Security Target

McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5

Document Version 1.3

October 12, 2011

Prepared For:	*Prepared By:*
McAfee, Inc.	Apex Assurance Group, LLC
2821 Mission College Blvd.	530 Lytton Avenue, Ste. 200
Santa Clara, CA 95054	Palo Alto, CA 94301
www.mcafee.com	www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1 Introduction

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

1.1 ST Reference

ST Title	Security Target: McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5
ST Revision	1.3
ST Publication Date	October 12, 2011
Author	Apex Assurance Group and McAfee

1.2 TOE Reference

TOE Reference	McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5
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[1] 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

[1] Derived from the IDSPP

TERM	DEFINITION
OS	Operating System
OSP	Organizational Security Policy
PC	Personal Computer
PP	Protection Profile
RAM	Random Access Memory
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSFI	TOE Security Function Interface

Table 2 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

VSE is a software package designed to protect Microsoft Windows-based desktop and server computers from viruses, worms, Trojans, as well as unwanted code and programs. VSE can be configured to scan local and network drives, as well as Microsoft Outlook and Lotus Notes email messages and attachments. It is possible to configure VSE to respond to infections and malicious code that it finds by identifying the intrusive entities, removing them, and reporting on them.

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

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

1.7 TOE Description

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

1.7.1 VSE

The VSE software provides protection from viruses, worms, Trojans, as well as unwanted code and programs

1.7.2 ePolicy Orchestrator (ePO)

ePO distributes and manages agents that reside on client systems. By using ePO you can manage a large enterprise network. ePO provides the management interface and functionality for the administrators of the TOE. It also provides centralized audit collection and review functionality.

1.7.3 McAfee Agent

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

1.7.4 Physical Boundary

The TOE is a software TOE and includes:

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

The physical components of the TOE include the software that is installed during installation of VSE, 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 systems with resident operating systems, but the operating systems are not part of the TOE.

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

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

1. *McAfee VirusScan Enterprise 8.8 Product Guide*
2. *McAfee® VirusScan® Enterprise 8.8 Installation Guide*
3. *McAfee ePolicy Orchestrator 4.5 Installation Guide*
4. *McAfee ePolicy Orchestrator 4.5 Product Guide*

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

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	VSE 8.8 ePolicy Orchestrator 4.5 McAfee Agent 4.5[2] Database Capacity Monitor Extension 1.0

[2] McAfee Agent 4.5 is shipped/packaged with ePO 4.5. From a clean installation, no additional steps are necessary to install McAfee Agent 4.5.

TOE COMPONENT	VERSION/MODEL NUMBER
IT Environment	Specified in the following: • Table 4 – Management System Component Requirements • Table 5 – Managed System Platforms

Table 3 – Evaluated Configuration for the TOE

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

1. All user accounts defined in ePO must specify Windows authentication.
2. Remote viewing of TOE log files on the clients is disabled.
3. Only authorized processes may initiate network connections to remote port 25 (SMTP). The Central Administrator configures the list of authorized processes.
4. The U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments requires the TOE to restrict specific management functionality to the Central Administrator role. At least one ePO user must be defined as a Central Administrator. For this TOE, the Central Administrator role is defined as an authorized administrator with Global Administrator status.
5. Because the U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments requires the TOE to restrict specific management functionality to the Central Administrator role, the following permissions may never be assigned:
    a. View audit log
    b. View and purge audit log
    c. View VSE settings
    d. View and change VSE settings

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.

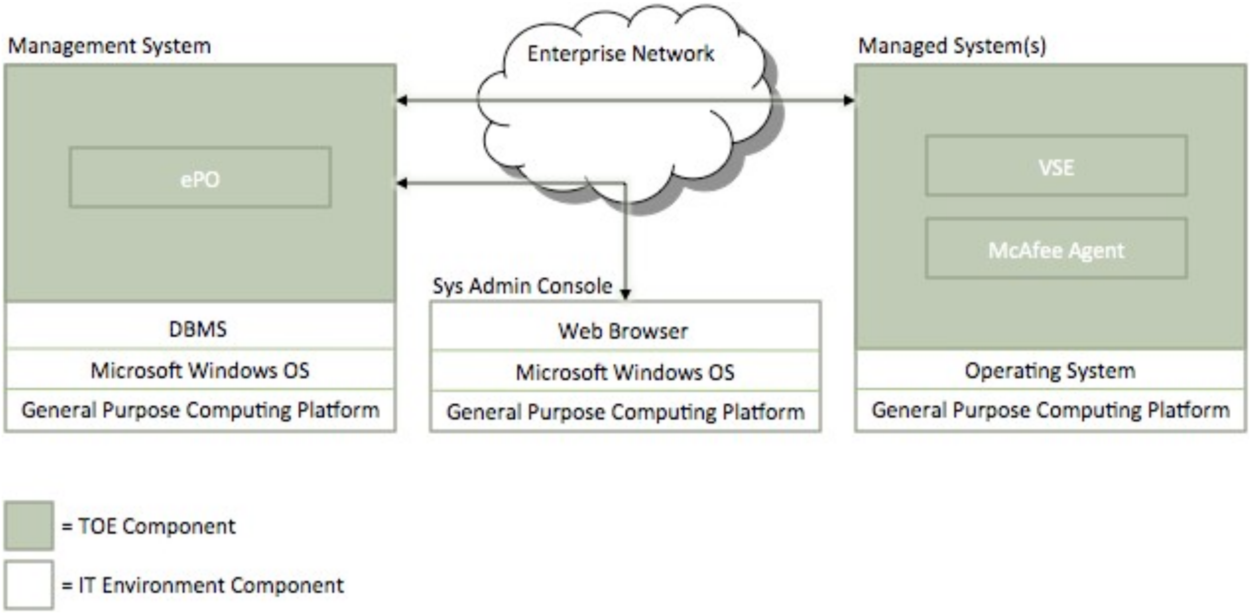

Figure 1 – TOE Boundary

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

1. The ability to protect against buffer overflows
2. The ability to identify spyware
3. The Scriptscan feature that scans JavaScript and VBScript scripts
4. The ability to update the TOE (scan engine). Note that the ability to update the virus signatures (DAT file) is included in the evaluation.
5. The optional Alert Manager product

1.7.5 Hardware and Software Supplied by the IT Environment

The TOE consists of a set of software applications. The hardware, operating systems and all third party support software (e.g., 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 III-class or higher; 1GHz or higher
Memory	1 GB RAM
Free Disk Space	1 GB
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	Windows Server 2003 Enterprise with Service Pack 2 or later Windows Server 2003 Standard with Service Pack 2 or later Windows Server 2003 Web with Service Pack 2 or later Windows Server 2003 R2 Enterprise with Service Pack 2 or later Windows Server 2003 R2 Standard with Service Pack 2 or later Windows Server 2008 Enterprise Windows Server 2008 Standard
DBMS	SQL Server 2005 SQL 2005 Express SQL 2008 SQL 2008 Express
Additional Software	MSXML 6.0 Internet Explorer 7 or 8, or Firefox 3.0 .NET Framework 2.0 Microsoft Visual C++ Redistributable Microsoft Visual C++ Redistributable - x86 9.0.21022 MDAC 2.8 Microsoft updates MSI 3.1 RSA Crypto-C ME 2.0 RSA Crypto-J 4.0
Network Card	Ethernet, 100Mb or higher
Disk Partition Formats	NTFS
Domain Controllers	The system must have a trust relationship with the Primary Domain Controller (PDC) on the network

Table 4 – Management System Component Requirements

The supported platforms for McAfee Agent and VSE are:

COMPONENT	MINIMUM REQUIREMENTS
Processor	Intel Pentium or Celeron processor running at a minimum of 166 MHz or Pentium II processor running at a minimum of 350 MHz
Memory	128MB RAM (minimum) for a Pentium or Celeron processor running at 166 MHz and 256MB RAM (minimum) for a Pentium II processor running at 350 MHz
Free Disk Space	240 MB
Browser	Microsoft Internet Explorer version 6.0 or later

COMPONENT	MINIMUM REQUIREMENTS
Operating System	**Server Operating Systems:** Microsoft Windows 2000 Server with SP4 Microsoft Windows 2000 Advanced Server with SP4 Microsoft Windows 2000 Datacenter Server with SP4 Microsoft Windows Server 2003 Standard (32-bit and 64-bit) with SP1 or SP2 Microsoft Windows Server 2003 Enterprise (32-bit and 64-bit) with SP1 or SP2 Microsoft Windows Server 2003 Web Edition (32-bit and 64-bit) with SP1 or SP2 Microsoft Windows Server 2003 R2 (32-bit and 64-bit) Standard, Enterprise, Web Edition Microsoft Windows Server 2003 R2 Datacenter Edition (32-bit and 64-bit) Microsoft Windows Storage Server 2003 Microsoft Windows Server 2008 (32-bit and 64-bit) Microsoft Windows Server 2008 Datacenter (32-bit and 64-bit) Microsoft Windows Server 2008 Datacenter (32-bit and 64-bit) Microsoft Windows Server Core 2008 (32-bit and 64-bit) Microsoft Windows 7 Home Premium, Professional, and Ultimate (32 and 64 bit) **Workstation Operating Systems:** Microsoft Windows 2000 Professional with SP4 Microsoft Windows XP Home with SP1, SP2, or SP3 Microsoft Windows XP Professional with SP1, SP2, or SP3 Microsoft Windows XP Tablet PC Edition with SP3 Microsoft Windows Vista Home Basic Microsoft Windows Vista Home Premium Microsoft Windows Vista Business Microsoft Windows Vista Enterprise Microsoft Windows Vista Ultimate 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 Platforms

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.

1.7.6 Logical Boundary

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

The TOE includes management interfaces that the administrator uses to configure the VSE policies and review the log files. The management interface is provided by both ePO and VSE. The virus scanning functionality is provided by VSE.

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	VSE provides the following functionality related to virus scanning and alerts: 1. Access Protection - This function protects ports, files, the registry and processes resident in memory from intrusions by restricting access to them. You can create rules to block either inbound or outbound ports, and by doing so, restrict access to files and residual data allocated in memory. If an outbreak occurs, the administrator can restrict access to the infected areas to prevent further infection until new signature files are released. 2. Email Scanning - This function provides scanning of messages and databases in order to identify viruses, worms, and Trojans for the purpose of removing them and reporting on them. 3. Automatic Updates – Allows signature (DAT) files to be updated automatically per the configured schedule.
Audit	The OnAccess Scan Log provides audit viewing capabilities on the client for that system. Audit information is concurrently generated for transmission to the ePO management databases. Audit logs for all clients can be reviewed from the ePO console.
Management	ePO enables the Central 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 audit logs.
Cryptographic Operation	VirusScan anti-virus packages are distributed to the workstation with a SHA-1 hash value used to verify the integrity of the package.

Table 6 – Logical Boundary Descriptions

1.7.7 TOE Data

TOE data consists of both TSF data and user data (information). TSF data consists of authentication data, security attributes, and other generic configuration information. Security attributes enable the 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.			✓
Dashboards	Collections of chart-based queries that are refreshed at a user-configured interval.			✓
Email Server	SMTP server name and port used to send email messages for notifications. Credentials may optionally be specified for authenticated interactions.			✓
ePO User Accounts	ePO user name, authentication configuration, enabled status, Global Administrator status and permission sets for each user authorized to access TOE functionality on ePO.	✓		
Global Administrator Status	Individual ePO user accounts may be configured as Global Administrators, which means they have read and write permissions and rights to all operations.		✓	
Groups	Node on the hierarchical System Tree that may contain subordinate groups or systems.			✓
Notification Rules	Rules associated with groups or systems used to generate email messages and/or SNMP traps upon receipt of specified events			✓
Permission	A privilege to perform a specific function.		✓	
Permission Set	A group of permissions that can be granted to any 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.			✓
VSE Access Protection Policies	Policies used to restrict access to specified ports, files, shares, registry keys, and registry values on the client systems.			✓
VSE DAT Files	Detection definition files used by VSE on the client systems.			✓
VSE On-Access Default Processes Policies	Policies that define the processes included in the default category, defining when scans for these processes are performed and the actions taken upon detection on the client systems.			✓
VSE On-Access General Policies	Policies that enable and configuration the operation of on-access scanning on the client systems.			✓
VSE On-Access High-Risk Processes Policies	Policies that define the processes included in the High-Risk category, defining when scans for these processes are performed and the actions taken upon detection on the client systems.			✓

TSF Data	Description	AD	UA	GE
VSE On-Access Low-Risk Processes Policies	Policies that define the processes included in the Low-Risk category, defining when scans for these processes are performed and the actions taken upon detection on the client systems.			✓
VSE On-Demand Scan Tasks	Tasks that define the configuration of on-demand scans that may be invoked on the client systems.			✓
VSE Quarantine Policies	Policies that specify where quarantined files are stored on the client systems and how long they are kept.			✓
VSE Quarantined Files	Collection of files on a client system that have been quarantined by VSE.			✓
VSE Unwanted Programs Policies	Policies that specify unwanted programs on the client systems.			✓
VSE User Interface Policies	Policies that control the access users have to the VirusScan Enterprise interface on the client systems.			✓

Table 7 – 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 claims demonstrable conformance to the U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments, version 1.2, dated 25 July 2007. Even though SFRs for the operational environment are not required to be identified in the security target under CC Version 3.1, the end user must refer to and comply with those SFRs in the PP in order to be compliant with the Protection Profile.

2.2.1 TOE Type Consistency

Both the PP and the TOE describe anti-virus systems.

2.2.2 Security Problem Definition Consistency

This ST claims demonstrable conformance to the referenced PP. The threats, assumptions, and organizational security policies in the ST are identical to the threats, assumptions, and organizational security policies in the PP.

2.2.3 Security Objectives Consistency

This ST claims demonstrable conformance to the referenced PP.

In conformance to the errata sheet of the PP, OE.AUDIT_SEARCH has been added to the security objectives of the Operational Environment and mapped to T.UNIDENTIFIED_ACTIONS. No other additions or deletions to the objectives have been made. All objectives are consistent with the PP.

2.2.4 Security Functional Requirements Consistency

This ST claims demonstrable conformance to the referenced PP.

In conformance to the errata sheet of the PP, FAU_SAR.3 has been levied on the Operational Environment.

An instance of FMT_SMR.1 has been added (as an iteration) to address functionality in the TOE to define additional administrative roles based upon user permissions. These additional roles may not be granted permission to view or manage VSE-specific policies, but may be granted permissions for other management functionality in the TOE (e.g. using or creating dashboards to review virus-related events).

An instance of FMT_SMF.1 has been added (as an iteration) to address functionality in the TOE to perform additional management operations based upon user permissions. These additional operations are not directly related to VSE, but provide support functions for effective management of the TOE.

An instance of FMT_MTD.1 has been added (as an iteration) to address the specific TSF data and operations on that data that may be performed by authorized administrators based upon their permissions.

FIA_ATD.1 and FIA_USB.1 have been added to the ST. These SFRs address the mechanisms used by the TOE to associate a role with each user, as required by FMT_SMR.1.

The TOE SFRs included in the ST are more restrictive than the TOE SFRs specified in the PP (after accounting for the errata sheets).

2.2.5 Security Assurance Requirements Consistency

The ST assurance claims are EAL2 augmented by ALC_FLR.2, which are the same as the assurance claims required by the PP (EAL2 augmented by ALC_FLR.2).

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.ACCIDENTAL_ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.AUDIT_ COMPROMISE	A user or process may gain unauthorized access to the audit trail and cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a security relevant event.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources
T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_IMPLEMENTATION	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_TEST	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being discovered thereby causing potential security vulnerabilities.
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.

THREAT	DESCRIPTION
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 via network traffic or removable media to compromise data on that workstation, or use that workstation to attack additional systems.

Table 8 – 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 key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e. encryption, decryption, signature, hashing, key exchange, and random number generation services)
P.MANUAL_SCAN	The authorized users of the workstations shall initiate manual anti-virus scans of removable media (e.g., floppy disks, CDs) introduced into the workstation before accessing any data on the removable media.
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 9 – Organizational Security Policies

3.3 Assumptions

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

ASSUMPTION	DESCRIPTION
A.AUDIT_BACKUP	Administrators will back up audit files and monitor disk usage to ensure audit information is not lost.

ASSUMPTION	DESCRIPTION
A.NO_EVIL	Administrators are non-hostile, appropriately trained, and follow all administrative guidance.
A.PHYSICAL	It is assumed that the appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
A.SECURE_COMMS	It is assumed that the IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.
A.SECURE_UPDATES	Administrators will implement secure mechanisms for receiving and validating updated signature files from the Anti-Virus vendors, and for distributing the updates to the central management systems.

Table 10 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure management.
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 selectively view audit information.
O.CONFIGURATION_IDENTIFICATION	The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified.
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 cryptographic services.
O.DOCUMENTED_DESIGN	The design of the TOE is adequately and accurately documented.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE.
O.PARTIAL_FUNCTIONAL_TEST	The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.
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.
O.VIRUS	The TOE will detect and take action against known viruses introduced to the workstation via network traffic or removable media.
O.VULNERABILITY_ANALYSIS	The TOE will undergo some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.

Table 11 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION

OBJECTIVE	DESCRIPTION
OE.AUDIT_BACKUP	Audit log files are backed up and can be restored, and audit log files 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 log files.
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_COMMS	The IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.
OE.SECURE_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 12 – Operational Environment Security Objectives

Application Note: OE.AUDIT_SEARCH has been added to the security objectives of the IT Environment in conformance to the PP errata sheet concerning FAU_SAR.3.

4.3 Security Objectives Rationale

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

	A.AUDIT_BACKUP	A.NO_EVIL	A.PHYSICAL	A.SECURE_COMMS	A.SECURE_UPDATES	T.ACCIDENTAL_ADMIN_ERROR	T.AUDIT_ COMPROMISE	T.MASQUERADE	T.POOR_DESIGN	T.POOR_IMPLEMENTATION	T.POOR_TEST	T.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNATTENDED_SESSION	T.UNIDENTIFIED_ACTIONS	T.VIRUS	P.ACCESS_BANNER	P.ACCOUNTABILITY	P.CRYPTOGRAPHY	P.MANUAL_SCAN	P.ROLES
O.ADMIN_GUIDANCE						✓															
O.ADMIN_ROLE																					✓
O.AUDIT_GENERATION															✓			✓			
O.AUDIT_PROTECT							✓														
O.AUDIT_REVIEW															✓						
O.CONFIGURATION_IDENTIFICATION									✓	✓											
O.CORRECT_TSF_OPERATION											✓		✓								
O.CRYPTOGRAPHY																			✓		
O.DOCUMENTED_DESIGN									✓		✓										
O.MANAGE													✓							✓	
O.PARTIAL_FUNCTIONAL_TEST										✓	✓										
O.PARTIAL_SELF_PROTECTION							✓						✓								
O.VIRUS																✓				✓	
O.VULNERABILITY_ANALYSIS									✓	✓	✓										
OE.AUDIT_BACKUP	✓																				
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					✓																

	A.AUDIT_BACKUP	A.NO_EVIL	A.PHYSICAL	A.SECURE_COMMS	A.SECURE_UPDATES	T.ACCIDENTAL_ADMIN_ERROR	T.AUDIT_COMPROMISE	T.MASQUERADE	T.POOR_DESIGN	T.POOR_IMPLEMENTATION	T.POOR_TEST	T.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNATTENDED_SESSION	T.UNIDENTIFIED_ACTIONS	T.VIRUS	P.ACCESS_BANNER	P.ACCOUNTABILITY	P.CRYPTOGRAPHY	P.MANUAL_SCAN	P.ROLES
OE.TIME_STAMPS															✓			✓			
OE.TOE_ACCESS								✓						✓				✓			

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

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

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
T.ACCIDENTAL_ADMIN_ ERROR: An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.	O.ADMIN_GUIDANCE: The TOE will provide administrators with the necessary information for secure management.	O.ADMIN_GUIDANCE helps to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is insecure.
T.AUDIT_ COMPROMISE: A user or process may cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	O.AUDIT_PROTECT: The TOE 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 log. OE.RESIDUAL_ INFORMATION: The TOE will ensure that any information contained in a protected resource within its Scope of Control	O.AUDIT_PROTECT contributes to mitigating this threat by controlling access to the individual audit log records. No one is allowed to modify audit records, 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

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
	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.	Environment to access the audit log file. 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 access to the resources under its control, which includes the audit trail which are always invoked is also critical to the migration of this threat. OE.NO_BYPASS ensures audit compromise can not occur simply by bypassing the TSF.
T.MASQUERADE: A user or process may	OE.TOE_ACCESS: The IT Environment will provide	OE.TOE_ACCESS mitigates this threat by requiring authorized

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
masquerade as another entity in order to gain unauthorized access to data or TOE resources.	mechanisms that control a user's logical access to the TOE.	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.POOR_DESIGN: Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.	O.CONFIGURATION_IDENTIFICATION: The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified. O.DOCUMENTED_DESIGN: The design of the TOE is adequately and accurately documented. O.VULNERABILITY_ANALYSIS: The TOE will undergo some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.CONFIGURATION_IDENTIFICATION plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design. O.DOCUMENTED_DESIGN ensures that the design of the TOE is documented, permitting detailed review by evaluators. O.VULNERABILITY_ANALYSIS_TEST ensures that the design of the TOE is analyzed for design flaws.
T.POOR_IMPLEMENTATION: Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.	O.CONFIGURATION_IDENTIFICATION: The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified. O.PARTIAL_FUNCTIONAL_TESTING: The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements. O.VULNERABILITY_ANALYSIS: The TOE will undergo some	O.CONFIGURATION_IDENTIFICATION plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's implementation. O.PARTIAL_FUNCTIONAL_TESTING increases the likelihood that any errors that do exist in the implementation will be discovered through testing. O.VULNERABILITY_ANALYSIS_TEST helps reduce errors in the

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
	vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	implementation that may not be discovered during functional testing. Ambiguous design documentation and the fact that exhaustive testing of the external interfaces is not required may leave bugs in the implementation undiscovered in functional testing.
T.POOR_TEST: Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities.	O.DOCUMENTED_DESIGN The design of the TOE will be adequately and accurately documented. O.PARTIAL_FUNCTIONAL_TESTING: The TOE will undergo some security functional testing that demonstrates the TSF satisfies the security functional requirements. 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.VULNERABILITY_ANALYSIS: The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.DOCUMENTED_DESIGN helps to ensure that the TOE's documented design satisfies the security functional requirements. In order to ensure the TOE's design is correctly realized in its implementation, the appropriate level of functional testing of the TOE's security mechanisms must be performed during the evaluation of the TOE. O.PARTIAL_FUNCTIONAL_TESTING increases the likelihood that any errors that do exist in the implementation will be discovered through testing. O.CORRECT_TSF_OPERATION provides assurance that the TSF continues to operate as expected in the field. O.VULNERABILITY_ANALYSIS_TEST addresses this concern by requiring a vulnerability analysis be performed in conjunction with testing that goes beyond functional testing. This objective provides a measure of confidence that the TOE does not contain security flaws that may not be identified through functional testing.
T.RESIDUAL_DATA: A user or process may gain unauthorized access to data through	OE.RESIDUAL_INFORMATION: The IT Environment will ensure that any information contained in a protected resource within the TOE	OE.RESIDUAL_INFORMATION counters this threat by ensuring that memory contents are not persistent when resources are

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
reallocation of memory used by the TOE to scan files or process administrator requests.	Scope of Control is not released when the resource is reallocated.	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: 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.
T.UNATTENDED_ SESSION: A user may gain	OE.TOE_ACCESS: The IT environment will provide mechanisms that control a user's	OE.TOE_ACCESS helps to mitigate this threat by including mechanisms that place controls on

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
unauthorized access to an unattended session.	logical access to the TOE.	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 selectively 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 Security 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 logs by making it easier to focus on particular events of interest. O.AUDIT_GENERATION helps to mitigate this threat by recording actions for later review. OE.TIME_STAMPS helps to mitigate this threat by ensuring that audit records have correct timestamps.
T.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 via network traffic or removable media.	O.VIRUS mitigates this threat by providing mechanisms to prevent a virus from being introduced onto a workstation.
P.ACCESS_BANNER: The system shall display an initial banner	OE.DISPLAY_BANNER: The IT Environment will display an advisory warning regarding use of	OE.DISPLAY_BANNER satisfies this policy by ensuring that the system displays a banner that provides all

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.	the system.	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, this PP allows unauthenticated users 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 key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption,	O.CRYPTOGRAPHY: The TOE shall use NIST FIPS 140-2 validated cryptographic services.	O.CRYPTOGRAPHY requires that cryptographic services conform to the policy by mandating FIPS 140-2 validation.

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
decryption, signature, hashing, key exchange, and random number generation services).		
P.MANUAL_SCAN: The authorized users of the workstations shall initiate manual anti-virus scans of removable media (e.g., floppy disks, CDs) introduced into the workstation before accessing any data on that removable media.	O.VIRUS: The TOE will detect and take action against known viruses introduced to the workstation via network traffic or removable media. 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 requires the TOE to provide the capability to perform manual scans of removable media. O.MANAGE provides the workstation user with the ability to invoke the manual scan capability.
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 files and monitor disk usage to ensure audit information is not lost.	OE.AUDIT_BACKUP: Audit log files are backed up and can be restored, and audit log files will not run out of disk space.	OE.AUDIT_BACKUP addresses the assumption by requiring the audit log files to be backed up, and by requiring monitoring of disk space usage to ensure space is available.
A.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.
A.PHYSICAL:	OE.PHYSICAL:	OE.PHYSICAL restates the

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
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.	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.	assumption.
A.SECURE_COMMS: It is assumed that the IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.	OE.SECURE_COMMS: The IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.	OE.SECURE_COMMS restates the assumption. The workstation OS will provide a secure line of communication for the TOE.
A.SECURE_UPDATES: Administrators will implement secure mechanisms for receiving and validating updated signature files from 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 14 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 Anti-Virus (FAV) Class of SFRs

All of the components in this section are taken from the *U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments*, version 1.2, dated 25 July 2007.

This class of requirements is taken from the Anti-Virus PP to specifically address the detection and response capabilities of anti-virus products. 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 memory based virus, the TSF shall prevent the virus from further execution.

FAV_ACT_(EXT).1.2 Upon detection of a file-based virus, the TSF shall perform the action(s) specified by the Central Administrator. Actions are administratively configurable on a per-workstation basis and consist of:

a) Clean the virus from the file

b) Quarantine the file,

c) Delete the file,

d) [selection: [assignment: list of other actions], no other actions].

FAV_ACT_(EXT).1.3 The TSF shall actively monitor processes attempting to access a remote system using TCP or UDP remote port 25 (SMTP) and block traffic from unauthorized processes defined by [assignment: ST author to complete] and simultaneously permit traffic from authorized process defined by [assignment: ST author to complete].

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.

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 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.

FAV_ALR_(EXT).1.2 The TSF shall continue to display the alerts on the screen of the workstation until they are acknowledged by the user of the workstation, or the user session ends.

FAV_ALR_(EXT).1.3 Upon receipt of an audit event from a workstation indicating detection of a virus, the TSF shall display an alert on the screen of the Central Administrator if a session is active. The alert shall identify the workstation originating the audit event, the virus that was detected, and the action taken by the TOE.

FAV_ALR_(EXT).1.4 The TSF shall continue to display the alerts on the screen of the Central Administrator until they are acknowledged by the Central Administrator, or the Central Administrator session ends.

Application Note: The deletion of such audit alerts is necessary in some scenarios (e.g. a rampant outbreak of virus infection) to prevent failure due to the enormous number of generated alerts exhausting system or administrator resources. FAV_ALR_(EXT).1.4 requires the administrator acknowledge the alerts generated. A large number of alerts requiring acknowledgement, particularly during a short period of time, may prevent the administrator from adequately responding to the overall incident. If deletion of alerts is deemed necessary, the vendor must analyze the different scenarios that could occur in order to derive a comprehensive justification for deleting alerts. The solution must take into account such factors as the type of alerts, whether to delete the oldest or the newest alerts generated, and any other relevant factors based on the scenarios that might occur.

Application Note: The analysis used to determine which alerts are deleted should be publicly documented in the Security Target and noted in the associated Validation Report.

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.

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 memory based viruses based upon known signatures.

FAV_SCN_(EXT).1.2 The TSF shall perform real-time, scheduled, and on-demand scans for file-based viruses based upon known signatures.

FAV_SCN_(EXT).1.3 The TSF shall perform scheduled scans at the time and frequency configured by the Central Administrator.

FAV_SCN_(EXT).1.4 The TSF shall perform manually invoked scans when directed by the Workstation User.

Management:

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

a) Configuration of scheduled scans.

b) 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-NIAP-0347	Audit Data Generation
	FAU_GEN.2-NIAP-0410	User Identity Association
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_STG.1-NIAP-0429	Protected Audit Trail Storage
	FAU_STG.NIAP-0414-NIAP-0429	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_COP.1	Cryptographic Operation
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_USB.1	User-Subject Binding
Security Management	FMT_MOF.1	Management of Security Functions Behavior
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles

Table 15 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1.1-NIAP-0347 Audit Data Generation

FAU_GEN.1.1-NIAP-0347 The TSF shall be able to generate an audit record of the following auditable events:

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

b) All auditable events for the *minimum* level of audit; and

c) *The events identified in the following table*

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

a) Date and time of the event, type of event, subject identity, 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-NIAP-0347	None	Not applicable
FAU_GEN.2-NIAP-0410	None	Not applicable
FAU_SAR.1	None	Not applicable
FAU_SAR.2	None	Not applicable
FAU_STG.1-NIAP-0429	None	Not applicable
FAU_STG.NIAP-0414-NIAP-0429	Selection of an action	Action selected
FAV_ACT_(EXT).1	Action taken in response to detection of a virus	Virus detected, action taken, file or process identifier where virus is detected
FAV_ALR_(EXT).1	None	Not applicable
FAV_SCN_(EXT).1	None	Not applicable
FCS_COP.1	Success and failure, and the type of cryptographic operation	Not applicable
FIA_ATD.1	None (No tested secrets apply).	Not applicable
FIA_USB.1	None (The binding of attributes to the subject never fails, per TOE design).	Not applicable
FMT_MOF.1	None	Not applicable
FMT_MTD.1	None	Not applicable
FMT_SMF.1	Use of the management functions	User identity, function used
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Table 16 – Audit Events and Details

Application Note: FAU_SAR.3 has been levied on the Operational Environment rather than the TOE in conformance to the PP errata sheet. Therefore FAU_SAR.3 was removed from the table above.

6.1.1.2 FAU_GEN.2-NIAP-0410 User Identity Association

FAU_GEN.2.1-NIAP-0410 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1(1) **Refinement:** The TSF shall provide the Central Administrator with the capability to read all audit information from the audit records **on the central management system.**

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

Application Note: Audit logs related to VSE are referred to as events in ePO, while audit logs related to administrator actions are referred to as audits in ePO. Since the PP refers to all of these logs as audits, this requirement is interpreted as requiring both event log and audit log review on ePO.

FAU_SAR.1.1(2) **Refinement:** The TSF shall provide the Central Administrator and Workstation Users with the capability to read all audit information from the audit records **on the workstation being used.**

FAU_SAR.1.2(2) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application Note: The Workstation User is permitted to review all audit records saved on the workstation being used by that user. The Central Administrator is permitted to review all logs on a specific workstation (which will only apply to that workstation) or on the central management system (which will apply to all workstations within that domain).

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-NIAP-0429 Protected Audit Trail Storage

FAU_STG.1.1-NIAP-0429 **Refinement:** The TSF shall protect the stored audit records in the audit trail from unauthorised deletion **via the TSFI.**

FAU_STG.1.2-NIAP-0429 **Refinement:** The TSF shall be able to *prevent* unauthorised modifications to the audit records in the audit trail **via the TSFI.**

Application Note: FAU_STG.1-NIAP-0429 applies to both the central management system and the individual workstations.

Application Note: This instance of FAU_STG.1-NIAP-0429 applies to protection of the audit records via the TSFI. The IT Environment (OS) is responsible for preventing deletion of the audit file via OS interface.

6.1.1.6 FAU_STG.-0414-NIAP-0429 Site-Configurable Prevention of Audit Loss

FAU_STG.NIAP-0414-1-NIAP-0429(1) **Refinement:** The TSF shall provide the administrator the capability to select one or more of the following actions overwrite the oldest stored audit records and *no other actions* to be taken if the **workstation permanent** audit trail is full.

FAU_STG.NIAP-0414-2-NIAP-0429(1) **Refinement:** The TSF shall overwrite the oldest stored audit records if the **workstation permanent** audit trail is full and no other action has been selected.

FAU_STG.NIAP-0414-3-NIAP-0429(1) **Refinement:** The TSF shall alert the administrator **on a configured** percent free audit storage space available before **workstation permanent** audit storage reaches capacity.

Application Note: The selection has been refined to clarify that the alert is generated at a percentage of storage space configured by an administrator rather than a fixed amount.

Application Note: Workstation permanent audit trail and workstation permanent audit storage refer to the permanent log of audit records maintained on each workstation on which the TOE is installed..

FAU_STG.NIAP-0414-1-NIAP-0429(2) **Refinement:** The TSF shall provide the administrator the capability to select one or more of the following actions ignore auditable events and *no other actions* to be taken if the **workstation transient or central management system** audit trail is full.

FAU_STG.NIAP-0414-2-NIAP-0429(2) **Refinement:** The TSF shall ignore auditable events if the **workstation transient or central management system** audit trail is full and no other action has been selected.

FAU_STG.NIAP-0414-3-NIAP-0429(2) **Refinement:** The TSF shall alert the administrator **on a configured percentage of** free audit storage space available before **central management system** audit storage reaches capacity.

Application Note: The selection has been refined to clarify that the alert is generated at a percentage of storage space configured by a administrator rather than a fixed amount.

Application Note: The single instance of this SFR from the PP has been iterated and refined. Audit records generated on the workstation are stored locally as well as being forwarded to the central management system. The first iteration applies to the audit file that is permanently maintained on the workstation for review by the local workstation user. The second iteration applies to audit records being forwarded from the workstations to the central management system and to the database on the central management system in which the audit records are stored. Since permanent storage is only provided on *the central management system, the third element in the second iteration only applies to the central management system.*

Application Note: Workstation transient audit trail and workstation transient audit storage refer to the temporary storage of audit records waiting to be transmitted from a workstation on which the TOE is installed to ePO.

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 memory based virus, the TSF shall prevent the virus from further execution.

FAV_ACT_(EXT).1.2 Upon detection of a file-based virus, the TSF shall perform the action(s) specified by the Central Administrator. Actions are administratively configurable on a per-workstation basis and consist of:

a. Clean the virus from the file

b. Quarantine the file,

c. Delete the file,

d. <u>No other actions</u>.

FAV_ACT_(EXT).1.3 The TSF shall actively monitor processes attempting to access a remote system using TCP or UDP remote port 25 (SMTP) and block traffic from unauthorized processes defined by *comparing a request for network port access to the VSE Access Protection Policies* and simultaneously permit traffic from authorized process defined by *taking no additional actions*.

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.

FAV_ALR_(EXT).1.2 The TSF shall continue to display the alerts on the screen of the workstation until they are acknowledged by the user of the workstation, or the user session ends.

FAV_ALR_(EXT).1.3 Upon receipt of an audit event from a workstation indicating detection of a virus, the TSF shall display an alert on the screen of the Central Administrator if a session is active. The alert shall identify the workstation originating the audit event, the virus that was detected, and the action taken by the TOE.

FAV_ALR_(EXT).1.4 The TSF shall continue to display the alerts on the screen of the Central Administrator until they are acknowledged by the Central Administrator, or the Central Administrator session ends.

6.1.2.3 FAV_SCN_(EXT).1 Anti-Virus Scanning

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

FAV_SCN_(EXT).1.2 The TSF shall perform real-time, scheduled, and on-demand scans for file-based viruses based upon known signatures.

FAV_SCN_(EXT).1.3 The TSF shall perform scheduled scans at the time and frequency configured by the Central Administrator.

FAV_SCN_(EXT).1.4 The TSF shall perform manually invoked scans when directed by the Workstation User.

6.1.3 Cryptographic Support (FCS)

6.1.3.1 FCS_COP.1 Cryptographic Operation

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

a. *ePO User name;*

b. *Enabled or disabled;*

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

d. *Global Administrator status; and*

e. *Permission Sets*.

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

6.1.4.2 FIA_USB.1 User-Subject Binding

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

a. ePO User name;

b. Permissions.

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

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

Application Note: The TOE binds security attributes to subjects for ePO sessions. Windows binds security attributes to subjects for workstation sessions.

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 login.

6.1.5 Security Management (FMT)

6.1.5.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1(1) The TSF shall restrict the ability to *determine the behaviour of, disable, enable* the functions

a. Auditing,

b. Real-time virus scanning, and

c. Scheduled virus scanning

to the Central Administrator.

FMT_MOF.1.1(2) The TSF shall restrict the ability to *modify the behavior of* the functions manually invoked virus scanning to Workstation Users.

6.1.5.2 FMT_MTD.1 Management of TSF Data

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

a) Actions to be taken on workstations when a virus is detected,

b) Files to be scanned automatically on workstations,

c) Minimum depth of file scans on workstations,

d) Scheduled scan frequency on workstations,

e) Processes authorized to transmit data to a remote system using TCP or UDP remote port 25 (SMTP)

f) Virus scan signatures and

g) Audit logs on the central management system

to the Central Administrator.

Application Note: The TSF data referenced in this SFR corresponds to the VSE policies identified in Table 7 – TOE Data (Legend: AD=Authentication data; UA=User attribute; GE=Generic Information)*.*

FMT_MTD.1.1(2) The TSF shall restrict the ability to *modify* the

a) Depth of file scans on manually invoked scans on workstations and

b) Files to be scanned manually on workstations

to the Central Administrator and Workstation Users.

FMT_MTD.1.1(3) The TSF shall restrict the ability to *query, delete* the audit logs on the workstation being used to the Central Administrator and Workstation Users.

FMT_MTD.1.1(4) The TSF shall restrict the ability to query, modify, delete, *create and use* the *TSF data identified in the following table* to *a user with the permissions identified in the following table or a Global Administrator*.

TSF Data	Associated Permission	Operations Permitted
Contacts	Create and edit contacts	Query, create, delete and modify
	Use contacts	Use
Dashboards	Use public dashboards	Query and use public dashboards
	Use public dashboards; create and edit personal dashboards	Query and use public dashboards; create and modify personal dashboards
	Use public dashboards; create and edit personal dashboards; make personal dashboards public	Query and use public dashboards; create, delete and modify personal dashboards
Email Servers	View notification rules and Notification Log	Query
	Create and edit notification rules; view Notification Log	Query

TSF Data	Associated Permission	Operations Permitted
	Create and edit notification rules; view and purge Notification Log; create and edit SNMP servers and external commands	Query, create, delete and modify
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	n/a (only allowed by a Global Administrator)	Query, create, delete and modify
Notification Rules	View notification rules and Notification Log	Query
	Create and edit notification rules; view Notification Log	Query, create, delete and modify
	Create and edit notification rules; view and purge Notification Log; create and edit SNMP servers and external commands	Query, create, delete and modify
Permission Set	n/a (only allowed by a Global Administrator)	Query, create, delete, modify
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
SNMP Trap Destination(s)	View notification rules and Notification Log	Query
	Create and edit notification rules; view Notification Log	Query
	Create and edit notification rules; view and purge Notification Log; create and edit SNMP servers and external commands	Query, create, delete and modify
System Event Audit Configuration	n/a	Query and modify

TSF Data	Associated Permission	Operations Permitted
System Information	Access to the specific group node in the tree	Query
	"View System Tree tab", access to the specific group node in the tree, and "Edit System Tree groups and systems"	Query, create, delete and modify
System Tree	View System Tree tab and access to the specific group node in the tree	Query
	"View System Tree tab", access to the specific group node in the tree, and "Edit System Tree groups and systems"	Query, create, delete and modify

Table 17 - TSF Data Access Permissions

Application Note: This iteration of the SFR has been included to address additional capabilities of the TOE beyond that required by the PP.

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

6.1.5.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1(1) The TSF shall be capable of performing the following **security management functions**:

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

b) Configure operation of the TOE on workstations,

c) Update virus scan signatures,

d) Acknowledge alert notification from the central management system,

e) Review audit logs on the central management system,

f) Increase the depth of file scans on manually invoked scans,

g) Acknowledge alert notifications on the workstation being used, and

h) Review audit logs on the workstation being used.

Application Note: Audit logs related to VSE are referred to as events in ePO, while audit logs related to administrator actions are referred to as audits in ePO. Since the PP refers to all of these logs as audits, item e above is interpreted as requiring both event log and audit log review on ePO.

FMT_SMF.1.1(2) 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.*

Application Note: This iteration of the SFR has been included to address additional capabilities of the TOE beyond that required by the PP.

6.1.5.4 FMT_SMR.1 Security Roles

FMT_SMR.1.1(1) The TSF shall maintain the roles Central Administrator, Workstation User, Network User.

FMT_SMR.1.2(1) The TSF shall be able to associate users with roles.

Application Note: Per the evaluated configuration, the Central Administrator is an authorized ePO user with Global Administrator status.

Application Note: A Network User is a user of a remote IT system that sends network traffic to a workstation on which the TOE is installed. Although the Network User does not necessarily have any knowledge that s/he is interacting with the TOE, network traffic invokes the TSF. Network Users have no administrative access.

FMT_SMR.1.1(2) The TSF shall maintain the roles ePO users assigned any of the following permissions or combinations of permissions:

a. *Create and edit contacts*

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

c. *Create and edit notification rules; view Notification Log*

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

e. *Edit System Tree groups and systems*

f. *System permissions (to specific nodes)*

g. *Use contacts*

h. *Use public dashboards*

i. *Use public dashboards; create and edit personal dashboards*

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

k. *Use public queries*

l. *Use public queries; create and edit personal queries*

m. *View notification rules and Notification Log*

n. *View System Tree tab.*

FMT_SMR.1.2(2) The TSF shall be able to associate users with roles.

6.2 Security Assurance Requirements

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

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 18 – 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-NIAP-0347	None	FPT_STM.1	Satisfied by the Operational Environment
FAU_GEN.2-NIAP-0410	None	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied by the Operational Environment
FAU_SAR.1	None	FAU_GEN.1	Satisfied
FAU_SAR.2	None	FAU_SAR.1	Satisfied
FAU_STG.1-NIAP-0429	None	FAU_GEN.1	Satisfied
FAU_STG.NIAP-0414-NIAP-0429	FAU_STG.4	FAU_STG.1, FMT_MTD.1	Satisfied 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	Not satisfied. The only cryptographic function is a message digest that does not use keys.
FIA_ATD.1	None	None	None
FIA_USB.1	None	FIA_ATD.1	Satisfied
FMT_MOF.1	None	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	None	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	None	None	None
FMT_SMR.1	None	FIA_UID.1	Satisfied by the Operational Environment

Table 19 – TOE SFR Dependency Rationale

6.4 Security Requirements Rationale

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

6.4.1 Security Functional Requirements for the TOE

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

	O.ADMIN_GUIDANCE	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.CONFIGURATION_IDENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.DOCUMENTED_DESIGN	O.MANAGE	O.PARTIAL_FUNCTIONAL_TEST	O.PARTIAL_SELF_PROTECTION	O.VIRUS	O.VULNERABILITY_ANALYSIS
ALC_CMC.2						✓								
ALC_DEL.1	✓													
AGD_PRE.1	✓													
ADV_FSP.2									✓					
ADV_TDS.1									✓					
AGD_OPE.1	✓													
ALC_FLR.2						✓								
ATE_COV.1											✓			
ATE_FUN.1											✓			
ATE_IND.2											✓			
AVA_VAN.2														✓
FAU_GEN.1-NIAP-0347			✓				✓							
FAU_GEN.2-NIAP-0410			✓				✓							
FAU_SAR.1					✓		✓							
FAU_SAR.2				✓										
FAU_STG.1-NIAP-0429				✓										
FAU_STG.NIAP-0414-NIAP-0429				✓										
FAV_ACT_(EXT).1							✓						✓	
FAV_ALR_(EXT).1							✓						✓	
FAV_SCN_(EXT).1							✓						✓	
FCS_COP.1								✓						
FIA_ATD.1		✓												
FIA_USB.1		✓												
FMT_MOF.1		✓								✓				
FMT_MTD.1		✓								✓				
FMT_SMF.1		✓								✓				
FMT_SMR.1		✓								✓				
ADV_ARC.1												✓		

Table 20 – Mapping of TOE SFRs to Security Objectives

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

OBJECTIVE	REQUIREMENTS THAT ADDRESS THE OBJECTIVE	SFR AND RATIONALE
O.ADMIN_GUIDANCE The TOE will provide the administrators with the necessary information for secure management.	ALC_DEL.1 AGD_PRE.1 AGD_OPE.1	ALC_DEL.1 ensures that the administrator is provided documentation that instructs them how to ensure the delivery of the TOE, in whole or in parts, without tampering or corruption during delivery. This requirement ensures the administrator has the ability to begin their TOE installation with a clean (e.g. malicious code has not been inserted once it has left the developer's control) version of the TOE, which is necessary for secure management of the TOE. AGD_PRE.1 ensures the administrator has the information necessary to install the TOE in the evaluated configuration. Often times a vendor's product contains software that is not part of the TOE and has not been evaluated. The documentation ensures that once the administrator has followed the installation and configuration guidance the result is a TOE in a secure configuration. AGD_OPE.1 mandates the developer provide the administrator with guidance on how to operate the TOE in a secure manner. This includes describing the interfaces the administrator uses in managing the TOE, security parameters that are configurable by the administrator, how to configure the TOE's rule set and the implications of any dependencies of individual rules. The documentation also provides a description of how to setup and review the auditing features of the TOE.

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_MOF.1 FMT_MTD.1 FMT_SMR.1 FIA_ATD.1 FIA_USB.1	FMT_SMR.1 requires that the TOE establish a Central Administrator role. FMT_MOF.1 and FMT_MTD.1 specify the privileges that only the Central 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-NIAP-0347 FAU_GEN.2-NIAP-0410	FAU_GEN.1-NIAP-0347 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-NIAP-0410 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-NIAP-0429 FAU_STG.NIAP-0414-1-NIAP-0429	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-NIAP-0429 restricts the ability to delete audit records to the Security Administrator. FAU_STG.NIAP-0414-0429 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 Security 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 selectively view audit information.	FAU_SAR.1	FAU_SAR.1 provides the ability to review the audits in a user-friendly manner.
O.CONFIGURATION_IDENTIFICATION The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified.	ALC_CMC.2 ALC_FLR.2	ALC_CMC.2 addresses this objective by requiring that there be a unique reference for the TOE, and that the TOE is labeled with that reference. It also requires that there be a CM system in place, and that the configuration items that comprise the TOE be uniquely identified. This provides a clear identification of the composition of the TOE. ALC_FLR.2 addresses this objective by requiring that there be a mechanism in place for identifying flaws subsequent to fielding, and for distributing those flaws to entities operating the system.

OBJECTIVE	REQUIREMENTS THAT ADDRESS THE OBJECTIVE	SFR AND RATIONALE
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-NIAP-0347 FAU_GEN.2-NIAP-0410 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 services.	FCS_COP.1	FCS_COP.1 requires that the message digest used to verify integrity of the signature file utilizes a FIPS 140-2 Approved cryptographic algorithm.
O.DOCUMENTED_DESIGN The design of the TOE is adequately and accurately documented.	ADV_FSP.2 ADV_TDS.1	ADV_FSP.2 requires that the interfaces to the TOE be documented and specified. ADV_TDS.1 requires that the TOE design be documented and specified and that said design be shown to correspond to the interfaces.
O.MANAGE The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE.	FMT_MOF.1 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1	Restricted privileges are defined for the Central Administrator and Workstation Users. FMT_MOF.1 defines particular TOE capabilities that may only be used by the users. 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.

OBJECTIVE	REQUIREMENTS THAT ADDRESS THE OBJECTIVE	SFR AND RATIONALE
O.PARTIAL_FUNCTIONAL_TEST The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.	ATE_COV.1 ATE_FUN.1 ATE_IND.2	ATE_FUN.1 requires that developer provide test documentation for the TOE, including test plans, test procedure descriptions, expected test results, and actual test results. These needs to identify the functions tested, the tests performed, and test scenarios. They require that the developer run those tests, and show that the expected results were achieved. ATE_COV.1 requires that there be a correspondence between the tests in the test documentation and the TSF as described in the functional specification. ATE_IND.2 requires that the evaluators test a subset of the TSF to confirm correct operation, on an equivalent set of resources to those used by the developer for testing. These sets should include a subset of the developer run tests.
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.	ADV_ARC.1	ADV_ARC.1 provides the security architecture description of the security domains maintained by the TSF that are consistent with the SFRs. Since self-protection is a property of the TSF that is achieved through the design of the TOE and TSF, and enforced by the correct implementation of that design, self-protection will be achieved by that design and implementation.
O.VIRUS The TOE will detect and take action against known viruses introduced to the workstation via network traffic or removable media.	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.

OBJECTIVE	REQUIREMENTS THAT ADDRESS THE OBJECTIVE	SFR AND RATIONALE
O.VULNERABILITY_ANALYSIS The TOE will undergo some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.	AVA_VAN.2	The AVA_VAN.2 component provides the necessary level of confidence that vulnerabilities do not exist in the TOE that could cause the security policies to be violated. AVA_VAN.2 requires the evaluator to perform a search for potential vulnerabilities in all the TOE deliverables. For those vulnerabilities that are not eliminated by the developer, a rationale must be provided that describes why these vulnerabilities cannot be exploited by a threat agent with a basic attack potential, which is in keeping with the desired assurance level of this TOE. This component provides the confidence that security flaws do not exist in the TOE that could be exploited by a threat agent of basic attack potential to violate the TOE's security policies.

Table 21 – Rationale for Mapping of TOE SFRs to Objectives

6.4.2 Security Assurance Requirements

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

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Architecture Description: McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5
ADV_TDS.1: Basic Design	Basic Design: McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ALC_DEL.1: Delivery Procedures	Delivery Procedures: McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5
ATE_COV.1: Evidence of Coverage	Security Testing: McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5
ATE_FUN.1: Functional Testing	Security Testing: McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5
ATE_IND.2: Independent Testing – Sample	Security Testing: McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5

Table 22 – Security Assurance Measures

6.4.2.1 Rationale for TOE Assurance Requirements Selection

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

The general level of assurance for the TOE is:

1. Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.
2. Hierarchically stronger than or the same as the assurance requirements specified in the referenced PP.
3. The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 augmented byALC_FLR.2 from part 3 of the Common Criteria.

7 TOE Summary Specification

7.1 Virus Scanning & Alerts

The TOE provides real-time virus detection based on the settings that have been configured. The settings can be configured for all processes, or based on whether a process is classified as having a low-risk or high-risk of infection. Scanning occurs when files are either read from, or written to the computer the TOE client agent is installed on. Identification of a virus, worm, or Trojan is referred to as an "infection."

When an infection occurs, the TOE takes certain actions depending on what has been configured. There are Primary and Secondary actions that the TOE takes when an infection occurs. The primary actions that the TOE takes when an infection occurs:

- Cleaning of files automatically (after quarantining the original)
- Denying access to infected files
- Move infected files to a quarantine folder in email scanning. For stored files, the file is quarantined off-host before being deleted

Secondary actions are actions that the TOE takes if the Primary action fails. Secondary actions that the TOE takes on discovery of an infection include:

- Move infected files to a quarantine folder
- Denying access to infected files (quarantine)
- Delete infected files automatically

When a virus is detected (e.g. an infection occurs) the On-Access Scan Messages box pops up and remains on the screen until the user session ends, or until the alert is acknowledged.

Using ePO, an alert indicating a virus can be configured to display on the screen of the Central Administrator's console if a session is active (the Virus Alert List Box). The alert identifies the system where the infection has occurred, the name of the virus, and the action taken by the TOE.

An outbreak of virus infection in an enterprise environment could generate an enormous number of alerts. Unless the administrator is at his/her console and devoting himself or herself exclusively to the task of acknowledging alerts, and depending on the size of the server's memory, it is likely that the server will become disabled before the scope of the infection is realized.

In outbreak situations it is important to transmit adequate information about the outbreak to the administrator quickly. However, in order to free the administrator to take effective containment and repair activities, it is important that he or she not be required to remain seated at the console trying to acknowledge myriad events. The display of events on the console should not continue to display new events ad infinitum. The number of events displayed must be generous but limited in order to provide sufficient information while moderating the use of system memory.

The Virus Alert List Box meets these needs by providing a listbox on the console. When 1,000,000 events have been displayed, the listbox stops accepting new entries but the total number of events continues to be tallied and displayed. At any time, the administrator can clear the display of records, thus allowing new events to be displayed.

The Virus Scanning & Alert function provides the following capabilities:

- Email Scanning - This function provides scanning of messages in order to identify viruses, worms, and Trojans for the purpose of removing them and reporting on them. This capability is available for Microsoft Outlook and IBM Lotus Notes.
- Archive Scanning - The TOE can scan inside archives such as .zip files and MIME encoded files.
- Memory protection - The TOE provides in-memory process scanning and by doing so, stops viruses, worms, Trojans and their associated files from executing in memory. When a memory-based virus is detected, the process is stopped. Only a single pass of the On-Access scanner is required to remove all instances of a virus from memory.
- The TOE prevents unauthorized processes from sending email (via SMTP port 25) from the end-user's workstation.
- Anti-virus Scanning – By default, VSE examines executables and self-decompressing files by decompressing each file in memory and checking for virus signatures. These scan examinations occur in real-time, and alternatively can be scheduled by the Central Administrator, or performed on an ad-hoc manual basis by the workstation user. When manually invoked, the workstation user may control execution of the scan by specifying the files to be included.

7.2 Audit (AUDIT)

7.2.1 Audit Generation

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

VSE generates audits when viruses are detected. The audit event record includes 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 or process in which the virus was detected. The audit events for each workstation are stored on the workstation (permanent storage), and forwarded to the ePO event log.

If workstation storage limits for the audit log file are exceeded, VSE automatically discards the oldest events sufficient to free 20% of the configured file size and continues to record the most recent events. The default file size is 1 MB, but the administrator is directed to set the file size to a minimum of 10 MB.

Therefore, the TOE will retain at least the most recent 8 MB worth of audit records when the oldest events are discarded. During operation, the following information is periodically reported from each managed system to ePO: total drive space, total system drive space, free drive space and free system drive space. During TOE installation, a query is generated that identifies any systems with less than the desired percentage of free system drive space. A server task executes the query at configured intervals and emails the list of systems to a designated recipient, alerting the administrator that those systems are low on audit storage space.

Copies of all audits from the workstations are sent to a central management system (ePO), where they can be reviewed by the Central Administrator. The audit records are queued on the workstations for transmission to the management system (transient storage). In the unlikely event that the queue space is exhausted, new events are discarded and the oldest events are retained. Once events are transferred to a central management system and accepted, they are deleted from the queue on the workstations.

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

Audit records generated by ePO or VSE are stored in the ePO database. In the unlikely event that the storage (database) space is exhausted, new events are discarded and the oldest events are retained. During TOE installation, a server task is created to monitor the amount of storage space available for audits. If the storage space is low, an event is generated to alert administrators to the condition.

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

In the event that a VSE 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 also involves both the ePO server and the workstations executing VSE. VSE provides the capability to review audits generated on the local system, while ePO provides the capability to review audit records generated on all the systems.

7.2.2.1 Audit Review on Workstations

The TOE includes a VirusScan Console that generates an activity log for the virus scanning operations. The activity log is known in the GUI as the OnAccess Scan Log. The OnAccess Scan Log shows the engine and signature file version numbers (a.k.a. version number of DAT files) that were in effect when the scanning took place. The OnAccess Scan Log also shows the number of viruses found, and the actions the scanner took (e.g. cleaned, deleted, moved) in response to the viruses.

Using the On-Access Scan Statistics on the user workstation, the Workstation User or Central Administrator can find out a variety of information about the files that have been scanned including the number of viruses that were found, and the actions that it took in response to the viruses.

The Workstation User may delete any or all of the audit records maintained in the permanent log file on the workstation (this does not impact the copy maintained on ePO or the transient audit storage on the workstation for records to be sent to ePO). No mechanism is provided to modify audit records. No access to the audit records is provided to unauthorized users.

This function requires that the default setting, which enables activity logging on the Reports tab for all managed computers, be preserved.

7.2.2.2 Audit Record Review on ePO

ePO maintains a record of user actions and actions taken in response to detection of a virus. The auditable events are specified in the Audit Events and Details table in the FAU_GEN.1 section. ePO distinguishes between the records for user actions and virus-related events, referring to the former as “audits” and the latter as “events”.

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

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

Audit Log entries can be queried against by a Central Administrator. The Audit Log entries are automatically purged based upon a configured age. Audit records may be deleted via automatic purging, or a Central 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 VSE 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 VSE 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 VSE events include:

1. Compliance History — Retrieves information on compliance counts over time.
2. Events — Retrieves information on events sent from VSE.
3. Managed Systems — Retrieves information about systems running VSE.

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.

VSE 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 Central 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. VSE Policies,
10. VSE DAT File,
11. VSE On-Demand Scan Tasks.

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:

1. View audit log
2. View and purge audit log
3. View VSE settings
4. View and change VSE 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 Audit Log 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 Log 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 and external commands" permission may configure the SMTP server name and port used to send email or the destination(s) for SNMP traps. Credentials may optionally be specified if authentication is to be performed with the email server.

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

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

The permissions associated with Notification management are:

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

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

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

7.3.6 System Tree Management

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 VSE Policies

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

1. View VSE settings
2. View and change VSE settings

Per the evaluated configuration, these permissions are never used, so only Central Administrators have access to the VSE policies.

The following policies related to VSE may be configured:

1. VSE Access Protection Policies - Policies used to restrict access to specified ports, files, shares, registry keys, and registry values on the client systems.
2. VSE On-Access Default Processes Policies - Policies that define the processes included in the default category for on-access scanning, defining when scans for these processes are performed and the actions taken upon detection on the client systems.
3. VSE On-Access General Policies - Policies that enable and configure the operation of on-access scanning on the client systems.
4. VSE On-Access High-Risk Processes Policies - Policies that define the processes included in the High-Risk category for on-access scanning, defining when scans for these processes are performed and the actions taken upon detection on the client systems.
5. VSE On-Access Low-Risk Processes Policies - Policies that define the processes included in the Low-Risk category for on-access scanning, defining when scans for these processes are performed and the actions taken upon detection on the client systems.
6. VSE Quarantine Policies - Policies that specify where quarantined files are stored on the client systems and how long they are kept.
7. VSE Unwanted Programs Policies - Policies that specify unwanted programs on the client systems.
8. VSE User Interface Policies - Policies that control the access Workstation Users have to the VirusScan Enterprise interface on the client systems.

7.3.10 VSE DAT File

VSE 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. The Central Administrator may obtain updated DAT files from McAfee and then distribute the updated information to the VSE clients.

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

7.3.11 VSE On-Demand Scan Tasks

Workstation Users may invoke on-demand scans on their client systems. When an on-demand scan is invoked, the Workstation Users may select one of the VSE On-Demand Scan Tasks configured on ePO and distributed to the VSE clients.

7.4 Cryptographic Operations

ePO has the ability to create and deploy VirusScan anti-virus packages. The signature provided with the package includes calculation of a message digest using the Secure Hash Algorithm (SHA-1).