Security Target

McAfee Deep Defender 1.0.1 and ePolicy Orchestrator 4.6.1

Document Version 1.0

October 1, 2012

Prepared For:

McAfee, Inc.

2821 Mission College Blvd.

Santa Clara, CA 95054

www.mcafee.com

Prepared By:

Primasec Limited

Le Domaine de Loustalviel

11420 Pech Luna, France

www.primasec.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the McAfee Deep Defender 1.0.1 and ePolicy Orchestrator 4.6.1. 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 that meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1 Introduction

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

1.1 ST reference

ST Title	Security Target: McAfee Deep Defender 1.0.1 and ePolicy Orchestrator 4.6.1
ST Revision	1.0
ST Publication Date	October 1, 2012
Authors	Primasec Limited and McAfee Incorporated

1.2 TOE reference

TOE Reference	McAfee Deep Defender 1.0.1 and ePolicy Orchestrator 4.6.1
TOE Type	Anti Malware

1.3 Document organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organisational 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 address the threats
5	Extended Components Definition	Describes extended components of the evaluation
6	Security Requirements	Contains the functional and assurance requirements for the TOE

SECTION	TITLE	DESCRIPTION
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document conventions

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

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by *italicized* text, contained within square brackets.
- 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, contained within square brackets.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FIA_UAU.1.1 (1) and FIA_UAU.1.1 (2) refer to separate instances of the FIA_UAU.1 security functional requirement component.

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

1.5 Document terminology

The following tables describe the terms and acronyms used in this document:

TERM	DEFINITION
CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
GB	Giga-Byte

TERM	DEFINITION
GUI	Graphical User Interface
I&A	Identification and Authentication
IT	Information Technology
MB	Mega-Byte
MDD	McAfee Deep Defender
OS	Operating System
OSP	Organisational Security Policy
PC	Personal Computer
PP	Protection Profile
RAM	Random Access Memory
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSFI	TOE Security Function Interface

Table 2 –Acronyms Used in Security Target

Term	Definition
Authorized administrator	An ePO user assigned the appropriate permission for the operation being performed
Intel® VT	Intel® Virtualization Technology – defines the VMX-root mode of operation of the CPU, a higher privilege level used by Virtual Machine Monitors to execute Operating system in a guest (VMX non-root) environment.
TMSL	Trusted Memory Service Layer – a memory virtualization software layer executing in VMX-root mode – the ring-level of operation is ring-0p (privileged)
Guest OS	An unmodified OS that operates in VMX-non-root mode – the notation for the OS kernel mode of operation is ring-0d (de-privileged)
IB Agent	In-band security agent – a software entity executing within a guest OS ring-0p environment.
Handler	An independently executing software entity scheduled by the TMSL – executing in ring-0d, but with elevated privileges managed by the TMSL

Table 3 –Terms Used in Security Target

1.6 TOE overview

MDD is a software package designed to protect Microsoft Windows-based desktop computers from unwanted code and programs, specifically rootkits. MDD monitors the memory and CPU registers:

- Protecting against loading of known hostile code, and
- Preventing access to protected areas.

The CPU is responsible for controlling access between User Mode and Kernel Mode components and, with part of the MDD solution residing under the kernel, MDD is able to monitor and control access to kernel memory, preventing the loading of known hostile code, and protecting unauthorized access to memory locations that require protection. Known malicious code and new attack agents can be identified, reported and removed.

The management capabilities for MDD are provided by ePO. ePO manages McAfee Agents and MDD software that reside on client systems. By using ePO a large enterprise network can be managed from a centralized system. ePO also provides scheduling capabilities to distribute updated MDD security policies and signature files, and maintains audit files.

Communication between the distributed components of the TOE is protected from disclosure and modification by cryptographic functionality provided by the operational environment.

1.7 TOE Description

The TOE consists of three components: MDD, ePO and McAfee Agent.

1.7.1 MDD

The MDD software provides protection from unwanted code and programs, specifically rootkits hidden within drivers. It makes use of Intel VT technology on Intel i3, i5 and i7 processors to specify and protect kernel memory and CPU registers, such that MDD can monitor and prevent rootkit attacks that operate at kernel level. Once the malicious software is detected MDD carries out the configured remedial actions.

1.7.2 ePolicy Orchestrator (ePO)

ePO distributes and manages agents that reside on client systems. ePO provides the central management interface and functionality for the administrators of the TOE. It also provides centralized audit collection and review functionality.

1.7.3 McAfee Agent

McAfee Agent is a vehicle of information and enforcement between the ePO server and each managed system. It provides common communication functionality between ePO and all of McAfee's product-specific software (such as MDD).

1.7.4 Physical boundary

The TOE is a software TOE and includes:

1. The ePO application executing on a dedicated server;
2. The McAfee Agent and MDD software on each client to be protected.

The physical components of the TOE include the software that is installed during installation of MDD, McAfee Agent and ePO. The TOE software is installed on a centralized ePO server and on client workstations. The computer hardware platforms that the TOE software is installed on are not part of the TOE.

The components of the TOE are installed on systems with resident operating systems, but the operating systems are not part of the TOE.

ePO requires a database, but the DBMS is not part of the TOE.

The following documentation provided to end users is included in the TOE boundary:

1. *McAfee Deep Defender 1.0 Product Guide*
2. *McAfee Deep Defender 1.0 Installation Guide*
3. *McAfee ePolicy Orchestrator 4.6 Product Guide*
4. *McAfee ePolicy Orchestrator 4.6 Installation Guide*
5. *McAfee Deep Defender 1.0 and ePolicy Orchestrator 4.6 Common Criteria Evaluated Configuration Guide*

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

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	MDD 1.0.1.706 ePolicy Orchestrator 4.6.1.1192 McAfee Agent 4.6.0.2292[1]
IT Environment	Specified in the following: • Table 5 – Management System Component Requirements • Table 6 – Managed System Platforms

[1] McAfee Agent is shipped/packaged with ePO 4.6.1.

Table 4 – Evaluated Configuration for the TOE

The evaluated configuration includes one or more instances of McAfee Agent and MDD and an instance of ePO. The following configuration options must be selected for the evaluated configuration:

1. All user accounts defined in ePO must specify Windows authentication;
2. Specify the binaries to be protected.

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

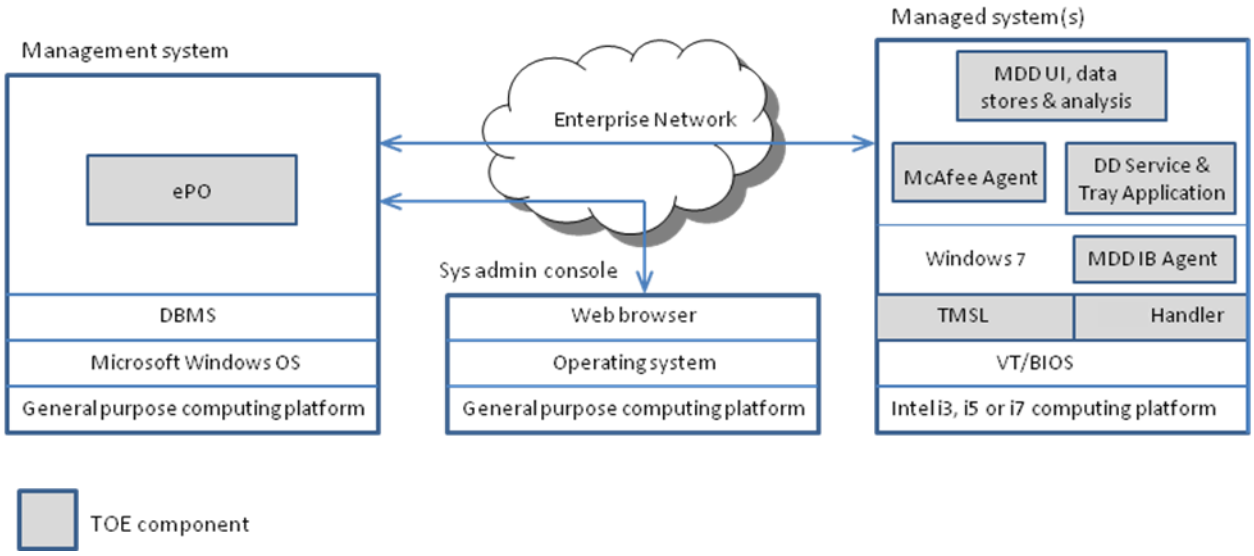

Figure 1 – TOE boundary

The following are the main components of the overall solution:

- MA: The McAfee Agent (MA) is software that resides on the workstation along with the MDD software and is responsible for communicating with the ePO server.
- ePO Console: This is part of the ePO server infrastructure in the enterprise network through which the IT organization will deploy and manage the McAfee security solution on the devices.
- Deep Defender service: a Windows service application that receives security events from the IB Agent and delivers them to the ePO server and other user-mode applications for inspection by the user.
- Deep Defender UI: A notification dialog that runs with the privilege of the logged on user(s).

- Deep Defender Tray: a (sys)tray application for notifying and visualizing events collected by the McAfee Deep Defender service and for presenting overall protection status information.
- Guest OS: An unmodified OS (Windows 7) that operates in VMX-non-root mode – the notation for the OS kernel mode of operation is ring-0d (de-privileged).
- TMSL: Trusted Memory Service Layer: a memory virtualization software layer executing in VMX-root mode – the ring-level of operation is ring-0p (privileged).
- Handler: An independently executing software entity scheduled by the TMSL – executing in ring-0p however with elevated privileges managed by the TMSL. The Handler communicates with the IB Agent.
- IB Agent: In-band security agent – a Windows device driver executing within a guest OS ring-0p environment. The IB Agent provides information to the TMSL on which memory and register resources require protection, and makes access decisions.
- DBMS: (Operational Environment) The database stores ePO user accounts, permissions, permission sets, assets, audit logs, policies, policy templates, events, and SNMP trap destinations (used in the event the audit log becomes full).

The functionality that is not included in the evaluation is itemized below:

1. The ability to update the TOE (scan engine). Note that the ability to update the rootkit signatures (DAT file) is included in the evaluation.

1.7.5 Hardware and software supplied by the IT environment

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

The platform on which ePO is installed must be dedicated to functioning as the management system. ePO operates as a distribution system and management system for a client-server architecture offering components for the server part of the architecture (not the clients). The TOE requires the following hardware and software configuration on this platform.

COMPONENT	MINIMUM REQUIREMENTS
Processor	Intel Pentium 4-class or higher; 1.3 GHz or higher
Memory	4 GB RAM
Free Disk Space	2.5 GB
Monitor	1024x768, 256-color, VGA monitor or higher

COMPONENT	MINIMUM REQUIREMENTS
Operating System	Any of the following: Windows Server 2003 Enterprise with SP2 or later Windows Server 2003 Standard with SP2 or later Windows Server 2003 Datacenter with SP2 or later Windows Server 2008 R2 Enterprise Windows Server 2008 R2 Standard Windows Server 2008 R2 Datacenter Windows Server 2008 Enterprise with SP2 or later Windows Server 2008 Standard with SP2 or later Windows Server 2008 Datacenter with SP2 or later Windows 2008 Small Business Server
DBMS	Any of the following: SQL Server 2005 with SP3 or higher SQL 2008 Express with SP1 SQL 2008 Standard with SP2 SQL 2008 R2 Work Group Edition
Additional Software	MSXML 6.0 Internet Explorer 7.0 or 8.0, or Firefox 3.5 or 3.6 .NET Framework 2.0 Microsoft Visual C++ 2005 SP1 Redistributable Microsoft Visual C++ 2008 Redistributable - x86 MDAC 2.8 Microsoft updates MSI 3.1 RSA Crypto-C ME 2.0 RSA Crypto-J 4.0
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

Table 5 – Management System Component Requirements

The supported platforms for McAfee Agent and MDD are:

COMPONENT	MINIMUM REQUIREMENTS
Processor	Intel i3, i5 or i7 (Intel VT must be enabled in BIOS)
Memory	2GB (32-bit, 4GB (64-bit)
Free Disk Space	240 MB
Browser	Microsoft Internet Explorer version 7.0 or 8.0
Operating System	Microsoft Windows 7 Home Premium, Professional, Enterprise or Ultimate (32 and 64 bit) inc SP1
Network Card	Ethernet, 10Mb or higher

Table 6 – Managed System Platforms

The management system is accessed from remote systems via a browser.

Identification and authentication services for ePO users and workstation users are provided by the operational environment. Windows services are invoked by the TOE to validate user credentials. Windows may be integrated with a credential store to perform the credential validation.

Protection of communications between the MDD client and ePO, and between ePO and a remote management browser, is handled by Windows in the TOE environment. The TOE environment also provides integrity protection for the DAT files.

1.7.6 Logical boundary

The logical boundaries of the TOE are defined by the functions provided by the TOE and are described in the following sections.

The TOE includes management interfaces that administrators use to configure the MDD policies and review the log files. The management interface is provided by both ePO and MDD. The rootkit detection functionality is provided by MDD.

The logical boundaries of the TOE include the security functions that the TOE provides to the system that utilises the product for the detection of and protection against rootkits. The security functions include Audit, Management, and Malware Scanning (Kernel Protection against rootkits) and Alerts.

TSF	DESCRIPTION
Malware Scanning and Alerts	MDD provides the following functionality related to malicious code scanning and alerts: 1. Access Protection - This function protects the registry and processes resident in memory from intrusions by controlling access to them. 2. Automatic Updates – Allows signature (DAT) files to be updated automatically per the configured schedule.
Audit	The tray application allows the user to review the history of notification messages reported on the client. Audit information is concurrently generated for transmission to the ePO management databases. Audit logs for all clients can be reviewed from the ePO console.
Management	ePO enables an administrator to centrally manage security settings for the managed workstations and manage the audit logs.

Table 7 – Logical Boundary Descriptions

1.7.7 TOE data

TOE data consists of both TSF data and user data (information). TSF data consists of authentication data, security attributes, and other generic configuration information. Security attributes enable the TSF to enforce the security policy. Authentication data enables the TSF to identify and authenticate users.

TSF Data	Description	AD	UA	GE
Contacts	A list of email addresses that ePolicy Orchestrator uses to send email messages to specified users in response to events.			✓
Dashboards	Collections of chart-based queries that are refreshed at a user-configured interval.			✓
Email Server	SMTP server name and port used to send email messages for notifications. Credentials may optionally be specified for authenticated interactions.			✓
ePO User Accounts	ePO user name, authentication configuration, enabled status, Global Administrator status and permission sets for each user authorized to access TOE functionality on ePO.	✓		
Global Administrator Status	Individual ePO user accounts may be configured as Global Administrators, which means they have read and write permissions and rights to all operations.		✓	
Groups	Node on the hierarchical system tree that may contain subordinate groups or systems.			✓
Notification Rules	Rules associated with groups or systems used to generate email messages and/or SNMP traps upon receipt of specified events			✓
Permission	A privilege to perform a specific function.		✓	
Permission Set	A group of permissions that can be granted to any user by assigning it to the user's account.		✓	
Queries	Configurable objects that retrieve and display data from the database.			✓
Server Settings	Control how the ePolicy Orchestrator server behaves.			✓
SNMP Trap Destination(s)	Name and address of an SNMP server to receive trap messages as a result of notification rules.			✓
System Information	Information specific to a single managed system (e.g. internet address) in the system tree.			✓
system tree	A hierarchical collection of all of the systems managed by ePolicy Orchestrator.			✓
MDD Access Protection Policies	Policies used to restrict access to specified ports, files, shares, registry keys, and registry values on the client systems.			✓
MDD DAT Files	Detection definition files used by MDD on the client systems.			✓
MDD White lists and Black lists	MDD can be configured to allow or block specific drivers from running on the endpoint, using White or Black lists, respectively.			✓

TSF Data	Description	AD	UA	GE
MDD binaries to protect	Specific components of the MDD software to be protected during operation of the TOE.			✓
MDD Quarantine Policies	Policies that specify where quarantined files are stored on the client systems and how long they are kept.			✓
MDD Quarantined Files	Collection of files on a client system that have been quarantined by MDD.			✓

Table 8 – TOE Data (Legend: AD=Authentication data; UA=User attribute; GE=Generic Information)

1.8 Rationale for non-bypassability and separation of the TOE

The TOE is an application that executes on top of an underlying hardware system (Intel i3, i5 and i7 processors), in conjunction with a Windows operating system. Responsibility for non-bypassability and separation are split between the TOE, the OS and the hardware IT Environment.

All access to objects in the TOE IT environment is validated by the IT environment security policies before they can succeed. An attacker will not be able to access any of the TOE security functions or any of the TOE files or directories. Arbitrary entry into the TOE is not possible, and therefore the TSF is protected against external interference by untrusted objects.

Because the TOE is isolated in its own domain, partly in Ring 0p, the TOE's IT environment maintains and controls execution for the TSF separately from other processes. For MDD this control is at a level below the operating system.

The TOE provides strictly controlled functionality to the users within the TSC. By limiting access through ePO role based access control, the TSF is protected from corruption or compromise from users within the TSC. The TOE interfaces are separated into 2 categories – security enforcing and security supporting. Security enforcing interfaces invoke the TSF and ensure that all enforcement functions complete successfully before allowing the user invoked action to proceed. Security supporting interfaces ensure that the TSF cannot be interfered with via those interfaces (i.e. they are isolated from the TSF). The security enforcing role is separate from the security supporting role and each role has its own unique set of privileges associated with it. Multiple simultaneous users (and roles) are supported.

The TOE associates distinct attributes and privileges with each process and restricts access according to the configured security policies. Processes are separate from each other, each with their own memory buffer and it is impossible for one process to directly access the memory of another. The OS and hardware support non-bypassability by ensuring that access to protected resources pass through the TOE and is limited to access within the OS scope of control, which is enforced by the security policies for the OS and the IT environment. The hardware and OS provide separate process spaces in which the TOE

executes; these process spaces are protected from interference from other processes except through the defined TOE interfaces.

2 Conformance claims

2.1 Common Criteria conformance claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 extended and Part 3 conformant at Evaluation Assurance Level 2 and augmented by ALC_FLR.2 – Flaw Reporting Procedures.

2.2 Protection Profile conformance claim

The TOE does claim conformance to any Protection Profile.

3 Security problem definition

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

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

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

3.1 Threats

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

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.ACCIDENTAL_ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.AUDIT_ COMPROMISE	A user or process may gain unauthorized access to the audit trail and cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a security relevant event.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of memory used by the TOE to scan files or process administrator requests.
T.TSF_COMPROMISE	A user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted)
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.
T.UNIDENTIFIED_ACTIONS	Failure of the authorized administrator to identify and act upon unauthorized actions may occur.
T.MALWARE	A malicious agent may attempt to introduce malware onto a workstation via network traffic or removable media to compromise data on that workstation, or use that workstation to attack additional systems.

Table 9 – Threats Addressed by the TOE

3.2 Organisational security policies

The following organisational security policy applies to the TOE:

POLICY	DESCRIPTION
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.

Table 10 – Organisational Security Policy

3.3 Assumptions

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

ASSUMPTION	DESCRIPTION
A.AUDIT_BACKUP	Administrators will back up audit files and monitor disk usage to ensure audit information is not lost.
A.NO_EVIL	Administrators are non-hostile, appropriately trained, and follow all administrative guidance.
A.PHYSICAL	It is assumed that the appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
A.SECURE_COMMS	It is assumed that the IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.
A.SECURE_UPDATES	Administrators will implement secure mechanisms for receiving and validating updated signature files from McAfee, and for distributing the updates to the central management systems.
A.DEDICATED_PLAT	The hardware platform used for ePO will not be used to host other applications.

Table 11 – Assumptions

4 Security objectives

4.1 Security objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ADMIN_ROLE	The TOE must provide authorized administrator roles to isolate administrative actions.
O.AUDIT_GENERATION	The TOE must provide the capability to detect and create records of security-relevant events.
O.AUDIT_PROTECT	The TOE must provide the capability to protect audit information.
O.AUDIT_REVIEW	The TOE must provide the capability to selectively view audit information.
O.CORRECT_TSF_OPERATION	The TOE must provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.
O.MANAGE	The TOE must provide all the functions and facilities necessary to support the authorized users in their management of the TOE.
O.DETECT	The TOE must detect and take action against known malicious device drivers.
O.PROTECT	The TOE must protect critical kernel memory and CPU registers against unauthorized access.

Table 12 – TOE Security Objectives

4.2 Security objectives for the operational environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.AUDIT_BACKUP	The operational environment must provide the capability to backup and restore Audit log files, and must ensure that audit log files do not run out of disk space.
OE.AUDIT_SEARCH	The operational environment must provide the capability to search and sort the audit information.
OE.AUDIT_STORAGE	The operational environment must provide a means for secure storage of the TOE audit log files.
OE.NO_EVIL	Sites using the TOE must ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.PHYSICAL	Physical security must be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

OBJECTIVE	DESCRIPTION
OE.RESIDUAL_INFORMATION	The operational environment must ensure that any information contained in a protected resource within the TOE Scope of Control is not released when the resource is reallocated.
OE.SECURE_COMMS	The operational environment must provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.
OE.SECURE_UPDATES	Enterprises using the TOE must ensure that signature file updates are received from McAfee via secure mechanisms, the updates are validated before being used, and the updates are distributed to central management systems with the enterprise via secure mechanisms.
OE.TIME_STAMPS	The operational environment must provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.
OE.TOE_ACCESS	The operational environment must provide mechanisms that control a user's logical access to the TOE.
OE.DEDICATED_PLAT	The hardware platform used to host ePO must not be used to host other applications.
OE.SEC_DBMS	The operational environment must protect the confidentiality and integrity of ePO data stored in the DBMS.
OE.SEC_PROC	The processors on the client hardware platform must enforce the operation of privilege levels.
OE.ADMIN_GUIDANCE	The administrators shall be provided with the necessary information (TOE Product Guides) for secure management.

Table 13 – Operational Environment Security Objectives

4.3 Security objectives rationale

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

	A.AUDIT_BACKUP	A.NO_EVIL	A.PHYSICAL	A.SECURE_COMMS	A.SECURE_UPDATES	A.DEDICATED_PLAT	T.ACCIDENTAL_ADMIN_ERROR	T.AUDIT_ COMPROMISE	T.MASQUERADE	T.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNATTENDED_SESSION	T.UNIDENTIFIED_ACTIONS	T.MALWARE	P.ACCOUNTABILITY

	A.AUDIT_BACKUP	A.NO_EVIL	A.PHYSICAL	A.SECURE_COMMS	A.SECURE_UPDATES	A.DEDICATED_PLAT	T.ACCIDENTAL_ADMIN_ERROR	T.AUDIT_ COMPROMISE	T.MASQUERADE	T.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNATTENDED_SESSION	T.UNIDENTIFIED_ACTIONS	T.MALWARE	P.ACCOUNTABILITY
O.ADMIN_ROLE								✓	✓						
O.AUDIT_GENERATION													✓		✓
O.AUDIT_PROTECT								✓							
O.AUDIT_REVIEW													✓		
O.CORRECT_TSF_OPERATION											✓				
O.MANAGE											✓				
O.DETECT														✓	
O.PROTECT														✓	
OE.AUDIT_BACKUP	✓														
OE.AUDIT_SEARCH													✓		
OE.AUDIT_STORAGE								✓							
OE.NO_EVIL		✓													
OE.PHYSICAL			✓												
OE.RESIDUAL_INFORMATION								✓		✓	✓				
OE.SECURE_COMMS				✓											
OE.SECURE_UPDATES					✓										
OE.TIME_STAMPS													✓		✓
OE.TOE_ACCESS									✓			✓			✓
OE.DEDICATED_PLAT						✓									
OE.SEC_DBMS											✓				
OE.SEC_PROC											✓				
OE.ADMIN_GUIDANCE							✓								

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

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

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
T.ACCIDENTAL_ADMIN_ ERROR: An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.	OE.ADMIN_GUIDANCE: The administrators shall be provided with the necessary information (TPE Product Guides) for secure management.	OE.ADMIN_GUIDANCE helps to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is insecure.
T.AUDIT_ COMPROMISE: A user or process may cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	O.AUDIT_PROTECT: The TOE must provide the capability to protect audit information. O.ADMIN_ROLE: The TOE must provide authorized administrator roles to isolate administrative actions. OE.AUDIT_STORAGE: The operational environment must provide a means for secure storage of the TOE audit log files. OE.RESIDUAL_ INFORMATION: The operational envionnment must ensure that any information contained in a protected resource within the TOE Scope of Control is not released when the resource is reallocated.	O.AUDIT_PROTECT contributes to mitigating this threat by controlling access to the individual audit log records. No one is allowed to modify audit records, an administrator must be granted explicit permission to delete audit records, and the TOE has the capability to prevent auditable actions from occurring if the audit trail is full. O.ADMIN_ROLE mitigates this threat by requiring the enforcement of administrator roles that restrict access to audit data. OE.AUDIT_STORAGE contributes to mitigating this threat by restricting the ability of users in the IT Environment to access the audit log file. OE.RESIDUAL_INFORMATION pre-vents a user not authorized to read the audit trail from access to audit information that might otherwise be persistent in a resource used by the TOE (e.g., memory). By

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
		preventing residual information in a resource, audit information will not become available to any user or process except those explicitly authorized for that data.
T.MASQUERADE: A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.ADMIN_ROLE: The TOE must provide authorized administrator roles to isolate administrative actions. OE.TOE_ACCESS: The operational environment must provide mechanisms that control a user's logical access to the TOE.	O.ADMIN_ROLE mitigates this threat by requiring the enforcement of administrator roles that restricts access to data and TOE resources. OE.TOE_ACCESS mitigates this threat by requiring authorized administrators and workstation users to be identified and authenticated, a necessary step in controlling the logical access to the TOE and its resources by constraining how and when users can access the TOE. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.
T.RESIDUAL_DATA: A user or process may gain unauthorized access to data through reallocation of memory used by the TOE to scan files or process administrator requests.	OE.RESIDUAL_INFORMATION: The operational environment must ensure that any information contained in a protected resource within the TOE Scope of Control is not released when the resource is reallocated.	OE.RESIDUAL_INFORMATION counters this threat by ensuring that memory contents are not persistent when resources are released by the TOE and allocated to another user/process.
T.TSF_COMPROMISE: A user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).	OE.RESIDUAL_INFORMATION: The operational environment must ensure that any information contained in a protected resource within the TOE Scope of Control is not released when the resource is reallocated.	OE.RESIDUAL_INFORMATION is necessary to mitigate this threat, because even if the security mechanisms do not allow a user to explicitly view TSF data, if TSF data were to inappropriately reside in a resource that was made available

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
	O.MANAGE: The TOE must provide all the functions and facilities necessary to support the authorized users in their management of the TOE. O.CORRECT_TSF_OPERATION: The TOE must provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site. OE.SEC_DBMS: The operational environment must protect the confidentiality and integrity of ePO data stored in the DBMS. OE.SEC_PROC: The processors on the client hardware platform must enforce the operation of privilege levels.	to a user, that user would be able to inappropriately view the TSF data. O.MANAGE is necessary because an access control policy is not specified to control access to TSF data. This objective is used to dictate who is able to view and modify TSF data, as well as the behavior of TSF functions. O.CORRECT_TSF_OPERATION provides assurance that the TSF continues to operate as expected in the field. OE.SEC_DBMS provides assurance that data stored by ePO in its associated DBMS is not inappropriately accessed directly via the host operating system. OE.SEC_PROC requires the hardware protection mechanisms of the Intel processors to enforce privilege levels.
T.UNATTENDED_ SESSION: A user may gain unauthorized access to an unattended session.	OE.TOE_ACCESS: The operational environment must provide mechanisms that control a user's logical access to the TOE.	OE.TOE_ACCESS helps to mitigate this threat by including mechanisms that place controls on user's sessions. Locking a session reduces the opportunity of someone gaining unauthorized access to the session when the console is unattended.
T.UNIDENTIFIED_ACTIONS: Failure of the authorized administrator to identify and act upon unauthorized actions may occur.	O.AUDIT_REVIEW: The TOE must provide the capability to selectively view audit information. OE.AUDIT_SEARCH: The operational environment must provide the capability to search and sort the audit information.	O.AUDIT_REVIEW helps to mitigate this threat by providing the administrator with a required minimum set of configurable audit events that could indicate a potential security violation. By configuring these auditable events, the TSF monitors the occurrences of these events (e.g. set number of

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
	O.AUDIT_GENERATION: The TOE must provide the capability to detect and create records of security relevant events. OE.TIME_STAMPS: The operational environment must provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.	authentication failures, set number of information policy flow failures, self-test failures, etc.). OE.AUDIT_SEARCH assists the administrator in reviewing the audit logs by making it easier to focus on particular events of interest. O.AUDIT_GENERATION helps to mitigate this threat by recording actions for later review. OE.TIME_STAMPS helps to mitigate this threat by ensuring that audit records have correct timestamps.
T.MALWARE: A malicious agent may attempt to introduce malware onto a workstation via network traffic or removable media to compromise data on that workstation, or use that workstation to attack additional systems.	O.DETECT: The TOE must detect and take action against known malicious device drivers. O.PROTECT: The TOE must protect critical kernel memory and CPU registers against unauthorized access.	O.DETECT mitigates this threat by detecting the presence of, or attempts to install known hostile drivers. O.PROTECT mitigates this threat by providing mechanisms to prevent unauthorised access to designated critical areas of kernel memory and CPU registers.
P.ACCOUNTABILITY: The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.AUDIT_GENERATION: The TOE must provide the capability to detect and create records of security-relevant events. OE.TIME_STAMPS: The operational environment must provide reliable time stamps and the capability for the administrator to set the time used for these time stamps. OE.TOE_ACCESS: The TOE must provide mechanisms that control a user's logical access to the TOE.	O.AUDIT_GENERATION addresses this policy by recording security-relevant events. The administrator's ID is recorded when any security relevant change is made to the TOE. OE.TIME_STAMPS plays a role in supporting this policy by requiring the IT environment to provide a reliable time stamp. The audit mechanism is required to include the current date and time in each audit record. OE. TOE_ACCESS supports this policy by requiring the IT

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
		environment to identify and authenticate all authorized administrators and workstation users prior to allowing any TOE access.
A.AUDIT_BACKUP: Administrators will back up the audit files and monitor disk usage to ensure audit information is not lost.	OE.AUDIT_BACKUP: The operational environment must provide the capability to backup and restore Audit log files, and must ensure that audit log files do not run out of disk space.	OE.AUDIT_BACKUP addresses the assumption by requiring the audit log files to be backed up, and by requiring monitoring of disk space usage to ensure space is available.
A.NO_EVIL: Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	OE.NO_EVIL: Sites using the TOE must ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.	OE.NO_EVIL restates the assumption.
A.PHYSICAL: It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.	OE.PHYSICAL: Physical security must be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.	OE.PHYSICAL restates the assumption.
A.SECURE_COMMS: It is assumed that the IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.	OE.SECURE_COMMS: The IT environment must provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.	OE.SECURE_COMMS restates the assumption. The workstation OS will provide a secure line of communication for the TOE.
A.SECURE_UPDATES: Administrators will implement secure mechanisms for receiving and validating updated signature files from McAfee, and for distributing the updates to	OE.SECURE_UPDATES: Enterprises using the TOE must ensure that signature file updates are received from McAfee via secure mechanisms, the updates are validated before being used, and the updates are distributed to central management systems within	OE.SECURE_UPDATES restates the assumption. Administrators use secure mechanisms to receive and validate the updates from McAfee, then use secure mechanisms to distribute the updates to the central management systems.

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
the central management systems.	the Enterprise via secure mechanisms.	
A.DEDICATED_PLAT: The hardware platform used for ePO will not be used to host other applications.	OE.DEDICATED_PLAT: The hardware platform used to host ePO must not be used to host other applications.	OE.DEDICATED_PLAT restates the assumption.

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

5 Extended Components Definition

5.1 Malware (FAM) Class of SFRs

This class of requirements specifically addresses the detection and response capabilities of anti malware products. The purpose of this class of requirements is to address the unique nature of anti malware products, and to provide for requirements about detecting and responding to malware on protected IT resources.

5.1.1 Anti-malware scanning FAM_SCN_(EXT)

Family Behaviour

This family addresses requirements for actions to be taken on detection of memory or file based malware.

Component Levelling

FAM_SCN_(EXT).1 Anti-malware scanning	1

FAM_SCN_(EXT).1 Anti-malware scanning allows the specification of actions to be taken on detection of memory or file based malware.

Management: FAM_SCN_(EXT).1

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

a) Configuration of the actions to be taken.

Audit: FAM_SCN_(EXT).1

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

a) Basic: Action taken in response to detection of malware.

FAM_SCN_(EXT).1 Anti-malware scanning

Hierarchical to: No other components.

Dependencies: None

FAM_SCN_(EXT).1 .1 The TOE shall monitor processes and memory for unauthorized changes.

FAM_SCN_(EXT).1.1 Upon detection of a memory based malware, the TSF shall [assignment: *action to be taken*].

FAM_SCN_(EXT).1.2 Upon detection of a file-based malware, the TSF shall [assignment: *action to be taken*].

5.1.2 FAM_ALR_(EXT).1 Anti-malware alerts

Family Behaviour

This family addresses requirements for alerting actions to be taken on detection of memory or file based malware.

Component Levelling

FAM_ALR_(EXT).1 Anti-malware alerts	1

FAM_ALR_(EXT).1 Anti-malware alerts allows the specification of alerting actions to be taken on detection of memory or file based malware.

Management: FAM_ALR_(EXT).1

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

a) Configuration of the alerts to be generated.

Audit: FAM_ALR_(EXT).1

There are no auditable events foreseen.

FAM_ALR_(EXT).1 Anti-malware alerts

Hierarchical to: No other components.

Dependencies: FAM_ALR_(EXT).1 Anti-malware alerts

FAM_ALR_(EXT).1.1 Upon detection of malware, the TSF shall [assignment: *alerting action to be taken*].

6 Security Requirements

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

6.1 Security functional requirements

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

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_STG.1	Protected audit trail storage
	FAU_SEL.1	Selective audit
	FAU_STG.3	Action in case of possible audit data loss
Anti malware	FAM_SCN_(EXT).1	Anti-malware scanning
	FAM_ALR_(EXT).1	Anti-malware alerts
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_USB.1	User-subject binding
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles

Table 16 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1.1 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 [minimum] level of audit; and

c) [*The events identified in the following table*].

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

a) Date and time of the event, type of event, subject identity (if applicable),

and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*the information detailed in the following table*].

COMPONENT	EVENT	DETAILS
FAU_GEN.1	None	Not applicable
FAU_GEN.2	None	Not applicable
FAU_SAR.1	None	Not applicable
FAU_SAR.2	None	Not applicable
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	Note that this event is not applicable since the audit filter file is read on start-up and subsequent changes do not alter filtering performed while the audit collection functions are operating.
FAU_STG.1	None	Not applicable
FAU_STG.3	None	Not applicable
FAM_SCN_(EXT).1	Action taken in response to detection of malware	Malware detected, action taken, file or process identifier where malware is detected
FAM_ALR_(EXT).1	None	Not applicable
FIA_ATD.1	None (No tested secrets apply).	Not applicable
FIA_USB.1	None (The binding of attributes to the subject never fails, per TOE design).	Not applicable
FMT_MOF.1	None	Not applicable
FMT_MTD.1	None	Not applicable
FMT_SMF.1	Use of the management functions	User identity, function used
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Table 17 – Audit Events and Details

6.1.1.2 FAU_GEN.2 User identity association

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

6.1.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1(1) The TSF shall provide [*authorized administrators*] with the capability to read [*all audit information*] from the audit records **on the central management system.**

FAU_SAR.1.2(1) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application Note: Audit logs related to MDD are referred to as events in ePO, while audit logs related to administrator actions are referred to as audits in ePO. This requirement is interpreted as requiring both event log and audit log review on ePO.

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_SEL.1 Selective audit

FAU_SEL.1.1 The TSF shall be able to select the set of audited events from the set of all auditable events based on the following attributes:

a) [event type]

b) [*no other attributes*].

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 unauthorised deletion**.**

FAU_STG.1.2 The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail**.**

Application Note: This instance of FAU_STG.1 applies to protection of the audit records via the TSFI. The IT Environment (OS) is responsible for preventing deletion of the audit file via OS interface.

6.1.1.7 FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall [*archive the workstation audit log file and open a new log file*] if the **workstation transient** audit trail exceeds [*the size limit set using ePO*].

Application Note: Workstation transient audit trail refers to the temporary storage of event records waiting to be transmitted from a workstation on which the TOE is installed to ePO. If the local event storage is exhausted (the allocated maximum log size is reached), the file is archived and a new one opened. This continues until the connection to ePO is restored and event records can be transferred.

6.1.2 Anti-malware (FAM)

6.1.2.1 FAM_SCN_(EXT).1 Anti-malware scanning

FAM_SCN_(EXT).1 .1 The TOE shall monitor processes and memory for unauthorized changes.

FAM_SCN_(EXT).1.2 Upon detection of a memory based malicious software, the TSF shall [*prevent the malicious software from accessing the protected memory or CPU register*].

FAM_SCN_(EXT).1.3 Upon detection of a file-based malware, the TSF shall [*perform the action(s) specified by an authorized administrator. Actions are administratively configurable on a per-workstation basis and consist of:*

a) Prevent the file from installing,

b) Clean the file,

b) Quarantine the file,

c) Delete the file].

6.1.2.2 FAM_ALR_(EXT).1 Anti-malware alerts

FAM_ALR_(EXT).1.1 Upon detection of malware, the TSF shall [*display an alert on the screen of the workstations on which the malware is detected. The alert shall identify the malware that was detected and the action taken by the TOE*].

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. *Enabled or disabled;*

c. *Authentication configuration (must be configured for Windows);*

d. *Global Administrator status; and*

e. *Permission Sets*].

Application Note: The TOE maintains security attributes for ePO users. Windows maintains security attributes for Workstation Users.

6.1.3.2 FIA_USB.1 User-subject binding

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

a. *ePO User name;*

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 **ePO** 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 **ePO** 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_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [determine the behaviour of, disable, enable] the functions [

a. *Auditing,*

b. *Operation of an instance of MDD on a workstation]*

to [*an authorized administrator*].

6.1.4.2 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1(1) The TSF shall restrict the ability to [query, modify, delete] the [

a) Binaries to be protected on workstations,

b) Blacklist and whitelist of drivers to block and permit (respectively)

c) CPU features to protect on workstations

d) Malware scan signatures

e) Enabled status of MDD

f) Quarantine settings

g) Global Threat Intelligence settings

h) *User interface option settings*]

to [*an authorized administrator*].

Application Note: The TSF data referenced in this SFR corresponds to the MDD policies identified in Table 8 – TOE Data (Legend: AD=Authentication data; UA=User attribute; GE=Generic Information).

FMT_MTD.1.1(2) The TSF shall restrict the ability to [query, modify, delete, *create and use*] the [*TSF data identified in the following table*] to [*a user with the permissions identified in the following table or a Global Administrator*].

TSF Data	Associated Permission	Operations Permitted
Contacts	Create and edit contacts	Query, create, delete and modify
	Use contacts	Use
Dashboards	Use public dashboards	Query and use public dashboards
	Use public dashboards; create and edit personal dashboards	Query and use public dashboards; create and modify personal dashboards
	Use public dashboards; create and edit personal dashboards; make personal dashboards public	Query and use public dashboards; create, delete and modify personal dashboards
ePO User Accounts	n/a (only allowed by a Global Administrator)	Query, create, delete and modify
Event Filtering	n/a (only allowed by a Global Administrator)	Query and modify
Audit logs	View audit log; View and purge audit log	Query and delete
Event Logs	View Client Events; View, delete, and purge client events	Query and delete
Global Administrator Status	n/a (only allowed by a Global Administrator)	Query and modify
Groups	n/a (only allowed by a Global Administrator)	Query, create, delete and modify
Permission Set	n/a (only allowed by a Global Administrator)	Query, create, delete and modify
Queries	Use public queries	Query
	Use public queries; create and edit personal queries	Query, create, delete and modify
	Edit public queries; create and edit personal queries; make personal queries public	Query, create, delete and modify
SNMP Trap Destination(s)	View notification rules and Notification Log	Query
	Create and edit notification rules; view Notification Log	Query, create, delete and modify

TSF Data	Associated Permission	Operations Permitted
	Create and edit notification rules; view and purge Notification Log; create and edit SNMP servers and external commands	Query, create, delete and modify
System Event Audit Configuration	n/a (only allowed by a Global Administrator)	Query and modify
System Information	Access to the specific group node in the tree	Query
	"View system tree tab", access to the specific group node in the tree, and "Edit system tree groups and systems"	Query, create, delete and modify
system tree	View system tree tab and access to the specific group node in the tree	Query
	"View system tree tab", access to the specific group node in the tree, and "Edit system tree groups and systems"	Query, create, delete and modify

Table 18 - TSF Data Access Permissions

Application Note: The Notification Log is a log of all email and SNMP trap notifications generated by ePO. This log is not TSF data. The only references to the Notification Log in this ST are in the permission names that control access to other notification parameters that are TSF data. Because the permission names are used verbatim from the product, the Notification Log term is retained in the ST as part of the permission name.

6.1.4.3 FMT_SMF.1 Specification of management functions

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

a) Enable and disable operation of the TOE on workstations,

b) Configure operation of the TOE on workstations,

c) Update known malicious code scan signatures,

d) Review audit logs on the central management system,

e) Acknowledge alert notifications on the workstation being used,

f) ePO user account management,

g) Permission set management,

h) Audit log management,

i) Event log management,

j) Notification management,

k) System tree management,

l) Dashboard management

m) Management of quarantined items via the system tray].

Application Note: Audit logs related to MDD are referred to as events in ePO, while audit logs related to administrator actions are referred to as audits in ePO. Item d above is interpreted as requiring both event log and audit log review on ePO.

6.1.4.4 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [global administrator, and *ePO administrator assigned any of the following permissions or combinations of permissions:*

a. Create and edit contacts

b. Create and edit notification rules; view and purge Notification Log; create and edit SNMP servers and external commands

c. Create and edit notification rules; view Notification Log

d. Edit public queries; create and edit personal queries; make personal queries public

e. Edit system tree groups and systems

f. System permissions (to specific nodes)

g. Use contacts

h. Use public dashboards

i. Use public dashboards; create and edit personal dashboards

j. Use public dashboards; create and edit personal dashboards; make personal dashboards public

k. Use public queries; create and edit personal queries

l. View Notification Log

m. View system tree tab][2].

[2] An administrator having all permissions is referred to as a Global Administrator.

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

6.2 Security assurance requirements

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

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 19 – Security Assurance Requirements

6.3 CC component hierarchies and dependencies

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

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN.1	None	FPT_STM.1	Satisfied by the Operational Environment
FAU_GEN.2	None	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied by the Operational Environment
FAU_SAR.1	None	FAU_GEN.1	Satisfied
FAU_SAR.2	None	FAU_SAR.1	Satisfied
FAU_SEL.1	None	FAU_GEN.1, FMT_MTD.1	Satisfied Satisfied
FAU_STG.1	None	FAU_GEN.1	Satisfied
FAU_STG.3	None	FAU_STG.1	Satisfied
FAM_SCN_(EXT).1	None	None	Satisfied

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAM_ALR_(EXT).1	None	FAM_SCN_(EXT).1	Satisfied
FIA_ATD.1	None	None	Not applicable
FIA_USB.1	None	FIA_ATD.1	Satisfied
FMT_MOF.1	None	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	None	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	None	None	Not aplicable
FMT_SMR.1	None	FIA_UID.1	Satisfied by the Operational Environment

Table 20 – TOE SFR Dependency Rationale

6.4 Security requirements rationale

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

6.4.1 Security functional requirements for the TOE

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

	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.CORRECT_TSF_OPERATION	O.MANAGE	O.DETECT	O.PROTECT
FAU_GEN.1		✓			✓			
FAU_GEN.2		✓						
FAU_SAR.1				✓	✓			
FAU_SAR.2			✓					
FAU_SEL.1		✓						
FAU_STG.1			✓					
FAU_STG.3			✓					
FAM_ALR_(EXT).1					✓		✓	✓
FAM_SCN_(EXT).1					✓		✓	✓
FIA_ATD.1	✓							

	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.CORRECT_TSF_OPERATION	O.MANAGE	O.DETECT	O.PROTECT
FIA_USB.1	✓							
FMT_MOF.1	✓					✓		
FMT_MTD.1	✓					✓		
FMT_SMF.1	✓					✓		
FMT_SMR.1	✓					✓		

Table 21 – Mapping of TOE SFRs to Security Objectives

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

OBJECTIVE	REQUIREMENTS THAT ADDRESS THE OBJECTIVE	SFR AND RATIONALE
O.ADMIN_ROLE The TOE must provide authorized administrator roles to isolate administrative actions.	FMT_MOF.1 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1 FIA_ATD.1 FIA_USB.1	FMT_SMR.1 requires that the TSF establish a set of administrator roles, including Global Administrator and roles with more restricted permission sets. FMT_SMF.1 lists the administrative functions related to the TSF. FMT_MOF.1 and FMT_MTD.1 specify the privileges that only an authorized administrator may perform. FIA_ATD.1 supports the objective by requiring the TOE to maintain security attributes that enable users to be assigned to an authorized administrator role. FIA_USB.1 supports the objective by requiring the TOE to associate security attributes (including the role) with user sessions.
O.AUDIT_GENERATION	FAU_GEN.1 FAU_GEN.2	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This

OBJECTIVE	REQUIREMENTS THAT ADDRESS THE OBJECTIVE	SFR AND RATIONALE
The TOE must provide the capability to detect and create records of security-relevant events.	FAU_SEL.1	requirement ensures that an authorized administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements. FAU_GEN.2 ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the userid. In all other cases, the association is based on the source network identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated. FAU_SEL.1 allows the specification of a filter to select a reduced set of audited events.
O.AUDIT_PROTECT The TOE must provide the capability to protect audit information.	FAU_SAR.2 FAU_STG.1 FAU_STG.3	FAU_SAR.2 restricts the ability to read the audit trail to an authorized administrator, thus preventing the disclosure of the audit data to any other user. However, the TOE is not expected to prevent the disclosure of audit data if it has been archived or saved in another form (e.g. moved or copied to an ordinary file). The FAU_STG family dictates how the audit trail is protected. FAU_STG.1 restricts the ability to delete audit records to an authorized administrator. FAU_STG.3 defines the action to be taken if the maximum audit file size is reached. This helps to ensure that audit records are kept until an authorized administrator deems they are no longer necessary. This requirement also ensures that no one has the ability to modify audit records (e.g. edit any of the information contained in an

OBJECTIVE	REQUIREMENTS THAT ADDRESS THE OBJECTIVE	SFR AND RATIONALE
		audit record). This ensures the integrity of the audit trail is maintained.
O.AUDIT_REVIEW The TOE must provide the capability to selectively view audit information.	FAU_SAR.1	FAU_SAR.1 provides the ability to review the audits in a user-friendly manner.
O.CORRECT_TSF_OPERATION The TOE must provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.	FAU_GEN.1 FAU_SAR.1 FAM_SCN_(EXT).1 FAM_ALR_(EXT).1	Correct TSF operation can be determined by running a test executable and kernel driver, delivered with the TOE, and ensuring that the proper events occur. The FAM class will detect and act upon the malware. FAU_GEN.1 requires the TSF to generate an event when the malware is detected. FAU_SAR.1 enables an authorized administrator to review the audit events. This allows the administrator to determine the TOE is properly installed and is active.
O.MANAGE The TOE must provide all the functions and facilities necessary to support the authorized users in their management of the TOE.	FMT_MOF.1 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1	The TSF can control permissions assigned to administrators and workstation users. FMT_MOF.1 defines particular TSF capabilities that may only be used by the users. FMT_MTD.1 defines particular TSF data that may only be altered by these users. FMT_SMF.1 and FMT_SMR.1 define the administrative functions and roles provided by the TSF.
O.DETECT The TOE must detect and take action against known malicious device drivers.	FAM_ALR_(EXT).1 FAM_SCN_(EXT).1	FAM_SCN_(EXT).1 requires that the TSF scan for malware and take action once it is detected. FAM_ALR_(EXT).1 defines alerting requirements to ensure that users are aware that malware was detected.
O.PROTECT The TOE must protect critical kernel memory and CPU registers against	FAM_ALR_(EXT).1 FAM_SCN_(EXT).1	FAM_SCN_(EXT).1 requires that the TSF scan for malware and take action once it is detected. FAM_ALR_(EXT).1 defines alerting

OBJECTIVE	REQUIREMENTS THAT ADDRESS THE OBJECTIVE	SFR AND RATIONALE
unauthorized access.		requirements to ensure that users are aware that malware was detected.

Table 22 – Rationale for Mapping of TOE SFRs to Objectives

6.4.2 Security assurance requirements

This section identifies the Configuration Management, Delivery/Operation, Development, Test, and Guidance measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Architecture Description: McAfee Deep Defender 1.0 and ePolicy Orchestrator 4.6
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: McAfee Deep Defender 1.0 and ePolicy Orchestrator 4.6
ADV_TDS.1: Basic Design	TOE Design: McAfee Deep Defender 1.0 and ePolicy Orchestrator 4.6
AGD_OPE.1: Operational User Guidance	Common Criteria Evaluated Configuration Guide: McAfee Deep Defender 1.0 and ePolicy Orchestrator 4.6
AGD_PRE.1: Preparative Procedures	Common Criteria Evaluated Configuration Guide: McAfee Deep Defender 1.0 and ePolicy Orchestrator 4.6
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: McAfee Deep Defender 1.0 and ePolicy Orchestrator 4.6
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: McAfee Deep Defender 1.0 and ePolicy Orchestrator 4.6
ALC_DEL.1: Delivery Procedures	McAfee Software Delivery Process
ALC_FLR.2: Flaw reporting procedures	McAfee Product Flaw Remediation Process
ATE_COV.1: Evidence of Coverage	Security Testing: McAfee Deep Defender 1.0.1 and ePolicy Orchestrator 4.6.1
ATE_FUN.1: Functional Testing	Security Testing: McAfee Deep Defender 1.0.1 and ePolicy Orchestrator 4.6.1
ATE_IND.2: Independent Testing – Sample	Security Testing: McAfee Deep Defender 1.0.1 and ePolicy Orchestrator 4.6.1

Table 23 – Security Assurance Measures

6.4.2.1 Rationale for TOE assurance requirements selection

The general level of assurance for the TOE (EAL2 plus ALC_FLR.2) is 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. The TOE

assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 augmented by ALC_FLR.2 from part 3 of the Common Criteria.

7 TOE Summary Specification

7.1 Malicious code identification & alerts

(FAM_SCN_(EXT).1, FAM_ALR_(EXT).1, FMT_SMF.1 item m)

The TOE provides real-time detection of unauthorized access to kernel memory or CPU register based on the settings that have been configured. Scanning occurs when files are either read from, or written to the computer on which the TOE client agent is installed. Identification of malware is referred to as an "infection".

Two distinct types of protection are provided:

1. Memory protection - MDD provides in-memory process scanning and by doing so, stops malware and its associated files from executing in memory. When a memory-based malware is detected, the process is stopped.
2. Anti-malware Scanning –MDD examines attempts to install device drivers in real-time.

Prevention and detection events are generated whenever MDD blocks or identifies unauthorized access attempts to monitored protection areas. These events are passed to the user-mode service application and are made available in the MDD tray application for review.

When an infection is detected the Notification Message box pops up on the screen.

Details of infections detected are passed to ePO, where they can be monitored, reviewed and reported. Each alert identifies the system where the infection has occurred, the name of the malware (if known), and the action taken by the TOE.

Items that are detected as infections are cleaned or deleted. A copy of the item is converted to a non-executable format and saved in the designated Quarantine folder. This allows the quarantined items to be processed after a later version of the DAT files have been downloaded, that possibly contains information that can clean the threat. This processing may be done using ePO or the MDD client console. This additional processing includes:

1. Restore
2. Delete
3. Download
4. View detection properties

Further protection against malware is provided by the MDD Access Protection feature. The Access Protection feature compares an action being requested against a list of predefined Security rules. Each rule can be configured to block or report, or block and report access violations when they occur. Access

protection prevents unwanted changes to the MDD client computer by restricting access to specified ports, files, shares, registry keys, and registry values. It also protects MDD processes by preventing users from stopping them.

The Handler function, running in the context of the TMSL, delivers information about violating access attempts to the IB Agent for further processing. Only those triggers that relate to areas protected by MDD are forwarded. Others will be implicitly allowed directly within the Handler.

The IB Agent incorporates shortcut evaluation of received access triggers. If one of the following conditions evaluates to true, no event is generated and the originating operation will be allowed once respective functionality has been integrated. Shortcut conditions are:

- Executing module is the operating system kernel
- Executing module is the IB Agent kernel driver
- Executing module is white listed
- Executing and target module (for memory accesses) are the same

7.2 Audit (AUDIT)

7.2.1 Audit generation (FAU_GEN.1, FAU_GEN.2, FAU_SEL.1, FAU_STG.1, FAU_STG.3, FMT_MTD.1(2), FMT_SMF.1)

Audit Generation involves both the ePO server and the workstations executing MDD. MDD generates audits related to malware detections while ePO generates audits related to user actions performed via ePO.

MDD generates audits when malware is detected. The event record includes details of the system on which the malware was detected (subject identity), the specific malware detected, the action taken to counteract the malware, and the file or process in which the malware was detected. The events for each workstation are stored on the workstation, and forwarded to the ePO event log.

Copies of all events from the workstations are sent to a central management system (ePO), where they can be reviewed by an authorized administrator. The event records are queued on the workstations for transmission to the management system (transient storage). In the unlikely event that the queue space is exhausted, the audit log file is archived and a new one opened. Once events are transferred to a central management system and accepted, they are deleted from the queue on the workstations.

ePO generates audit records for actions performed by ePO users, recording details of the event and the associated user. The auditable events and record contents are specified in the Audit Events and Details table in the FAU_GEN.1 section.

Audit records generated by ePO or MDD are stored in the ePO database, protected against unauthorized modification or deletion. This protection is provided by the ePO permissions mechanism within the TOE, with reliance on the operating system platform to protect DBMS objects.

The audit function operates whenever ePO/MDD are operating. If an instance of MDD is enabled or disabled on a workstation by an authorized administrator, an audit record is generated.

In the event that a MDD client is not able to communicate with the ePO repository, audit events are queued until communication is again available.

Event filters may be configured to specify which possible malware related events do not result in audit records being generated. Event filters for the Selective Audit function are specified in a configuration file using any text editor. The audit filter file is read whenever the TOE is started. This file is located in the "conf" directory of the ePO server. Typically this will be located at %Program Files%\McAfee\ePolicy Orchestrator\ \conf\orion\audit-filter.txt.

7.2.2 Audit record review (FAU_SAR.1, FAU_SAR.2, FMT_MTD.1(2))

Audit record review also involves both the ePO server and the workstations executing MDD. ePO provides the capability for an administrator with "View audit log" or "View and purge audit log" permissions to review audit records generated on all the systems.

ePO maintains a record of user actions and malicious code detected. The auditable events are specified in the Audit Events and Details table in the FAU_GEN.1 section. ePO distinguishes between the records for user actions and malware-related events, referring to the former as "audits" and the latter as "events".

The audit entries display in a sortable table. The Audit Log display includes:

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

Audit Log entries can be queried against by an authorized administrator. The Audit Log entries are automatically purged based upon a configured age. Audit records may be deleted via automatic purging, or an authorized administrator may manually delete all records older than a specified date.

MDD events are automatically purged according to the configured Data Retention parameters. If the local audit storage is exhausted, all I/O processing is suspended on the workstation until the connection

to ePO is restored and events can be transferred. The TOE does not provide any mechanism to modify event information. Event records may be deleted via automatic purging, or an authorized administrator may manually delete all records older than a specified date.

7.3 Management (MGMT)

(FIA_ATD.1, FIA_USB.1, FMT_SMF.1, FMT_SMR.1, FMT_MOF.1)

The TOE's Management Security Function provides support functionality that enables an authorized administrator to configure and manage TOE components. Management of the TOE may be performed via the ePO GUI. There is also a limited amount of configurable management functionality available on the MDD client via the MDD Tray Application.

ePO management permissions are defined per-user. Configuring Global Administrator status to an ePO account implicitly grants all user permissions to that user. Upon successful authentication (as determined by Windows), the Global Administrator status and the union of all the permissions from the permission sets from the user account configuration are bound to the session, along with the user name. Those attributes remain fixed for the duration of the session (until the user logs off).

The TOE provides functionality to manage the following:

1. ePO User Accounts,
2. Permission Sets,
3. Audit Log,
4. Event Log,
5. Notifications,
6. System tree,
7. Queries,
8. Dashboards,
9. MDD Policies,
10. MDD DAT File,
11. Tray application,
12. Operation of an instance of MDD.

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

7.3.1 ePO user account management (FMT_MTD.1(2))

Each user authorized for login to ePO must be defined with ePO. Only Global 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 (the evaluated configuration requires Windows authentication for all users)
4. Permission sets granted to the user
5. Global Administrator status

One or more permission sets may be associated with an account. Global Administrators are granted all permissions.

Permissions exclusive to Global Administrators (i.e. not granted via permission sets) include:

1. Change server settings.
2. Create and delete user accounts and groups.
3. Create, delete, and assign permission sets.
4. Limit events that are stored in ePolicy Orchestrator databases[3].

7.3.2 Permission set management (FMT_MTD.1(2))

A permission set is a group of permissions that can be granted to any users by assigning it to those users' accounts. One or more permission sets can be assigned to any users who are not Global Administrators (Global Administrators have all permissions to all products and features).

Permission sets only grant rights and access — no permission set 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 server tasks, but another permission set applied to the same account grants all permissions to server tasks, that account has all permissions to server tasks.

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

When a permission set is created or modified, the permissions granted via the permission set may be configured by a Global Administrator.

7.3.3 Audit log management (FMT_MTD.1(2))

A Global Administrator may configure the length of time Audit Log entries are to be saved. Entries beyond that time are automatically purged.

The audit log may also be purged manually by a Global Administrator, or a user with the "View and purge audit log" permission, using a GUI to specify that all events older than a specified date are to be

[3] Auditing comprises events that are observed on user workstations by the TOE, and also records of administrator actions on ePO. These are all stored in ePO databases.

deleted. This is a one-time operation, and the date specified is independent of the time period specified for automatic purging.

A Global Administrator or a user with either the “View audit log” or “View and purge audit log” permission may view events in the audit log.

7.3.4 Event log management (FMT_MTD.1(2))

A Global Administrator may configure the length of time event log entries are to be saved. Entries beyond that time are automatically purged.

The event log may also be purged manually by a Global Administrator using a GUI to specify that all events older than a specified date are to be deleted. This is a one-time operation and the date specified is independent of the time period specified for automatic purging.

7.3.5 Notification management (FMT_MTD.1(2))

Notifications sent by ePO may be specified in response to events generated by the TOE. Notifications cause email messages to be sent to the configured recipient(s) or SNMP traps to be generated.

A Global Administrator or user with the “Create and edit notification rules; view and purge Notification Log; create and edit SNMP servers and external commands” permission may configure the SMTP server name and port used to send email or the destination(s) for SNMP traps. Credentials may optionally be specified if authentication is to be performed with the email server.

A Global Administrator or user with the “Create and edit contacts” permission may create, view, edit and delete contacts. Each contact includes a first name, last name and email address. The contacts are used in email notifications; any Global Administrator or user with the “Use contacts” permission may cause a notification to be sent to the specified contact for that notification.

A Global Administrator or user with the appropriate permissions (see below) may configure independent rules at different levels of the system tree. The rules specify when and what type of notification should be sent under what conditions.

The permissions associated with Notification management are:

1. View notification rules and Notification Log - This permission also grants the ability to view SNMP servers, registered executables, and external commands.
2. Create and edit notification rules; view Notification Log - This permission also grants the ability to view SNMP servers, registered servers, and external commands.
3. Create and edit notification rules; view and purge Notification Log; create and edit SNMP servers and external commands

Users can configure when notification messages are sent by setting thresholds based on aggregation and throttling. Use aggregation to determine the thresholds of events at which the rule sends a notification message. Use throttling to ensure not too many notification messages are sent.

Once associated with a group or system, notification rules may be enabled and disabled by a Global Administrator or user with the “Create and edit contacts” permission.

7.3.6 System tree management (FMT_MTD.1(2))

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 systems to be organized within units called groups.

Groups have these characteristics:

1. Groups can be created by Global Administrators.
2. A group can include both systems and other groups.
3. Groups are modified or deleted by a Global Administrator.

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

The Lost&Found group has the following characteristics:

1. It can't be deleted;
2. It can't be renamed;
3. Its sorting criteria can't be changed (although sorting criteria can be provided for the subgroups created within it);
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, and if no such group exists, one is created.

Child groups in the system tree hierarchy inherit policies set at their parent groups. Inheritance is enabled by default for all groups and individual systems that you add to the system tree. Inheritance may be disabled for individual groups or systems by a Global 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.

User permissions in the Systems category that are relevant to this information are:

1. View the “system tree” tab;

2. Edit system tree groups and systems.

Systems may be deleted or moved between groups by a Global Administrator or users with both the "View the "system tree" tab" and "Edit system tree groups and systems" permissions. User access to groups in the system tree is controlled by individual check boxes in the permission sets for the system tree.

7.3.7 Query management (FMT_MTD.1(2))

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

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

7.3.8 Dashboard management (FMT_MTD.1(2))

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

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

7.3.9 MDD policies (FMT_MTD.1(1))

MDD policies are configured on ePO and automatically distributed to the client systems running MDD. The policies determine what malware-related functions are performed on the systems and what actions are taken when malware is detected. Permissions relevant to MDD policies are:

1. View MDD settings
2. View and change MDD settings

The following policies related to MDD may be configured:

General Policy Settings

1. Enable MDD: If this is enabled protection is turned on and the respective events are reported to ePO. When it is disabled MDD protection is turned off. Hence the MDD tray application is disabled. A predefined level of protection can be selected, or a custom level configured, with a set of actions for each level (see 6.1.4.2 e)).
2. Quarantine settings: The quarantine settings allow the quarantine folder to be specified and the number of days to retain data in quarantine. Items older than the specified retention period are deleted (see 6.1.4.2 f)).
3. Global Threat Intelligence settings: Enabling this option allows MDD to query McAfee Labs for better detections (see 6.1.4.2 g)).
4. Access protection settings: Enabling this option allows MDD to perform access protection. The access protection feature of MDD compares an action being requested against a list of predefined security rules. Each rule can be configured to block or report, or block and report access violations when they occur. Access protection prevents unwanted changes to the computer by restricting access to specified ports, files, shares, registry keys, and registry values. It also protects McAfee processes by preventing users from stopping them (see 6.1.4.2 a) & c)).

User Interface Options Settings

1. Tray options: MDD can be configured to display/not display the MDD tray menu icon in the system tray of the client system, allow the user to enable/disable MDD, and show/not show pop-up messages for MDD events to the user.
2. Configure alert messages level: MDD can be configured to display the different types of MDD message to the user as pop-up messages.
3. Restart dialog settings: If this setting is enabled a user can postpone a system restart caused by malware detection and cleaning by 0-100 seconds (see 6.1.4.2 h)).

Blacklist/whitelist drivers

An authorized administrator can select to allow or block specific drivers from running on the endpoint. The whitelist allows the selected driver to perform its functions, and also protects the driver against attacks (see 6.1.4.2 b)).

7.3.10 MDD DAT file (FMT_MTD.1(1))

When the scanning engine searches for threats, it compares the contents of the scanned files to known threat information stored in the detection definition (DAT) files. The known threat information, called signatures, is information gathered by McAfee Labs. Besides the signatures, the DAT files also include instructions on how to clean and counteract the damage created by the detected malware.

MDD uses the information in the DAT files to identify and take action on threats. Since new threats appear on a regular basis, it is important to be able to update the DAT files to address the latest threats. An authorized administrator may obtain updated DAT files from McAfee and then distribute the updated information to the MDD clients.

In the evaluated configuration, only authorized administrators may update the DAT files (see 6.1.4.2 d)).

7.3.11 MDD Tray Application (FAM_SCN_(EXT).1, FAM_ALR_(EXT).1, FMT_SMF.1)

The MDD features can be configured and managed from the MDD tray application running inside the system tray on the MDD client.

The McAfee Deep Defender tray application allows a user to:

1. View the general protection status of McAfee Deep Defender
2. Browse generated events
3. Update the content files and engine (engine updates are not permitted in the evaluated configuration)
4. View the quarantined items.

The application is automatically started at the end of the installation process and on every user logon, once the product is installed.

7.3.12 MDD Operation (FMT_MOF.1)

Policies can be deployed from ePO to an instance of MDD, and enabled and disabled remotely. This includes the ability to enable or disable the operation of an instance of MDD.