Security Target

McAfee Threat Intelligence Exchange 2.0.0 and Data Exchange Layer 3.0.0 with ePolicy Orchestrator 5.3.2

Document Version 1.0

November 23, 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), McAfee Threat Intelligence Exchange 2.0.0 and Data Exchange Layer 3.0.0 with ePolicy Orchestrator 5.3.2. 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

1 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 Threat Intelligence Exchange 2.0.0 and Data Exchange Layer 3.0.0 with ePolicy Orchestrator 5.3.2
ST Revision	1.0
ST Publication Date	November 23, 2016
Author	Primasec Ltd

1.2 TOE Reference

TOE Reference	McAfee Threat Intelligence Exchange 2.0.0 and Data Exchange Layer 3.0.0 with ePolicy Orchestrator 5.3.2
TOE Type	Threat management

1.3 Document Organization

2 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)

SECTION	TITLE	DESCRIPTION
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

3 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.

4 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

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

TERM	
CC	Common Criteria version 3.1 (ISO/IEC 15408)
DBMS	DataBase Management System
DXL	Data Exchange Layer
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
FIPS	Federal Information Processing Standard

TERM	
GTI	Global Threat Intelligence
GUI	Graphical User Interface
I&A	Identification & Authentication
IT	Information Technology
MLOS	McAfee Linux Operating System
MWG	McAfee Web Gateway
OS	Operating System
OSP	Organizational Security Policy
OVA	Open Virtual Appliance
PP	Protection Profile
RAM	Random Access Memory
SFP	Security Function Policy
SFR	Security Functional Requirement
SP	Service Pack
SQL	Structured Query Language
ST	Security Target
TIE	Threat Intelligence Exchange
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
VGA	Video Graphics Array

Table 2 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

6 The TOE is McAfee Threat Intelligence Exchange (TIE) 2.0.0 and Data Exchange Layer (DXL) 3.0.0 with ePolicy Orchestrator (ePO) 5.3.2.

7 McAfee TIE analyses files and certificates found on the network and makes informed security decisions. These decisions are based on a file's security reputation, and on criteria set by the administrator using ePO and product related extensions. TIE uses the communication framework provided by DXL to support this activity. It is possible to identify the system where a threat was first detected, where it went from there, and to take policy based action to prevent further spread.

8 TIE provides the ability to block or allow specific files and certificates based on their threat reputations and specified risk criteria.

9 TIE is used with McAfee Global Threat Intelligence (GTI) to provide detailed assessment and data on malware classification. GTI is in the TOE environment, and is not part of the TOE.

10 TIE includes the following components:

a) TIE Client - A module for McAfee VirusScan Enterprise[1] that allows creation of policies for blocking and allowing a file or certificate, based on its reputation;

b) TIE Server - A server that stores information about file and certificate reputations, then passes that information to other systems.

11 DXL provides communications to allow threat information to be shared rapidly with other services and devices. It has the following components:

a) DXL Brokers – Installed on managed systems and route messages between connected clients. An example of a connected client is the TIE module. When a client requests a service, or when an update is broadcast, the network of brokers relays the messages. Clients maintain a persistent connection to their brokers.

b) DXL Fabric – Consists of DXL clients and brokers, communicating using TLS 1.2.

c) Hubs – Contain one or two brokers and provide failover protection in a multi-broker environment.

d) DXL Clients – Clients receive and process messages from the brokers.

12 Both TIE and DXL include extensions for McAfee ePolicy Orchestrator that add new management features and reports to its capabilities.

13 McAfee Agent is also employed to provide communications between ePO, TIE Server, DXL Brokers and TIE/DXL clients.

1.7 TOE Description

1.7.1 Physical Boundary

14 The TOE is a software TOE and includes:

- The ePO application executing on a dedicated server
- Five McAfee ePO managed extensions
  - TIE server extension
  - TIE module for VirusScan Enterprise extension
  - DXL Broker management
  - DXL Client
  - DXL Client management extension

[1] VirusScan Enterprise is in the TOE environment, and is not part of the TOE.

- The TIE server
- A TIE module for VirusScan Enterprise on each managed system
- DXL Broker(s)
- A DXL Client on each managed system
- McAfee Agent on TIE Server, DXL Brokers and each managed system[2]

15 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.

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

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	TIE Server v2.0.0: *TIE Server v2.0.0 Build 645* (TIEServer_2.0.0.645.x86_64-MAIN.ova.zip) *TIE ePO extension with help file* (TIEServerMgmt_2.0.0_Build_645_Package_1_(ENU-LICENSED-RELEASE-Main).zip and help_tie_200.zip) *TIE Module for VirusScan Enterprise 1.0.2.112 extension* (TIEmMeta.zip) *TIE Module for VirusScan Enterprise 1.0.2.112 package* (JTICAgent.zip)
	DXL 3.0.0: *DXL Broker (* DXLBroker_3.0.0.285.x86_64-MAIN.zip) *DXL Client package* (DXL_3.0.0_Build_285_Package_7_(ENU-LICENSED-RELEASE-MAIN).zip) *DXL Broker Management ePO extension* (DXLBrokerMgmt_3.0.0_Build_285_Package_1_(ENU-LICENSED-RELEASE-MAIN).zip) *DXL ePO Client ePO extension* (DXLClient_3.0.0_Build_285_Package_1_(ENU-LICENSED-RELEASE-MAIN).zip) *DXL Client Management ePO extension* *(*DXLClientMgmt_3.0.0_Build_285_Package_1_(ENU-LICENSED-RELEASE-MAIN).zip)

[2] McAfee Agent (version 5.0.3.272) is integrated with the TIE Server and DXL Broker components. The McAfee Agent deployed to (Windows) managed systems is version 5.0.4.283.

TOE COMPONENT	VERSION/MODEL NUMBER
	ePO 5.3.2: *ePolicy Orchestrator 5.3.2.156* (EPO532L.zip) *Hotfix 1151890* (EPO5xHF1151890.zip) *Hotfix 1147158* (EPO5xHF1147158.zip) *McAfee Agent 5.0.4.283 for Windows managed systems* (MA504WIN.zip) *MA ePO Server extension*[3] *5.0.4.104* (EPOAGENTMETA.zip) *McAfee Agent Help* (help_ma_503.zip[4])
IT Environment	Specified in the following: • Table 4 – ePO Server System Requirements • Table 5 – Supported Client Platforms • Table 6 –Client Platform Hardware Requirements

Table 3 – Evaluated Configuration for the TOE

17 The evaluated configuration consists of a single instance of the management system (with ePO and the TIE/DXL extensions), a TIE Server, one or more DXL Brokers and one or more instances of managed systems (with McAfee Agent the DXL Client, and the TIE Module for VirusScan).

18 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.

19 The ePO, server and endpoint components must be installed in FIPS mode (as detailed in *McAfee Threat Intelligence Exchange 2.0.0 and Data Exchange Layer 3.0.0 with ePolicy Orchestrator 5.3.2 Common Criteria Evaluated Configuration Guide* and *User Guide McAfee ePolicy Orchestrator 5.3.0 Software FIPS Mode)* to ensure that cryptographic services used by the TOE are FIPS validated.

20 The following figure presents an example of an operational configuration. The area enclosed by the blue dotted line in the figure represents the TOE boundary.

[3] This extension is the McAfee Agent v5.0.4 ePO Policy and Reporting Extension

[4] Equally applicable to MA 5.0.4.283

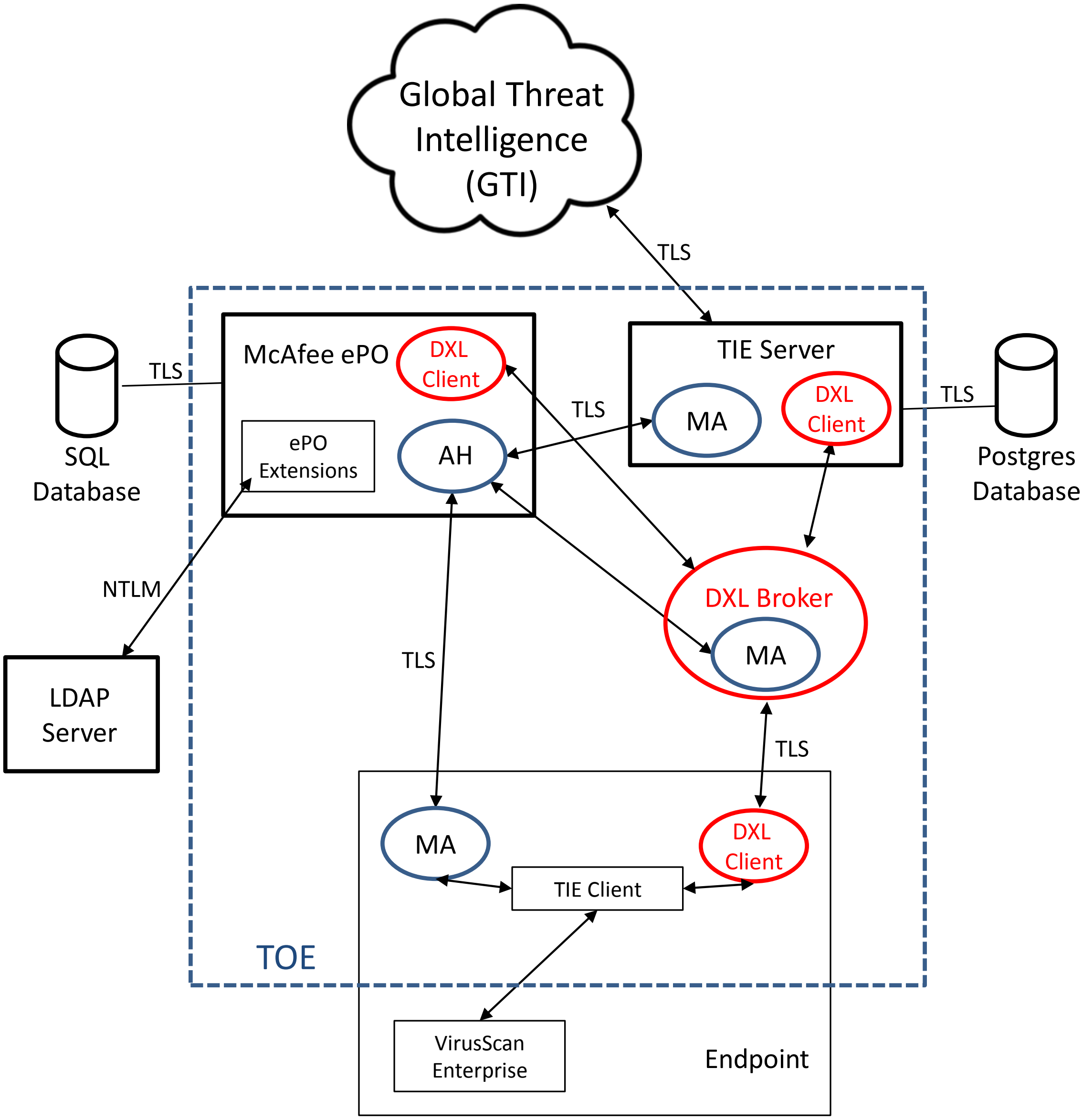

Figure 1 - TOE components and TOE boundary

21 Note that the data stored within the DBMS for both ePO and the TIE Server are part of the TOE, but the third party DBMS software is not.

22 The following specific ePO/MA configuration options apply to the evaluated configuration:

1. Incoming connections to McAfee Agents are only accepted from the configured address of the ePO server.
2. The repository is where ePO stores software and signatures for distribution to network platforms. The only software and update repository supported is the ePO server (see section 1.7.8.3).

1.7.2 Hardware and Software Supplied by the IT Environment

23 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. McAfee GTI and McAfee VirusScan Enterprise are required in the TOE environment to support TOE operation, but do not form part of the TOE.

24 The platform on which the ePO and TIE/DXL extensions 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).

25 The TOE requires the following hardware and software configuration.

1.7.2.1 ePO

26 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	20 GB — Recommended minimum
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	Windows Server 2012 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 3.5 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

27 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.

28 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.

29 The following ePO product extension is required and must be checked in:

- McAfee VirusScan Enterprise 8.8 patch 8.

1.7.2.2 TIE Server

30 The TIE Server requires VMware vSphere 5.1.0 with ESXi 5.1, 5.5 or 6.0. The TIE Platform, which includes MLOS 2.4, MA and scripts, is installed as part of the TIE Server OVA installation. The TIE Server includes a PostgreSQL DBMS for its own use.

1.7.2.3 DXL Broker

31 The DXL Broker requires VMware vSphere ESXi 5.1, 5.5 or 6.0. The TIE Platform, which includes MLOS 2.4, MA and scripts, is installed as part of the DXL Broker OVA installation.

1.7.2.4 Client platforms

32 The McAfee Agent, TIE Module and DXL Client execute on one or more systems whose files and certificates are to be monitored. The client platforms within the scope of the evaluation are:

SUPPORTED OS FOR CLIENTS	PLATFORM
Windows 10 version 1607	X64 platforms
Windows 2012 R2 Server	X64 platforms

Table 5 – Supported Client Platforms

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

COMPONENT	MINIMUM HARDWARE REQUIREMENTS
Processor speed	1 GHz or higher
Memory	2Gb RAM
Free Disk Space	500MB, excluding log files
Network Card	Ethernet, 10Mb or higher
Graphics card	DirectX 9 graphics device with WDDM 1.0 or higher driver

Table 6 –Client Platform Hardware Requirements

1.7.3 TOE Guidance

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

- *Product Guide: McAfee Threat Intelligence Exchange 2.0.0 for use with McAfee ePolicy Orchestrator*
- *Product Guide: McAfee Data Exchange Layer 3.0.0 for use with McAfee ePolicy Orchestrator*

- *Installation Guide McAfee ePolicy Orchestrator 5.3.0 Software*[5]
- *Product Guide for McAfee ePolicy Orchestrator 5.3.0 Software*
- *Product Guide McAfee Agent 5.0.3*[6]
- *McAfee Threat Intelligence Exchange 2.0.0 and Data Exchange Layer 3.0.0 with ePolicy Orchestrator 5.3.2 Common Criteria Evaluated Configuration Guide*

1.7.4 Logical Boundary

35 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 TIE policies on managed systems and audits end-user action against those policies. The TOE ensures that identified threats are assessed and managed as specified by an administrator through a TIE policy. TIE 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. The DXL client and server carry out mutual authentication when establishing a connection.
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.

[5] The Product Guide and Installation Guides for ePO 5.3.0 are equally relevant to ePO 5.3.2

[6] The Product Guide for McAfee Agent 5.0.3 is equally relevant to McAfee Agent 5.0.4

TSF	DESCRIPTION
TSF Data Protection	The TOE provides TLS v1.2 protection of all communication: a) Between the McAfee Agent and ePO, using the crypto services provided by RSA BSAFE Crypto-C Micro Edition v4.0.1 and OpenSSL v1.0.2h library with FIPS module v2.0.12 respectively; b) Between the TIE server and the TIE module (the DXL service), using the crypto services provided by provided by OpenSSL library (v1.0.2i and v1.02h respectively) with FIPS module v2.0.12 and RSA BSAFE Crypto-J Micro Edition 6.2.1[7] (for the Java client).

Table 7 –Logical Boundary Descriptions

36 Seamless integration with McAfee ePolicy Orchestrator® (ePO™) eases deployment of components that reside on the clients, and allows 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 users 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 policy application via ePO. Access to this information is controlled by per-user permissions.

37 The module and server communicate file reputation information. The Data Exchange Layer framework immediately passes that information to managed endpoints.

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

1.7.5 Threat Intelligence Exchange

1.7.5.1 How Threat Intelligence works

39 Threat Intelligence Exchange enables file reputation to be controlled at a local level. You decide which files can run and which are blocked, and the Data Exchange Layer shares the information immediately throughout your environment.

40 Scenarios for using Threat Intelligence Exchange

- **Immediately block a file** — Threat Intelligence Exchange alerts the administrator of an unknown file in the environment. Instead of sending the file information to McAfee for analysis, the administrator blocks the file immediately. The administrator can then use Threat Intelligence Exchange to learn whether the file is a threat, and how many systems ran the file.
- **Allow a custom file to run** — A company routinely uses a file whose default reputation is suspicious or malicious, for example a custom file created for the company. Because this

[7] The same crypto module is used in RSA BSAFE Crypto-J Micro Edition 6.2.1 as in RSA BSAFE Crypto-J Micro Edition 6.2.0.x

file is allowed, instead of sending the file information to McAfee and receiving an updated DAT file, the administrator can change the file's reputation to trusted and allow it to run without warnings or prompting.

- **Import known reputations** — A company has several files that are trusted and used regularly, and other files that are not allowed. Because the reputations are already known and set, the administrator can import a list of files and their reputations directly into the Threat Intelligence Exchange database. Those reputations are used immediately with no further action.
- **See additional information about a file** — Threat Intelligence Exchange notifies the administrator of an unknown file. The administrator can see several details about the file, such as the file's parent process when executed, company and version information, Hash information, and the systems that ran the file.

1.7.5.2 How a reputation is determined

41 File and certificate reputation is determined when a file attempts to run on a managed system. The following steps occur in determining a file or certificate's reputation.

1. A user or system attempts to run a file.
2. VirusScan Enterprise inspects the file and can't determine its validity and reputation (TOE environment).
3. The module for VirusScan Enterprise inspects the file and gathers file and local system properties of interest.
4. The module for VirusScan Enterprise checks the local reputation cache for the file Hash. If the file Hash is found, the module gets the enterprise prevalence and reputation data for the file from the cache.
5. If the file Hash is not found in the local reputation cache, the module for VirusScan Enterprise queries the TIE server. If the Hash is found, the module gets the enterprise prevalence data (and any available reputations) for that file Hash.
6. If the file Hash is not found in the TIE cache or database, the TIE server queries McAfee GTI (TOE environment) for the file Hash reputation. McAfee GTI sends the information it has available, for example "unknown reputation", and the server stores that information.
7. The TIE server returns the file Hash's enterprise age, prevalence data, and reputation to the module for VirusScan Enterprise based on the data that was found. If this is the first time the file is seen in the environment, the server also sends a first instance flag to the module.
8. The module for VirusScan Enterprise evaluates this metadata to determine the file's reputation:
   - File and system properties
   - Enterprise age and prevalence data
   - Reputation
9. The module for VirusScan Enterprise takes action based on the policy assigned to the system that is running the file.

10 The module for VirusScan Enterprise updates the server with the reputation information and whether the file is allowed or blocked. It also sends threat events to McAfee ePO via the McAfee Agent.

11 The TIE server publishes the reputation change event for the file Hash.

1.7.5.3 Threat Intelligence Exchange module

42 The module for VirusScan Enterprise allows the administrator to determine what happens when a file with a malicious or unknown reputation is detected in the environment. The administrator can also view threat history information and the actions taken.

43 The following tasks can be carried out using the Threat Intelligence Exchange module.

a) Create policies to

- Allow or block files and certificates depending on their reputation.
- Receive a prompt each time a file or certificate with a certain reputation attempts to run.
- Send files automatically to Advanced Threat Defense for further evaluation.

b) View events on the Threat Intelligence Exchange dashboards. Cleaned, blocked, and allowed events can be viewed for the past 30 days or by event type.

1.7.5.4 Threat Intelligence Exchange server

44 The server stores information about file and certificate reputations, then passes that information to other systems in the environment.

45 The server enables the administrator to carry out the following tasks.

- Control what is allowed to run in the environment. For example, if an organization routinely uses a file that has an unknown security reputation but is known to be safe, the administrator can set its reputation to allow the file to run.
- Identify and track new files that attempt to run in the environment. If the new file is allowed to run, the server identifies the first system to run the file, and all other systems that ran the file.
- Instantly stop threats from spreading throughout the environment. As soon as the reputation of a file or certificate is detected as malicious (or suspicious, depending on the settings) the file is immediately blocked from running anywhere in the environment.
- Identify which files were blocked and where they attempted to run. The administrator can see where threats originate and see patterns as they occur. For example, specific systems might be more prone to detecting and blocking malicious files, so the security settings on those systems can be increased.
- Specify the rules used in policies, based on the system type. Rules are available for:
  - Systems that change frequently (programs and files are often installed and uninstalled);
  - Typical business systems that change infrequently;
  - IT-managed systems that access critical or sensitive information and rarely change.

1.7.6 Data Exchange Layer

46 The Data Exchange Layer includes client software and brokers that allow bidirectional communication between endpoints on a network.

47 The Data Exchange Layer works in the background, communicating with services, databases, endpoints, and applications. The Data Exchange Layer client is installed on each managed endpoint, so that threat information from security products that use DXL can be shared immediately with all other services and devices. Sharing reputation information as soon as it is available reduces the security assumptions that applications and services make about each other when they exchange information. This shared information reduces the spread of threats.

48 DXL clients maintain a persistent TLS 1.2 connection to their brokers regardless of their location. Even if a managed endpoint running the client is behind a NAT (network address translation) boundary, it can receive updated threat information from its broker located outside the NAT.

1.7.7 McAfee Agent

49 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 (endpoint) back to ePO. McAfee Agent uses a secure channel (using TLS v1.2) to transfer data from/to the ePO server.

1.7.8 ePolicy Orchestrator

50 ePolicy Orchestrator (ePO) provides a platform for centralized policy management and enforcement of TIE policies 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.

51 Management permissions are defined per-user. The TOE maintains two types of roles:

- Where users are assigned to the “administrator” permission set, which is a superset of all other permission sets. This includes the default “admin” user account created when ePO is installed. Users assigned to this permission set are known as “Administrator”.
- Where Users are assigned to selected permission sets. Users assigned to permission sets (excluding the administrator permission) set are known as “Users with Selected Permissions”.

52 This ST uses the term “administrator” to refer generally to an ePO user, unless, for example when defining SFRs, a more precise term is required. When using the term in this sense the possession of necessary ePO permissions is assumed.

53 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 TIE/DXL features are configured correctly. Client tasks are the scheduled actions that run on the managed systems hosting the TIE module and DXL client. Client tasks are commonly used for product deployment, product functionality, upgrades, and updates.

54 Within the TOE configuration the ePO software is comprised of the following components.

1.7.8.1 ePO Server

55 The ePO server deploys DXL clients and TIE modules to managed systems (via the McAfee agent) and controls updates. It creates TIE policies and distributes them to the managed systems, and processes the events for all the managed systems. It allows the following tasks to be carried out:

- Building file prevalence and observing;
- Monitoring policy execution and making adjustments;
- Blocking or allowing files and certificates;
- Changing default threat reputations;
- Searching for files and certificates;
- Determining where a file or certificate ran in the environment;
- Monitoring events;
- Viewing reports.

1.7.8.2 Database

56 The database is the central storage component for all data created and used by ePO, other than software and signatures received from McAfee or from user-defined source sites. 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.

1.7.8.3 Master Repository

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

1.7.9 Features not part of the evaluated TOE

58 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.

59 The TOE can interact with Advanced Threat Defense to receive information on suspected threats, but its use is not part of the evaluated configuration.

60 Reputation data may also be accepted from McAfee Web Gateway (MWG), but its use is not part of the evaluated configuration.

61 Use of the TIE Server command line interface is disabled in the evaluated configuration.

62 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

63 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

64 In addition to the platforms given in Table 5, the DXL Client and TIE Module 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 and 64-bit)
- Windows 8 and 8.1 all editions (32-bit and 64-bit)
- Windows 10 (32-bit)
- Windows Server 2008 R2
- Windows Server 2012

1.8 Rationale for Non-bypassability and Separation of the TOE

65 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.

66 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 TIE/DXL extension TOE components execute is dedicated to that purpose.

67 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.

68 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.

69 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, and within the DXL Fabric to protect the information exchanged from disclosure or modification.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

70 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

71 The TOE does not claim conformance to a Protection Profile.

3 Security Problem Definition

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

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

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

3.1 Threats

74 The following are threats identified for the TOE and the IT systems that the TOE monitors. The TOE is responsible for addressing threats to the environment in which it resides, and there are also threats related to the TOE itself. The assumed level of expertise of the attacker for all the threats is unsophisticated.

75 The TOE addresses the following threats:

THREAT	DESCRIPTION
T.NODETECT	Data objects known to be malicious may be introduced to a network, either deliberately by an attacker or inadvertently by a user on the network, and may propagate without detection, causing loss of confidentiality, integrity or availability of network systems and data.
T.SOURCE	The entry point onto a network of malicious objects, introduced either deliberately by an attacker or inadvertently by a user on the network, may go undetected.

Table 8 – Threats in the TOE environment

THREAT	DESCRIPTION
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 threats 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 threat assessment functions by halting execution of the TOE.

THREAT	DESCRIPTION
T.TRANSIT	An attacker may compromise the integrity of TOE system data when in transit.
T.ACCOUNT	Users may not be accountable for their actions when administering the TOE.

Table 9 - Threats against the TOE

3.2 Organizational Security Policies

76 This section describes the Organizational Security Policies that the TOE is designed for use with.

POLICY	DESCRIPTION
P.CRYPTO	When carrying out cryptographic functions the TOE must use cryptographic modules that have been validated to FIPS 140.

Table 10 – Organizational Security Policies

3.3 Assumptions

77 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.GTI	McAfee GTI provides reliable and appropriate file reputation information when requested.
A.ACCESS	The TOE has access to all the IT system data it needs to perform its functions.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.
A.NOEVIL	The administrators assigned to manage the TOE are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PROTECT	The hardware on which the TOE and the IT environment software are installed will be protected from unauthorized physical modification.
A.PLATFORM	The hardware, operating system, and other software on which the TOE depends, operate correctly.

Table 11 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

78 The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.MONITOR	The TOE must be able to associate a reputation with a file or certificate that attempts to run on the network, to be used as the basis for access decisions.
O.FIRST_HIT	The TOE must be able to detect where the first incident related to a malicious object occurred.
O.BLOCK	It must be possible for an authorized user to configure the TOE to block or allow access to files and certificates according to defined policies.
O.ACCESS	The TOE must allow only authorized users to access the TOE management system, and must restrict their access to 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.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data on the management system.
O.PROTECT_DATA	The TOE must ensure the integrity of audit and system data by protecting it from unauthorized modifications and access during transfer.
O.CRYPTO	The TOE must use only cryptographic modules that have been validated to FIPS 140.

Table 12 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

79 The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.GTI	GTI must provide reliable and appropriate file reputation data on request.

OBJECTIVE	DESCRIPTION
OE.PHYSICAL	Those responsible for the TOE must ensure that the hardware on which the TOE and IT environment software are installed is 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 installed, managed, and operated in a manner which is consistent with provided guidance.
OE.IDAUTH	The IT environment must also be able to identify and authenticate user credentials on the management systems when requested by the TOE.
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.
OE.STORAGE	The IT environment must manage the storage and retrieval of TOE data in the databases as directed by the TOE.
OE.TIME	The IT Environment must provide reliable timestamps to the TOE.
OE.PLATFORM	The hardware, operating system, and other software on which the TOE depends, must operate correctly.

Table 13 – Operational Environment Security Objectives

Application Note: With regard to OE.PHYSICAL it should be noted that different levels of protection will be appropriate for different hardware platforms. Whereas, to avoid large scale compromise of the TOE, it may be appropriate to protect the ePO, TIE Server, DXL Brokers and DBMS hardware in server rooms with limited access, this may not be appropriate for managed PCs and laptops. For such managed computers network users should provide protection appropriate to the data being stored and processed, and no special measures would be expected.

4.3 Security Objectives Rationale

80 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.MONITOR	O.FIRST_HIT	O.BLOCK	O.ACCESS	O.AUDITS	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.EADMIN	O.IDAUTH	O.PROTECT_DATA	O.CRYPTO	OE.GTI	OE.PHYSICAL	OE.CREDEN	OE.INSTALL	OE.IDAUTH	OE.INTEROP	OE.PERSON	OE.DATABASE	OE.STORAGE	OE.TIME	OE.PLATFORM
T.NODETECT	✓		✓					✓				✓					✓			✓		
T.SOURCE		✓																				
T.COMINT				✓					✓	✓			✓	✓		✓		✓	✓			
T.IMPCON				✓				✓	✓					✓	✓	✓						
T.LOSSOF				✓					✓	✓			✓	✓		✓			✓			
T.NOHALT				✓					✓				✓			✓						
T.TRANSIT										✓	✓											
T.ACCOUNT					✓	✓	✓														✓	
P.CRYPTO											✓				✓							
A.GTI												✓										
A.ACCESS																	✓					
A.DATABASE													✓						✓			
A.NOEVIL													✓	✓	✓			✓				
A.PROTECT													✓									
A.PLATFORM																						✓

Table 14 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

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

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.NODETECT	Data objects known to be malicious may be introduced to a network, either deliberately by an attacker or inadvertently by a user on the network, and may propagate without detection, causing loss of confidentiality, integrity or availability of network systems and data. This threat relates to the undetected introduction to a network of files and certificates with the potential to do harm. The O.MONITOR objective addresses this by identifying and tracking files that run on the network, and O.BLOCK allows for an administrator to configure the TOE to block use of files and certificates, based on reputation. O.EADMIN provides the functions necessary to manage this process, and OE.INTEROP aims to ensure that the TOE is able to interact with the managed systems. To function most effectively the TOE requires a connection to GTI in the environment, and OE.GTI provides this. Reputation information to support the TOE is stored in a database, and OE.STORAGE is concerned with the management of this.
T.SOURCE	The entry point onto a network of malicious objects, introduced either deliberately by an attacker or inadvertently by a user on the network, may go undetected. The objective O.FIRST_HIT aims to ensure that the first entry point of a malicious object can be identified.
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.IDAUTH objective provides for identification and authentication of users by the TOE prior to any TOE data access. OE.IDAUTH provides this if identification and authentication is configured to be done by the IT environment. The O.ACCESS objective builds upon the O.IDAUTH and OE.IDAUTH objectives by permitting only authorized users to access the TOE and the functions and data for which they are authorised. The O.PROTECT_DATA objective helps to counter this threat by requiring the TOE to provide functionality and protocols to protect the data during transit. Direct access to the TOE is restricted through the OE.PHYSICAL objective, and unauthorized access through theft of credentials is addressed by OE.CREDEN. Access to the databases is addressed by the OE.DATABASE environment objective. Proper selection and training of administrators also helps to defend against such attacks, and this is addressed by OE.PERSON.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
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.IDAUTH and OE.IDAUTH objectives provide for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.IDAUTH objectives by permitting only authorized users to access the TOE and the function and data for which they are authorised. Unauthorized access through theft of credentials is addressed by OE.CREDEN.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. The O.IDAUTH and OE.IDAUTH objectives provide for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.IDAUTH objectives by permitting only authorized users to access the TOE and the functions and data for which they are authorised. Unauthorized access through theft of credentials is addressed by OE.CREDEN. Access to the databases is addressed by the OE.DATABASE and OE.PHYSICAL environment objectives. The TOE addresses the protection of data in transit with O.PROTECT_DATA.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's threat assessment functions by halting execution of the TOE. The O.IDAUTH and OE.IDAUTH objectives provide for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.IDAUTH objectives by permitting only authorized users to access the TOE functions and data for which they are authorised. Direct access to the TOE is restricted through the OE.PHYSICAL objective.
T.TRANSIT	An attacker may compromise the integrity of TOE system data when in transit. The TOE addresses the protection of data in transit with O.PROTECT_DATA. O.CRYPTO specifies protection using FIPS 140 validated modules.
T.ACCOUNT	Users may not be accountable for their actions when administering the TOE. This threat is addressed through provision of audit functionality (O.AUDITS), protection of audit data (O.AUDIT_PROTECT), and the capability to review the audit data (O.AUDIT_REVIEW). Accuracy of audit record timing is addressed through OE.TIME.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
P.CRYPTO	When carrying out cryptographic functions the TOE must use cryptographic modules that have been validated to FIPS 140. The TOE addresses this through O.CRYPTO, and the requirement that where options exist the correct modes are chosen on installation is addressed through OE.INSTALL.
A.GTI	McAfee GTI provides reliable and appropriate file reputation information when requested. The assumption that GTI provides reliable and appropriate file reputation information when requested is supported through the environment objective OE.GTI.
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 is interoperable with the systems that is monitors, and therefore can gain access to the system data required to carry out monitoring activities.
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. Direct access to the TOE is restricted through the OE.PHYSICAL objective.
A.NOEVIL	The administrators assigned to manage the TOE 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.PHYSICAL objective provides for physical protection of the TOE and its operational environment by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data. The OE.PERSON objective supports this by requiring careful selection and training of administrators.
A.PROTECT	The hardware on which the TOE and the IT environment software are installed will be protected from unauthorized physical modification. The OE.PHYSICAL objective provides for the physical protection of the hardware on which the TOE and IT environment software are installed.
A.PLATFORM	The hardware, operating system, and other software on which the TOE depends, operate correctly. The OE.PLATFORM objective provides for the correct operation of the hardware, operating system and other software on which the TOE depends.

Table 15 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

82 No extended components have been specified for this TOE.

6 Security Requirements

83 The security requirements for the TOE are specified in this section.

6.1 Security Functional Requirements

84 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 listed 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
Access Control	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
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_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Cryptographic Support	FCS_CKM.1	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
Trusted path/channels	FTP_ITC.1	Trusted channel

Table 16 – 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 17 – Audit Events and Details*

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the information detailed in Table 17 – Audit Events and Details.*

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

SFR	EVENT	ADDITIONAL DETAILS RECORDED
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.	
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.	
FDP_ACF.1	All requests for access to objects that are identified as malicious by a TIE rule.	The name of the object, reputation
FIA_ATD.1	All changes to TSF data (including passwords) result in an audit record being generated.	
FIA_UID.2	All use of the user identification mechanism	Location
FIA_UAU.2	All use of the user authentication mechanism	Location

SFR	EVENT	ADDITIONAL DETAILS RECORDED
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.	Function used
FMT_SMR.1	Modifications to the group of users that are part of a role	

Table 17 – Audit Events and Details

Application Note: The audit events as defined in this ST cover both the ePO management events that are audited, and the TIE events that are identified through application of TIE policies that are reported back to ePO from managed systems.

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 A*dministrators or users assigned to the 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*.

Event type	Field	Filter/Sort
ePO Operational Events	Action	Sort
	Completion time	Filter, Sort
	Details	Sort
	Priority	Sort

Event type	Field	Filter/Sort
	Start Time	Filter, Sort
	Success	Filter, Sort
	User Name	Sort
TIE Event Manager	Event type	Filter
	Date seen	Filter
	File hash	Filter
	System id	Filter
	Rule name	Filter

Table 18 – 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 stored audit records in the audit trail.

6.1.2 Access Control (FDP)

6.1.2.1 FDP_ACC.1 – Subset access control

FDP_ACC.1.1 The TSF shall enforce the *Access Control SFP* on

Subjects: Process executing on behalf of a User on a managed system

Objects: Files and certificates stored on the managed system

Operations: Execute, access.

6.1.2.2 FDP_ACF.1 –Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the *Access Control SFP* to objects based on the following:

Subjects: Users on a managed system

Objects: Files and certificates

Security attributes: Reputation

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) Execution of a file or access to a certificate by a process executing on behalf of a user on a managed system is not permitted unless the reputation of the object is known;

b) *Execution of a file or access to a certificate by a process executing on behalf of a user on a managed system is permitted if the reputation of the object, expressed as a numeric value (0-99) is greater than or equal to the minimum reputation setting for the managed system;*

c) *If the reputation of a file or certificate is within a policy specified range for prompting, then before the required access is permitted the managed system user shall be prompted with a warning, and asked to confirm before the required access is granted*.

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*.

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_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the *Access Control SFP* to restrict the ability to modify the security attributes *reputation* to *an Administrator or a user with McAfee TIE Reputations permission*.

6.1.4.2 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the *Access Control SFP* to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *Administrator or a user with McAfee TIE Reputations permission* to specify alternative initial values to override the default values when an object or information is created.

6.1.4.3 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, clear, *create, view, copy, export, access, assign and use* the *TSF data identified in Table 19 – TSF Data Access Permissions to an Administrator or a user with permissions*.

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
Audit Log	View Audit log	View
	View and purge audit log	View, delete
Dashboards	Use public dashboards	View public dashboards
	Use public dashboards, create and edit private dashboards	View public dashboards, create and modify private dashboards

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
	Use public dashboards, create and edit private dashboards, make private dashboards public	View public dashboards, create, delete and modify private dashboards, make private dashboards public
	View Audits and Assignments	Query audit event records
ePO User Accounts	Only allowed by an Administrator	Query, create, delete and modify
TIE 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	
TIE Rule Sets	User can use all rule sets McAfee TIE Server for Product	Assign rule sets to policies.
	User can view all rule sets McAfee TIE Server for Product	View rule sets content. Assign rule sets to policies.
	User has full permission to all rule sets McAfee TIE Server for Product	Create, delete and modify rule sets View rule sets content. Assign rule sets to policies.
	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	
TIE Reputations: Manual classification	McAfee TIE reputations	Modify the reputation of files and certificates on managed systems (endpoints) Import files of reputation data to the TIE Server database

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
Permission Set	n/a (only allowed by an Administrator	Query, create, copy, delete, modify, and assign (to a user) permissions
Queries and Reports (including TIE predefined 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, TIE Server	View registered servers Only allowed by an Administrator	View Create, modify, delete
Systems	View "System Tree" tab	View
System Tree access	Access nodes and portions of the System Tree;Edit system tree groups and systems	Access nodes and portions of the System Tree; create, modify or delete groups

Table 19 – TSF Data Access Permissions

6.1.4.4 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) *TIE/DXL policy and rules management and monitoring,*

e) *TIE reputation management and file import,*

f) *Registered servers,*

g) *Systems and system tree access,*

h) *Query and report management,*

i) *Dashboards.*

6.1.4.5 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles: *Administrator and users with Selected Permissions.*

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

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

6.1.5 Cryptographic Support (FCS)

6.1.5.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *see table below* and specified cryptographic key sizes *see table below* that meet the following*: list of standards (see table below).*

Component	Purpose	Algorithm	Key size	Standard
ePO	TLS	*CTR_DRBG for deterministic random bit generation*	256	*NIST Special Publication 800-90 (CAVP DRBG algorithm certificate #540)*
MA	TLS	*HMAC_DRBG for random number generation*	256	*NIST Special Publication 800-90A (CAVP DRBG algorithm certificate #191)*
TIE Server	TLS	RSA KeyGen 2048 SHA-256	256, 2048	PKCS #10
TIE Server	HTTPS to GTI	RSA KeyGen 2048 SHA-256	256, 2048	PKCS #10
DXL Broker	TLS	RSA KeyGen 2048 SHA-256	256, 2048	PKCS #10
DXL C/C++ Client	TLS	RSA KeyGen 2048 SHA-256	256, 2048	PKCS #10
DXL Java Client	TLS	RSA KeyGen 2048 SHA-256	256, 2048	PKCS #10

Table 20 - Key generation

6.1.5.2 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*.

6.1.5.3 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform *encryption/decryption, digital signature services, hashing services and keyed hash message authentication services to support TLS 1.2* in accordance with a specified cryptographic algorithm *(*see table below*)* and cryptographic key sizes *(see table below)* that meet the following: *list of standards (see table below)*.

Component	Cryptographic Algorithm	Key Sizes (bits)	Standards
ePO/MA	RSA	2048	FIPS 186-4
	AES (operating in GCM mode)	256	FIPS 197
	SHA-384	-	FIPS 180
TIE Server	RSA	2048	FIPS 186-4
	AES (operating in GCM mode)	256	FIPS 197
	HMAC	256	FIPS 198
	SHA-256	-	FIPS 180
DXL Broker	RSA	2048	FIPS 186-4
	AES (operating in GCM mode)	256	FIPS 197
	HMAC	256	FIPS 198
	SHA-256	-	FIPS 180
DXL Clients	RSA	2048	FIPS 186-4
	AES (operating in GCM mode)	256	FIPS 197
	HMAC	256	FIPS 198
	SHA-256	-	FIPS 180

Table 21 - Cryptographic operations

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.

6.1.7 Trusted path/channels (FTP)

6.1.7.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit *the TSF* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *retrieval of file reputation information from GTI*.

6.2 Security Assurance Requirements

85 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

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
	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 22 – Security Assurance Requirements at EAL2

6.3 CC Component Hierarchies and Dependencies

86 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_ACC.1	No other components	FDP_ACF.1	Satisfied
FDP_ACF.1	No other components	FDP_ACC.1 FMT_MSA.3	Satisfied
FIA_ATD.1	No other components	None	n/a

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
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_MSA.1	No other components	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	Satisfied by FDP_ACC.1, FMT_SMR.1 and FMT_SMF.1
FMT_MSA.3	No other components	FMT_MSA.1, FMT_SMR.1	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	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
FTP_ITC.1	No other components	None	n/a

Table 23 – TOE SFR Dependency Rationale

6.4 Security Requirements Rationale

87 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

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

OBJECTIVE SFR	O.MONITOR	O.FIRST_HIT	O.BLOCK	O.ACCESS	O.AUDITS	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.EADMIN	O.IDAUTH	O.PROTECT_DATA	O.CRYPTO
FAU_GEN.1		✓			✓						
FAU_GEN.2					✓						
FAU_SAR.1				✓			✓				
FAU_SAR.2				✓			✓				
FAU_SAR.3		✓					✓				
FAU_STG.1					✓	✓					
FDP_ACC.1			✓								
FDP_ACF.1			✓								
FIA_ATD.1									✓		
FIA_UID.2				✓					✓		
FIA_UAU.2				✓					✓		
FIA_USB.1				✓							
FMT_MSA.1	✓		✓	✓				✓			
FMT_MSA.3	✓		✓					✓			
FMT_MTD.1	✓			✓				✓		✓	
FMT_SMF.1	✓		✓	✓				✓			
FMT_SMR.1	✓		✓	✓				✓			
FCS_CKM.1										✓	✓
FCS_CKM.4										✓	✓
FCS_COP.1										✓	✓
FPT_ITT.1	✓		✓		✓					✓	

SFR \ OBJECTIVE	O.MONITOR	O.FIRST_HIT	O.BLOCK	O.ACCESS	O.AUDITS	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.EADMIN	O.IDAUTH	O.PROTECT_DATA	O.CRYPTO
FPT_TDC.1	✓										
FTP_ITC.1	✓				✓					✓	

Table 24 – Mapping of TOE SFRs to Security Objectives

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

OBJECTIVE	RATIONALE
O.MONITOR	The TOE must be able to associate a reputation with a file or certificate that attempts to run on the network, to be used as the basis for access decisions. The TOE can import reputation data from external sources (FPT_TDC.1, FMT_MTD.1, FMT_MSA.3, FMT_SMR.1, FMT_SMF.1), or reputations can be assigned by an administrator with appropriate permissions (FMT_MTD.1, FMT_MSA.1, FMT_SMR.1, FMT_SMF.1). It is then distributed around the network (FPT_ITT.1, FTP_ITC.1) as required to support policy decisions.
O.FIRST_HIT	The TOE must be able to detect where the first incident related to a malicious object occurred. The TOE records attempted access to potentially malicious objects, including the date/time of access (FAU_GEN.1) and allows sorting of data to identify first incidence (FAU_SAR.3).
O.BLOCK	It must be possible for an authorized user to configure the TOE to block or allow access to files and certificates according to defined policies. An authorized administrator can define and distribute access control policies (FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1, FMT_SMF.1). Policies are distributed around the network in a secure manner (FPT_ITT.1).

OBJECTIVE	RATIONALE
O.ACCESS	The TOE must allow authorized users to access only authorized 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_MSA.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). Audit data can be securely moved around the network (FPT_ITT.1, FTP_ITC.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 TIE events and to administrative actions (FAU_SAR.1, FAU_SAR.2, 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_MSA.1, FMT_MTD.1). Secure default values are assigned to security attributes (FMT_MSA.3).
O.IDAUTH	The TOE must be able to identify and authenticate 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).

OBJECTIVE	RATIONALE
O.PROTECT_DATA	The TOE must ensure the integrity of audit and system data by protecting it from unauthorized modifications and access during transfer. (FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FMT_MTD.1, FPT_ITT.1, FTP_ITC.1)
O.CRYPTO	The TOE must use only cryptographic modules that have been validated to FIPS 140 (FCS_CKM.1, FCS_CKM.4, FCS_COP.1).

Table 25 – Rationale for Mapping of TOE SFRs to Objectives

6.4.2 Rationale for TOE Assurance Requirements Selection

90 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.

91 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

92 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.

93 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	✓			✓		

Security Function SFR	Policy Enforcement	Identification & Authentication	Management	Audit	System Information Import	TSF Data Protection
FDP_ACC.1	✓					
FDP_ACF.1	✓					
FIA_ATD.1			✓			
FIA_UID.2		✓				
FIA_UAU.2		✓				
FIA_USB.1		✓				
FMT_MSA.1			✓			
FMT_MSA.3			✓			
FMT_MTD.1			✓		✓	
FMT_SMF.1			✓		✓	
FMT_SMR.1			✓			
FCS_CKM.1						✓
FCS_CKM.4						✓
FCS_COP.1						✓
FPT_ITT.1						✓
FPT_TDC.1					✓	
FTP_ITC.1						✓

Table 26 – SFR to Security Functions Mapping

SFR	SECURITY FUNCTION AND RATIONALE
FAU_GEN.1	**Audit –** ePO user actions are audited according to the events specified in the table with the SFR. **Policy Enforcement -** In addition to the ePO audit data, the TOE also stores event data concerning potentially malicious files identified on the network.
FAU_GEN.2	**Audit –** The audit log records include the associated user name when applicable.

SFR	SECURITY FUNCTION AND RATIONALE
FAU_SAR.1	**Audit –** Audit log records are displayed in a human readable table form from queries generated by authorized users. **Policy Enforcement –** TIE event data are displayed in a human readable table form in reports and from queries generated by authorized users.
FAU_SAR.2	**Audit –** Only authorized users have permission to query audit log records. **Policy Enforcement –** Only authorized users have permission to query TIE event data
FAU_SAR.3	**Audit –** The TOE provides functionality to sort and filter audit and TIE event data. **Policy Enforcement –** The TOE provides functionality to report on TIE events.
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. **Policy Enforcement –** The TOE protects TIE event data against unauthorized deletion within the ePO database.
FDP_ACC.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_ACF.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.
FIA_UID.2	**Identification** - 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** - 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 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.

SFR	SECURITY FUNCTION AND RATIONALE
FMT_MSA.1	**Management -** The Administrator permission set and user permission sets determine the ability to modify security attributes.
FMT_MSA.3	**Management –** The TOE defines restrictive default values for file and certificate reputation data.
FMT_MTD.1	**Management** – The Administrator permission set and user permission sets determine the access privileges of the user to TOE data. **System Information Import –** A user with the necessary permissions can import reputation information for files and certificates, and system information to populate the system tree.
FMT_SMF.1	**Management** – The management functions that must be provided for effective management of the TOE are defined and described. **System Information Import –** The TOE can import reputation information for files and certificates. The imported information associates file and certificate hash values with reputation scores. System information can also be imported to populate the system tree.
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	**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 protects TSF data while in transit between ePO and MA, and between DXL components.
FPT_TDC.1	**System Information Import** – The TOE provides the functionality to import asset authentication data information from Active Directory (LDAP servers) or NT Domains and correctly interpret the information. It also provides the ability to import reputation data from GTI and via formatted files.
FTP_ITC.1	**TSF Data Protection** – The TOE provides a secure channel to protect the TSF data while it is in transit between DXL components.

Table 27 – SFR to Security Function Rationale

7 TOE Summary Specification

7.1 Policy Enforcement

94 The TOE monitors access to executable files and certificates. If an attempt is made to run a file that is unknown or suspected to be malicious it can be blocked immediately. Subsequent investigation can determine whether the file is a threat, and how many systems ran the file.

95 If an organization routinely uses a file whose default reputation is suspicious or malicious, an administrator can change the file's reputation to trusted, and allow it to run without warnings or prompting.

96 If the reputations of regularly encountered files are known, an administrator can import a list of files and reputations into TIE, and those reputations can be used immediately.

97 TIE notifies the administrator of an unknown file. The administrator can see several details about the file, such as the file's parent process, company and version information, hash information, and the systems that ran the file.

98 Using TIE software involves the following tasks:

- Assigning policy — deploying the TIE policy to managed computers.
- Monitoring events — using the TIE reports, query facilities and TIE Events page to view, filter, and sort events in the enterprise network.
- Performing administrative maintenance — monitoring and managing file reputation data.

99 The administrator must first specify TIE policy rules for the managed systems. This is done using the ePO policy catalog.

100 After creating the rules required for the enterprise, these must be enforced by assigning the policy to managed computers. Once the policy is in place, it can be run in observation mode. This allows the TIE server to begin accumulating file reputation and prevalence information for the system without enforcing the policy. The policy is also associated with a security level (i.e.reputation), and the higher the security level the more files and certificates that are blocked and prompted when encountered.

101 Based upon policy settings the TOE will allow or block execution of a file or access to a certificate, or issue a prompt to the user on the managed system, according to its reputation. Reputation is recorded as a numeric value (0-99), where a higher value indicates a higher level of trust. Policy includes setting thresholds at which files are allowed, blocked or prompted on a managed system. If a prompt is issued the user on the managed system can decide whether to continue to use the file or not.

102 TIE reputation data is stored on the TIE Server in its database. Results of queries are cached locally by the TIE module for up to 30 days.

103 Event data on observed events (e.g. blocked files) is stored by ePO.

104 DXL policies allow the administrator to configure the DXL network: for example defining to which brokers a client is allowed to connect. The current connection status of all brokers can also be viewed.

105 DXL messages come in two forms:

- 1-1 – This is a direct message on a specific service. Examples include a file reputation query or a database update.
- 1-Many – This is a message broadcast to all interested parties. An example of this is a file reputation change or a request for all relevant clients to take an action.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FDP_ACC.1, FDP_ACF.1

7.2 Identification and Authentication

106 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.

107 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.

108 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.

109 The DXL server and DXL client carry out mutual authentication when establishing a connection. This authentication is done by verifying certificates, generated within the ePO extension, and presented during the TLS session establishment.

TOE Security Functional Requirements Satisfied: FIA_UID.2, FIA_UAU.2, FIA_USB.1

7.3 Management

110 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-ePO user.

111 The TOE provides functionality to manage the following:

1. ePO user accounts,
2. Permission sets,
3. Audit log,
4. TIE/DXL policy and rules,
5. Registered servers,
6. Systems and system tree access,

7. Queries and reports,
8. Dashboards.

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

7.3.1 ePO User Account Management

113 Each user authorized for login to ePO must be defined with ePO. Only 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

114 One or more permission sets may be associated with an account. ePO users granted permission as “Administrator” have access to everything in ePO.

115 Permissions exclusive to 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

116 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

117 When a user account is created in ePO, 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 “Administrator”.

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

119 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.

120 When a new ePO product extension (e.g., TIE) 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 Administrators can then grant permissions to users through existing or new permission sets.

121 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.

122 When a permission set is created or modified, the permissions granted via the permission set may be specified by an Administrator.

7.3.3 Audit Log Management

123 An Administrator may view and purge events in the audit log. A user with the appropriate permissions may view only, or view and purge events in the audit log.

7.3.4 TIE/DXL policy and rules

124 A product policy is a collection of settings that are created, configured, and then enforced. Product policies ensure that McAfee Agent and TIE/DXL components 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.

125 The TIE/DXL added permissions associated with policy management are:

1. McAfee TIE Server for Product: needed to access TIE policies and tasks;
2. McAfee TIE Reputations: needed for access to the Reputations page to modify reputations;
3. DXL McAfee MePO Certificate Creation: needed for ePO support;
4. McAfee DXL Broker Management: for DXL Broker management policies;
5. McAfee DXL Client Policies: for DXL Client management policies;
6. McAfee DXL Fabric: for viewing the DXL Fabric Management page.

126 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 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.

127 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 Administrator. When a product policy is deleted, all groups and systems where it is currently applied inherit the product policy of their parent group.

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

129 TIE/DXL policies are created, managed and assigned to managed systems using ePO. TIE policies determine:

- When a file or certificate with a specific reputation is allowed to run on a system;
- When a file or certificate is blocked;
- When the managed system user is prompted for what to do.

The McAfee TIE Server for Product permission is required for this.

130 Policies are applied to systems, or groups of systems, using defined rules. The rules govern how a given policy is to be applied on the network.

131 The TIE module for VSE Events page shows recent TIE events, and the actions taken, and allows policy to be adjusted as necessary.

132 Where an unknown file or certificate is encountered on an endpoint the default reputation causes the file to be blocked. The signature is sent to the TIE Server to determine whether a reputation is stored on the TIE Server database. If no information is held there a query is sent to GTI. If no reputation information is identified that would allow the file or certificate to be used under the defined policy, a TIE event is recorded and sent to ePO for storage. Reputation data may be manually modified by an Administrator or ePO user (either directly or through the import of files containing reputation data) with the appropriate permission via the Reputations page.

7.3.5 Registered Servers

133 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. 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.

134 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

135 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.

136 Groups have these characteristics:

1. Groups can be created by 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 an Administrator or user with both the “View "System Tree" tab” and “Edit System Tree groups and systems” permissions.

137 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.

138 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.

139 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 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.

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

7.3.7 Queries and reports

141 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 private queries/reports.
3. Edit public groups; create and edit private queries/reports; make private 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

142 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 private dashboards;
3. Edit public dashboards; create and edit private dashboards; make private dashboards public;
4. View audits and assignments.

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

7.4 Audit

7.4.1 ePO audit log

143 The Audit Log maintains a record of ePO user actions. The auditable events are specified in Table 17 – Audit Events and Details.

144 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.

145 Audit Log entries can be queried by an Administrator or users assigned to the Global reviewer permission set. The Administrator can elect 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 ePO database; if space is exhausted, new entries are discarded.

7.4.2 TIE events

146 TIE events that are recorded as a result of the application of TIE policies are also treated as audit data, but are stored separately in the ePO database. Recent events can be viewed via the

TIE Module for VirusScan Events page in ePO. This allows threat events to be filtered on the basis of event type, date, system id, rule name or file hash.

147 For these events the TOE provides the following TIE predefined reports through ePO:

1. New files and certificates seen in the enterprise
2. Files and certificates organized by reputation
3. Files and certificates with changed reputations
4. Top 10 systems with new files or certificates
5. Blocked, allowed and cleaned events
6. Observed events

148 These are accessed via the ePO Queries and Reports page, either for the TIE server, or for the module for VirusScan Enterprise. Information on items 1 to 4 above is derived from the TIE Server, and is based on the TIE Server reputation database. This is not considered to be audit data. Items 5 and 6 are derived from audited events data in the ePO database.

149 Event entries can be queried by an Administrator or users assigned to the Queries and Reports permission set. No mechanisms are provided for modification of event data. The event entries are stored in the ePO database; if space is exhausted, new entries are discarded.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1

7.5 System Information Import

150 TIE has provision for the import of XML formatted files, containing file or certificate hashes, reputation values, and optionally associated file names. These can be used to specify reputations that are organization specific. Structured Threat Information eXpression (STIX) files can also be used to import file reputations. Modification of reputation data requires an Administrator or a user with the McAfee TIE Reputations permission. Until a reputation is associated with a file or certificate the default when a blocking policy is defined is to block access.

151 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.

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

153 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.

154 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.

155 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.

156 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.

157 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 are 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: FMT_MTD.1, FMT_SMR.1, FPT_TDC.1

7.6 TSF Data protection

7.6.1 ePO and MA

158 Communications between McAfee Agents and ePO take the form of XML messages. Communications can include policies to implement, event data gathered by the TIE 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 256 bit key sizes (by default the cipher used by ePO and McAfee Agent is DHE-RSA-AES256-GCM-SHA384).

159 In FIPS mode, ePO uses OpenSSL v1.0.2h with FIPS module v2.0.12 (FIPS 140-2 certificate #2398) 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. Session keys are destroyed by overwriting when no longer required.

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards	CAVP Cert #
Key Transport	RSA encrypt/decrypt	2048	Allowed in FIPS mode	OpenSSL #1928 BSAFE #1046
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (operating in GCM mode)	256	FIPS 197	OpenSSL #3751 BSAFE #2017
Secure Hashing	SHA-384	Not Applicable	FIPS 180-3	OpenSSL #3121 BSAFE #1767

Table 28 - Cryptographic operations ePO/MA

7.6.2 TIE/DXL

160 The DXL client receives a policy via ePO. The policy includes the allowed DXL Brokers' names and IP addresses. The client instantiates a connection to the preferred broker and authenticates. The connection is protected using TLS 1.2. The key pair for authentication is generated by ePO, and supplied via the MA channel.

161 For ePO report population the Registered Servers feature of ePO is used to extract data from the TIE Server. This employs Java DataBase Connectivity over TLS 1.2.

162 The TIE Server communicates with GTI to obtain file and certificate reputation data. This external channel is protected using TLS 1.0.

163 The relevant cryptographic services for both TIE Server and DXL are provided by OpenSSL (TIE Server using the v1.0.2i library and DXL using the v1.0.2h library) with FIPS module v2.0.12 (FIPS 140-2 certificate #2398), and RSA BSAFE Crypto-J Micro Edition 6.2.1 (FIPS 140-2 certificate #2468[8]) for the Java client. 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. Session keys are destroyed by overwriting when no longer required.

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards	CAVP Cert #
Key Transport	RSA encrypt/decrypt	2048	Allowed in FIPS mode	OpenSSL #1928 -
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (operating in GCM mode)	256	FIPS 197	OpenSSL #3751 BSAFE #3263

[8] The same crypto module is used in RSA BSAFE Crypto-J Micro Edition 6.2.1 as in RSA BSAFE Crypto-J Micro Edition 6.2.0.x

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards	CAVP Cert #
Secure Hashing	SHA-256	Not Applicable	FIPS 180-3	OpenSSL #3121 BSAFE #2701

Table 29 - Cryptographic operations DXL

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