Security Target

McAfee MOVE 2.5 and ePolicy Orchestrator 4.6

Document Version 1.4

August 14, 2012

Prepared For:

McAfee, Inc.

2821 Mission College Blvd.

Santa Clara, CA 95054

www.mcafee.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the MOVE 2.5 and ePolicy Orchestrator 4.6. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Note that references to “MOVE 2.5” are to be understood to mean “MOVE AV 2.5 Multi-Platform”.

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 MOVE 2.5 and ePolicy Orchestrator 4.6
ST Revision	1.4
ST Publication Date	August 14, 2012
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	McAfee MOVE 2.5 and ePolicy Orchestrator 4.6
TOE Type	Antivirus

1.3 Document Organization

This Security Target follows the following format:

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

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

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

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

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

1.5 Document Terminology

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

TERM	DEFINITION
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CM	Configuration Management
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
GB	Giga-Byte
GUI	Graphical User Interface
I&A	Identification and Authentication
IT	Information Technology
MB	Mega-Byte
NIAP	National Information Assurance Partnership
OS	Operating System
OSP	Organizational Security Policy
PC	Personal Computer
PP	Protection Profile

TERM	DEFINITION
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 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

McAfee MOVE Antivirus is an anti-virus solution for virtual environments that removes the need to install an anti-virus application on every virtual machine (VM).

A traditional security solution for virtual environments uses an anti-virus application running on every VM on a hypervisor. This requirement reduces VM density per hypervisor and causes high disk, CPU, and memory usage. McAfee MOVE Antivirus solves this issue by offloading all on-access scanning to a dedicated VM that runs an offload scan server to improve performance related to anti-virus scanning. This results in increased VM density per hypervisor.

The management capabilities for MOVE are provided by ePO through the MOVE ePO Extension and McAfee Agent ePO manages McAfee Agents and MOVE Software that reside on client systems. By using ePO you can manage a large enterprise network from a centralized system. ePO through the McAfee Agent provides capabilities to distribute updated MOVE Security policies, DAT files to the Offload Scan Server. ePO also centrally manages Event and Log records.

Communication between the distributed components of the TOE is protected from disclosure and modification by cryptographic functionality provided by the FIPS approved components of the McAfee ePO and the McAfee Agent. It is assumed that the IT environment will provide a secure line of communications between the TOE and remote administrators.

1.7 TOE Description

The TOE includes these components:

- McAfee MOVE Antivirus Agent for Windows — Allows virtual desktops and servers to communicate with ePolicy Orchestrator.
- McAfee MOVE Antivirus Offload Server — Provides offloaded scanning support for virtual servers, minimizing the impact on virtual desktops.

- McAfee MOVE Antivirus ePolicy Orchestrator extension — Provides policies and controls for configuring McAfee MOVE Antivirus behavior.
- ePolicy Orchestrator – provides management capabilities for the TOE.
- McAfee Agent – provides common communication functionality between ePO and all of McAfee's product-specific software (such as MOVE).

1.7.1 Physical Boundary

The TOE is a software TOE and includes:

1. The ePO application executing on a dedicated server
2. The McAfee Agent and MOVE software on each client to be protected
3. Offload Scan Server

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

The components of the TOE are installed on virtual 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. *Product Guide: McAfee MOVE Antivirus 2.5.0*
2. *Deployment Guide: McAfee MOVE Antivirus 2.5.0*

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

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	MOVE AV 2.5 Multi-Platform ePolicy Orchestrator 4.6 McAfee Agent 4.6[1] VSE 8.8[2]
IT Environment	Specified in the following: • Table 4 – Management System Component Requirements • Table 5 – Managed System Platform Requirements

[1] McAfee Agent 4.6 is shipped/packaged with ePO 4.6. From a clean installation, no additional steps are necessary to install McAfee Agent 4.6.
[2] VSE is deployed with the MOVE installation.

Table 3 – Evaluated Configuration for the TOE

The evaluated configuration includes one or more instances of McAfee Agent and MOVE and an instance of ePO. The evaluated configuration is at least one instance of McAfee Agent and MOVE per virtual machine. It is recommended that all instances be on the same subnet for performance reasons. The ePO and McAfee Agent must be placed into the FIPS Mode of operation in order to comply with the evaluated configuration (see the Operational User Guidance and Preparative Procedures Supplement). No additional configuration or settings are required to maintain evaluated configuration. Note that VSE is not capable of scanning other platforms on the network; its functionality is only available to MOVE. VSE 8.8 is delivered with MOVE, and the full VSE functions and interfaces are not accessible outside of the TOE.

Per the evaluated configuration, only Global Administrators may update the DAT files.

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

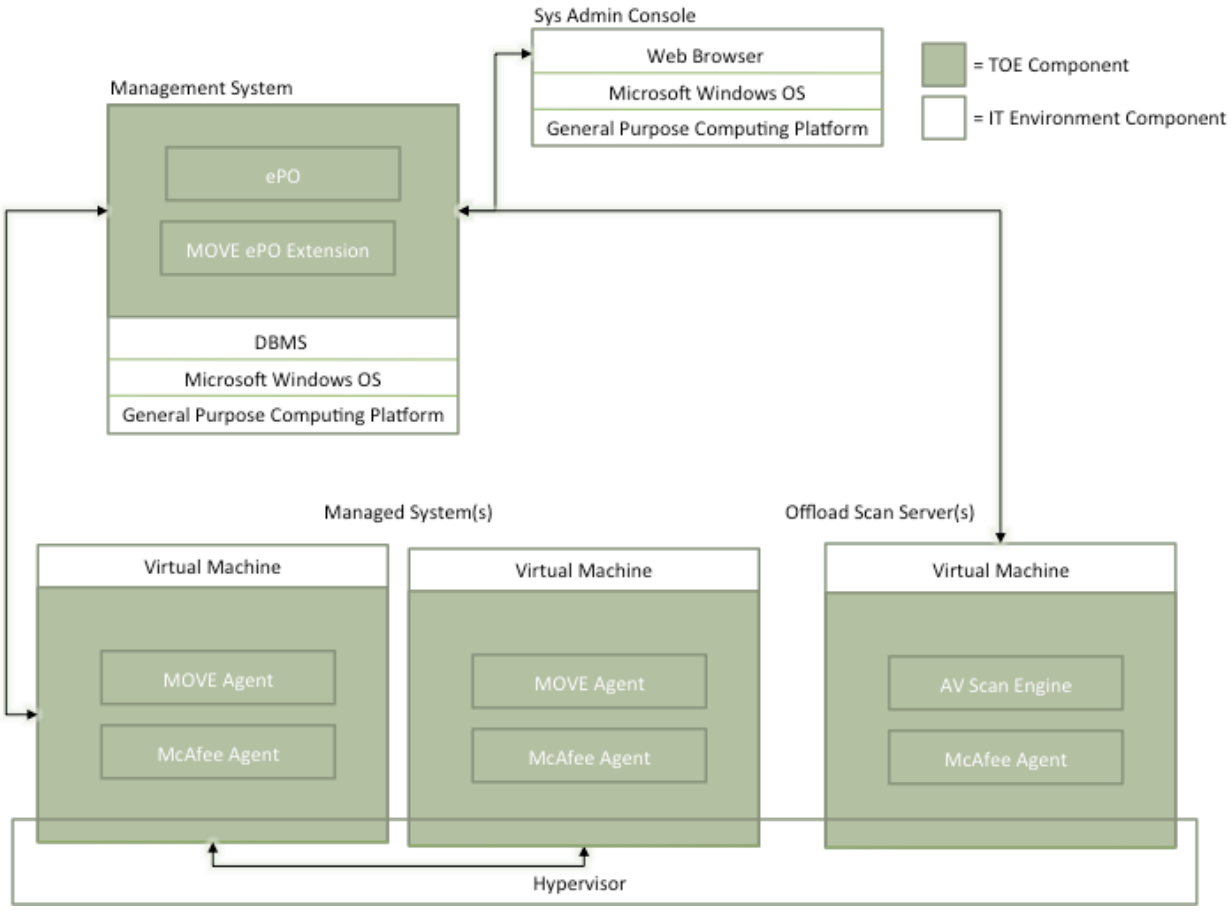

Figure 1 – TOE Boundary

1.7.2 Hardware and Software Supplied by the IT Environment

The TOE consists of a set of software applications. The hardware, operating systems and all third party support software (e.g., DBMS) 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	2 GB available RAM minimum 4 GB available RAM recommended minimum
Free Disk Space	1.5 GB — First-time installation minimum 2 GB — Upgrade minimum 2.5 GB — Recommended minimum
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	Windows Server 2008 Enterprise with Service Pack 2 or later Windows Server 2008 Standard with Service Pack 2 or later Windows Server 2008 Datacenter with Service Pack 2 or later Windows Server 2008 R2 Enterprise Windows Server 2008 R2 Standard Windows Server 2008 R2 Datacenter Windows 2008 Small Business Server Premium
Virtual Infrastructure	Citrix XenServer 5.5 Update 2 Microsoft Hyper-V Server 2008 R2 VMware ESX 3.5 Update 4 VMware ESX 4.0 Update 1
DBMS	Microsoft SQL Server 2005 (with Service Pack 3 or higher) Microsoft SQL Server 2008 SP1/SP2/R2
Network Card	Ethernet, 100Mb or higher
Disk Partition Formats	NTFS
Domain Controllers	The system must have a trust relationship with the Primary Domain Controller (PDC) on the network

COMPONENT	MINIMUM REQUIREMENTS
Miscellaneous	Microsoft .NET Framework 2.0 or later (Required — You must acquire and install this software manually. This software is required if you select an installation option that automatically installs the SQL Server Express 2005 software bundled with this ePolicy Orchestrator software.) Microsoft updates Microsoft Visual C++ Required — Installed automatically. 2005 SP1 Redistributable Microsoft Visual C++ Required — Installed automatically. 2008 Redistributable Package (x86) MSXML 6.0

Table 4 – Management System Component Requirements

The supported platforms for McAfee Agent and MOVE Agent are:

COMPONENT	MINIMUM REQUIREMENTS
Processor	One vCPU 2 GHz or higher
Memory	1 GB RAM
Free Disk Space	8 GB
Operating System	**Server Operating Systems:** Microsoft Windows Server 2008 SP2 (32-bit or 64-bit) Microsoft Windows Server 2008 R2 SP1 (64-bit) Microsoft Windows Server 2003 R2 SP2 (32-bit) **Workstation Operating Systems:** Microsoft Windows XP SP3 Microsoft Windows 7 Home Premium, Professional, and Ultimate (32 and 64 bit)
Additional Software	Microsoft Windows Installer (MSI) version 3.1 or later
Network Card	Ethernet, 10Mb or higher

Table 5 – Managed System Platform Requirements

The supported platforms for McAfee Offload Scan Server are:

COMPONENT	MINIMUM REQUIREMENTS
Processor	One vCPU 2 GHz or higher
Memory	1 GB RAM
Free Disk Space	8 GB
Operating System	**Server Operating Systems:** Microsoft Windows Server 2008 SP2 (64-bit) Microsoft Windows Server 2008 R2 SP1 (64-bit)
Additional Software	Microsoft Windows Installer (MSI) version 3.1 or later
Network Card	Ethernet, 10Mb or higher

Table 6 – Offload Scan Server Platform Requirements

The management system is accessed from remote systems via a browser. The supported browsers are Microsoft Internet Explorer 6.0 with Service Pack 1 or later or Microsoft Internet Explorer 7.0.

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.

1.7.3 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 the administrator uses to configure the MOVE policies and review the log files. The management interface is provided by ePO. The virus scanning functionality is provided by MOVE.

The logical boundaries of the TOE include the security functionalities that the TOE provides to the system that utilize the product for the detection of viruses and malicious code. The security functions include Audit, Management, Virus Scanning and Alerts, and Cryptographic operations.

TSF	DESCRIPTION
Virus Scanning and Alerts	The TOE provides for scanning and detection of file-based viruses. Users are alerted of actions on both the managed systems (via pop-up dialog) and the management system (via log). This functionality is supported in the VSE component of the Offload Scan Server.
Audit	Event information is concurrently generated for transmission to the ePO management databases. Event records for all clients can be reviewed from the ePO console.
Management	ePO enables the Global Administrator to centrally manage virus scan settings on workstations, configure and manage the actions the virus scan component takes when detection of an infection occurs, and manage the Event and Log records.
Cryptographic Operation	Anti-virus packages are distributed to the workstation with a SHA-1 hash value used to verify the integrity of the package. Communications between ePO and the McAfee Agent are encrypted using AES implemented by FIPS 140-2 validated modules.

Table 7 – Logical Boundary Descriptions

1.7.4 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 TOE to enforce the security policy. Authentication data enables the TOE 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.			✓

TSF Data	Description	AD	UA	GE
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 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 users by assigning it to those users' accounts.		✓	
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.			✓
MOVE DAT Files	Detection definition files used by MOVE.			✓
MOVE Default Policies	Policies that define the actions taken upon detection on the client systems.			✓
MOVE General Policies	Policies that enable and configuration the operation of real-time scanning on the client systems.			✓
MOVE Quarantine Policies	Policies that specify where quarantined files are stored on the client systems and how long they are kept.			✓
MOVE Quarantined Files	Collection of files on a client system that have been quarantined by MOVE.			✓

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 system that includes hardware and software required for operation. Therefore, responsibility for non-bypassability and separation are split between the TOE and the IT Environment.

All access to objects in the TOE IT environment is validated by the IT environment security policies before they can succeed. Unless a user has been authenticated by the IT environment, the user 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, the TOE's IT environment maintains and controls execution for the TSF separately from other processes.

The TOE provides strictly controlled functionality to the users within the TSC. By limiting access through 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. (A process is a program in execution.) 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 not claim conformance to a Protection Profile.

3 Security Problem Definition

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

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

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

3.1 Threats

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

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.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, through an unsophisticated attack, 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.VIRUS	A malicious agent may attempt to introduce a virus onto a workstation to compromise data on that workstation, or use that workstation to attack additional systems.

Table 9 – Threats Addressed by the TOE

3.2 Organizational Security Policies

The following Organizational Security Policies apply to the TOE:

POLICY	DESCRIPTION
P.ACCESS_BANNER	The system shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHY	Only NIST FIPS validated cryptography (methods and implementations) are acceptable for cryptographic hashing of DAT files.
P.ROLES	The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

Table 10 – Organizational Security Policies

3.3 Assumptions

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

ASSUMPTION	DESCRIPTION
A.AUDIT_BACKUP	Administrators will back up audit records 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 the TOE and remote administrators.
A.SECURE_UPDATES	Administrators will implement secure mechanisms for receiving and validating updated signature files from the Anti-Virus vendors, and for distributing the updates to the central management systems.

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 will provide an authorized administrator role to isolate administrative actions.
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events.
O.AUDIT_PROTECT	The TOE will provide the capability to protect audit information.
O.AUDIT_REVIEW	The TOE will provide the capability to view audit information.
O.CORRECT_TSF_OPERATION	The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.
O.CRYPTOGRAPHY	The TOE shall use NIST FIPS 140-2 validated cryptographic hashing of DAT files and encrypting communications between ePO and McAfee Agent.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE.
O.VIRUS	The TOE will detect and take action against known viruses introduced to the workstation.

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	Audit records are backed up and can be restored, and audit storage will not run out of disk space.
OE.AUDIT_SEARCH	The IT Environment will provide the capability to search and sort the audit information.
OE.AUDIT_STORAGE	The IT Environment will provide a means for secure storage of the TOE audit records.
OE.DISPLAY_BANNER	The IT environment will display an advisory warning regarding the use of the system.
OE.DOMAIN_SEPARATION	The IT environment will provide an isolated domain for the execution of the TOE.
OE.NO_BYPASS	The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.
OE.NO_EVIL	Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.

OBJECTIVE	DESCRIPTION
OE.PHYSICAL	Physical security will 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.RESIDUAL_INFORMATION	The IT environment will 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 IT environment will provide a secure line of communications between the TOE and remote administrators.
OE.SECURE_UPDATES	Enterprises using the TOE shall ensure that signature file updates are received from the vendor 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 IT Environment will provide reliable time stamps.
OE.TOE_ACCESS	The IT environment will provide mechanisms that control a user's logical access to the TOE.

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:

THREAT / ASSUMPTION / POLICY / OBJECTIVE	A.AUDIT_BACKUP	A.NO_EVIL	A.PHYSICAL	A.SECURE_COMMS	A.SECURE_UPDATES	T.AUDIT_ COMPROMISE	T.MASQUERADE	T.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNATTENDED_SESSION	T.UNIDENTIFIED_ACTIONS	T.VIRUS	P.ACCESS_BANNER	P.ACCOUNTABILITY	P.CRYPTOGRAPHY	P.ROLES
O.ADMIN_ROLE																✓
O.AUDIT_GENERATION											✓			✓		
O.AUDIT_PROTECT						✓										
O.AUDIT_REVIEW											✓					
O.CORRECT_TSF_OPERATION									✓							
O.CRYPTOGRAPHY															✓	
O.MANAGE									✓							
O.VIRUS												✓				
OE.AUDIT_BACKUP	✓															

THREAT / ASSUMPTION / POLICY / OBJECTIVE	A.AUDIT_BACKUP	A.NO_EVIL	A.PHYSICAL	A.SECURE_COMMS	A.SECURE_UPDATES	T.AUDIT_ COMPROMISE	T.MASQUERADE	T.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNATTENDED_SESSION	T.UNIDENTIFIED_ACTIONS	T.VIRUS	P.ACCESS_BANNER	P.ACCOUNTABILITY	P.CRYPTOGRAPHY	P.ROLES
OE.AUDIT_SEARCH											✓					
OE.AUDIT_STORAGE						✓										
OE.DISPLAY_BANNER													✓			
OE.DOMAIN_SEPARATION						✓			✓							
OE.NO_BYPASS						✓			✓							
OE.NO_EVIL		✓														
OE.PHYSICAL			✓													
OE.RESIDUAL_INFORMATION						✓		✓	✓							
OE.SECURE_COMMS				✓												
OE.SECURE_UPDATES					✓											
OE.TIME_STAMPS											✓			✓		
OE.TOE_ACCESS							✓			✓				✓		

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

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
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 will provide the capability to protect audit information. OE.AUDIT_STORAGE: The IT environment will contain mechanisms to provide secure storage and management of the audit records. OE.RESIDUAL_ INFORMATION: The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. O.PARTIAL_SELF_PROTECTION: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces. OE.DOMAIN_SEPARATION: The IT environment will provide an isolated domain for the execution of the TOE. OE.NO_BYPASS: The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	O.AUDIT_PROTECT contributes to mitigating this threat by controlling access to the individual audit records. No one is allowed to modify audit records, the System Administrator is the only one allowed to delete audit records, and the TOE has the capability to prevent auditable actions from occurring if the audit trail is full. OE.AUDIT_STORAGE contributes to mitigating this threat by restricting the ability of users in the IT Environment to access the audit records. OE.RESIDUAL_INFORMATION prevents 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 preventing residual information in a resource, audit information will not become available to any user or process except those explicitly authorized for that data. O.PARTIAL_SELF_PROTECTION contributes to countering this threat by ensuring that the TSF can protect itself from users via its own interfaces. This limits access to the audit information to the functions defined for the specified roles. OE.DOMAIN_SEPARATION contributes to countering this threat by ensuring that the TSF is protected from users through mechanisms other than its own interfaces. If the OS could not maintain and control a domain of execution for the TSF separate from other processes, the TSF could not be trusted to control

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
T.MASQUERADE: A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	OE.TOE_ACCESS: The IT Environment will provide mechanisms that control a user's logical access to the TOE.	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 IT Environment will 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.

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
T.TSF_COMPROMISE: A user or process may cause, through an unsophisticated attack, TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).	OE.RESIDUAL_INFORMATION: The IT Environment will ensure that any information contained in a protected resource within the TOE Scope of Control is not released when the resource is reallocated. O.PARTIAL_SELF_PROTECTION: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces. OE.DOMAIN_SEPARATION: The IT environment will provide an isolated domain for the execution of the TOE. O.MANAGE: The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE. O.CORRECT_TSF_OPERATION: The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site. OE.NO_BYPASS: The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	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 to a user, that user would be able to inappropriately view the TSF data. O.PARTIAL_SELF_PROTECTION is necessary so that the TSF protects itself and its resources from inappropriate access through its own interfaces. OE.DOMAIN_SEPARATION is necessary so that the TSF is protected from other processes executing on the workstation. 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.NO_BYPASS ensures TSF compromise can not occur simply by bypassing the TSF.

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
T.UNATTENDED_ SESSION: A user may gain unauthorized access to an unattended session.	OE.TOE_ACCESS: The IT environment will 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: The administrator may not have the ability to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.	O.AUDIT_REVIEW: The TOE will provide the capability to view audit information. OE.AUDIT_SEARCH: The IT Environment will provide the capability to search and sort the audit information. O.AUDIT_GENERATION: The TOE will provide the capability to detect and create records of security relevant events associated with users. OE.TIME_STAMPS: The IT environment shall provide reliable time stamps for accountability and protocol purposes.	O.AUDIT_REVIEW helps to mitigate this threat by providing the Global Administrator with a required minimum set of configurable audit events that could indicate a potential security violation. By configuring these auditable events, the TOE monitors the occurrences of these events (e.g. set number of authentication failures, set number of information policy flow failures, self-test failures, etc.). OE.AUDIT_SEARCH assists the Administrator in reviewing the audit records 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.VIRUS: A malicious agent may attempt to introduce a virus onto a workstation via network traffic or removable media to compromise data on that workstation, or use that workstation to attack additional systems.	O.VIRUS: The TOE will detect and take action against known viruses introduced to the workstation.	O.VIRUS mitigates this threat by providing mechanisms to prevent a virus from being introduced onto a workstation.

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
P.ACCESS_BANNER: The system shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.	OE.DISPLAY_BANNER: The IT Environment will display an advisory warning regarding use of the system.	OE.DISPLAY_BANNER satisfies this policy by ensuring that the system displays a banner that provides all authorized users with a warning about the unauthorized use of the system.
P.ACCOUNTABILITY: The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.AUDIT_GENERATION: The TOE will provide the capability to detect and create records of security-relevant events associated with users. OE.TIME_STAMPS: The IT environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps. OE.TOE_ACCESS: The TOE will 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 environment to identify and authenticate all authorized administrators and workstation users prior to allowing any TOE access. While the user ID of these users can be assured, since they are authenticated, unauthenticated users are permitted to access the TOE and the identity is then a presumed network identifier (e.g., IP address).

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
P.CRYPTOGRAPHY: Only NIST FIPS validated cryptography (methods and implementations) are acceptable for for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e. encryption, decryption, signature, hashing of DAT files.	O.CRYPTOGRAPHY: The TOE shall use NIST FIPS 140-2 validated cryptographic hashing of DAT files and encrypting communications between ePO and McAfee Agent.	O.CRYPTOGRAPHY requires that cryptographic hashing and encryption conform to the policy by mandating FIPS 140-2 validation.
P.ROLES: The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.	O.ADMIN_ROLE: The TOE will provide an authorized administrator role to isolate administrative actions.	O.ADMIN_ROLE addresses this policy by requiring the TOE to support an administrator role, and restrict specific actions to that role.
A.AUDIT_BACKUP: Administrators will back up the audit records and monitor disk usage to ensure audit information is not lost.	OE.AUDIT_BACKUP: Audit records are backed up and can be restored, and audit storage will not run out of disk space.	OE.AUDIT_BACKUP addresses the assumption by requiring the audit records to be backed up, and by requiring monitoring of disk space usage to ensure space is available.
A.DOMAIN_SEPARATION: The IT environment will provide a separate domain for the TOE's operation.	OE.DOMAIN_SEPARATION: The IT environment will provide an isolated domain for the execution of the TOE.	OE.DOMAIN_SEPARATION restates the assumption. The workstation OS and hardware provide domain separation between processes.
A.NO_BYPASS: The IT environment will ensure the TSF cannot be bypassed.	OE.NO_BYPASS: The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	OE.NO_BYPASS restates the assumption. The workstation OS ensures the TSF is invoked.
A.NO_EVIL: Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	OE.NO_EVIL: Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.	OE.NO_EVIL restates the assumption.

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
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 will 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 the TOE and remote administrators.	OE.SECURE_COMMS: The IT environment will provide a secure line of communications 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 the Anti-Virus vendors, and for distributing the updates to the central management systems.	OE.SECURE_UPDATES: Enterprises using the TOE shall ensure that signature file updates are received from the vendor via secure mechanisms, the updates are validated before being used, and the updates are distributed to central management systems within the Enterprise via secure mechanisms.	OE.SECURE_UPDATES restates the assumption. Administrators use secure mechanisms to receive and validate the updates from the vendor, then use secure mechanisms to distribute the updates to the central management systems.

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

5 Extended Components Definition

5.1 Anti-Virus (FAV) Class of SFRs

The purpose of this class of requirements is to address the unique nature of anti-virus products and provide for requirements about detecting and responding to viruses on protected IT resources.

5.1.1 FAV_ACT_(EXT).1 Anti-Virus Actions

Hierarchical to: No other components.

Dependencies: FAV_SCN_(EXT).1 Anti-Virus Scanning

FAV_ACT_(EXT).1.1 Upon detection of a file-based virus, the TSF shall perform the action(s) specified by the [assignment: role]. Actions are administratively configurable on a per-workstation basis and consist of: [assignment: list of actions].

Management:

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

a) Configuration of the actions to be taken.

Audit:

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 a virus.

Application note: The file is deleted and is quarantined to a local folder, and saved with a .vir extension. See Product Guide: McAfee MOVE Antivirus 2.5.0 For use with ePolicy Orchestrator® 4.5.0 and 4.6.0 Software.

5.1.2 FAV_ALR_(EXT).1 Anti-Virus Alerts

Hierarchical to: No other components.

Dependencies: FAV_SCN_(EXT).1 Anti-Virus Scanning

FAV_ALR_(EXT).1.1 Upon detection of a virus, the TSF shall:

- display Detection Alerts on the client VM until the user acknowledges with a click.

The alert shall identify the virus that was detected and the action taken by the TOE.

Management:

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

a) Configuration of the alerts to be generated.

Audit:

There are no auditable events foreseen.

Application note: No alert is displayed on ePO.

5.1.3 FAV_SCN_(EXT).1 Anti-Virus Scanning

Hierarchical to: No other components.

Dependencies: None

FAV_SCN_(EXT).1.1 The TSF shall perform real-time scans for file-based viruses based upon known signatures.

Management:

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

a) Configuration of parameters for all types of scans.

Audit:

There are no auditable events foreseen.

5.2 Extended Security Assurance Components

None

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_STG.4	Site-Configurable Prevention of Audit Loss
Antivirus	FAV_ACT_(EXT).1	Anti-Virus Actions
	FAV_ALR_(EXT).1	Anti-Virus Alerts
	FAV_SCN_(EXT).1	Anti-Virus Scanning
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1(1)	Cryptographic Operation (Encryption/Decryption)
	FCS_COP.1(2)	Cryptographic Operation (Hashing)
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UID.1	User Authentication
	FIA_USB.1	User-Subject Binding
Security Management	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles

Table 16 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

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

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

b) All auditable events for the *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 least the following information:

a) Date and time of the event, type of event, subject identity, 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	Start-up and shutdown of audit functions	
FAU_GEN.2	Access to the TOE and System data	Object IDs, Requested access
FAV_ACT_(EXT).1	Action taken in response to detection of a virus	Virus detected, action taken, file where virus is detected
FAV_ALR_(EXT).1	None	Not applicable
FAV_SCN_(EXT).1	None	Not applicable
FIA_ATD.1	None (No tested secrets apply).	Not applicable
FIA_UID.1	All use of the user identification mechanism	User identity, location
FIA_USB.1	None (The binding of attributes to the subject never fails, per TOE design).	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 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *authorized users with Global Administrator status* with the capability to read *all information* from the audit records.

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

6.1.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users

that have been granted explicit read-access.

6.1.1.5 FAU_STG.1 Protected Audit Trail Storage

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

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

6.1.1.6 FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4.1 The TSF shall ignore auditable events and *perform null action* if the audit trail is full.

Application Note: The TOE relies on the IT Environment to monitor disk space and send the appropriate alarm. The TOE sends audit events to the IT Environment, and if full, the database ignores the new audit events and alarms the administrator with a notification indicating low disk space.

6.1.2 Anti-Virus (Explicitly Stated)

6.1.2.1 FAV_ACT_(EXT).1 Anti-Virus Actions

FAV_ACT_(EXT).1.1 Upon detection of a file-based virus, the TSF shall perform the action(s) specified by *the Global Administrator*. Actions are administratively configurable and consist of:

a. *Deny the operation OR delete the file*

AND

b. *Optionally quarantine the file.*

6.1.2.2 FAV_ALR_(EXT).1 Anti-Virus Alerts

FAV_ALR_(EXT).1.1 Upon detection of a virus, the TSF shall display an alert on the screen of the workstations on which the virus is detected. The alert shall identify the virus that was detected and the action taken by the TOE. The alert remains on the screen until dismissed by the user.

6.1.2.3 FAV_SCN_(EXT).1 Anti-Virus Scanning

FAV_SCN_(EXT).1.1 The TSF shall perform real-time scans for file-based viruses based upon known signatures.

6.1.3 Cryptographic Support (FCS)

6.1.3.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *FIPS 186-3* and specified cryptographic key sizes *128 or 256-bit* that meet the following: *FIPS 197 for AES.*

6.1.3.2 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwrite* that meets the following: *FIPS 140-2.*

6.1.3.3 FCS_COP.1(1) Cryptographic Operation (Encryption/Decryption)

FCS_COP.1.1(1) The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm *AES CBC mode* and cryptographic key sizes *128 or 256-bit* that meet the following: *FIPS 197.*

OPERATION	ALGORITHM MODE	KEY SIZE	CAVP CERTIFICATE	STANDARDS
Encryption / Decryption	AES	128 or 256-bits	670, 860, 501	FIPS 197
Random Number Generator	FIPS 186-2	127 or 256-bits	390, 492, 270	Digital Signature Standard (DSS) Appendix 3.1

6.1.3.4 FCS_COP.1(2) Cryptographic Operation (Hashing)

FCS_COP.1.1(2) The TSF shall perform *calculate a message digest to verify the integrity of the signature files* in accordance with a specified cryptographic algorithm *Secure Hash Algorithm (SHA-1)* and cryptographic key sizes (*not applicable*) that meet the following: *FIPS 180-2 (CAVP certificate #431)*.

6.1.4 Identification and Authentication (FIA)

6.1.4.1 FIA_ATD.1 User Attribute Definition

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

6.1.4.2 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow *no actions* on behalf of the user to be performed **on the management system** before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user **on the management system**.

Application Note and Refinement Rationale: The TOE performs identification on the management system then relies upon Windows for authentication.

Application Note: Authentication on the managed systems is the responsibility of the operating environment.

6.1.4.3 FIA_USB.1 User-Subject Binding

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

a) Global Administrator status; and

b) Permissions.

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

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

Application Note: Permissions are determined by the union of all permissions in any permission set associated with a user.

Application Note: 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 page refresh.

6.1.5 Security Management (FMT)

6.1.5.1 FMT_MTD.1 Management of TSF Data

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

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
Antivirus	Files to be scanned	Modify

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
Settings	Actions to be taken on workstations when a virus is detected	Query, Modify, Delete
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; make personal dashboards public
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
Event Logs	n/a (only allowed by a Global Administrator)	Query and delete
Global Administrator Status	n/a (only allowed by a Global Administrator)	Query and modify
Groups	View "System Tree" tab	Query
	View "System Tree" tab along with Edit System Tree groups and systems	Query, create, delete and modify
Permission Set	n/a (only allowed by a Global Administrator)	Query, create, delete, modify, and assign (to a user) permissions
Queries	Use public queries	Query and use public queries
	Use public queries; create and edit personal queries	Query and use public queries; create and modify personal queries
	Edit public queries; create and edit personal queries; make personal queries public	Query, delete, modify and use public queries; create, delete and modify (including make public) personal queries
Server Settings	n/a (only allowed by a Global Administrator)	Query and modify
System Information	Create and edit systems	Query, create, delete and modify
System Tree	View System Tree	Query

Table 18 – TSF Data Access Permissions

6.1.5.2 FMT_SMF.1 Specification of Management Functions

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

a. *ePO User Account management,*

b. *Permission Set management,*

c. *Audit Log management,*

d. *Event Log management,*

e. *Notification management,*

f. *System Tree management,*

g. *Query management,*

h. *Dashboard management.*

i. *Virus Scanning and associated action management.*

j. *Update virus scan signatures.*

6.1.5.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles: *Global Administrator and User*.

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

Application Note: A Global Administrator is a defined user account with Global Administrator status. Users are defined user accounts without Global Administrator status but with specific permissions.

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

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
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 at EAL2

6.3 CC Component Hierarchies and Dependencies

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

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN.1	None	FPT_STM.1	Satisfied by the Operational Environment
FAU_GEN.2	None	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied
FAU_SAR.1	None	FAU_GEN.1	Satisfied
FAU_SAR.2	None	FAU_SAR.1	Satisfied
FAU_STG.1	None	FAU_GEN.1	Satisfied
FAU_STG.4	FAU_STG.3	FAU_STG.1	Satisfied
FAV_ACT_(EXT).1	None	FAV_SCN_(EXT).1	Satisfied
FAV_ALR_(EXT).1	None	FAV_SCN_(EXT).1	Satisfied
FAV_SCN_(EXT).1	None	None	None
FCS_COP.1	None	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	Satisfied.
FIA_ATD.1	None	None	None
FIA_UID.1	No other components	None	n/a
FIA_USB.1	None	FIA_ATD.1	Satisfied
FMT_MTD.1	None	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	None	None	None
FMT_SMR.1	None	FIA_UID.1	Satisfied

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:

OBJECTIVE / SFR	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.MANAGE	O.VIRUS
FAU_GEN.1		✓			✓			
FAU_GEN.2		✓			✓			
FAU_SAR.1				✓	✓			
FAU_SAR.2			✓					
FAU_STG.1			✓					
FAU_STG.4			✓					
FAV_ACT_(EXT).1					✓			✓
FAV_ALR_(EXT).1					✓			✓
FAV_SCN_(EXT).1					✓			✓
FCS_CKM.1						✓		
FCS_CKM.4						✓		
FCS_COP.1(1)						✓		
FCS_COP.1(2)						✓		
FIA_ATD.1	✓							
FIA_UID.1							✓	
FIA_USB.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

OBJECTIVE	REQUIREMENTS THAT ADDRESS THE OBJECTIVE	SFR AND RATIONALE
O.ADMIN_ROLE The TOE will provide an authorized administrator role to isolated administrative actions.	FMT_MTD.1 FMT_SMR.1 FIA_ATD.1 FIA_USB.1	FMT_SMR.1 requires that the TOE establish a Global Administrator role. FMT_MTD.1 specify the privileges that only the Global 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_GEN The TOE will provide the capability to detect and create records of security relevant events.	FAU_GEN.1 FAU_GEN.2	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that the 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.

OBJECTIVE	REQUIREMENTS THAT ADDRESS THE OBJECTIVE	SFR AND RATIONALE
O.AUDIT_PROTECT The TOE will provide the capability to protect audit information.	FAU_SAR.1 FAU_STG.1 FAU_STG.4	FAU_SAR.2 restricts the ability to read the audit trail to the Audit 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 the Global Administrator. FAU_STG.4 defines the actions that must be available to the administrator, as well as the action to be taken if there is no response. This helps to ensure that audit records are kept until the Global 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 audit record). This ensures the integrity of the audit trail is maintained.
O.AUDIT_REVIEW The TOE will provide the capability to 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 will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAV_SCN_(EXT).1 FAV_ALR_(EXT).1 FAV_ACT_(EXT).1	Correct TSF operation can be determined by injecting a known virus into the TOE and ensuring that the proper events occur. The FAV class will detect and act upon the virus. The FAU_GEN family will generate an audit event when the virus is detected. FAU_SAR.1 enables the administrator to review the audit events.
O.CRYPTOGRAPHY The TOE shall use NIST FIPS 140-2 validated cryptographic hashing of DAT files.	FCS_CKM.1 FCS_CKM.4 FCS_COP.1(1) FCS_COP.1(2)	FCS_CKM.1, FCS_CKM.4, FCS_COP.1(1), and FCS_COP.1(2)requires that the message digest used to verify integrity of the signature file and the secure communications between ePO and the McAfee Agent utilizes a FIPS 140-2 Approved cryptographic algorithm.

OBJECTIVE	REQUIREMENTS THAT ADDRESS THE OBJECTIVE	SFR AND RATIONALE
O.MANAGE The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE.	FIA_UID.1 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1	Restricted privileges are defined for the Global Administrator. Users authorized to access the TOE are determined using an identification process [FIA_UID.1]. FMT_MTD.1 defines particular TOE 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 TOE.
O.VIRUS The TOE will detect and take action against known viruses introduced to the workstation.	FAV_ACT_(EXT).1 FAV_ALR_(EXT).1 FAV_SCN_(EXT).1	FAV_SCN_(EXT).1 requires that the TOE scan for viruses. FAV_ACT_(EXT).1 requires that the TOE take action against viruses once they are detected. FAV_ALR_(EXT).1 defines alerting requirements to ensure the users aware that a virus 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	Security Architecture: McAfee MOVE 2.5 and ePolicy Orchestrator 4.6
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: McAfee MOVE 2.5 and ePolicy Orchestrator 4.6
ADV_TDS.1: Basic Design	Basic Design: McAfee MOVE 2.5 and ePolicy Orchestrator 4.6
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: McAfee MOVE 2.5 and ePolicy Orchestrator 4.6
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: McAfee MOVE 2.5 and ePolicy Orchestrator 4.6
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: McAfee MOVE 2.5 and ePolicy Orchestrator 4.6

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: McAfee MOVE 2.5 and ePolicy Orchestrator 4.6
ALC_DEL.1: Delivery Procedures	Delivery Procedures: McAfee MOVE 2.5 and ePolicy Orchestrator 4.6
ALC_FLR.2: Flaw Reporting Procedures	Flaw Reporting Procedures: McAfee MOVE 2.5 and ePolicy Orchestrator 4.6
ATE_COV.1: Evidence of Coverage	Security Testing: McAfee MOVE 2.5 and ePolicy Orchestrator 4.6
ATE_FUN.1: Functional Testing	Security Testing: McAfee MOVE 2.5 and ePolicy Orchestrator 4.6
ATE_IND.2: Independent Testing – Sample	Security Testing: McAfee MOVE 2.5 and ePolicy Orchestrator 4.6

Table 23 – Security Assurance Measures

6.4.2.1 Rationale for TOE Assurance Requirements Selection

EAL2 was chosen to provide a low to moderate level of independently assured security. The chosen assurance level is consistent with the threat environment. Specifically, that the threat of malicious attacks is not greater than moderate and the product will have undergone a search for obvious flaws. ALC_FLR.2 was added to provide assurance that the vendor will respond to reports of new threats and reported defects in the TOE. Selection of this assurance package aims to support the assurance needs of McAfee customers.

7 TOE Summary Specification

7.1 Virus Scanning & Alerts

The TOE provides real-time virus detection, and scanning occurs when files are either read from or written to the computer the TOE client agent is installed on.

When an infection occurs, the TOE takes certain actions depending on what has been configured:

- display Detection Alerts on the client VM until the user acknowledges with a click.

The alert shall identify the virus that was detected and the action taken by the TOE.

7.2 The alert identifies the system where the infection has occurred, the name of the virus, and the action taken by the TOE. Audit (AUDIT)

7.2.1 Audit Generation

Audit Generation within the TOE consists of two types of records, “Events” and “Logs”. “Events” record actions taken by the TOE such as threat detections, and “Logs” record user actions. Events are generated by both the ePO server and the workstations executing MOVE. Logs are generated on the ePO server.

User action event types are stored in the Audit Log. The Event Log stores the following event types:

1. Threat Events
2. Client Events
3. Server Events

The ePO can be configured to automatically trigger an action in response to the various types of events; including threat, client, and sever events.

MOVE generates Events when viruses are detected. Event records include details of the system on which the virus was detected (subject identity), the specific virus detected, the action taken to counteract the virus, and the file in which the virus was detected. Events for each workstation are queued on the workstation, and forwarded to the ePO event log.

ePO generates Log records for actions performed by ePO users. The auditable events and record contents are specified in the Audit Events and Details table in the FAU_GEN.1 section.

Event records generated by ePO or MOVE are stored in the ePO database. Queued Events are uploaded to the ePO server. The client uses disk space available on the workstation for queuing events. The IT environment manages shortages of available disk space on the workstation. On the ePO server, Events are inserted into the Event Log for storage. In the unlikely event that the storage (database) space is exhausted, agent connections are refused and Event records remain in the queue on the workstation until the ePO server is again able to accept connections.

The audit function operates whenever ePO/MOVE are operating. If an instance of MOVE is enabled or disabled on a workstation by the Global Administrator, an audit record is generated.

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

7.2.2 Audit Record Review

Audit record review is provided by the ePO server. ePO maintains a record of user actions and system actions, referred to as "Logs" and "Events", respectively. "Logs" record user actions within the user interface, and "Events" record actions taken by the TOE such as threat detections. The auditable events are specified in the Audit Events and Details table in the FAU_GEN.1 section.

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.

The Audit Log entries are automatically purged based upon a configured age. Audit records may be deleted via automatic purging, or a Global Administrator may manually delete all records older than a specified date. Event filters may be configured to specify which possible 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. The following audit event types can be selectively audited:

- CommonEvents
- EPO Core
- CommonEvents
- View IPS Events

- Delete Site (System)
- Move Branch Node
- Move Leaf Node
- New User
- Delete User
- Failed to Login to Reports
- Run Query
- Run Report (Dashboard)
- Set Policy Setting Value
- Set Policy User Role
- Uninstall Branch Node
- Uninstall Leaf Node
- EPO Core Startup Error
- Purge Client Events
- Purge Audit Log
- Add Dashboard
- View Audit Log
- View Audit Events
- Server Restart

Queries are configurable objects that retrieve and display collected event records from MOVE from the database. The TOE provides predefined queries and users can also generate custom queries. The custom queries may specify the data to be displayed in the results. The results of queries are displayed in charts or tables. Query results displayed in tables (and drill-down tables) have a variety of actions available for selected items in the table. Results from queries that include MOVE events may be viewed by Global Administrators.

Queries can be personal or public. Private queries are only available to their creator. Public queries are available to everyone who has permissions to use public queries. To run queries, the user may also need permissions to the feature sets associated with their result types.

The result type for each query identifies what type of data the query will be retrieving. This selection determines what the available parameters are in the rest of the query. Result types associated with MOVE events include:

1. Events — Retrieves information on events sent from MOVE.
2. Managed Systems — Retrieves information about systems running MOVE.

Dashboards are an alternative mechanism for viewing the collected events. Individual users with the "Permission to use public dashboards" may add public dashboards to their personal dashboard display. The charts on the dashboard may provide drill-down capability to provide more detailed information about the information displayed in the chart.

MOVE events are automatically purged according to the configured Data Retention parameters. If the storage capacity of the database is exceeded, new event records are discarded. The TOE does not provide any mechanism to modify event information. Event records may be deleted via automatic purging, or a Global Administrator may manually delete all records older than a specified date.

7.3 Management (MGMT)

The TOE's Management Security Function provides administrator support functionality that enables a user to configure and manage TOE components. Management of the TOE may be performed via the ePO GUI. Management permissions are defined per-user. Configuring Global Administrator status to an 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. Antivirus settings,
10. Virus scan signatures.

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

7.3.1 ePO User Account Management

Each user authorized for login to ePO must be defined with ePO. Only 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.
3. Create, delete, and assign permission sets.
4. Limit events that are stored in ePolicy Orchestrator databases.

Per the evaluated configuration, the following permissions may never be assigned to a role other than the Global Administrator:

1. View audit log
2. View and purge audit log
3. View MOVE settings
4. View and change MOVE settings

7.3.2 Permission Set Management

A permission set is a group of permissions that can be granted to any users by assigning it to those users' accounts. 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 Log Record Management

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 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.

Per the evaluated configuration, the "View audit log" and "View and purge audit log" permissions are never used.

7.3.4 Event Record Management

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

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" 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.
2. Create and edit notification rules; view Notification Log - This permission also grants the ability to view SNMP servers.
3. Create and edit notification rules; view and purge Notification Log; create and edit SNMP servers.

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

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 you can provide sorting criteria for the subgroups you create 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. 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

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

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 Antivirus Settings

When an infection occurs, the TOE takes certain actions depending on what has been configured

- display Detection Alerts on the client VM until the user acknowledges with a click.

The alert shall identify the virus that was detected and the action taken by the TOE.

7.3.10 MOVE DAT File

The TOE depends on the information in the detection definition (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. These DAT updates may include minor updates to the virus scanning engine. The Global Administrator may obtain updated DAT files from McAfee and then distribute the updated information to the clients. When the DATs are downloaded, the hashes are checked with a FIPS validated algorithm.

Per the evaluated configuration, only Global Administrators may update the DAT files.

7.3.11 Quarantined Files

Quarantined files are stored on the local machine where they are discovered. McAfee MOVE Antivirus provides methods for dealing with malicious files beyond events and notifications. When an item is detected as a threat, an event is logged. In addition, the malicious file can also be isolated in a quarantine folder.

Quarantining is enabled by default, and quarantined items are placed in the C:\Quarantine folder on the system where the file was discovered. Quarantined files are protected by encapsulation and thereby rendered unexecutable. Quarantined items are sorted in the quarantine folder by threat category, and are automatically deleted after a configurable period of time. Quarantine behavior can be modified through McAfee MOVE Antivirus policy changes.

7.4 Cryptographic Operations

The TOE has the ability to deploy MOVE AV agent packages. The signature provided with the package includes calculation of a message digest using the Secure Hash Algorithm (SHA-1). MOVE AV packages come pre-made from McAfee. Upon download to the workstation, the hash is verified. The SHA-1 hash is used to verify the integrity of the packages.

The TOE uses FIPS 140-2 validated modules for securing the communications between EPO and the McAfee Agent.

The cryptographic algorithms used to provide cryptography are provided by two specific FIPS 140-2 cryptographic modules. These are the McAfee ePO Client Cryptographic Module (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm#1587) and the McAfee Agent Cryptographic Module (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm#1588). These modules have been successfully validated against the FIPS 140-2 criteria.