Security Target

McAfee Management for Optimized Virtual Environments (MOVE) Antivirus 3.0 with ePolicy Orchestrator 5.1.1

Document Version: 1.3
Date: November 7, 2014

Prepared For:

McAfee, Inc.
2821 Mission College Blvd.
Santa Clara, CA 95054
www.mcafee.com

Prepared By:

CGI Global IT Security Labs.

1410 Blair Place, 7th floor
Ottawa, ON K1J 9B9, Canada
www.cgi.com/securitylab

Revision History

Ver #	Description of changes	Modified by	Date
0.1	Initial Draft	Swapna Katikaneni	01/20/2014
0.2	Updated the ST to include only the agentless configuration	Swapna Katikaneni	02/06/2014
0.3	Updates for Lab observations	Shawn Pinet	04/03/2014
0.4	Updates to threats and objectives to clarify mappings	Shawn Pinet	04/15/2014
0.5	Updates to address Lab and CB OR's	Shawn Pinet	05/14/2014
0.6	Additional guidance documentation for FIPS mode configurations	Shawn Pinet	06/16/2014
0.7	Minor fix to table 12	Shawn Pinet	06/23/2014
0.8	Responses to observations, update to ePO 5.1.1	Shawn Pinet	10/01/2014
0.9	Updated FIPS certificate numbers	Shawn Pinet	10/15/2014
1.0	Updates following on-site from certifier	Shawn Pinet	10/27/2014
1.1	Final updates for publication	Shawn Pinet	10/29/2014
1.2	Response to CB OR #3	Shawn Pinet	11/4/2014
1.3	Additional updates for clarity	Shawn Pinet	11/7/2014

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

This section identifies the Security Target (ST), Target of Evaluation (TOE), document conventions, and terminology. It also provides TOE overview and describes the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE.

1.1 ST Reference

ST Title	Management for Optimized Virtual Environments (MOVE) Antivirus 3.0 with ePO 5.1.1
ST Revision	1.3
ST Publication Date	November 7, 2014
ST Author	CGI Global IT Security Labs – Canada Swapna Katikaneni Shawn Pinet

1.2 Target of Evaluation Reference

TOE Developer	McAfee, Inc.
TOE Name	Management for Optimized Virtual Environments (MOVE) Antivirus 3.0 with ePO 5.1.1
TOE Version	MOVE Agentless 3.0.0 with ePO 5.1.1 and hotfix 983758
TOE Type	Antivirus

1.3 Conventions

The Common Criteria allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and selected presentation choices are discussed below to aid the Security Target reader:

An assignment operation is indicated by [*italicized text within brackets*].

Selections are denoted by [underlined text within brackets].

Refinement of security requirements is identified using **bold text**. Any text removed is indicated with a strikethrough (Example: ~~TSF~~).

Iterations are identified by appending a number in parentheses following the component title, for example, FIA_UAU.1 (1) and FIA_UAU.1 (2) refer to two iterations of the FIA_UAU.1 security functional requirement component.

1.4 TOE Overview

Management for Optimized Virtual Environments (MOVE) Antivirus 3.0 with ePO 5.1.1 (the TOE) is an antivirus solution for virtual environments that removes the need to install an antivirus application on every virtual machine (VM).

A traditional security solution for virtual environments uses an antivirus application running on every VM on a hypervisor. This requirement reduces VM density per hypervisor and causes high disk, CPU, and memory usage. The TOE solves this issue by offloading all on-access scanning to a dedicated VM, Security Virtual Appliance (SVA). This security virtual appliance runs McAfee Virus Scan Enterprise for Linux and the McAfee Agent version 4.8 software inside a dedicated appliance designed to optimize performance related to anti-virus scanning. This results in increased VM density per hypervisor.

The TOE contains a Security Virtual Appliance (SVA) delivered as an Open Virtualization Format (OVF) package and can be installed without the need for a McAfee-specific agent to be installed on the protected VM's. The TOE provides antivirus functionality by leveraging VMWare's vShield antivirus offloading capability in VMWare vCNS (vCloud Networking Security) – installed as a component of VMWare vCenter. The VMware vShield Endpoint API, which is provided by VMWare rather than McAfee, is utilized for offloading all on-access scanning to the SVA

The management capabilities for MOVE are provided by ePO through the MOVE ePO Extension that manages MOVE Software that reside on the host hypervisors. ePO can be used to manage a large enterprise network from a centralized system. ePolicy Orchestrator communicates policy information to the SVA on a regular interval. ePO, through the McAfee Agent, provides capabilities to distribute updated MOVE Security policies and DAT files to the SVA. ePO also centrally manages Event and Log records.

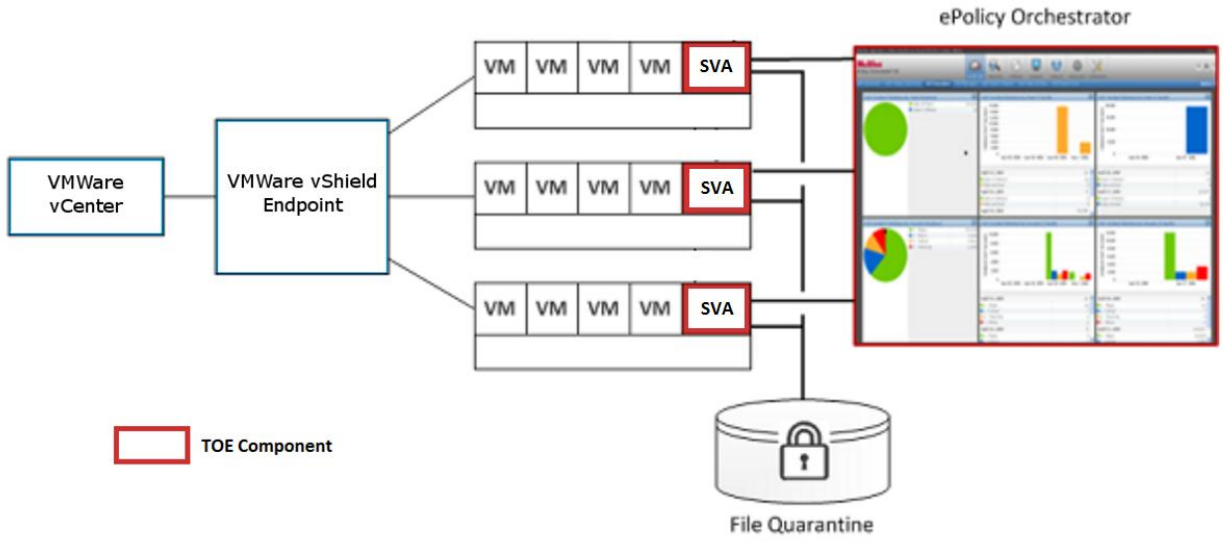
Communications between the distributed components of the TOE architecture are protected from disclosure and modification by cryptographic functionality provided by the FIPS approved components of the McAfee ePO and the McAfee Agent. It is assumed that the IT environment will provide a secure line of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

The TOE provides the following security functionality: Auditing of security relevant events, Identification and Authentication, Security Management, Virus Scanning, Cryptographic operations and trusted communication between TOE components

1.5 TOE Description

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

Figure 1: McAfee MOVE 3.0.0 Agentless deployment using VMWare vShield Endpoint.



1.5.1 Physical Boundary

McAfee Management for Optimized Virtual Environments (MOVE) Antivirus 3.0 is a software-based TOE including:

1. The ePO application version 5.1.1 with hotfix 983758 applied executing on a dedicated server. This Communicates with the McAfee Agent, manages and provides reports on malware discovered within the virtual environment.
2. The McAfee MOVE AV Agentless component called the Security Virtual Appliance (SVA) version 3.0.0; The SVA gets the notification of every file event of every guest VM from the Operational Environment

The physical components of the TOE include the software that is installed during installation of SVA and ePO. The TOE software is installed on a centralized ePO server and on VMWare ESXi hypervisor hosts

1.5.1.1 Guidance Documentation

The following lists the TOE Guidance Documentation to install, configure, and maintain the TOE.

- McAfee MOVE AntiVirus 3.0.0 For use with ePolicy Orchestrator 4.6.0, 5.0.0 Software Product Guide
- ePolicy Orchestrator 5.1.0 Product Guide
- Supported Platforms, Environments and Operating Systems for ePolicy Orchestrator KB51569
- McAfee ePolicy Orchestrator 5.1.0 Software FIPS Mode User Guide ePO 5.x installation/patch upgrade checklist for known issues KB76739
- McAfee ePolicy Orchestrator 5.1.0 Software installation guide
- Release Notes Hotfix 983758-2 McAfee ePolicy Orchestrator 5.1.1
- MOVE Agentless fix for BASH/Shellshock KB83017
- Operational User Guidance and Preparative Procedures McAfee Management for Optimized Virtual Environments (MOVE) Antivirus Agentless 3.0 with ePolicy Orchistrator 5.1.1 Document Version: 0.8

1.5.2 Logical Boundary

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

Virus Scanning

The TOE provides for scanning and detection of file-based viruses. Users are alerted of actions on the management system (via log). This functionality is supported by the Security Virtual Appliance (SVA) running an edition of McAfee VirusScan Enterprise for Linux.

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.

Identification and Authentication:

The TOE requires all users to provide unique identification and authentication data before any administrative access to the system is granted. User identification and authentication is done by the TSF through username/password authentication or by an external authentication server. All authorized TOE users must have an account with security attributes that control the user's access to TSF data and management functions. Identification and Authentication in the evaluated configuration may rely on ePO user accounts or may also be configured such that the the Operational Environment provides an external authentication server. It also depends on the Operational Environment to provide a secure communications path between the TOE and the external authentication server. The TOE will allow a protected VM to have virus scanning performed based on the administrator defined policy with appropriate identification from the vShield Endpoint framework.

TOE Access

In order to protect administrative sessions ePO enforces a session timeout value on all administrative sessions. ePO also allows for an administrator to terminate their session when they no longer require access to the TOE administrative interface.

Management

ePO enables the Global Administrator to centrally manage virus scan settings on protected Virtual Machines, 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

Antivirus packages are distributed to the ePO server 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.

Trusted Communications between the TOE Components:

The TOE consists of distributed components. The communication between the ePO and McAfee agent in the SVA relies upon cryptographic functionality provided by the ePO and McAfee agent components to protect the information exchanged from disclosure or modification.

1.5.3 Hardware, firmware, and Software provided by the IT environment

The following hardware, firmware and software, which are supplied by the IT environment, are required for the operation of the TOE

Software requirements for SVA:

1) VMware ESXi 5.0 Patch 1,5.1 or 5.5
2) VMware vCenter 5.0, 5.1 or 5.5
3) VMware vShield Manager 5.0,5.1 or 5.5
4) VMware vShield Endpoint 5.0, 5.1 or 5.5
5) VMware vSphere Client 5.0, 5.1 or 5.5

Table 1 MOVE 3.0.0 SVA VM requirements

COMPONENT	REQUIREMENTS
Processor	2 vCPU, 1.6 GHZ or higher
Memory	2 GB RAM or higher
Free Disk Space	8 GB or higher
Network Card	1 or more

ePO requirements:

The platform on which ePO 5.1.1 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.

Table 2 ePO 5.1.1 System Requirements

COMPONENT	MINIMUM REQUIREMENTS
Processor	Intel Pentium 4-class or higher 1.3 GHz or higher
Memory	1 GB available RAM minimum 4 GB available RAM recommended minimum
Free Disk Space	1.5 GB — First-time installation minimum 2 GB — Recommended minimum
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	Windows Server 2008 with SP2 Standard, Enterprise, or Datacenter Windows Server 2008 R2 Standard, Enterprise, or Datacenter Windows Server 2008 for Small Business Premium
Web Browser	Google Chrome 17 and later

COMPONENT	MINIMUM REQUIREMENTS
	Firefox 10.0 and later Firefox 5.x Firefox 4.x Firefox 3.5 Firefox 3.6 Internet Explorer 9.0 and later Internet Explorer 7.0 Internet Explorer 8.0
Virtual Infrastructure	VMware ESX/ESXi 5.x and later VMware ESX/ESXi 4.x Citrix XenServer 6.0 Citrix XenServer 5.5 Update 2 Windows Server 2012 Hyper-V Windows Server 2008 R2 Hyper-V Windows Server 2008 Hyper-V
DBMS	SQL Server 2012 Express SQL Server 2012 SQL Server 2008 with SP1/SP2/R2 Standard, Enterprise, Workgroup, Express SQL Server 2005 with SP3 Standard, Enterprise, Workgroup, Express
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 if configured for Windows Authentication in a Domain

1.5.4 Product Physical/Logical Features and Functions not included in the TOE Evaluation

Features/Functions that are not part of the evaluated configuration of the TOE are:

- Windows services invoked by the TOE to validate user credentials.
- The use of the Agent Handler and super agent functionality
- The GTI servers provided by McAfee labs.
- 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.
- The database which stores all data created and used by ePolicy Orchestrator
- VMWare vCenter, VMWare ESXi, VMWare vShield and vShield Endpoint are not part of the TOE.
- Remote quarantine file server.

1.5.5 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.

Table 3 TOE data

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.			X
Dashboards	Collections of chart-based queries that are refreshed at a user-configured interval.			X
Email Server	SMTP server name and port used to send email messages for notifications. Credentials may optionally be specified for authenticated interactions.			X
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.	X		
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.		X	
Groups	Node on the hierarchical System Tree that may contain subordinate groups or systems.			X
Notification Rules	Rules associated with groups or systems used to generate email messages upon receipt of specified events			X
Permission	A privilege to perform a specific function.		X	
Permission Set	A group of permissions that can be granted to any		X	

TSF Data	Description	AD	UA	GE
	users by assigning it to those users' accounts.			
Queries	Configurable objects that retrieve and display data from the database.			X
Server Settings	Control how the ePolicy Orchestrator server behaves.			X
SNMP Trap Destinations	Name and address of an SNMP server to receive trap messages as a result of notification rules.			X
System Tree	Information specific to a single managed system (e.g. internet address) in the System Tree.			X
System Tree	A hierarchical collection of all of the systems managed by ePolicy Orchestrator.			X
MOVE DAT Files	Detection definition files used by MOVE.			X
MOVE Default Policies	Policies that define the actions taken upon detection on the client systems.			X
MOVE General Policies	Policies that enable and configuration the operation of real-time scanning on the client systems.			X
MOVE Quarantine Policies	Policies that specify where quarantined files are stored on the client systems and how long they are kept.			X
MOVE Quarantined Files	Collection of files on a client system that have been quarantined by MOVE.			X

1.5.6 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. When configured for external authentication, 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 Security Target is conformant to Common Criteria Version 3.1 Revision 4, September 2012, Part 2 extended and Part 3 conformant. The ST claims conformance to Evaluation Assurance Level 2 augmented with ALC_FLR.2

2.2 Protection Profile Conformance Claim

The Security Target does not make any PP conformance claims.

3 SECURITY PROBLEM DEFINITION

This section defines the security problem which the TOE and its operational environment are supposed to address. Specifically, the security problem makes up the following:

- Any known or assumed threats countered by the TOE or its operational environment.
- Any organizational security policies 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 section identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

This section identifies the threats to the assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.

TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

The table below lists threats applicable to the TOE and its operational environment:

Table 4 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.INTERCEPT	An attacker may gain access to and/or modify secure data while it is being transmitted between TOE components.
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

Threat	Description
	unauthorized actions may occur.
T.VIRUS	A malicious agent may attempt to introduce a virus onto a Virtual Machine to compromise data on that Virtual Machine, or use that Virtual Machine to attack additional systems.

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The following table lists Organizational Security Policies (OSP) applicable to the TOE and its operational environment:

Table 5 Organizational Security Policies

OSP	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.

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to operate. The following specific conditions are assumed to exist in an environment where the TOE is employed.

Table 6 Assumptions

Assumption	Description
A.AUDIT_BACKUP	Administrators will back up audit records and monitor disk usage to ensure audit information is not lost.
A.DOMAIN_SEPARATION	The IT environment will provide a separate domain for the TOE's operation.

Assumption	Description
A.NO_BYPASS	The IT environment will ensure the TSF cannot be bypassed.
A.NO_EVIL	Administrators including administrators of the IT environment 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_AUTH	It is assumed that the IT environment will provide a secure line of communications between the TOE and the authentication server.
A.SECURE_UPDATES	Administrators will implement secure mechanisms for receiving and validating updated signature files from the antivirus vendors, and for distributing the updates to the central management systems.

4 SECURITY OBJECTIVES

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition. This high-level solution is divided into two parts: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are as follows:

Table 7 TOE Security Objectives

Security 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 anti-virus detection, auditing and enforcement at a customer's site.
O.CRYPTOGRAPHY	The TOE shall use NIST FIPS 140-2 validated cryptographic hashing of DAT files and encrypting sensitive 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.PROTECTCOM	The TOE will provide a trusted communications path that provides for the protection of the data from modification or disclosure while transfer between TOE components
O.TOEACESS	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data
O.VIRUS	The TOE will detect and take action against known viruses introduced to the Virtual Machine.

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

Table 8 Operational Environment Security Objectives

Security 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.
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_AUTH	The IT environment will provide a secure line of communications between the TOE and the remote authentication server.
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 must provide an authentication service for user identification and authentication that can be invoked by the TSF to control a user's logical access to the TOE.

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:

Table 9 Cross Reference of Threats, Assumptions and Policies

Objectives mapped to Assumptions , threats and policies	A.AUDIT_BACKUP	A.NO_EVIL	A.DOMAIN_SEPERATION	A.NO_BYPASS	A.PHYSICAL	A.SECURE_AUTH	A.SECURE_UPDATES	T.AUDIT_COMPROMISE	T.INTERCEPT	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																			X
O.AUDIT_GENERATION														X			X		
O.AUDIT_PROTECT								X											
O.AUDIT_REVIEW														X					
O.CORRECT_TSF_OPERATION												X							
O.CRYPTOGRAPHY									X									X	
O.MANAGE												X	X						
O.PROTECTCOM									X										
O.TOEACCESS										X			X				X		
O.VIRUS															X				
OE.AUDIT_BACKUP	X																		
OE.AUDIT_SEARCH														X					
OE.AUDIT_STORAGE								X											
OE.DISPLAY_BANNER																X			
OE.DOMAIN_SEPARATION			X					X				X							
OE.NO_BYPASS				X				X				X							
OE.NO_EVIL		X																	
OE.PHYSICAL				X	X														

Objectives mapped to Assumptions , threats and policies	A.AUDIT_BACKUP	A.NO_EVIL	A.DOMAIN_SEPERATION	A.NO_BYPASS	A.PHYSICAL	A.SECURE_AUTH	A.SECURE_UPDATES	T.AUDIT_COMPROMISE	T.INTERCEPT	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.RESIDUAL_INFORMATION								X			X	X							
OE.SECURE_AUTH				X		X													
OE.SECURE_UPDATES							X												
OE.TIME_STAMPS														X			X		
OE.TOE_ACCESS										X			X				X		

Table 10 - Detailed Rationale of Threats, Policies and Assumptions

Threats, Policies and Assumptions	Objectives	Rationale
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.	O.AUDIT_PROTECT OE.AUDIT_STORAGE OE.RESIDUAL_INFORMATION OE.DOMAIN_SEPARATION OE.NO_BYPASS	O.AUDIT_PROTECT provides protection for the audit data produced by the TOE. The TOE provides restricted access to audit records. The TOE also prevents loss of audit data when 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.

Threats, Policies and Assumptions	Objectives	Rationale
		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 the resources under its control, which includes the audit trail. OE.NO_BYPASS contributes to countering this threat by ensuring that the TSF cannot be bypassed by components of the operational environment such as the management station or ESX hypervisor.
T.INTERCEPT An attacker may gain access to and/or modify secure data while it is being transmitted between TOE components.	O.CRYPTOGRAPHY O.PROTECTCOM	O.CRYPTOGRAPHY requires that cryptographic hashing and encryption conform to the policy by mandating FIPS 140-2 validation. O.PROTECTCOM helps in mitigating this threat by ensuring that the TOE only uses secure communications paths that have been established by the TOE components for the transfer of data.
T.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources	O.TOEACESS OE.TOE_ACCESS	O.TOEACESS mitigates this threat by permitting authorized users to access TOE data and its resources OE.TOE_ACCESS mitigates this threat by requiring authorized ePO administrators 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.
T.RESIDUAL_DATA A user or process may gain	OE.RESIDUAL_INFORMATION	OE.RESIDUAL_INFORMATION counters this threat by

Threats, Policies and Assumptions	Objectives	Rationale
unauthorized access to data through reallocation of memory used by the TOE to scan files or process administrator requests.		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, through an unsophisticated attack, TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted)	OE.RESIDUAL_INFORMATION OE.DOMAIN_SEPARATION O.MANAGE O.CORRECT_TSF_OPERATION OE.NO_BYPASS	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. OE.DOMAIN_SEPARATION is necessary so that the TSF is protected from other processes executing on the ePO server. 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 behaviour 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 cannot occur simply by bypassing the TSF
T.UNATTENDED_SESSION A user may gain unauthorized access to an unattended session.	O.TOE_ACCESS O.MANAGE OE.TOE_ACCESS	O.TOE_ACCESS helps to mitigate this threat by having the TOE control the user credentials and require a valid session prior to allowing access to the TSF. Locked sessions will no longer be considered valid and the administrator will have to re-authenticate. 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

Threats, Policies and Assumptions	Objectives	Rationale
		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 OE.AUDIT_SEARCH O.AUDIT_GENERATION OE.TIME_STAMPS	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 Virtual Machine to compromise data on that Virtual Machine, or use that Virtual Machine to attack additional systems.	O.VIRUS	O.VIRUS mitigates this threat by providing mechanisms to prevent a virus from being introduced onto a virtual machine
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	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	O.AUDIT_GENERATION O.TOE_ACCESS OE.TIME_STAMPS	O.AUDIT_GENERATION addresses this policy by recording security-relevant events. The administrator's ID

Threats, Policies and Assumptions	Objectives	Rationale
TOE shall be held accountable for their actions within the TOE.	OE. TOE_ACCEfSS	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. O.TOE_ACCESS supports this policy by allowing the TOE to identify and authenticate authorized administrators and prior to allowing any access to the TOE and its management functions. OE. TOE_ACCESS supports this policy by requiring the IT environment to identify and authenticate all authorized administrators and ePO Server 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).
P.CRYPTOGRAPHY Only NIST FIPS validated cryptography (methods and implementations) are acceptable for cryptographic hashing of DAT files.	O.CRYPTOGRAPHY	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	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 audit records and monitor disk	OE.AUDIT_BACKUP	OE.AUDIT_BACKUP addresses the assumption by requiring the audit records to be backed up, and by

Threats, Policies and Assumptions	Objectives	Rationale
usage to ensure audit information is not lost.		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	OE.DOMAIN_SEPARATION restates the assumption. The ePO Server's OS and hardware provide domain separation between processes
A.NO_BYPASS The IT environment will ensure the TSF cannot be bypassed.	OE.NO_BYPASS	OE.NO_BYPASS restates the assumption. The ePO Server's OS ensures the TSF is invoked.
A.NO_EVIL Administrators are non-hostile, appropriately trained, and follow all administrative guidance.	OE.NO_EVIL	OE.NO_EVIL restates the assumption.
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.	OE.PHYSICAL	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	OE.SECURE_COMMS restates the assumption. The ePO Server's 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 antivirus vendors, and for distributing the updates to the central management systems.	OE.SECURE_UPDATES	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.

5 EXTENDED SECURITY REQUIREMENT COMPONENTS DEFINITION

This section defines the extended Security Functional Requirements (SFRs) and extended Security Functional Assurance Requirements (SARs) met by the TOE.

5.1 Extended TOE Security Functional Requirement Components

This section specifies the extended SFRs for the TOE.

5.1.1 AntiVirus (FAV) Class of SFRs

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

5.1.1.1 FAV_ACT_EXT .1 Antivirus Actions

Hierarchical to: No other components.
Dependencies: FAV_SCN_EXT .1 Antivirus Scanning

FAV_ACT_EXT .1.1 Upon detection of a file based virus, the TSF shall perform the actions specified by the [assignment: role]. Actions are administratively configurable on a per Virtual Machine basis and consist of: [assignment: list of actions].

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

- 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:

- Basic: Action taken in response to detection of a virus.

Rationale
This SFR had to be defined because Part 2 of Common Criteria v3.1 does not provide a Security Functional Requirement for the action to be taken in the event of detection of a virus

5.1.1.2 FAV_SCN_EXT .1 Antivirus 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:

- Configuration of parameters for all types of scans.

Audit:
There are no auditable events foreseen.

Rationale
This SFR had to be defined because Part 2 of Common Criteria v3.1 does not provide a Security Functional Requirement that define the scanning process to detect the viruses.

5.2 Extended TOE Security Assurance Requirement Components

There are no extended TOE Security Assurance Requirement Components.

6 SECURITY REQUIREMENTS

This section defines the Security Functional Requirements (SFRs) and Security Functional Assurance Requirements (SARs) met by the TOE. .

6.1 Security Functional Requirements

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

Table 11 TOE Security Functional Requirements

Requirement Class	Requirement Name	Description
FAU 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
FAV Antivirus	FAV_ACT_EXT.1	Antivirus Actions
	FAV_SCN_EXT.1	Antivirus Scanning
FCS Cryptographic support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1(1)	Cryptographic operation (for McAfee Agent)
	FCS_COP.1(2)	Cryptographic operation (for ePO)
FIA Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UID.1	User Authentication
	FIA_UAU.1	Timing of authentication
	FIA_USB.1	User Subject Binding
FMT Security Management	FMT_MTD.1	Management of TSF data (for general TSF data)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security Roles
FPT Protection of TSF	FPT_ITT.1	Basic Internal TSF Data Transfer Protection

Requirement Class	Requirement Name	Description
FTA TOE Access	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

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[1];
b) All auditable events for the [not specified] level of audit;
c) [*Specifically defined auditable events listed in Table 12*]

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*the information detailed in Table 12*].

Table 12 Auditable Events

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_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

[1] The audit log is enabled on the TOE as soon as it starts and cannot be disabled or shut down independently. Thus if the TOE is running the audit log is considered to be running

COMPONENT	EVENT	DETAILS
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
FCS_CKM.1	None	None
FCS_CKM.4	None	None
FCS_COP.1(1)	None	None
FCS_COP.1(2)	None	None
FPT_ITT.1	None	None

6.1.1.2 FAU_GEN.2 User Identity Association

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*authorized users with Global Administrator status*] with the capability to read [*all the audit data*] 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

Hierarchical to: No other components.
Dependencies: FAU_SAR.1 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.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall **[**ignore auditable events**] and** [*restricts access to the ePO GUI*] if the audit trail **is full.**

Application Note: The TOE relies on the IT Environment to monitor disk space and send the appropriate alarm.

6.1.1.6 FAU_STG.1 Protected Audit Trail Storage

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

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

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

6.1.2 AntiVirus (FAV)

6.1.2.1 FAV_ACT_EXT .1 Antivirus Actions

Hierarchical to: No other components.
Dependencies: FAV_SCN_EXT .1 Antivirus Scanning

FAV_ACT_EXT .1.1 Upon detection of a file based virus, the TSF shall perform the actions specified by the [*Global Administrator*]. Actions are administratively configurable on a per Virtual Machine basis and consist of: [
a) deny the operation or delete the file AND
b) *optionally quarantine the file*].

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 3.0.0 for use with ePolicy Orchestrator® 4.6.0 and 5.0.0 Software"

6.1.2.2 FAV_SCN_EXT .1 Antivirus 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.

6.1.3 Cryptographic Support (FCS)

6.1.3.1 FCS_CKM.1 Cryptographic Key Generation

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

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

6.1.3.2 FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

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

6.1.3.3 FCS_COP.1 (1) Cryptographic Operation (for SVA)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 (1) The TSF shall perform [*the operations described below*] in accordance with a specified cryptographic algorithm [*algorithms in the modes of operation described below*] and cryptographic key sizes [*key sizes described below*] that meet the following: [*standards described below*].

Table 13 Cryptographic Operations

OPERATION	ALGORITHM (MODE)	KEY SIZE IN BITS	CAVP CERTIFICATE	STANDARDS
Encryption and Decryption	AES CBC and ECB mode	128, 192, 256	490	FIPS 197
	TDES in CBC	168	501	FIPS 46-3
Hashing	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		560	FIPS 180-3
Digital Signatures	DSA	Modulus Size: 1024	199	FIPS 186-3
	RSA	Modulus Size: 2048	203	ANSI X9.31 PKCS #1 v1.5
Random Number Generation	FIPS 186-2	N/A	270	FIPS 186-2

6.1.3.4 FCS_COP.1 (2) Cryptographic Operation (for ePO[2])

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 (2) The TSF shall perform [*the operations described below*] in accordance with a specified cryptographic algorithm [*algorithms in the modes of operation described below*] and cryptographic key sizes [*key sizes described below*] that meet the following: [*standards described below*].

Table 14 – Cryptographic Operations

OPERATION	ALGORITHM (MODE)	KEY SIZE IN BITS	CAVP CERTIFICATE	STANDARDS
Encryption and Decryption	AES CBC and ECB mode	128, 192, 256	2249, 2017	FIPS 197
	TDES in CBC	168	1408, 1302	FIPS 46-3
Hashing	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		1938, 1767	FIPS 180-3
Digital Signatures	DSA	Modulus Size: 1024	701, 642	FIPS 186-3
	RSA	Modulus Size: 2048,3072	1154 , 1046	ANSI X9.31 PKCS #1 v1.5

[2] This constitutes both the Crypto J-Save module as well as the Crypto-C module contained within the ePO code

OPERATION	ALGORITHM (MODE)	KEY SIZE IN BITS	CAVP CERTIFICATE	STANDARDS
Random Number Generation	FIPS 186-2	N/A	1057, 1123	FIPS 186-2

6.1.4 Identification and Authentication (FIA)

6.1.4.1 FIA_ATD.1 User Attribute Definition

Hierarchical to: No other components.
Dependencies: No Dependencies

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;

d) Global Administrator status; and

e) Permission Sets.

6.1.4.2 FIA_UAU.1 Timing of Authentication

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

FIA_UAU.1.1 The TSF shall allow [Antivirus actions] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.3 FIA_UID.1 Timing of Identification

Hierarchical to: No other components.
Dependencies: No Dependencies

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 IT environment for authentication when configured for external authentication. Authentication on the managed systems is the responsibility of the operating environment in that scenario.

6.1.4.4 FIA_USB.1 User-Subject Binding

Hierarchical to: No other components.
Dependencies: No Dependencies

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

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
Antivirus Scan Policy Settings	Files to be scanned	Modify, exclude
	Actions to be taken on a Virtual Machine 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
System Tree	View System Tree	Query

6.1.5.2 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No Dependencies

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

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

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 read-only permissions.

6.1.6 Protection of the TSF (FPT)

6.1.6.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

Hierarchical to: No other components.
Dependencies: No Dependencies

FPT_ITT.1.1 The TSF shall protect **non-public** TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE **through the use of TLS**.

Application Note: This requirement ensures all sensitive communications between McAfee Agent and ePO are protected through the use of an encrypted communications channel. Public data reflects the antivirus signature updates which are publically available from McAfee. These updates are downloaded over HTTP and verified against a known SHA hash.

6.1.7 TOE Access (FTA)

6.1.7.1 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.
Dependencies: No Dependencies

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [configurable duration in minutes].

6.1.7.2 FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.
Dependencies: No Dependencies

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

Application Note: This requirement ensures all communications between McAfee Agent and ePO are protected through the use of an encrypted communications channel.

6.2 Security Assurance Requirements

This section defines the Security Assurance Requirements (SARs) for the TOE. The assurance requirements are taken from EAL 2 components as specified in Part 3 of the CC and are augmented with ALC_FLR.2 requirements. The assurance components are summarized in the following table:

Table 15 – Security Assurance Requirements

CLASS	FAMILY	DESCRIPTION
ASE: Security Target	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
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

6.3 Dependency Rationale

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.

Table 16 – Dependency 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
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_SCN_EXT.1	None	None	None
FCS_CKM.1	None	[FCS_CKM.2 , or FCS_COP.1] FCS_CKM.4	Satisfied
FCS_CKM.4	None	[FDP_ITC.1, or FDP_ITC.2 , or FCS_CKM.1]	Satisfied
FCS_COP.1	None	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1],FCS_CKM.4	Satisfied.
FIA_ATD.1	None	None	None
FIA_UAU.1	None	FIA_UID.1	Satisfied.
FIA_UID.1	None	None	None
FIA_USB.1	None	FIA_ATD.1	Satisfied
FMT_MTD.1	None	FMT_SMF.1,FMT_SMR.1	Satisfied
FMT_SMF.1	None	None	None
FMT_SMR.1	None	FIA_UID.1	Satisfied
FPT_ITT.1	None	None	None
FTA_SSL.3	None	None	None
FTA_SSL.4	None	None	None

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:

Table 17 – Mapping of SFR's to Objectives

SFR Mapped to Objectives	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.MANAGE	O.PROTECTCOM	O.TOEACCESS	O.VIRUS
FAU_GEN.1		X			X					
FAU_GEN.2		X			X					
FAU_SAR.1				X	X					
FAU_SAR.2			X							
FAU_STG.1			X							
FAU_STG.4			X							
FAV_ACT_EXT.1					X					X
FAV_SCN_EXT.1					X					X
FCS_CKM.1						X				
FCS_CKM.4						X				
FCS_COP.1						X				
FIA_ATD.1	X									
FIA_UAU.1									X	
FIA_UID.1							X			
FIA_USB.1	X									
FMT_MTD.1	X						X			
FMT_SMF.1							X			
FMT_SMR.1	X						X			
FPT_ITT.1								X		

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

Security Objective	SFR	Rationale

Security Objective	SFR	Rationale
O.ADMIN_ROLE	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_GENERATION	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.
O.AUDIT_PROTECT	FAU_SAR.2 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. 000 FAU_STG.1 restricts the ability to delete audit records to the Global Administrator. This requirement also ensures that no one has the ability to modify audit records (e.g., edit any of

Security Objective	SFR	Rationale
		the information contained in an audit record). This helps to ensure that audit records are kept until the Global Administrator deems they are no longer necessary as well as the integrity of the audit log. 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.
O.AUDIT_REVIEW	FAU_SAR.1	FAU_SAR.1 provides the ability to review the audits in a user-friendly manner.
O.CORRECT_TSF_OPERATION	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAV_SCN_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	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.
O.MANAGE	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.PROTECTCOM	FPT_ITT.1	FPT_ITT.1 protects all data from modification and ensures its integrity when the data is transmitted to another TOE component
O.TOEACESS	FIA_UAU.1	FIA_UAU.1 requires authorized access to the TOE using an identification and authentication process
O.VIRUS	FAV_SCN_EXT .1	FAV_SCN_EXT .1 requires that the TOE scan for viruses.

Security Objective	SFR	Rationale
	FAV_ACT_EXT .1	FAV_ACT_EXT .1 requires that the TOE take action against viruses once they are detected..

7 TOE SUMMARY SPECIFICATION

This section presents information to detail how the TOE meets the security functional requirements described in previous sections of this ST.

7.1 Audit

7.1.1 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 the ePO server and the VM's monitored by the SVA. Logs are generated on the ePO server and transmitted over TLS between the components. Regardless of their origin, both of these types of logs are stored in the DBMS within the ePO server of the TOE.

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

Client events— Events that occur on managed systems. For example, "Product update succeeded."

- Threat events— Events that indicate a possible threat is detected. For example, "Virus detected."
- Server events— Events that occur on the server. For example, "Repository pull failed.

The ePO can be configured to automatically trigger an action in response to the various types of events; including threat, client, and server events. SVA 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 VM are queued on the VM, 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 SVA are stored in the ePO database. Queued Events are uploaded to the ePO server. The client uses disk space available on the ePO Server for queuing events. The IT environment manages shortages of available disk space on the ePO Server. 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 VM until the ePO server is again able to accept connections. The audit function operates whenever ePO/SVA are operating. If an instance of an SVA on a Hypervisor is enabled or disabled by the Global Administrator, an audit record is generated.

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

7.1.2 Audit Record Review

Audit record review is provided by the ePO server and stored in the DBMS of this 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 table. The Audit Log display includes:

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

The Audit Log entries are automatically purged from the database 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.

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.

7.2 Virus Scanning

The TOE provides real-time virus detection, and scanning occurs when files are either read from or written to the VM the SVA is protecting.

When an infection occurs, the TOE takes certain actions depending on what has been configured, the files can be either quarantined to a specified location or the file with the malicious content can be blocked. An audit record is written to ePO detailing this action.

7.3 Authentication and Management

The TOE's Management Security Function provides administrator support functionality that enables a user to configure and manage TOE components. Management of the TOE 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 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:

- ePO User Accounts and Permission Sets,
- Audit Log,
- Event Log,
- Notifications,
- System Tree,
- Queries,
- Dashboards,

- Antivirus settings,
- Virus scan signatures.
- Quarantined files
- Policy

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

7.3.1 ePO User Account Management and Permission Sets

Each user authorized for login to ePO must be defined with ePO as having permissions to the TOE. Credentials for each user can be defined locally within the ePO application or within Windows on the ePO server. Both configurations are covered by this evaluation.

Each individual must be successfully identified and authenticated using a username and password by the ePO before access is allowed to the TOE. The verification of the user may happen in two ways. The first is through an application account within ePO which is solely used for ePO. The second method of storing and validating credentials relies on Windows. ePO can be configured to use a Windows service for user identification and authentication. This user Identification & Authentication relies on the Operational Environment to provide an external authentication service if Windows authentication is configured. The operational environment will provide a trusted communication between the external authentication server and the TOE.

Only Global Administrators may perform ePO user account management functions (create, view, modify and delete). For each defined account, the following information is configured:

- User name
- Enabled or disabled
- Whether authentication for this user is to be performed by McAfee ePO authentication, Windows authentication, or Certificate Based Authentication
- Permission sets granted to the user
- 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:

- Create, edit, and delete source and fallback sites
- Change server settings, including session timeout value.
- Create and delete user accounts.
- Create, delete, and assign permission sets.
- Import events and 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:

- View audit log
- View and purge audit log
- View MOVE settings
- View and change MOVE settings

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.

7.3.2 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.

7.3.3 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.

7.3.4 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 recipients 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 destinations) 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:

- View notification rules and Notification Log - This permission also grants the ability to view SNMP servers.
- Create and edit notification rules; view Notification Log - This permission also grants the ability to view SNMP servers.
- 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.

7.3.5 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:

- Groups can be created by global administrators.
- A group can include both systems and other groups.
- 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:

- It can't be deleted.
- It can't be renamed.
- Its sorting criteria can't be changed (although you can provide sorting criteria for the subgroups you create within it.)
- It always appears last in the list and is not alphabetized among its peers.
- All users with view permissions to the System Tree can see systems in Lost Found.

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:

- View the "System Tree" tab
- 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.

7.3.6 Query Management

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

- Use public queries — Grants permission to use any queries that have been created and made public.
- 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.
- 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.

7.3.7 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:

- Use public dashboards
- Use public dashboards; create and edit personal dashboards
- Edit public dashboards; create and edit personal dashboards; make personal dashboards public

7.3.8 Antivirus Settings

When an infection occurs, the TOE takes certain actions depending on what has been configured to either quarantine or deny access to a file. Audit messages related to anti-virus actions can be displayed in the audit log of the ePolicy Orchestrator threat event log.

The scan policy determines which files are scanned for threats and when. By default, the TOE deployment option scans all uncompressed files when read from or written to disk. The McAfee program files and Windows service are excluded from scans.

7.3.9 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.

7.3.10 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.

7.3.11 Policy Management

ePolicy Orchestrator communicates policy information to the SVA on a regular interval through the McAfee Agent. The McAfee Agent enforces policies on the SVA, collects event information, and transmits the information back to ePolicy Orchestrator. Policy information is grouped into two categories: SVA and Scan. The SVA policy allows the administrator to define how and when anti-virus scans run on a hypervisor. These policies are applied to the hypervisor instead of the VM or system. The Scan policy allows the administrator to configure scan settings for when a threat is found. Administrators can create, modify, or delete as many policies as needed under these categories.

Policies are applied to any System Tree group or system by inheritance or assignment. Inheritance determines whether the policy settings for any system are taken from its parent. By default, inheritance is enabled throughout the System Tree and can be broken by direct policy assignment.

The Agentless deployment option, as managed by ePolicy Orchestrator, enables administrators to create policies and assign them without regard to inheritance. All groups and systems that are children of the selected system inherit the new policy in such scenarios

Using the VM-based scan configuration setting, the McAfee ePO administrator can enforce unique scan policies to different groups, resource pool, or specific virtual machines protected by MOVE-SVA on a hypervisor, even when McAfee Agent is not deployed to the client systems. The Scan policy can be applied to SVA machines or to a specific virtual machine, or group. When you enable the VM-based scan configuration setting, all VMs are protected by the Scan policy, which is assigned to VM or group. However, when this is disabled, the Scan policy that is assigned to SVA would be enforced to individual virtual machines. The Scan policy can be assigned to the system using system-based assignment or rule-based assignment in McAfee ePO. The Exclusions tab under the Scan policy enables an administrator to configure the Path Exclusions by adding, editing, or removing a path with explicit file, which is required to be prevented from being scanned. Scans against the administrator defined policy occur through identification of the guest VM using the vShield Endpoint framework and do not require authentication with the TOE.

7.4 Cryptographic Operations

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

The TOE also secures communications between components using cryptography. Specifically ePO implements a HTTPS secured GUI for the administration of the TOE. Additionally the TOE secures all

management between ePO and the various SVA appliances with TLS with the exception of the anti-virus updates which come from McAfee.

The TOE also uses a SHA-1 message digest in order to confirm the integrity of all antivirus updates which are downloaded to the SVA. The ePO server will download the updates to the ePO server and include an indication that there are updated antivirus signatures during the next agent-to-server communication. When the SVA sees a notification of updated signatures it will download them from the ePO server and compare them against the provided SHA-1 message digest.

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/140-1/1401val2013.htm#2056) and http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2013.htm#2057) 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. McAfee affirms that the RSA modules contained within ePO have been implemented according to their security policy when the TOE is configured in FIPS mode and that the TOE cryptographic operations run as expected.

7.5 Protection of the TSF

The agent has to talk to an ePolicy Orchestrator server periodically to ensure all settings are current and send events. These communications are referred to as agent-to-server communication. During each Agent-to-server communication, the agent collects its current system properties, as well as events that have not yet been sent, and sends them to the server. The server sends new or changed policies and tasks to the agent, and the repository list if it has changed since the last Agent-to-server communication. The agent enforces the new policies locally on the managed system and applies any task or repository changes. Should these changes include an update to the antivirus signatures used by the TOE they will be downloaded through a separate communication channel.

The ePolicy Orchestrator server uses an industry‑standard Transport Layer Security (TLS v1.2) network protocol for secure network transmissions. Communications between ePO and the McAfee Agent are encrypted using AES implemented by FIPS 140-2 validated modules. The TOE provides cryptography via CAVP-validated algorithm implementations, and the cryptographic module fulfills the requirements of FIPS 140-2 Overall Level 2 (see certificates 1588, 2056 and 2057).

7.6 TOE Access

The ePO Web GUI allows for sessions to be expired either manually via the logout button or automatically if they are left idle. The Administrator can configure the timeout value in the ePO GUI which is configured for all administrators globally. When this timer is reached ePO will remove the administrator's session from the session database and force re-authentication prior to any administrative actions being able to be performed.

8 ACRONYMS

Table 18 – Acronyms

Acronym	Definition
CBC	Cipher Block Chaining
CC	Common Criteria
CEM	Common Evaluation Methodology
CFB	Cipher Feedback
CSP	Critical Security Parameters
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ePO	ePolicy Orchestrator
FIPS	Federal Information Processing Standard
OFB	Output Feedback
OSP	Organizational Security Policy
PP	Protection Profile
RBG	Random Bit Generator
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality