity, location
FIA_USB.1	Successful binding of attributes to subjects is reflected in the audit record for successful authentication. Unsuccessful binding does not occur in the TOE design.	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMF.1	Use of the management functions.	User identity, function used
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity
FPT_TDC.1	Use of the asset import function	Data Source, result, identification of which TSF data have been imported

Table 16 – Audit Events and Details

6.1.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *authorized users assigned to ePO Administrator permission set or Global reviewer permission set* with the capability to read *all information* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.5 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to apply *sorting and filtering* of audit data based on *the fields listed in the table below*.

Component	Field	Filter/Sort
ePO Operational Events	Action	Sort
	Completion time	Filter, Sort
	Details	Sort
	Priority	Sort
	Start Time	Filter, Sort
	Success	Filter, Sort
	User Name	Sort
DLP Incident Manager	Event ID	Filter
	Event Type	Filter
	File Type	Filter
	Reactions	Filter
	Resolution	Filter
	Status	Filter

Table 17 – Selectable audit review fields

6.1.1.6 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized

deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the audit records in the audit trail.

6.1.2 Information Flow Control (FDP)

6.1.2.1 FDP_IFC.1 – Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the *DLP Information Flow Control SFP* on

Subjects: Endpoint user and external IT entities attempting to transfer or transmit sensitive data

Information: Files and content stored on the managed system or transferred from the managed system

Operations: copy (to a different destination, e.g. USB device, file server), upload (to web/ftp destination), send to printer, send by email .

Application Note: The following table gives examples of subject/information/object relationships on which the DLP Information Flow Control SFP is enforced:

Subject	Operation	Information
an endpoint user at managed workstation	*copying to a USB device*	*a file*
an endpoint user, using email client on managed workstation	*sending an email*	*with an attachment*
an endpoint user at managed workstation	*sending to a printer*	*a document*
an endpoint user using ftp client on managed workstation	*uploading to a FTP server*	*a file*
an endpoint user at managed workstation	*copying to a different file server*	*a file*

6.1.2.2 FDP_IFF.1 – Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the *DLP Information Flow Control SFP* based on the following types of subject and information security attributes:

Subject: Context:

- *User identity or membership in AD Group*
- *Computer on which the TSF is running*
- *Application performing the copy / transmission action*

Information Security Attributes: Content Classification

- *Dictionary*
- *File Extension*
- *Source File Server – source location from where the file was copied (e.g. the finance file share)*
- *Registered document repository*[4]
- *Text Pattern*
- *Whitelisted text (to reduce false positive detection)*
- *Email Destination (recipients)*
- *Printer to which the information is transmitted*
- *Web Destination to where the file is uploaded or sent*
- *Destination File server to where the file is copied (e.g. copying of sensitive information to the public share is not allowed)*

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *unless an explicit DLP data protection rule is enabled to deny the information flow (see FDP_IFF.1.5 below)*.

FDP_IFF.1.3 The TSF shall enforce ~~the~~ *no other additional rules.*

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: *no explicit authorization rules*.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *a DLP data protection rule is enabled for the subject and information attributes and has a block reaction*.

[4] This refers to a set of confidential documents that are manually selected by DLP administrators and uploaded to the DLP management console in order create fingerprints of these documents. The fingerprints are distributed to all DLP endpoint clients, and allow DLP endpoint client to detect fragments of text from these confidential documents and block (or report) the copy or transmission of content from these files by FTP, email or web-upload.

Application note: *For example, block send email if the sender is member of the finance (AD group) and the information contains more than 1 social security number (text patterns) and more than 1 credit card number (text pattern) and email is sent to email recipients outside the corporate domain.*

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual ePO users:

a) ePO User name;

b) Authentication configuration (either Windows authentication or local ePO password);

c) *Permission Sets.*

6.1.3.2 FIA_UID.2 User Identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.3 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note: The TOE performs identification on the management system, and then, depending on the configuration of the user account, either relies upon Windows for authentication or performs authentication based on the local ePO password. Hence, authentication on the management system is the responsibility of the operating environment when Windows authentication is configured.

6.1.3.4 FIA_USB.1 User-Subject Binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user:

a) ePO user name; and

b) Permissions.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: *user security attributes are bound upon successful login with a valid ePO User Name*.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: *user security attributes do not change during a session.*

Application Note: The TOE binds security attributes to subjects for ePO sessions. Windows binds security attributes to subjects for workstation sessions. Permissions are determined by the union of all permissions in any permission set associated with a user. If the security attributes for a user are changed while that user has an active session, the new security attributes are not bound to a session until the next login.

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, clear, *create, export and use* the *TSF data identified in* Table 18 – TSF Data Access Permissions *to an ePO Administrator or a user with appropriate permissions*.

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
Audit Log	View Audit log	View
	View and purge audit log	View, delete
Dashboards	Use public dashboards	Use public dashboards
	Use public dashboards, create and edit private dashboards	Use public dashboards, create and modify private dashboards
	Use public dashboards, create and edit private dashboards, make private dashboards public	Use public dashboards, create, delete and modify private dashboards, make private dashboards public
	View Audits and Assignments	Query DLP policy audit event records
ePO User Accounts	Only allowed by an ePO Administrator	Query, create, delete and modify
DLP Policies	User can view all Policies	View
	User has full permissions to all Policies	View, create, delete, modify
	Override permissions for a specific policy to be: - user has no no-permission to access specific policy - user can view specific policy - user has full permission to specific policy	
DLP Rule Sets	User can use all rule sets	- Assign rule sets to policies. - Assign rule sets to scans.

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
	User can view all rule sets	- View rule sets content. - Assign rule sets to policies. - Assign rule sets to scans.
	User has full permission to all rule sets	- Create, delete and modify rule sets - View rule sets content. - Assign rule sets to policies. - Assign rule sets to scans.
	Override permissions for a specific rule set to be: - user can use specific rule set - user can view specific rule set - user has full permission to specific rule set	
DLP Classifications: Manual classification	User can manage manual classifications	Select AD users and groups that are allowed to manually classify files on managed systems (endpoints)
DLP Classifications: Registered documents and whitelisted text	User can manage Registered documents and whitelisted text creation	Upload files to be indexed as registered documents or as whitelisted text
DLP Classifications: Classifications access control	User can use all classifications	- Select classifications in DLP protection rules
	User can view all classifications	- View classification criteria and tagging criteria. - Select classification in DLP protection rules.
	User has full permission to classifications	- Create, delete and modify classifications - Create, delete and modify classification criterions. - Create, delete and modify tagging criterions. - View classification criterion - view tagging criterions - select classifications in DLP protection rules

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
	Override permissions for a specific classification to be: - user can use specific classification - user can view specific classification - user has full permission to specific classification	
DLP Definitions. Note: there are 29 different types of definitions. Each type can have use or view or full permission	User can use items of this definition type	- Use items of this type in classification criterions, discovery scans and DLP protection rules.
	User can view items of this definition type	- Use items of this type in classification criterions, discovery scans and DLP protection rules.
	User has full permission to items of this definition type	- Use items of this type in classification criterions, discovery scans and DLP protection rules. - View the content of a definition item. - create, delete and modify items of this type.
DLP Incidents: Incidents Access Control	User can see incidents assigned to him	View, set reviewer, add comments, set severity, set resolution
	User can see incidents assigned to members of the following permission sets <list>	View, set reviewer, add comments, set severity, set resolution
	User can see all incidents	View, set reviewer, add comments, set severity, set resolution
DLP Incidents: Incidents Data redaction	Sensitive data is redacted	Limited view – IP, usernames and computer names are obfuscated
	Sensitive data is in clear	View
	User can reveal redacted sensitive data (4 eyes)	View
DLP Incidents: Incident task Creation	User can create a Mail Notification task	View, create, delete, modify
	User can create a Purge task	View, create, delete, modify
	User can create a Set Reviewer task	View, create, delete, modify
DLP Incidents: Operational Events	User can see operational events assigned to him	View, set reviewer, add comments, set severity, set resolution
	User can see operational events assigned to members of the following permission sets <list>	View, set reviewer, add comments, set severity, set resolution
	User can see all operational events	View, set reviewer, add comments, set severity, set resolution

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
Permission Set	n/a (only allowed by an ePO Administrator	Query, create, duplicate, delete, modify, and assign (to a user) permissions
Queries and Reports	Use public groups	Query and use public groups
	Use public groups; create and edit private queries/reports	Query and use public groups; create and modify private queries/reports
	Edit public groups; create and edit private queries/reports; make private queries/reports public	Query, delete, modify and use public groups; create, delete and modify (including make public) private queries/reports
Registered Servers – LDAP	View registered servers	View
Systems	View "System Tree" tab	View
System Tree access	Access nodes and portions of the System Tree	Access nodes and portions of the System Tree

Table 18 – TSF Data Access Permissions

6.1.4.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

a) ePO user account management,

b) Permission set management,

c) Audit Log,

d) DLP Policy and rules (including policy management, Incidents Access Control, DLP Incidents Data redaction, Incident task Creation, Operational Events)

e) Registers Servers,

f) Systems and System tree access,

g) Query and Report management,

h) Dashboards.

6.1.4.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles: *ePO Administrator and ePO User assigned to a permission set comprised of any of the following permissions:*

a. Audit Log

b. *Dashboards*
c. *DLP Policies*
d. *DLP Rule Sets*
e. *DLP Classifications*
f. *DLP Definitions*
g. *DLP Incidents Access Control;*
h. *DLP Incidents Data redaction;*
i. *DLP Incident task Creation;*
j. *DLP Operational Events*
k. *Queries and Reports*
l. *Registered Servers*
m. *Systems*
n. *System Tree access.*

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application Note: An ePO Administrator is a user account assigned to the built-in Global Administrator permission set. Users are defined ePO user accounts without Administrator permission set but with other specific permission sets.

Application Note: In ePO a role is called a permission set.

6.1.5 Cryptographic Support (FCS)

6.1.5.1 FCS_CKM.1(1) Cryptographic key generation (ePO AES)

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *CTR_DRBG for deterministic random bit generation* and specified cryptographic key sizes *256 bits for encryption/decryption* that meet the following *NIST Special Publication 800-90 (CAVP algorithm certificate #540)*.

6.1.5.2 FCS_CKM.1(2) Cryptographic key generation (ePO RSA)

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *CTR_DRBG for deterministic random bit generation* and specified cryptographic key sizes *2048 bits for key transport* that meet the following *NIST Special Publication 800-90 (CAVP algorithm certificate #540)*.

6.1.5.3 FCS_CKM.1(3) Cryptographic key generation (MA AES)

FCS_CKM.1.1(3) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *HMAC_DRBG for random number generation* and specified cryptographic key sizes *256 bits for*

encryption/decryption that meet the following *NIST Special Publication 800-90A (CAVP algorithm certificate #191)*.

6.1.5.4 FCS_CKM.1(4) Cryptographic key generation (MA RSA)

FCS_CKM.1.1(4) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *HMAC_DRBG for random number generation* and specified cryptographic key sizes *2048 bits for key transport* that meet the following *NIST Special Publication 800-90A (CAVP algorithm certificate #191)*.

6.1.5.5 FCS_CKM.4 Cryptographic key destruction

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 level 1*.

6.1.5.6 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform *list of cryptographic operations – see Table 19 - Cryptographic Operations below i*n accordance with a specified cryptographic algorithm *– see Table 19 - Cryptographic Operations below* and cryptographic key sizes *– see Table 19 - Cryptographic Operations below* that meet the following: *list of standards – see Table 19 - Cryptographic Operations below*.

Table 19 - Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards
Key Transport	RSA encrypt/decrypt	2048	Allowed in FIPS mode
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (operating in GCM mode)	256	FIPS 197
Secure Hashing	SHA-384	Not Applicable	FIPS 180-3

6.1.6 Protection of the TSF (FPT)

6.1.6.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure and modification* when it is transmitted between separate parts of the TOE.

6.1.6.2 FPT_TDC.1 Inter-TSF Basic TSF Data Consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret *system information* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use *the following rules* when interpreting the TSF data from another trusted IT product.

a) For Active Directory (LDAP servers), the data is interpreted according to the LDAP version 3 protocol.

b) For NT Domains, the data is interpreted according to the NetBIOS protocol.

c) When conflicting information is received from different sources, highest priority is given to information learned from the McAfee Agent, then to Active Directory, and finally to NT Domains.

6.2 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2) augmented by ALC_FLR.2. The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle 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
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 20 – Security Assurance Requirements at EAL2

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN.1	No other components	FPT_STM.1	Satisfied by OE.TIME in the environment
FAU_GEN.2	No other components	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied by FIA_UID.2
FAU_SAR.1	No other components	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components	FAU_SAR.1	Satisfied
FAU_SAR.3	No other components	FAU_SAR.1	Satisfied
FAU_STG.1	No other components	FAU_GEN.1	Satisfied
FDP_IFC.1	No other components	FDP_IFF.1	Satisfied
FDP_IFF.1	No other components	FDP_IFC.1 FMT_MSA.3	Satisfied[5]
FIA_ATD.1	No other components	None	n/a
FIA_UID.2	FIA_UID.1	None	n/a
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2
FIA_USB.1	No other components	FIA_ATD.1	Satisfied
FMT_MTD.1	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components	None	n/a
FMT_SMR.1	No other components	FIA_UID.1	Satisfied by FIA_UID.2
FCS_CKM.1(1-4)	No other components	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	Satisfied by FCS_COP.1 and FCS_CKM.4
FCS_CKM.4	No other components	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	Satisfied by FCS_CKM.1
FCS_COP.1	No other components	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Satisfied by FCS_CKM.1 and FCS_CKM.4
FPT_ITT.1	No other components	None	n/a
FPT_TDC.1	No other components	None	n/a

Table 21 – TOE SFR Dependency Rationale

[5] FMT_MSA.3 does not impact the security required by FDP_IFF.1 for this particular TOE because there are no configurable security attributes

6.4 Security Requirements Rationale

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives

6.4.1 Security Functional Requirements for the TOE

The following table provides a high level mapping of coverage for each security objective:

SFR / OBJECTIVE	O.ACCESS	O.AUDITS	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.EADMIN	O.IDENTIFY	O.IMPORT	O.INTEGRITY	O.SENSITIVE_DATA	O.PROTECT_DATA
FAU_GEN.1		✓								
FAU_GEN.2		✓								
FAU_SAR.1	✓									
FAU_SAR.2	✓									
FAU_SAR.3				✓						
FAU_STG.1		✓	✓							
FDP_IFC.1									✓	
FDP_IFF.1									✓	
FIA_ATD.1						✓				
FIA_UID.2	✓					✓				
FIA_UAU.2	✓					✓				
FIA_USB.1	✓									
FMT_MTD.1	✓				✓		✓	✓		
FMT_SMF.1	✓				✓					
FMT_SMR.1	✓				✓					
FCS_CKM.1(1-4)										✓
FCS_CKM.4										✓
FCS_COP.1										✓
FPT_ITT.1										✓
FPT_TDC.1							✓			

Table 22 – Mapping of TOE SFRs to Security Objectives

The following table provides detailed evidence of coverage for each security objective:

OBJECTIVE	RATIONALE
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data. Users authorized to access the TOE are determined using an identification process [FIA_UID.2] and an authentication process (either enforcing its own authentication process or ensuring that provided by the operational environment is applied [FIA_UAU.2]. Upon successful I&A, the security attributes for the user are bound to the subject so that proper access controls can be enforced [FIA_USB.1]. The permitted access to TOE data by the roles and permissions is defined [FMT_MTD.1, FMT_SMF.1, FMT_SMR.1]. The audit log records may only be viewed by authorized users (FAU_SAR.1, FAU_SAR.2].
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions on the management system. Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The user associated with the events must be recorded [FAU_GEN.2]. The TOE does not provide any mechanism for users to modify or delete audit records other than via configuration of the data retention timeframe, and that functionality is limited to administrators [FAU_STG.1].
O.AUDIT_PROTECT	The TOE must provide the capability to protect audit information generated by the TOE. The TOE is required to protect the stored audit records from unauthorized deletion or modification [FAU_STG.1].
O.AUDIT_REVIEW	The TOE must provide the capability for authorized administrators to review audit information generated by the TOE. The TOE provides the capability to review stored audit records relating both to incidents and to administrative actions [FAU_SAR.3].
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The functions and roles required for effective management are defined [FMT_SMF.1, FMT_SMR.1], and the specific access privileges for the roles and permissions is enforced [FMT_MTD.1].
O.IDENTIFY	The TOE must be able to identify users prior to allowing access to TOE functions and data on the management system. Security attributes of subjects used to enforce the security policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are determined using an identification process [FIA_UID.2] and an authentication process (either that provided by the TOE or ensuring that provided by the operational environment is applied) [FIA_UAU.2].
O.IMPORT	The TOE must provide mechanisms to import system information from Active Directory (LDAP servers) and Domain Servers. The TOE defines management functionality to import system tree information [FMT_MTD.1] and the rules for interpreting data from those sources [FPT_TDC.1].

OBJECTIVE	RATIONALE
O.INTEGRITY	The TOE must ensure the integrity of all System data. Only authorized administrators of the System may query or add System data [FMT_MTD.1].
O.SENSITIVE_DATA	The TOE must take specified actions upon the access, transmission, printing, or copying of sensitive files or data. The TOE implements data classification to identify/track sensitive data and Protection Rules to act when sensitive data is handled inappropriately [FDP_IFC.1 and FDP_IFF.1].
O.PROTECT_DATA	The TOE must provide (cryptographic) protection of TSF data when it is being transferred between TOE components [FCS_CKM.1(1-4), FCS_CKM.4, FCS_COP.1, FPT_ITT.1]

Table 23 – Rationale for Mapping of TOE SFRs to Objectives

6.4.2 Security Assurance Requirements

This section identifies the Lifecycle, Development, Test, and Guidance measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Architecture Description: McAfee Data Loss Prevention Endpoint 10.0 and ePolicy Orchestrator 5.1.3
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: McAfee Data Loss Prevention Endpoint 10.0 and ePolicy Orchestrator 5.1.3
ADV_TDS.1: Basic Design	Basic Design: McAfee Data Loss Prevention Endpoint 10.0 and ePolicy Orchestrator 5.1.3
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: McAfee Data Loss Prevention Endpoint 10.0 and ePolicy Orchestrator 5.1.3
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: McAfee Data Loss Prevention Endpoint 10.0 and ePolicy Orchestrator 5.1.3
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: McAfee Data Loss Prevention Endpoint 10.0 and ePolicy Orchestrator 5.1.3
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: McAfee Data Loss Prevention Endpoint 10.0 and ePolicy Orchestrator 5.1.3
ALC_DEL.1: Delivery Procedures	Delivery Procedures: McAfee Data Loss Prevention Endpoint 10.0 and ePolicy Orchestrator 5.1.3
ALC_FLR.2: Flaw Reporting	Flaw Reporting: McAfee Data Loss Prevention Endpoint 10.0 and ePolicy Orchestrator 5.1.3
ATE_COV.1: Evidence of Coverage	Security Testing: McAfee Data Loss Prevention Endpoint 10.0 and ePolicy Orchestrator 5.1.3
ATE_FUN.1: Functional Testing	Security Testing: McAfee Data Loss Prevention Endpoint 10.0 and ePolicy Orchestrator 5.1.3

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ATE_IND.2: Independent Testing – Sample	Security Testing: McAfee Data Loss Prevention Endpoint 10.0 and ePolicy Orchestrator 5.1.3
AVA_VAN.2: Vulnerability Analysis	Performed and provided by CCTL

Table 24 – Security Assurance Measures

6.4.2.1 Rationale for TOE Assurance Requirements Selection

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

1. Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.
2. The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.
3. Consistent with current best practice for tracking and fixing flaws and providing fixes to customers.

6.5 TOE Summary Specification Rationale

This section demonstrates that the Security Functions provided by the TOE (as described in the TOE Summary Specification in section 7 below) completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the Security Functions provided by the TOE and the SFRs and the rationale.

Security Function / SFR	Policy Enforcement	Identification & Authentication	Management	Audit	System Information Import	TSF Data Protection
FAU_GEN.1				✓		
FAU_GEN.2				✓		
FAU_SAR.1				✓		
FAU_SAR.2				✓		
FAU_SAR.3				✓		
FAU_STG.1				✓		
FDP_IFC.1	✓					
FDP_IFF.1	✓					

Security Function / SFR	Policy Enforcement	Identification & Authentication	Management	Audit	System Information Import	TSF Data Protection
FIA_ATD.1			✓			
FIA_UID.2		✓				
FIA_UAU.2		✓				
FIA_USB.1		✓				
FMT_MTD.1			✓			
FMT_SMF.1			✓			
FMT_SMR.1			✓			
FCS_CKM.1(1-4)						✓
FCS_CKM.4						✓
FCS_COP.1						✓
FPT_ITT.1						✓
FPT_TDC.1					✓	

Table 25 – SFR to Security Functions Mapping

SFR	SECURITY FUNCTION AND RATIONALE
FAU_GEN.1	**Audit –** ePO user actions area audited according to the events specified in the table with the SFR.
FAU_GEN.2	**Audit –** The audit log records include the associated user name when applicable.
FAU_SAR.1	**Audit –** Audit log records are displayed in a human readable table form from queries generated by authorized users.
FAU_SAR.2	**Audit –** Only authorized users have permission to query audit log records.
FAU_STG.1	**Audit –** The only mechanism provided by the TOE to cause audit records to be deleted is configuration of the data retention timeframe, which is restricted to administrators. The TOE does not provide any mechanism for users to modify audit records.
FDP_IFC.1	**Policy Enforcement** – The TOE implements data classification to identify/track sensitive data and Protection Rules to act when sensitive data is handled inappropriately.
FDP_IFF.1	**Policy Enforcement** – The TOE implements data classification to identify/track sensitive data and Protection Rules to act when sensitive data is handled inappropriately.
FIA_ATD.1	**Management** – User security attributes are associated with the user account via ePO User Account management.

SFR	SECURITY FUNCTION AND RATIONALE
FIA_UID.2	**Identification & Authentication** - The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TOE. No action can be initiated before proper identification and authentication.
FIA_UAU.2	**Identification & Authentication** - The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TOE. No action can be initiated before proper identification and authentication.
FIA_USB.1	**Identification** - Upon successful login, the TOE binds the ePO Administrator permission set or the union of all the permissions from the permission sets that are assigned to the user account configuration to the session.
FMT_MTD.1	**Management** – The ePO Administrator permission set and user permission sets determine the access privileges of the user to TOE data.
FMT_SMF.1	**Management** – The management functions that must be provided for effective management of the TOE are defined and described.
FMT_SMR.1	**Management** – The TOE provides the roles specified in the SFR. When a User Account is created or modified, the role is specified by assigning one or more ePO permission sets for the user.
FCS_CKM.1(1-4)	**TSF Data Protection** – The TOE provides cryptographic services to protect the TSF data while it is in transit.
FCS_CKM.4	**TSF Data Protection** – The TOE provides cryptographic services to protect the TSF data while it is in transit.
FCS_COP.1	**TSF Data Protection** – The TOE provides cryptographic services to protect the TSF data while it is in transit.
FPT_ITT.1	**TSF Data Protection** – The TOE provides a secure channel to protect the TSF data while it is in transit.
FPT_TDC.1	**System Information Import** – The TOE provides the functionality to import asset data information from Active Directory (LDAP servers) or NT Domains and correctly interpret the information.

Table 26 – SFR to Security Function Rationale

7 TOE Summary Specification

7.1 Policy Enforcement

The TOE monitors and protects sensitive information from being disclosed through various channels, including email, print, upload to the web or copy to an external storage device. Protection rules control the flow of data by defining the action taken when an attempt is made to transfer or transmit sensitive data. Protection Rules link actions with definitions, content classification, and end-user groups.

Protection rules define the action taken when an attempt is made to transfer or transmit tagged data. The protection rule specifies the transfer method, content classification name(s) to protect, a set of specific conditions related to the transfer method (such as email recipients, printer names or network shares) and how the system should react to the event. Each event is given a severity level, and options for responding to the event. In some cases, protection rules merely log the event. In other cases, the protection rules prevent transfer of data and notify the user of the violation. Protection rules can be applied to specific users by setting the rule conditions to apply only for specific end-user groups.

ACTIONS / RULES	Apply RM Policy	Block	Set classification tag	Report Incident	Notify User	Quarantine	Read Only	Request Justification	Store Evidence
Plug and Play device rules		✓		✓	✓				
Removable storage device rules		✓		✓	✓		✓		
Removable Storage File Access Rule		✓		✓	✓				
Citrix XenApp Device Rule		✓							
Fixed Hard Drive Rule		✓		✓	✓		✓		
TrueCrypt Device rule		✓		✓	✓		✓		
Application file access protection rules		✓		✓	✓				✓
Clipboard protection rules		✓		✓	✓				✓
Cloud protection rules	✓	✓		✓				✓	✓
Email protection rules		✓		✓	✓			✓	✓
Network communication protection rules		✓		✓	✓				
Network Share protection rules				✓	✓			✓	✓
Printing protection rules		✓		✓	✓			✓	✓
Removable storage protection rules		✓		✓	✓			✓	✓
Screen capture protection rules		✓		✓	✓				✓
Web post protection rules		✓		✓	✓			✓	✓
Local file system discovery rules	✓		✓	✓	✓(1)	✓			✓
Local email storage discovery rule			✓	✓	✓(1)	✓			✓

Table 27 – Rules and their actions

(1) Application note: since discovery rules run at-rest and not as result of a user action, therefore the user may not notice the "user notification" hence the "user notification" action in discovery rules is not showing a popup dialog to the end-user, instead it logs the event in the DLP endpoint console and also leaves a "placeholder" file instead of a file if the file is quarantined.

After creating the rules and definitions required for the enterprise, they must be enforced by assigning the policy to managed computers. Once the policy is in place, the DLP Incident Manager is used to audit the state of the enterprise's sensitive information.

Using McAfee Data Loss Prevention software involves the following tasks:

- Assigning policy — deploying the DLP policy to managed computers.
- Monitoring events — using the DLP Incidents Manager to audit, view, filter, and sort events in the enterprise network.
- Performing administrative maintenance — Keeping the DLP Agents up-to-date and generating agent override, agent uninstall, and quarantine release keys as required.

The table below shows the predefined dashboards and available functions for the Policy Enforcement TSF:

NAME	DESCRIPTION
Agent version	Displays the distribution of agents in the enterprise. Used to monitor agent deployment progress.
Agent Status	Displays the status of agents in the enterprise. Used to monitor how many agents running and enforcing rules, how many installations failed and how many have no policies.
Policy Distribution	Displays the number of endpoint per DLP policy instance. for example: 2,500 systems with the DLP Japan policy and 15,000 with DLP EMEA policy.
Bypassed agents	Displays how many DLPe nodes are in policy bypass mode. This is a real-time view that refreshes when a bypass begins or expires.
Agent Operations Mode	Displays how many agents are in device control mode and how many are enforcing data protection & device control.
Enforced Rule sets	Displays the number of computers enforcing each Rule set
Privileged Users	Displays how many DLPe sessions are running by a privileged user mode. Policy rules with a block action will not block and simply report an incident if running on a system with a logged on privileged user (e.g. Senior VP, CFO)
Policy Revision Distribution	Displays the number of endpoint enforcing each DLP policy revision. Used to monitor progress when deploying a new policy. Example: ePO has 2 DLP policies (Japan, EMEA) and some machines might not get the latest revision of the Japan policy (because they were disconnected from network for long time)

Table 28 – Predefined DLP Dashboards

7.2 Identification and Authentication

Users must log in to ePO with a valid user name and password supplied via a GUI before any access is granted by the TOE to TOE functions or data. When the credentials are presented by the user, ePO determines if the user name is defined and enabled. If not, the login process is terminated and the login GUI is redisplayed.

If Windows authentication is enabled the supplied password is passed to Windows for validation, otherwise it is validated against ePO's internal password store. If authentication is successful, the TOE grants access to additional TOE functionality. If the validation is not successful, the login GUI is redisplayed. Note that all the Windows I&A protection mechanisms (e.g., account lock after multiple consecutive login failures) that may be configured still apply since Windows applies those constraints when performing the validation.

Upon successful login, the union of all the permissions from the permission sets from the user account configuration are bound to the session (if a user account is assigned as an "Administrator", no other permissions sets can be bound to that account). Those attributes remain fixed until the user refreshes their session by logging out and logging back in.

7.3 Management

The TOE's Management Security Function provides administrator support functionality that enables a user to configure and manage TOE components. Management of the TOE is performed via the ePO GUI. Management permissions are defined per-user.

The TOE provides functionality to manage the following:

1. ePO User Accounts,
2. Permission Sets,
3. Audit Log,
4. DLP Policy and rules,
5. Registered Servers,
6. Systems and System Tree access,
7. Queries and Reports,
8. Dashboards.

Each of these items is described in more detail in the following sections.

7.3.1 ePO User Account Management

Each user authorized for login to ePO must be defined with ePO. Only ePO Administrators may perform ePO user account management functions (create, view, modify and delete). For each defined account, the following information is configured:

1. User name
2. Enabled or disabled
3. Whether authentication for this user is to be performed by ePO or Windows
4. Permission sets granted to the user

One or more permission sets may be associated with an account. ePO Administrators are only granted permission as "Administrator" and have access to everything in ePO.

Permissions exclusive to ePO administrators (i.e., not granted via permission sets) include:

1. Create and delete user accounts.
2. Create, delete, and assign permission sets.

7.3.2 Permission Set Management

A permission set is a group of permissions that can be granted to any users by assigning it to those users' accounts. ePO provides the following predefined permission sets:

- Executive Reviewer
- Global Reviewer
- Group Admin
- Group Reviewer

When a user account is created, the user can be assigned to either a permission set (pre-defined or administrator defined) or assigned as an "Administrator". If the new user account is assigned to a permission set they are considered to be an "ePO user", whereas if they are assigned to "Administrator" they are considered to be an "ePO administrator".

One or more permission sets can be assigned to any users who are not ePO administrators (ePO administrators can only be assigned as an administrator).

Permission sets only grant rights and access — no permission ever removes rights or access. When multiple permission sets are applied to a user account, they aggregate. For example, if one permission set does not provide any permissions to registered servers, but another permission set applied to the same account grants all permissions to registered servers, that account has all permissions to registered servers.

When a new ePO product extension (e.g., DLP) is installed into ePO it may add one or more groups of permissions to the permission sets. Initially, the newly added section is listed in each permission set as being available but with no permissions yet granted. The ePO Administrators can then grant permissions to users through existing or new permission sets.

ePO Administrators may create, view, modify and delete permission sets. Each permission set has a unique name so that it can be appropriately associated with ePO users.

When a permission set is created or modified, the permissions granted via the permission set may be specified by a ePO administrator.

7.3.3 Audit Log Management

An ePO Administrator may purge events in the audit log.

7.3.4 DLP Policy and rules

A product policy is a collection of settings that are created, configured, and then enforced. Product policies ensure that McAfee Agent and DLP Endpoint are configured and perform accordingly on the managed systems. Different policy rules for the same product may be configured for different groups. When product policy settings are reconfigured, the new settings are delivered to, and enforced on, the managed systems at the next agent-server communication.

The permissions associated with product policy management are:

1. Policy - This permission can be used to grant the ability to view and save policies.
2. Rule Sets – this permission can be used to grant the ability to view, create, modify and delete rule sets
3. Classifications – this permission can be used to grant the ability to view, create, modify and delete classifications, classification criterions and tagging criterions
4. Manage manual classification – this permission can be used to grant the ability to define which end-users will be allowed to manually classify files.
5. Manage registered documents and whitelisted text – this permission can be used to grand the ability to upload files to be indexed and registered as well as upload and register whitelisted text snippets.
6. Definitions – this permission can be used to grant the ability to view, create, modify and delete different types of definitions, such as Text Patterns, Dictionaries, Email lists, URL lists and end-user groups as well as many other definition types.
7. Incidents Access Control - This permission grants the ability to view incidents.
8. Incidents data redaction - This permission grants the ability control whether data is redacted or in clear text.
9. Incident task creation - This permission grants the ability to view, create, delete and modify mail notification tasks, purge tasks or set a reviewer task.

10. Operational events - This permission grants the ability to view, create, delete and modify operational events.

Product policies are applied to any group or system by one of two methods, inheritance or assignment. Inheritance determines whether the product policy settings for a group or system are taken from its parent. By default, inheritance is enabled throughout the System Tree. When this inheritance is broken by assigning new product policies anywhere in the System Tree, all child groups and systems that are set to inherit the product policy from this assignment point do so. An ePO Administrator can assign any product policy in the Policy Catalog to any group or system. Assignment allows the definition of product policy settings once for a specific need and then the application of this product policy to multiple locations.

All product policies are available for use by any user, regardless of who created the product policy. To prevent any user from modifying or deleting other users' named product policies, each product policy is assigned an owner — the user who created it. Ownership provides that no one can modify or delete a product policy except its creator or an ePO administrator. When a product policy is deleted, all groups and systems where it is currently applied inherit the product policy of their parent group.

Once associated with a group or system, enforcement of individual product policies may be enabled and disabled by an ePO Administrator.

7.3.5 Registered Servers

Registered servers allows for integration of ePO with other external servers. For example an LDAP server may be registered to facilitate connection to an Active Directory server for synchronization of active directory system and user data with ePO. ePO Administrators may create, view, modify and delete registered servers. Servers may be registered as:

- McAfee ePO – additional McAfee ePO servers for use with the main ePO server to collect or aggregate data,
- LDAP – as above, to synchronize directory system and user data,
- SNMP – to receive SNMP traps,
- Database servers – to retrieve data from a database server.

ePO Users can only be granted permission to view registered server settings by assigning the "View registered servers" permission from the Registered Servers permission set.

7.3.6 Systems and System Tree Access

The System Tree organizes managed systems in units for monitoring, assigning policies, scheduling tasks, and taking actions. The System Tree is a hierarchical structure that allows organization of systems within units called groups.

Groups have these characteristics:

1. Groups can be created by ePO administrators or users with both the “View "System Tree" tab” and “Edit System Tree groups and systems” permissions.
2. A group can include both systems and other groups.
3. Groups are modified or deleted by a ePO administrator or user with both the “View "System Tree" tab” and “Edit System Tree groups and systems” permissions.

The System Tree root includes a Lost&Found group. Depending on the methods for creating and maintaining the System Tree, the server uses different characteristics to determine where to place systems. The Lost&Found group stores systems whose locations could not be determined.

The Lost&Found group has the following characteristics:

1. It can't be deleted.
2. It can't be renamed.
3. Its sorting criteria can't be changed (although sorting criteria for subgroups can be created)
4. It always appears last in the list and is not alphabetized among its peers.
5. All users with view permissions to the System Tree can see systems in Lost&Found.
6. When a system is sorted into Lost&Found, it is placed in a subgroup named for the system’s domain. If no such group exists, one is created.

Child groups in the System Tree hierarchy inherit policies set at their parent groups. Inheritance is enabled by default for all groups and individual systems that are added to the System Tree. Inheritance may be disabled for individual groups or systems by an ePO Administrator. Inheritance can be broken by applying a new policy at any location of the System Tree (provided a user has appropriate permissions). Users can lock policy assignments to preserve inheritance.

Groups may be created manually or automatically (via synchronization with Active Directory or NT Domains). Systems may be deleted or moved between groups by a Global Administrator or user with both the “View "System Tree" tab” and “Edit System Tree groups and systems” permissions.

7.3.7 Queries and reports

Users may create, view, modify, use and delete queries/reports based upon their permissions. Permissions associated with queries/reports are:

1. Use public groups — Grants permission to use any groups that have been created and made public.
2. Use public groups; create and edit private queries/reports — Grants permission to use any groups that have been created and made public by users with the same permissions, as well as the ability to create and edit personal queries/reports.
3. Edit public groups; create and edit private queries/reports; make personal queries/reports public — Grants permission to use and edit any public queries/reports, create and modify any private queries/reports, as well as the ability to make any private query/reports available to anyone with access to public groups.

7.3.8 Dashboard Management

User-specific dashboards may be configured to display data of interest to each user; these chart-based displays are updated at a configured rate to keep the information current. Permissions relevant to dashboards are:

1. Use public dashboards
2. Use public dashboards; create and edit personal dashboards
3. Edit public dashboards; create and edit personal dashboards; make personal dashboards public

7.4 Audit

The Audit Log maintains a record of ePO user actions. The auditable events are specified in Table 16 – Audit Events and Details.

The Audit Log entries display in a sortable table. For added flexibility, the log can be filtered so that it only displays failed actions, or only entries that are within a certain age. The Audit Log displays seven columns:

1. Action — The name of the action the ePO user attempted.
2. Completion Time — The date and time the action finished.
3. Details — More information about the action.
4. Priority — Importance of the action.
5. Start Time — The date and time the action was initiated.
6. Success — Specifies whether the action was successfully completed.
7. User Name — User name of the logged-on user account that was used to take the action.

Audit Log entries can be queried by an ePO Administrator or users assigned to the Global reviewer permission set. The ePO Administrator can selected to purge Audit Log entries. No mechanisms are provided for modification of audit log entries, or for ePO Users to delete entries. The audit log entries are stored in the database; if space is exhausted, new entries are discarded.

Additionally, the TOE provides the following DLP Information Flow Control SFP events:

NAME	DESCRIPTION
Number of Incidents per day	Displays the number of incidents that were triggered each day.
Local file system scan status	Display the number of endpoint systems per each status of local file system scan (i.e. running, completed, unknown, no scan defined)
Operational events per type	Display the number of operational events per type of operation issue
Incidents by Incidents Type	Displays the number of DLP incidents for each event type

NAME	DESCRIPTION
Number of operational events per day	Displays the number of incidents that were triggered each day.
Incidents per Rule Set	Displays the number of incidents for each rule set.
Incidents by Severity	Displays the number of DLP incidents for each severity level.
Local email storage scan status	Display the number of endpoint systems per each status of local file system scan (i.e. running, completed, unknown, no scan defined)
Undefined Device Classes	Lists and shows a bar graph of the devices whose device class cannot be determined.

Table 29 – Predefined DLP Event Reports

DLP agents inspects all end-user attempts to transmit/copy/email/print/etc. data , but record only those attempts that violate a DLP rule (that is included in the policy). DLP agents record the violation only if the rule is configured to record the incident. The TOE can be configured to block the action without recording the incident, although the default is to record. This information is recorded in the DLP Incidents Manager (not in ePO audit log), and can be reviewed there using filters.

7.5 System Information Import

ePO offers integration with both Active Directory and Windows domains as a source for systems, and even (in the case of Active Directory) as a source for the structure of the System Tree.

Active Directory synchronization can be used to create, populate, and maintain part or all of the System Tree with Active Directory synchronization. Once defined, the System Tree is updated with any new systems (and sub-containers) in Active Directory.

There are two types of Active Directory synchronization (systems only and systems and structure) that can be used based on the desired level of integration with Active Directory.

With each type, the following synchronization options are available:

1. Deploy agents automatically to systems new to ePolicy Orchestrator.
2. Delete systems from ePolicy Orchestrator (and remove their agents) when they are deleted from Active Directory.
3. Prevent adding systems to the group if they exist elsewhere in the System Tree.
4. Exclude certain Active Directory containers from the synchronization. These containers and their systems are ignored during synchronization.

The System Tree can be populated with the systems in the Windows domain. When synchronizing a group to a Windows domain, all systems from the domain are put in the group as a flat list. Those systems can be managed in a single group or via subgroups for more granular organizational needs.

When systems are imported, their placement in the System Tree may be automatically determined by criteria-based sorting of two forms. IP address sorting may be used if IP address organization coincides with the management needs for the System Tree. Tag based sorting may be used to sort systems based on tags associated with them.

The server has three modes for criteria-based sorting:

1. Disable System Tree sorting
2. Sort systems on each agent-server communication — Systems are sorted again at each agent-server communication. When the sorting criteria on groups is changed, systems move to the new group at their next agent-server communication.
3. Sort systems once — Systems are sorted at the next agent-server communication and marked to never be sorted again.

TOE Security Functional Requirements Satisfied: FPT_TDC.1

7.6 TSF Data protection

Communications between McAfee Agents and ePO take the form of XML messages. Communications can include policies to implement, properties collected from the Endpoint machine, event data gathered

by the DLP application, or tasks to be run on the Endpoint. The messages are transferred via HTTPS. The TOE protects these transmissions between the ePO and the McAfee Agent from disclosure and modification by encrypting the transmissions under TLS, using AES operating in GCM mode, with 128 bit or 256 bit key sizes (by default the cipher used by ePO and McAfee Agent is DHE-RSA-AES256-GCMSHA384).

In FIPS mode, ePO uses OpenSSL v1.0.1m with FIPS module v2.0.8 (FIPS 140-2 certificate #1747) for TLS 1.2. McAfee Agent uses RSA BSAFE Crypto-C Micro Edition v4.0.1 (FIPS 140-2 certificate #2097) to provide cryptographic services for this link. McAfee affirms that the cryptographic modules have been implemented in accordance with their FIPS 140 security policies, and when the TOE is configured in FIPS mode the cryptographic functions operate as intended.

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards	CAVP Cert #
Key Transport	RSA encrypt/decrypt	2048	Allowed in FIPS mode	OpenSSL #1535 BSAFE #1046
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (operating in GCM mode)	256	FIPS 197	OpenSSL #2929 BSAFE #2017
Secure Hashing	SHA-384	Not Applicable	FIPS 180-3	OpenSSL #2465 BSAFE #1767

TOE Security Functional Requirements Satisfied: FCS_CKM.1(1-4), FCS_CKM.4, FCS_COP.1, FPT_ITT.1