McAfee®

Security Target

McAfee Policy Auditor 5.2 and ePolicy Orchestrator 4.5

Document Version 2.0.2

February 2, 2011

Prepared For:

McAfee, Inc.

2821 Mission College Blvd.

Santa Clara, CA 95054

www.mcafee.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Policy Auditor 5.2 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 Policy Auditor 5.2 and ePolicy Orchestrator 4.5
ST Revision	2.0.2
ST Publication Date	February 2, 2011
Author	Apex Assurance Group and McAfee

1.2 TOE Reference

TOE Reference	McAfee Policy Auditor 5.2 and ePolicy Orchestrator 4.5
TOE Type	Security Management

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
AD	Active Directory
CC	Common Criteria version 3.1 (ISO/IEC 15408)
CPU	Central Processing Unit
DBMS	DataBase Management System
DNS	Domain Name System
DSS	Data Security Standard
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information Security Management Act
GUI	Graphical User Interface
HIPAA	Health Insurance Portability and Accountability Act
I&A	Identification & Authentication

[1] Derived from the IDSPP

TERM	DEFINITION
IDS	Intrusion Detection System
IIS	Internet Information Services
IP	Internet Protocol
IT	Information Technology
JDBC	Java DataBase Connectivity
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MDAC	Microsoft Data Access Components
MSDE	MS Data Engine
NTFS	New Technology File System
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
OS	Operating System
OSP	Organizational Security Policy
OVAL	Open Vulnerability Assessment Language
PCI	Payment Card Industry
PDC	Primary Domain Controller
PP	Protection Profile
RAM	Random Access Memory
SCAP	Security Content Automation Protocol
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Mail Protocol
SOF	Strength Of Function
SP	Service Pack
SQL	Structured Query Language
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
VGA	Video Graphics Array
XCCDF	eXtensible Configuration Checklist Description Format
XML	eXtensible Markup Language

Table 2 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

McAfee Policy Auditor 5.2 is an agent-based, purpose-built IT policy audit solution that leverages the XCCDF and OVAL security standards to automate the processes required for internal and external IT audits. McAfee Policy Auditor evaluates the status of managed systems relative to audits that contain benchmarks. Benchmarks contain rules that describe the desired state of a managed system. Benchmarks are distributed with the TOE or imported into McAfee Benchmark Editor and, once activated, can be used by Policy Auditor. Benchmarks are written in the open-source XML standard formats Extensible Configuration Checklist Description Format (XCCDF) and the Open Vulnerability Assessment Language (OVAL). XCCDF describes what to check while OVAL specifies how to perform the check.

Seamless integration with McAfee ePolicy Orchestrator® (ePO™) eases agent deployment, management, and reporting. ePO provides the user interface for the TOE via a GUI accessed from remote systems using web browsers. The ePO web dashboard represents policy compliance by benchmark. Custom reports can be fully automated, scheduled, or exported. ePO requires user to identify and authenticate themselves before access is granted to any data or management functions. Audit records are generated to record configuration changes made by users. The audit records may be reviewed via the GUI.

Based upon per-user permissions, users may configure the systems to be audited for policy compliance (the “managed systems”) along with the benchmarks to be checked. The Policy Auditor Agent Plug-In executing on the managed systems performs the policy audit and returns the results to Policy Auditor. Policy Auditor allows you to conduct policy audits on various releases of the following operating systems:

- Microsoft Windows
- Macintosh OS X
- HP-UX
- Solaris
- Red Hat Linux
- AIX

Users can review the results of the policy audits via ePO. Access to this information is again limited by per-user permissions.

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

Policy Auditor 5.2 received SCAP validation certificate number 66 (http://nvd.nist.gov/validation_mcafee.cfm).

1.7 TOE Description

The TOE helps organizations monitor policy compliance on their assets by performing audits on those assets. This solution allows managers to continuously monitor the state of their assets.

Administrators configure the system, including user accounts. Users schedule policy audits and review the results.

1.7.1 Physical Boundary

The TOE is a software TOE and includes:

1. The ePO application executing on a dedicated server
2. The Policy Auditor application on the same system as the ePO application
3. The Benchmark Editor application on the same system as the ePO application
4. The McAfee Agent application on each managed system to be audited
5. The Policy Auditor Agent Plug-In software on each managed system to be audited

Note specifically that the hardware, operating systems and third party support software (e.g. DBMS) on each of the systems are excluded from the TOE boundary.

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

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	Policy Auditor 5.2 Benchmark Editor 5.2[2] Policy Auditor Agent Plug-In 5.2 ePolicy Orchestrator 4.5 McAfee Agent 4.5[3]
IT Environment	Specified in the following: • Table 4 – Management System Component Requirements • Table 5 – Supported Agent Platforms • Table 6 – Agent Platform Hardware Requirements

Table 3 – Evaluated Configuration for the TOE

The evaluated configuration consists of a single instance of the management system (with ePO, Policy Auditor and Benchmark Editor) and one or more instances of managed systems (with McAfee Agent and the Policy Auditor Agent Plug-in).

ePO supports both ePO authentication and Windows authentication of user account credentials. The evaluated configuration requires the use of Windows authentication only. User accounts (other than the password) are still required to be defined in ePO so that attributes can be associated with the account.

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.

[2] Benchmark Editor 5.2 and Policy Auditor Agent 5.2 are shipped/packaged with Policy Auditor 5.2. From a clean installation, no additional steps are necessary to install Benchmark Editor 5.2 and Policy Auditor Agent 5.2.

[3] 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.

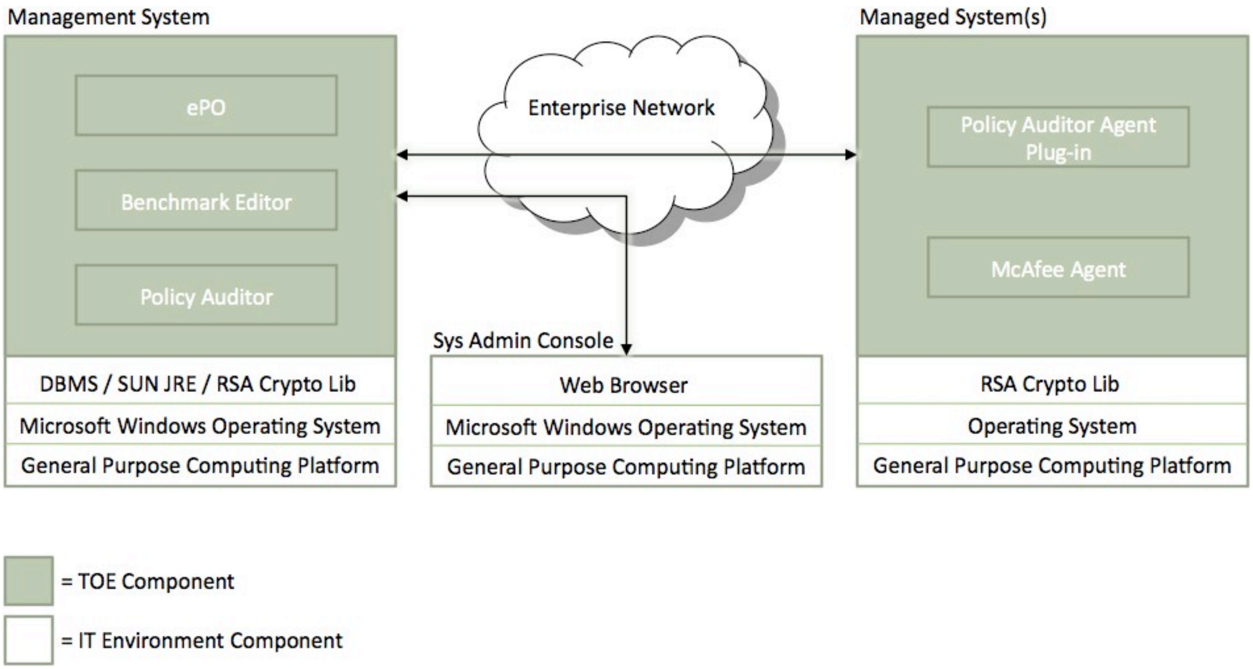

Management System
ePO
Benchmark Editor
Policy Auditor
DBMS / SUN JRE / RSA Crypto Lib
Microsoft Windows Operating System
General Purpose Computing Platform
Enterprise Network
Sys Admin Console
Web Browser
Microsoft Windows Operating System
General Purpose Computing Platform
Managed System(s)
Policy Auditor Agent Plug-in
McAfee Agent
RSA Crypto Lib
Operating System
General Purpose Computing Platform
= TOE Component
= IT Environment Component

Figure 1 – TOE Boundary

The following specific configuration options apply to the evaluated configuration:

1. The McAfee Agent system tray icon is not displayed on managed systems.
2. McAfee Agent wake-up calls are enabled.
3. Incoming connections to McAfee Agents are only accepted from the configured address of the ePO server
4. The only repository supported is the ePO server.
5. SQL Server 2005 Express and 2008 Express must not be used. Only Microsoft SQL Server 2005 and Microsoft SQL Server 2008 are supported in the evaluated configuration.
6. Updates to the TOE software or benchmarks are not permitted in the evaluated configuration.

Please note that the installation of the TOE will not have an adverse effect on other McAfee products that may be installed or supported by ePO. Similarly, other McAfee products installed within the ePO framework will not have an adverse effect on the TOE. The architecture of the ePO framework (i.e., the use of product extensions to support specific functionality) facilitates the use of multiple McAfee products on a single ePO server.

1.7.2 Hardware and Software Supplied by the IT Environment

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

The platform on which the ePO, Policy Auditor and Benchmark Editor software 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	Microsoft SQL Server 2005 Microsoft SQL Server 2008
Additional Software	MDAC 2.8 MSI 3.1 Apache 2.0.54.0 Tomcat 5.5.25 Sun JRE 1.6.0_06 RSA SSL-J 4.1.4 RSA Crypto-J 3.3.4_01 RSA Cert-J 2.0.3
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 McAfee Agent and Policy Auditor Agent Plug-In execute on one or more systems whose policy settings are to be audited. The supported platforms for these components are:

SUPPORTED AGENT OS	PLATFORM
Windows 2000 Server with SP 1, 2, 3, or 4	X86 platforms
Windows 2000 Advanced Server with SP 1, 2, 3, or 4	X86 platforms
Windows 2000 Professional with SP 1, 2, 3, or 4	X86 platforms
Windows XP Professional with SP1	X86 and X64 platforms
Windows Server 2003 Standard Edition	X86 and X64 platforms
Windows Server 2003 Enterprise Edition	X86 and X64 platforms
Windows Vista	X86 and X64 platforms
Windows 2008 Server	X86 and X64 platforms

SUPPORTED AGENT OS	PLATFORM
Mac OS X 10.4	X86 and X64 platforms, PowerPC
Mac OS X 10.5	X86 and X64 platforms, PowerPC
HP-UX 11i v1	RISC
HP-UX 11i v2	RISC
Solaris 8	SPARC
Solaris 9	SPARC
Solaris 10	SPARC
Red Hat Linux AS, ES, WS 4.0	X86 and X64 platforms
Red Hat Enterprise Linux 5.0, 5.1	X86 and X64 platforms
AIX 5.3 (TL8 of later) and AIX 6.1	Power 5

Table 5 – Supported Agent Platforms

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

COMPONENT	MINIMUM HARDWARE REQUIREMENTS
Memory	20MB RAM
Free Disk Space	80MB
Network Card	Ethernet, 10Mb or higher

Table 6 – Agent Platform Hardware Requirements

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

The TOE relies on Windows to authenticate user credentials during the logon process. User accounts must also be defined within ePO in order to associate permissions with the users.

1.7.3 Logical Boundary

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

TSF	DESCRIPTION
Policy Audits	The TOE audits managed systems to determine policy compliance on those systems. Results of the policy audits are stored in the database (the DBMS is in the IT Environment), and reports based upon completed policy audits may be retrieved via the GUI interface or by generating SCAP-conformant XML files to be shared with external systems.

TSF	DESCRIPTION
Identification	On the management system, the TOE requires users to identify and authenticate themselves before accessing the TOE software. User accounts must be defined within ePO, but authentication of the user credentials is performed by Windows. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with their user account that define the functionality the user is allowed to perform. On the management system and all managed systems, I&A for local login to the operating system (i.e., via a local console) is performed by the local OS (IT Environment).
Management	The TOE's Management Security Function provides support functionality that enables users to configure and manage TOE components. Management of the TOE may be performed via the GUI. Management privileges are defined per-user.
Audit	The TOE's Audit Security Function provides auditing of management actions performed by administrators. Authorized users may review the audit records via ePO.
System Information Import	The TOE may be configured to import information about systems to be managed from Active Directory (LDAP servers) or NT domain controllers. This functionality ensures that all the defined systems in the enterprise network are known to the TOE and may be configured to be managed.
SCAP Data Exchange	The TOE must be able to import and export SCAP benchmark assessment data. This functionality ensures that the assessments remain current as new benchmarks are developed and allows custom-designed benchmarks in the TOE to be made available to other systems

Table 7 – Logical Boundary Descriptions

1.7.4 TOE Data

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

TSF Data	Description	AD	UA	GE
Benchmarks	Contain an organized set of rules that describe the desired state of a set of managed systems.			✓
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.			✓
Data Retention	Parameters controlling the length of time policy audit event records are saved in the database.			✓

TSF Data	Description	AD	UA	GE
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 the management system.	✓		
Event Filtering	Specifies which events are forwarded to the server from the agents on the managed systems.			✓
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.			✓
Maximum Low Score	The scoring threshold at which systems are considered to fail the policy audit.			✓
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.		✓	
Policy Audit	Causes managed systems to be analyzed relative to a specified benchmark at a configured frequency.			✓
Product Policy	A collection of settings that you create, configure, then enforce to ensure that the managed security software products (e.g., Policy Auditor) are configured and perform accordingly on the managed systems.			✓
Queries	Configurable objects that retrieve and display data from the database.			✓
Scoring Model	Specifies which of the XCCDF 1.1.4 scoring models is used to calculate the compliance score for the results of a policy audit.			✓
Server Settings	Control how the ePolicy Orchestrator server behaves.			✓
System Data	Results of audits performed on managed systems.			✓
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.			✓
Tags	Labels that you can apply to one or more systems, automatically (based on criteria) or manually.			✓
Waivers	Specify temporary affects to the scoring of policy audits.			✓
File Integrity Monitoring	Designate a set of files to monitor for changes.			✓

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

1.8 Rationale for Non-bypassability and Separation of the TOE

The responsibility for non-bypassability and non-interference is split between the TOE and the IT Environment. TOE components are software only products and therefore the non-bypassability and non-interference claims are dependent upon hardware and OS mechanisms. The TOE runs on top of the IT Environment supplied operating systems.

The TOE ensures that the security policy is applied and succeeds before further processing is permitted whenever a security relevant interface is invoked: the interfaces are well defined and insure that the access restrictions are enforced. Non-security relevant interfaces do not interact with the security functionality of the TOE. The TOE depends upon OS mechanisms to protect TSF data such that it can only be accessed via the TOE. The system on which ePO, Policy Auditor and Benchmark Editor execute is dedicated to that purpose. The McAfee Agent and Policy Auditor Agent Plug-In execute on non-dedicated systems; these components only perform policy audits and do not enforce access control policies for users.

The TOE is implemented with well-defined interfaces that can be categorized as security relevant or non-security relevant. The TOE is implemented such that non-security relevant interfaces have no means of impacting the security functionality of the TOE. Unauthenticated users may not perform any actions within the TOE. The TOE tracks multiple users by sessions and ensures the access privileges of each are enforced.

The server hardware provides virtual memory and process separation, which the server OS utilizes to ensure that other (non-TOE) processes may not interfere with the TOE; all interactions are limited to the defined TOE interfaces. The OS and DBMS restrict access to TOE data in the database to prevent interference with the TOE via that mechanism.

The TOE consists of distributed components. Communication between the components relies upon cryptographic functionality provided by the OS or third party software (operational environment) to protect the information exchanged from disclosure or modification. .

Additional information concerning non-bypassability and non-interference is provided in the *McAfee Policy Auditor Security Architecture* document.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

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

2.2 Protection Profile Conformance Claim

The TOE does not claim conformance to a Protection Profile.

3 Security Problem Definition

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

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

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

3.1 Threats

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

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data

Table 9 – Threats Addressed by the TOE

The following table identifies threats to the managed systems that may be indicative of vulnerabilities in or misuse of IT resources:

THREAT	DESCRIPTION
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on data acquired from managed systems.
T.SCNCFG	Improper security configuration settings may exist in the managed systems.

THREAT	DESCRIPTION
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.

Table 10 – Threats Addressed by the IT Environment

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The following Organizational Security Policies apply to the TOE:

POLICY	DESCRIPTION
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to data received from data sources and appropriate response actions taken.
P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.IMPORT	The TOE shall be able to import data about managed systems from LDAP servers and NT Domains.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.
P.SCAP	The TOE shall be able to exchange SCAP Benchmark Assessment data with external systems.

Table 11 – 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.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the IT Systems the TOE monitors.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.

ASSUMPTION	DESCRIPTION
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

Table 12 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ACCESS	The TOE must allow authorized users to access only authorized TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions on the management system.
O.AUDIT_PROTECT	The TOE will provide the capability to protect audit information generated by the TOE.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDANLZ	The TOE must apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.IDENTIFY	The TOE must be able to identify users prior to allowing access to TOE functions and data on the management system.
O.IDSCAN	The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
O.IMPORT	The TOE shall provide mechanisms to import system data from Active Directory (LDAP servers) and NT Domain Controllers.
O.INTEGR	The TOE must ensure the integrity of all System data.
O.OFLOWS	The TOE must appropriately handle potential System data storage overflows.
O.SCAP	The TOE shall provide mechanisms to exchange SCAP Benchmark Assessment data.
O.SD_PROTECTION	The TOE will provide the capability to protect system data.

Table 13 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
O. PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
O.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
O.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
O.INTROP	The TOE is interoperable with the managed systems it monitors

OBJECTIVE	DESCRIPTION
O.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.AUDIT_PROTECT	The IT Environment will provide the capability to protect audit information generated by the TOE via mechanisms outside the TSC.
OE.AUDIT_REVIEW	The IT Environment will provide the capability for authorized administrators to review audit information generated by the TOE.
OE.CRYPTO	The IT Environment will provide the cryptographic functionality and protocols required for the TOE to securely transfer information between distributed portions of the TOE.
OE.DATABASE	Those responsible for the TOE must ensure that access to the database via mechanisms outside the TOE boundary (e.g., DBMS) is restricted to authorized users only.
OE.IDAUTH	The IT Environment must be able to identify and authenticate users prior to them gaining access to TOE functionality on the managed system. It must also be able to authenticate user credentials on the management system when requested by the TOE.
OE.PROTECT	The IT environment will protect itself and the TOE from external interference or tampering.
OE.SD_PROTECTION	The IT Environment will provide the capability to protect system data via mechanisms outside the TSC.
OE.STORAGE	The IT Environment will store TOE data in the database and retrieve it when directed by the TOE.
OE.TIME	The IT Environment will provide reliable timestamps to the TOE

Table 14 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

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

OBJECTIVE THREAT / ASSUMPTION	O.IDSCAN	O.IDANLZ	O.EADMIN	O.ACCESS	O.IDENTIFY	O.OFLOWS	O.INTEGR	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP	O.AUDITS	O.AUDIT_PROTECT	O.IMPORT	O.SCAP	O.SD_PROTECTION	OE.TIME	OE.PROTECT	OE.SD_PROTECTION	OE.IDAUTH	OE.DATABASE	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW	OE.CRYPTO	OE.STORAGE
A.ACCESS												✓														
A.ASCOPE												✓														
A.DATABASE																						✓				
A.DYNMIC											✓	✓														
A.LOCATE									✓																	
A.MANAGE											✓															
A.NOEVIL								✓	✓	✓																

OBJECTIVE THREAT / ASSUMPTION	O.IDSCAN	O.IDANLZ	O.EADMIN	O.ACCESS	O.IDENTIFY	O.OFLOWS	O.INTEGR	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP	O.AUDITS	O.AUDIT_PROTECT	O.IMPORT	O.SCAP	O.SD_PROTECTION	OE.TIME	OE.PROTECT	OE.SD_PROTECTION	OE.IDAUTH	OE.DATABASE	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW	OE.CRYPTO	OE.STORAGE
A.PROTCT									✓																	
P.ACCACT					✓								✓								✓			✓		
P.ACCESS				✓	✓												✓			✓	✓	✓				
P.ANALYZ		✓																								
P.DETECT	✓												✓					✓								
P.IMPORT															✓											
P.INTGTY							✓							✓									✓		✓	✓
P.MANAGE			✓	✓	✓			✓		✓	✓										✓					
P.PROTCT						✓			✓										✓						✓	✓
P.SCAP																✓										
T.COMDIS				✓	✓														✓		✓					
T.COMINT				✓	✓		✓												✓		✓					
T.FALREC		✓																								
T.IMPCON			✓	✓	✓			✓													✓					
T.LOSSOF				✓	✓		✓														✓					
T.NOHALT	✓	✓		✓	✓																✓					
T.PRIVIL				✓	✓																✓					
T.SCNCFG	✓																									
T.SCNMLC	✓																									
T.SCNVUL	✓																									

Table 15 – 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	RATIONALE
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions. The O.INTROP objective ensures the TOE has the needed access.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors. The O.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users. The OE.DATABASE objective ensures that access to any mechanisms outside the TOE boundary that may be used to access the database is configured by the administrators such that only authorized users may utilize the mechanisms.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors. The O.INTROP objective ensures the TOE has the proper access to the IT System. The O.PERSON objective ensures that the TOE will managed appropriately.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The O.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The O.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The O.INSTAL objective ensures that the TOE is properly installed and operated and the O.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. The O.PHYCAL provides for the physical protection of the TOE hardware and software.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE. The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDENTIFY objective supports this objective by ensuring each user is uniquely identified. The OE.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The OE.AUDIT_REVIEW objective provides the ability for administrators to review the audit records generated by the TOE so that accountability for administrator actions can be determined.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes. The O.IDENTIFY objective provides for identification of users prior to any TOE function accesses via the ePO web interface. The OE.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDENTIFY and OE.IDAUTH objectives by only permitting authorized users to access TOE functions. The OE.SD_PROTECTION and OE.DATABASE objectives counter this threat for mechanisms outside the TSC via IT Environment protections of the system data trail and the database used to hold TOE data. The O.SD_PROTECTION and O.ACCESS objectives counter this threat for mechanisms inside the TSC via TOE protections of the system data trail and the database used to hold TOE data.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to data received from data sources and appropriate response actions taken. The O.IDANLZ objective addresses this policy by requiring the TOE to apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected. The O.AUDITS and O.IDSCAN objectives address this policy by requiring collection of audit and policy audit data. The OE.TIME objective supports this policy by providing a time stamp for insertion into the system data records.
P.IMPORT	The TOE shall be able to import data about managed systems from LDAP servers and NT Domains. The O.IMPORT objective addresses this policy by requiring the TOE to provide functionality to import data about managed systems from LDAP servers and NT Domains.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification. The O.INTEGR objective ensures the protection of System data from modification. The O.AUDIT_PROTECT and OE.AUDIT_PROTECT objectives ensure the integrity of audit records in the database generated by the TOE using access mechanisms inside and outside the TSC respectively. The OE.CRYPTO objective requires the IT Environment to provide cryptographic functionality and protocols that can be used by the TOE to protect the data during transit. The OE.STORAGE objective requires the IT Environment to provide storage and retrieval mechanisms for System data for use by the TOE.
P.MANAGE	The TOE shall only be managed by authorized users. The O.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The O.INSTAL objective supports the O.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDENTIFY objective provides for identification of users prior to any TOE function accesses. The OE.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions. The O.CREDEN objective requires administrators to protect all authentication data.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The O.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports the TOE protection from the IT Environment. The OE.CRYPTO objective requires the IT Environment to provide cryptographic functionality and protocols that can be used by the TOE to protect the data during transit. The OE.STORAGE objective requires the IT Environment to provide storage and retrieval mechanisms for System data for use by the TOE.
P.SCAP	The TOE shall be able to exchange SCAP Benchmark Assessment data with external systems. The O.SCAP objective addresses this policy by requiring the TOE to provide mechanisms to exchange SCAP data with external sources.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE data. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no System data will be modified. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on data received from each data source. The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. The O.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no System data will be deleted.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions. The O.IDSCAN and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions.
T.SCNCFG	Improper security configuration settings may exist in the managed systems. The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change.
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions. The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of malicious code.
T.SCNVUL	Vulnerabilities may exist in an IT System the TOE monitors. The O.IDSCAN objective counters this threat by requiring a TOE that contains a Scanner, collect and store static configuration information that might be indicative of a vulnerability.

Table 16 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 IDS Class of SFRs

All of the components in this section are taken from the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments.

This class of requirements is copied from the IDS System PP to specifically address the data collected and analysed by an IDS scanner and analyzer. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of system data and provide for requirements about collecting, reviewing and managing the data.

5.1.1 IDS_SDC.1 System Data Collection

Management: IDS_SDC.1

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

a) Configuration of the events to be collected

Audit: IDS_SDC.1

There are no auditable events foreseen.

IDS_SDC.1 System Data Collection

Hierarchical to: No other components

Dependencies: No dependencies

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) [selection: *Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration., accountability policy configuration, detected known vulnerabilities*]; and

b) [assignment: *other specifically defined events*].

IDS_SDC.1.2 At a minimum, the System shall collect and record 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) The additional information specified in the Details column of the table below:

COMPONENT	EVENT	DETAILS
IDS_SDC.1	Startup and shutdown	None
IDS_SDC.1	Identification and authentication events	User identity, location, source address, destination address
IDS_SDC.1	Data accesses	Object IDS, requested access, source address, destination address
IDS_SDC.1	Service requests	Specific service, source address, destination address
IDS_SDC.1	Network traffic	Protocol, source address, destination address
IDS_SDC.1	Security configuration changes	Source address, destination address
IDS_SDC.1	Data introduction	Object IDS, location of object, source address, destination address
IDS_SDC.1	Startup and shutdown of audit functions	None
IDS_SDC.1	Detected malicious code	Location, identification of code
IDS_SDC.1	Access control configuration	Location, access settings
IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols
IDS_SDC.1	Authentication configuration	Account names for cracked passwords, account policy parameters
IDS_SDC.1	Accountability policy configuration	Accountability policy configuration parameters
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

Table 17 – System Data Collection Events and Details

Application Note: The rows in this table must be retained that correspond to the selections in IDS_SDC.1.1 when that operation is completed. If additional events are defined in the assignment in IDS_SDC.1.1, then corresponding rows should be added to the table for this element.

5.1.2 IDS_ANL.1 Analyzer Analysis

Management: IDS_ANL.1

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

a) Configuration of the analysis to be performed

Audit: IDS_ANL.1

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

a) Minimal: Enabling and disabling of any of the analysis mechanisms

IDS_ANL.1 Analyzer Analysis

Hierarchical to:	No other components
Dependencies:	No dependencies

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all IDS data received:

a) [selection: *statistical, signature, integrity*]; and

b) [assignment: *other analytical functions*].

IDS_ANL.1.2 The System shall record within each analytical result at least the following information:

a. Date and time of the result, type of result, identification of data source; and

b. [assignment: *other security relevant information about the result*]. (EXT)

5.1.3 IDS_RDR.1 Restricted Data Review (EXT)

Management: IDS_RDR.1

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

a) maintenance (deletion, modification, addition) of the group of users with read access right to the system data records.

Audit: IDS_RDR.1

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

a) Basic: Attempts to read system data that are denied.

b) Detailed: Reading of information from the system data records.

Application Note: The audit event definition is consistent with CCEVS Policy Letter #15, which states that only access failures are auditable at the Basic level of audit.

IDS_RDR.1 Restricted Data Review

Hierarchical to:	No other components	
Dependencies:	IDS_SDC.1	System Data Collection
	IDS_ANL.1	Analyzer Analysis

IDS_RDR.1.1 The System shall provide [assignment: *authorized users*] with the capability to read [assignment: *list of System data*] from the System data.

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

5.1.4 IDS_STG.1 Guarantee of System Data Availability

Management: IDS_STG.1

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

a) maintenance of the parameters that control the system data storage capability.

Audit: IDS_STG.1

There are no auditable events foreseen.

IDS_STG.1 Guarantee of System Data Availability

Hierarchical to:	No other components	
Dependencies:	IDS_SDC.1	System Data Collection
	IDS_ANL.1	Analyzer Analysis

IDS_STG.1.1 The System shall protect the stored System data from unauthorized deletion.

IDS_ STG.1.2 The System shall protect the stored System data from modification.

Application Note: Authorized deletion of data is not considered a modification of System data in this context. This requirement applies to the actual content of the System data, which should be protected from any modifications.

IDS_ STG.1.3 The System shall ensure that [assignment: *metric for saving System data*] System data will be maintained when the following conditions occur: [selection: *System data storage exhaustion, failure, attack*].

5.1.5 IDS_STG.2 Prevention of System Data Loss

Management: IDS_STG.2

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

a) maintenance (deletion, modification, addition) of actions to be taken in case system data storage capacity has been reached.

Audit: IDS_STG.2

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

a) Basic: Actions taken if the storage capacity has been reached.

IDS_STG.2 Prevention of System data loss

Hierarchical to: No other components

Dependencies:	IDS_SDC.1	System Data Collection
	IDS_ANL.1	Analyzer Analysis

IDS_STG.2.1 The System shall [selection: *'ignore System data', 'prevent System data, except those taken by the authorized user with special rights', 'overwrite the oldest stored System data '*] and send an alarm if the storage capacity has been reached.

6 Security Requirements

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

6.1 Security Functional Requirements

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

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG.4	Prevention of Audit Trail Data Loss
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UID.1	Timing of Identification
	FIA_USB.1	User-Subject Binding
Security Management	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_TDC.1(1)	Inter-TSF Basic TSF Data Consistency
	FPT_TDC.1(2)	Inter-TSF Basic TSF Data Consistency
IDS Component Requirements	IDS_SDC.1	System Data Collection
	IDS_ANL.1	Analyzer Analysis
	IDS_RDR.1	Restricted Data Review
	IDS_STG.1	Guarantee of System Data Availability
	IDS_STG.2	Prevention of System Data Loss

Table 18 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

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

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

b) All auditable events for the not specified level of audit; and

c) *The events identified in 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*.

Application Note: The auditable events for the respective level of auditing are included in the following table:

COMPONENT	EVENT	DETAILS
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to the TOE and System data	Object IDs, Requested access
FAU_SAR.2	Note: Unsuccessful attempts to read information from the audit records do not occur because the TOE does not present that capability to users that are not authorized to read the audit records.	
FAU_STG.4	Note: New audit records are discarded when storage space is exhausted, the IT Environment alarms the administrator with anotification indicating low disk space.	
FIA_ATD.1	All changes to TSF data (excluding password changes) result in an audit record being generated. Note that passwords are not configured, so no audit records for rejection of a tested secret will be generated.	
FIA_UID.1	All use of the user identification mechanism	User identity, location
FIA_USB.1	Successful binding of attributes to subjects is reflected in the audit record for successful authentication. Unsuccessful binding does not occur in the TOE design.	
FMT_MTD.1	All modifications to the values of TSF data, with the exception of Waiver Management functions.	
FMT_SMF.1	Use of the management functions, with the exception of Waiver Management functions.	User identity, function used
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity
FPT_TDC.1	Use of the asset import function	Data Source, result, identification of which TSF data have been imported

COMPONENT	EVENT	DETAILS
	Detection of modified TSF data	Data Source, Identification of which TSF data have been modified
IDS_ANL.1	None (the analysis function is always enabled)	
IDS_RDR.1	None (the user is not given the option of accessing unauthorized system data)	
IDS_STG.2	Note: Since new audit records are discarded when storage space is exhausted (system data and audit records are stored in the same database), an SNMP trap is generated (rather than an audit record) in response to storage failure.	

Table 19 – Audit Events and Details

6.1.1.2 FAU_GEN.2 User Identity Association

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

6.1.1.3 FAU_SAR.1 Audit Review

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

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

6.1.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.5 FAU_STG.1 Protected Audit Trail Storage

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

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

6.1.1.6 FAU_STG.4 Prevention of Audit Data Loss

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

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

6.1.2 Identification and Authentication (FIA)

6.1.2.1 FIA_ATD.1 User Attribute Definition

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

a) ePO User name;

b) Enabled or disabled;

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

d) Global Administrator status; and

e) *Permission Sets.*

6.1.2.2 FIA_UID.1 Timing of Identification

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

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

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

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

6.1.2.3 FIA_USB.1 User-Subject Binding

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

a) Global Administrator status; and

b) Permissions.

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

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

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

Application Note: If the security attributes for a user are changed while that user has an active session, the new security attributes are not bound to a session until the next page refresh.

6.1.3 Security Management (FMT)

6.1.3.1 FMT_MTD.1 Management of TSF Data

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

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
Benchmarks	Activate benchmarks	Modify (activate) benchmarks
	Apply labels	Query and modify (apply) labels
	Create, delete and apply labels	Query, create, delete and modify (apply) labels
	Create, delete and import checks	Query, create (manually or by importing) and delete checks
	Create, delete, modify and import benchmarks	Query, create (manually or by importing), delete and modify benchmarks
	Create, delete, modify, import and unlock benchmarks	Query, create (manually), delete, and modify (unlock) benchmarks
	Edit benchmark tailoring	Query and modify benchmark tailoring
	Edit existing benchmarks	Query and modify benchmarks
	View and export benchmarks	Query and export benchmarks
	View and export checks	Query and export checks
Contacts	Create and edit contacts	Query, create, delete and modify
	Use contacts	Use
Dashboards	Use public dashboards	Query and use public dashboards

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
	Use public dashboards; create and edit personal dashboards	Query and use public dashboards; create and modify personal dashboards
	Use public dashboards; create and edit personal dashboards; make personal dashboards public	Query and use public dashboards; create, delete and modify personal dashboards; make personal dashboards public
Data Retention Settings	n/a (only allowed by a Global Administrator)	Query and modify
Event Records (Policy Audit)	Add, remove and change Audits and Assignments	Query policy audit event records
	View Audits and Assignments	Query policy audit event records
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
Global Administrator Status	n/a (only allowed by a Global Administrator)	Query and modify
Groups	View "System Tree" tab	Query
	View "System Tree" tab along with Edit System Tree groups and systems	Query, create, delete and modify
Maximum Low Score	n/a (only allowed by a Global Administrator)	Query and modify
Permission Set	n/a (only allowed by a Global Administrator)	Query, create, delete, modify, and assign (to a user) permissions
Policy Audit	Add, remove and change Audits and Assignments	Query, create, delete and modify policy audits
	View Audits and Assignments	Query policy audits
Product Policy	View settings (McAfee Agent and/or Policy Auditor Agent)	Query
	View and change settings (McAfee Agent and/or Policy Auditor Agent)	Query, create, delete, and modify (including enable)
	n/a (only allowed by a Global Administrator)	Query, create, delete, and modify (including assign and enable)
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

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
	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
Scoring Model	n/a (only allowed by a Global Administrator)	Query and modify
Server Settings	n/a (only allowed by a Global Administrator)	Query and modify
System Information	Create and edit systems	Query, create, delete and modify
System Tree	View System Tree	Query
Tags	Create and edit tags and tag criteria (all tags) Create and edit tags (tags w/o criteria only)	Query, create, delete and modify
	Apply, exclude, and clear tags	Query and modify
Waivers	View Waivers	Query and create (request)
	Grant and modify Waivers	Query, modify (expire or grant), and delete
File Integrity Monitoring	View File Integrity Monitoring	Query
	Manage File Integrity Monitoring	Create, apply, query, modify, and delete

Table 20 – TSF Data Access Permissions

6.1.3.2 FMT_SMF.1 Specification of Management Functions

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

a) *ePO User Account management,*

b) *Permission Set management,*

c) *Audit Log management,*

d) *Event Log management,*

e) *Event Filtering management,*

f) *System Tree management,*

g) *Tag management,*

h) *Product Policy management,*

i) *Query management,*

j) *Dashboard management,*

k) *Benchmark management,*

l) *Policy Auditor management,*

m) *Policy Audit management,*

n) *Waiver management, and*

o) *File Integrity Monitoring management.*

6.1.3.3 FMT_SMR.1 Security Roles

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

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

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

6.1.4 Protection of the TSF (FPT)

6.1.4.1 FPT_TDC.1 Inter-TSF Basic TSF Data Consistency

FPT_TDC.1.1(1) The TSF shall provide the capability to consistently interpret *system information* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2(1) The TSF shall use *the following rules* when interpreting the TSF data from another trusted IT product.

a) *For Active Directory (LDAP servers), the data is interpreted according to the LDAP version 3 protocol.*

b) *For NT Domains, the data is interpreted according to the NetBIOS protocol.*

c) *When conflicting information is received from different sources, highest priority is given to information learned from the McAfee Agent, then to Active Directory, and finally to NT Domains.*

FPT_TDC.1.1(2) The TSF shall provide the capability to consistently interpret *SCAP Benchmark Assessments* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2(2) The TSF shall use *the SCAP Benchmark Assessment XCCDF and OVAL standards* when interpreting the TSF data from another trusted IT product.

6.1.5 IDS Component Requirements (IDS)

6.1.5.1 IDS_SDC.1 System Data Collection

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) access control configuration, service configuration, authentication configuration, detected known vulnerabilities and

b) *no other events.*

IDS_SDC.1.2 At a minimum, the System shall collect and record 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) The additional information specified in the *Details* column **of the table below**.

COMPONENT	EVENT	DETAILS
IDS_SDC.1	Access control configuration	Location, access settings
IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols
IDS_SDC.1	Authentication configuration	Account policy parameters
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

Table 21 – System Data Collection Events and Details

Application Note: Access control configuration refers to configuration settings used to restrict access for individual users/roles. Service configuration refers to services made available to users via the network interface and protocol stack. Authentication configuration refers to settings regarding password content parameters and authentication attempts. The information collected for each managed system is determined by the benchmarks applied against that managed system.

6.1.5.2 IDS_ANL.1 Analyzer analysis

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all system data received:

a) signature; and

b) *scoring.*

IDS_ANL.1.2 The System shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) *The score for the system data.*

6.1.5.3 IDS_RDR.1 Restricted Data Review (EXP)

IDS_RDR.1.1 The System shall provide *a user with the View System Tree permission or a Global Administrator* with the capability to read *event records and scores* from the System data.

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

6.1.5.4 IDS_STG.1 Guarantee of System Data Availability

IDS_STG.1.1 The System shall protect the stored System data from unauthorized deletion.

IDS_ STG.1.2 The System shall protect the stored System data from modification.

Application Note: Authorised deletion of data is not considered a modification of System data in this context. This requirement applies to the actual content of the System data, which should be protected from any modifications.

IDS_ STG.1.3 The System shall ensure that *(to the limits of the storage space for the configured data retention period) the oldest* System data will be maintained when the following conditions occur: System data storage exhaustion.

6.1.5.5 IDS_STG.2 Prevention of System data loss

IDS_STG.2.1 The System shall ignore System data and send an alarm if the storage capacity has been reached.

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

6.2 Security Assurance Requirements

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

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 22 – 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	No other components	FPT_STM.1	Satisfied by OE.TIME in the environment
FAU_GEN.2	No other components	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied
FAU_SAR.1	No other components	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components	FAU_SAR.1	Satisfied
FAU_STG.1	No other components	FAU_GEN.1	Satisfied
FAU_STG.4	FAU_STG.3	FAU_STG.1	Satisfied
FIA_ATD.1	No other components	None	n/a
FIA_UID.1	No other components	None	n/a
FIA_USB.1	No other components	FIA_ATD.1	Satisfied
FMT_MTD.1	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components	None	n/a
FMT_SMR.1	No other components	FIA_UID.1	Satisfied
FPT_TDC.1	No other components	None	n/a
IDS_SDC.1	No other components	None	None

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
IDS_ANL.1	No other components	None	None
IDS_RDR.1	No other components	IDS_SDC.1, IDS_ANL.1	Satisfied Satisfied
IDS_STG.1	No other components	IDS_SDC.1, IDS_ANL.1	Satisfied Satisfied
IDS_STG.2	No other components	IDS_SDC.1, IDS_ANL.1	Satisfied Satisfied

Table 23 – TOE SFR Dependency Rationale

6.4 Security Requirements Rationale

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

6.4.1 Security Functional Requirements for the TOE

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

OBJECTIVE SFR	O.ACCESS	O.AUDITS	O.AUDIT_PROTECT	O.EADMIN	O.IDANLZ	O.IDENTIFY	O.IDSCAN	O.IMPORT	O.INTEGR	O.OFLOWS	O.SCAP	O.SD_PROTECTION
FAU_GEN.1		✓										
FAU_GEN.2		✓										
FAU_SAR.1	✓											
FAU_SAR.2	✓											
FAU_STG.1		✓	✓									
FAU_STG.4		✓										
FIA_ATD.1						✓						
FIA_UID.1	✓					✓						
FIA_USB.1	✓											
FMT_MTD.1	✓			✓				✓	✓		✓	
FMT_SMF.1	✓			✓								
FMT_SMR.1	✓			✓								
FPT_TDC.1(1)								✓				
FPT_TDC.1(2)											✓	
IDS_SDC.1							✓					
IDS_ANL.1					✓							
IDS_RDR.1	✓											
IDS_STG.1									✓			✓
IDS_STG.2										✓		

Table 24 – Mapping of TOE SFRs to Security Objectives

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

OBJECTIVE	RATIONALE
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. Users authorized to access the TOE are determined using an identification process [FIA_UID.1]. Upon successful I&A, the security attributes for the user are bound to the subject so that proper access controls can be enforced [FIA_USB.1]. The permitted access to TOE data by the roles and permissions is defined [FMT_MTD.1, FMT_SMF.1, FMT_SMR.1]. The audit log records may only be viewed by authorized users (FAU_SAR.1, FAU_SAR.2].
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions. Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The user associated with the events must be recorded [FAU_GEN.2]. In the event of audit event storage exhaustion, the oldest events are preserved and notification of the situation is provided [FAU_STG.4]. The TOE does not provide any mechanism for users to modify or delete audit records other than via configuration of the data retention timeframe, and that functionality is limited to administrators [FAU_STG.1].
O.AUDIT_PROTECT	The TOE will provide the capability to protect audit information generated by the TOE. The TOE is required to protect the stored audit records from unauthorized deletion or modification [FAU_STG.1].
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The functions and roles required for effective management are defined [FMT_SMF.1, FMT_SMR.1], and the specific access privileges for the roles and permissions is enforced [FMT_MTD.1].
O.IDANLZ	The TOE must apply analytical processes and information to derive conclusions about intrusions (past, present, or future). The TOE is required to perform analysis on the event records to produce a score indicative of the potential for intrusions on each managed system [IDS_ANL.1].
O.IDENTIFY	The TOE must be able to identify users prior to allowing access to TOE functions and data. Security attributes of subjects used to enforce the security policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are determined using an identification process [FIA_UID.1] and the TOE relies upon authentication services provided by the operational environment.

OBJECTIVE	RATIONALE
O.IDSCAN	The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System. The TOE is required to collect and store static configuration information of an IT System. The type of configuration information collected is defined [IDS_SDC.1].
O.IMPORT	The TOE shall provide mechanisms to import system information from Active Directory (LDAP servers) and NT Domains. The TOE defines management functionality to import system tree information [FMT_MTD.1] and the rules for interpreting data from those sources [FPT_TDC.1(1)].
O.INTEGR	The TOE must ensure the integrity of all System data. Only authorized administrators of the System may query or add System data [FMT_MTD.1]. The TOE is required to protect all system data from unauthorized modification or deletion [IDS_STG.1].
O.OFLOWS	The TOE must appropriately handle potential System data storage overflows. The System must prevent the loss of system data in the event its trail is full [IDS_STG.2].
O.SCAP	The TOE shall provide mechanisms to exchange SCAP Benchmark Assessment data. The TOE includes mechanisms to exchange SCAP Benchmark Assessment data with external systems [FPT_TDC.1(2)]. Access to this functionality is restricted [FMT_MTD.1].
O.SD_PROTECTION	The TOE will provide the capability to protect system data. The TOE is required to protect the System data from unauthorized deletion or modification [IDS_STG.1].

Table 25 – 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 Policy Auditor 5.2 and ePolicy Orchestrator 4.5
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: McAfee Policy Auditor 5.2 and ePolicy Orchestrator 4.5
ADV_TDS.1: Basic Design	Basic Design: McAfee Policy Auditor 5.2 and ePolicy Orchestrator 4.5
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: McAfee Policy Auditor 5.2 and ePolicy Orchestrator 4.5
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: McAfee Policy Auditor 5.2 and ePolicy Orchestrator 4.5

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: McAfee Policy Auditor 5.2 and ePolicy Orchestrator 4.5
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: McAfee Policy Auditor 5.2 and ePolicy Orchestrator 4.5
ALC_DEL.1: Delivery Procedures	Delivery Procedures: McAfee Policy Auditor 5.2 and ePolicy Orchestrator 4.5
ATE_COV.1: Evidence of Coverage	Security Testing: McAfee Policy Auditor 5.2 and ePolicy Orchestrator 4.5
ATE_FUN.1: Functional Testing	Security Testing: McAfee Policy Auditor 5.2 and ePolicy Orchestrator 4.5
ATE_IND.2: Independent Testing – Sample	Security Testing: McAfee Policy Auditor 5.2 and ePolicy Orchestrator 4.5

Table 26 – 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, 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. The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.
3. Consistent with current best practice for tracking and fixing flaws as well as providing fixes to customers.

6.5 TOE Summary Specification Rationale

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE's Security Functions and the SFRs and the rationale.

TSF SFR	Policy Audits	Identification	Management	Audit	System Information Import	SCAP Data Exchange
FAU_GEN.1				✓		
FAU_GEN.2				✓		
FAU_SAR.1				✓		
FAU_SAR.2				✓		
FAU_STG.1				✓		
FAU_STG.4				✓		
FIA_ATD.1			✓			
FIA_UID.1		✓				
FIA_USB.1		✓				
FMT_MTD.1			✓			
FMT_SMF.1			✓			
FMT_SMR.1			✓			
FPT_TDC.1(1)					✓	
FPT_TDC.1(2)						✓
IDS_SDC.1	✓					
IDS_ANL.1	✓					
IDS_RDR.1	✓					
IDS_STG.1	✓					
IDS_STG.2	✓					

Table 27 – SFR to TOE Security Functions Mapping

SFR	SF AND RATIONALE
FAU_GEN.1	**Audit –** ePO user actions area audited according to the events specified in the table with the SFR.
FAU_GEN.2	**Audit –** The audit log records include the associated user name when applicable.
FAU_SAR.1	**Audit –** Audit log records are displayed in a human readable table form from queries generated by authorized users.
FAU_SAR.2	**Audit –** Only authorized users have permission to query audit log records.
FAU_STG.1	**Audit –** The only mechanism provided by the TOE to cause audit records to be deleted is configuration of the data retention timeframe, which is restricted to administrators. The TOE does not provide any mechanism for users to modify audit records.
FAU_STG.4	**Audit –** If the database is full, new records are discarded and an SNMP trap is generated.

SFR	SF AND RATIONALE
FIA_ATD.1	**Management** – User security attributes are associated with the user user account via ePO User Account management.
FIA_UID.1	**Identification** - The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TSC. No action can be initiated before proper identification and authentication.
FIA_USB.1	**Identification** - Upon successful login, the TOE binds the Global Administrator status and the union of all the permissions from the permission sets from the user account configuration to the session.
FMT_MTD.1	**Management** – The Global Administrator status and user permissions determine the access privileges of the user to TOE data.
FMT_SMF.1	**Management** – The management functions that must be provided for effective management of the TOE are defined and described.
FMT_SMR.1	**Management** – The TOE provides the roles specified in the SFR. When a User Account is created or modified, the role is specified by setting or clearing the Global Administrator status for the user.
FPT_TDC.1(1)	**System Information Import** – The TOE provides the functionality to import asset data information from Active Directory (LDAP servers) or NT Domains and correctly interpret the information.
FPT_TDC.1(2)	**SCAP Data Exchange** – The TOE can import SCAP Benchmark Assessment data and export reports in SCAP-conformant XML files.
IDS_SDC.1	**Policy Audits** – The TOE performs policy audits of specified systems in order to detect policy compliance on each system, which includes vulnerability detection as defined in benchmarks. Policy audit results are stored in the database.
IDS_ANL.1	**Policy Audits** – The TOE analyzes the results of the policy audits performed to indicate vulnerabilities explicitly or via a likelihood based on the policy compliance score calculated for each managed system. Vulnerability information is stored in the database.
IDS_RDR.1	**Policy Audits** – The TOE provides the ability for authorized administrators to retrieve reports from the database that describe the results from the policy audits on the managed systems, which includes detected vulnerabilities.
IDS_STG.1	**Policy Audits** – The TOE protects the policy audit information from unauthorized deletion and modification via interfaces within the TSC because no mechanism exists for modification and the only mechanism for deletion is automatic purging. If the database is full, new policy audit information is discarded.
IDS_STG.2	**Policy Audits** – If the storage space is exhausted, the oldest data is saved and the most recent data is ignored.

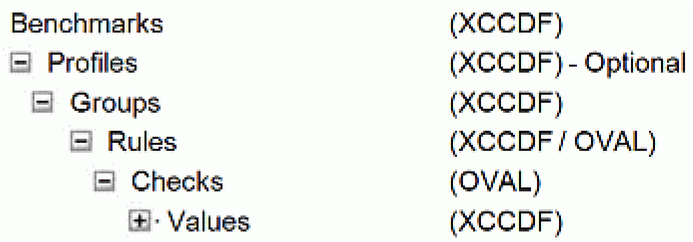
Table 28 – SFR to TSF Rationale

7 TOE Summary Specification

7.1 Policy Audits

The TOE evaluates the status of managed systems relative to audits that contain benchmarks. Benchmarks contain rules that describe the desired state of a managed system. Benchmarks are received through or imported into McAfee Benchmark Editor and, once activated, can be used by Policy Auditor. Benchmarks are written in the open-source XML standard formats Extensible Configuration Checklist Description Format (XCCDF) and the Open Vulnerability Assessment Language (OVAL). XCCDF describes what to check while OVAL specifies how to perform the check.

Benchmarks contain an organized set of rules that describe the desired state of a set of managed systems. Rules contain one or more checks that reference OVAL definitions. The structure of benchmarks is illustrated in the following figure.



Benchmarks	(XCCDF)
⊟ Profiles	(XCCDF) - Optional
⊟ Groups	(XCCDF)
⊟ Rules	(XCCDF / OVAL)
⊟ Checks	(OVAL)
⊞ Values	(XCCDF)

Figure 2 – Benchmark Structure

A benchmark typically contains one or more benchmark groups. Each benchmark group normally holds rules, values, and possibly additional child groups. Benchmark groups organize related rules and values into a common structure and provide descriptive text and references. Benchmark groups also allow users to select or deselect related rules. Finally, benchmark groups affect benchmark compliance scoring. A compliance score is calculated for each benchmark group, based on the rules and benchmark groups in it. The overall XCCDF score for the Benchmark is computed only from the scores on the benchmark objects benchmark groups and child rules.

Rules are the basic units of benchmarks. They describe the desired state or condition of a system and hold check references (signatures) and a scoring weight. Rules often contain a single check but may contain multiple checks combined with each other in a logical expression.

Policy Auditor analyzes managed systems to determine whether they comply with user-defined audits. Audits are composed of benchmarks that are generally supplied by McAfee, but may be imported from third-party sources or created by using Benchmark Editor. You must activate received or imported benchmarks in Benchmark Editor before you can use them in audits. Benchmarks contain rules that describe the desired state of a managed system.

The Policy Auditor Agent is a plug-in to the McAfee Agent. It extends the features of the McAfee Agent to support Policy Auditor. When audits are deployed to the McAfee Agent from Policy Auditor, the Policy Auditor Agent Plug-in decides when the audits can be run. The Agent Plug-in (executing as a system process) conducts the audits at the appropriate time and returns the results to the ePO server. The Policy Auditor Agent Plug-in can conduct audits when the managed system is not able to communicate with the ePO server (saving the audit results in process memory) and then return results to the ePO server once communication is re-established.

Policy Auditor provides the means to score audits according to four different scoring models (all of the scoring models described in the XCCDF 1.1.4 specifications). Policy Auditor uses the flat unweighted scoring model normalized to a value of 100 as its default scoring model. The other supported scoring models that may be configured are default scoring, flat scoring and absolute scoring.

Waivers provide a way to temporarily affect audit scoring for managed systems. Waivers are useful when you have a managed system that is non-compliant with a rule or a benchmark but you do not wish to bring the system into compliance for a temporary period. Policy Auditor provides three types of waivers that apply to a system being audited: exception waivers, exemption waivers and suppression waivers.

Exception waivers force the result of a benchmark rule to be Pass, thus potentially altering the benchmark score of a system. They have the following characteristics:

- Each waiver applies only to a single managed system. Exception waivers require you to select a benchmark and a rule contained in the benchmark that will not apply to an audit of the system.
- The selected benchmark and rule is included in an audit of the system, but the audit result of the particular rule is always Pass.
- Only benchmarks that are Active can be specified in the waiver.
- Exception waivers can be backdated. Scores for any results collected during the backdate time frame are recalculated.
- Rules used in an exception waiver appear in the audit results.

Exemption waivers are system-based and prevent a system from being audited. They have the following characteristics:

- Each waiver applies only to a single managed system.
- A system is not audited while the waiver is in effect.
- An exemption waiver can be created at any time for an existing system.
- An exemption waiver cannot be backdated.
- A system affected by an exemption waiver will not appear in the audit results.

Suppression waivers allow a rule to be included in an audit, but exclude the result, thus altering the benchmark score of a system. Suppression waivers have the following characteristics:

- Each waiver applies only to a single managed system.
- The benchmark's rule is included when the system is audited.
- Rule audit results are not included in the score.
- Only benchmarks that are Active can be specified in the waiver.
- Suppression waivers cannot be backdated.
- Rules used in a suppression waiver do not appear in the scoring for a system.
- Rules used in a suppression waiver appear in the audit results.

File integrity monitoring allows the designation of a set of files to monitor for changes. When a file is changed, the McAfee Policy Auditor agent plug-in generates an event that is sent to the ePO server. The file integrity interface allows the definition of one or more monitored paths, monitored files, and excluded paths and files. Excluded paths and files are not monitored. When coupled with a user-configured monitoring frequency, Policy Auditor creates a policy which is enforced on selected System Tree nodes by the agent plug-in.

Policy Auditor monitors the checksums of a file as well as the file size, create time, modified time, and file owner. When one or more of these values changes, the agent notes the change and sends an event back to the Policy Auditor server according to the monitoring frequency. The checksum is created by mathematically examining the file and creating a SHA-1 or MD5 digest to represent the file.

Policy Auditor creates a GUID to identify the baseline of each file. At each frequency check, it tests each file under the path and associates the information, including the last checked time, with the baseline GUID. Policy Auditor recalculates the information for each file. If a monitored file has been changed, the agent notifies the Policy Auditor server.

Queries are configurable objects that retrieve and display collected event records from policy audits 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 audits may be viewed by users with the "View System Tree" permission or 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 policy audit events include:

1. Compliance History — Retrieves information on compliance counts over time. This query type and its results depend on a Run Query server task that generates compliance events from the results of a (Boolean pie chart) query. Additionally, when creating a Compliance History query,

be sure the time unit matches the schedule interval for the server task. McAfee recommends creating the Boolean pie chart query first, followed by the server task that generates the compliance events, and finally the Compliance History query.

2. Events — Retrieves information on events sent from managed systems.
3. Managed Systems — Retrieves information about systems running the McAfee Security Agent.

Dashboards are an alternative mechanism for viewing the collected policy audit data. 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.

Policy audit data is automatically purged according to the configured Data Retention parameters. If the storage capacity of the database is exceeded, new policy audit event records are discarded and an SNMP trap is generated. The TOE does not provide any mechanism to modify policy audit data, and the only mechanism to delete policy audit data is the automatic purging based on the configured Data Retention parameters.

7.2 Identification

Users must log in to ePO with a valid user name and password supplied via a GUI before any access is granted by the TOE to TOE functions or data. When the credentials are presented by the user, ePO determines if the user name is defined and enabled. If not, the login process is terminated and the login GUI is redisplayed.

The supplied password is passed to Windows for validation. If it is successful, the TOE grants access to additional TOE functionality. If the validation is not successful, the login GUI is redisplayed. Note that all the Windows I&A protection mechanisms (e.g., account lock after multiple consecutive login failures) that may be configured still apply since Windows applies those constraints when performing the validation.

Upon successful login, 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. Those attributes remain fixed for the duration of the session (until the user logs off). If the attributes for a logged in user are changed, those changes will not be bound to a session until the next login by the user.

7.3 Management

The TOE's Management Security Function provides administrator support functionality that enables a user to configure and manage TOE components. Management of the TOE may be performed via the ePO GUI. Management permissions are defined per-user.

The TOE provides functionality to manage the following:

1. ePO User Accounts,
2. Permission Sets,
3. Audit Log,
4. Event Log,
5. Event Filtering,
6. System Tree,
7. Tags,
8. Product Policies,
9. Queries,
10. Dashboards,
11. Benchmarks,
12. Policy Auditor,
13. Policy Audits, and
14. Waivers.

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.

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 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.

When a new ePO product extension (e.g., Policy Auditor) is installed it may add one or more groups of permissions to the permission sets. Initially, the newly added section is listed in each permission set as being available but with no permissions yet granted. The global administrators can then grant permissions to users through existing or new permission sets.

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 specified 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. If the database space is exhausted, new entries are discarded and an SNMP trap is generated.

7.3.4 Policy Audit Event Log Management

A global administrator may configure the length of time policy audit event records are to be saved. Entries beyond that time are automatically purged.

The policy audit event records 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 Event Filtering Management

A global administrator may view and modify the list of events that are forwarded from the agents to the ePO server. The list of events is common to all agents.

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 you to organize your systems within units called groups.

Groups have these characteristics:

1. Groups can be created by global administrators or users with both the “View "System Tree" tab” and “Edit System Tree groups and systems” permissions.
2. A group can include both systems and other groups.
3. Groups are modified or deleted by a global administrator or user with both the “View "System Tree" tab” and “Edit System Tree groups and systems” permissions.

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.

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

7.3.7 Tag Management

Tags are like labels that you can apply to one or more systems, automatically (based on criteria) or manually. Once tags are applied, you can use them to organize systems in the System Tree or run queries that result in an actionable list of systems.

There are two types of tags:

1. Tags without criteria. These tags can be applied only to selected systems in the System Tree (manually) and systems listed in the results of a query.
2. Criteria-based tags. These tags are applied to all non-excluded systems at each agent-server communication. Such tags use criteria based on any properties sent by an agent. They can also be applied to non-excluded systems on demand.

Users with the “Create and edit tags and tag criteria” permission or a Global Administrator may manage all types of tags. Users with the “Create and edit tags” permission or a Global Administrator may manage tags without criteria only. In addition, users with the “Apply, exclude, and clear tags” permission may associate or disassociate tags from systems.

Tags can use criteria that are evaluated against every system:

1. Automatically at agent-server communication.
2. When the Run Tag Criteria action is taken.
3. Manually on selected systems, regardless of criteria.

Tags without criteria can only be applied manually to selected systems.

7.3.8 Product Policy Management

A product policy is a collection of settings that you create, configure, and then enforce. Product policies ensure that McAfee Agent and Policy Auditor are configured and perform accordingly on the managed systems. Different product policies for the same product may be configured for different groups. When you reconfigure product policy settings, the new settings are delivered to, and enforced on, the managed systems at the next agent-server communication.

The permissions associated with product policy management are:

1. View settings (McAfee Agent) - This permission grants the ability to view settings for the McAfee Agent product policy.
2. View settings (Policy Auditor Agent) - This permission grants the ability to view settings for the Policy Auditor Agent product policy.
3. View and change settings (McAfee Agent) - This permission grants the ability to view, create, delete, enable and modify settings for the McAfee Agent product policy.
4. View and change settings (Policy Auditor Agent) - This permission grants the ability to view, create, delete, enable and modify settings for the Policy Auditor Agent product policy.

Product policies are applied to any group or system by one of two methods, inheritance or assignment. Inheritance determines whether the product policy settings for a group or system are taken from its parent. By default, inheritance is enabled throughout the System Tree. When you break this inheritance by assigning new product policies anywhere in the System Tree, all child groups and systems that are set to inherit the product policy from this assignment point do so. A Global Administrator can assign any product policy in the Policy Catalog to any group or system. Assignment allows you to define product policy settings once for a specific need, and then apply the product policy to multiple locations.

All product policies are available for use by any user, regardless of who created the product policy. To prevent any user from modifying or deleting other users' named product policies, each product policy is assigned an owner — the user who created it. Ownership provides that no one can modify or delete a product policy except its creator or a global administrator. When you delete a product policy, all groups and systems where it is currently applied inherit the product policy of their parent group.

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

7.3.9 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.

7.3.10 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

7.3.11 Benchmark Management

You may create your own benchmarks. Benchmark Editor contains a Check Catalog that allows you to select any check that the system contains. You may also create your own checks. Operations on benchmarks and checks may be performed according to the following permissions that may be granted to users (a global administrator may perform all operations):

1. Activate benchmarks

2. Apply labels
3. Create, delete and apply labels
4. Create, delete and import checks
5. Create, delete, modify and import benchmarks
6. Create, delete, modify, import and unlock benchmarks
7. Edit benchmark tailoring
8. Edit existing benchmarks
9. View and export benchmarks
10. View and export checks

The TOE provides benchmarks to the Benchmark Editor. Benchmarks must be activated before they can be used in audits. Benchmark Editor may also be used to create, modify, tailor, and profile benchmarks. Benchmarks supplied by McAfee may not be modified (other than tailoring).

Tailoring is a way to customize or override some, but not all, aspects of benchmarks. Tailoring allows the user to enable and disable rules and override values. Tailored benchmarks can be updated by the original benchmark author and still retain its tailoring. You can tailor McAfee-provided benchmarks.

Profiling allows you to create sets of tailored groups, rules, and values that are targeted toward different computer system configurations and threat risks. Profiles cannot be added to or deleted from McAfee-supplied benchmarks.

A benchmark will have one of these status types:

1. Received – The default state when a benchmark is created.
2. Edit — when you edit a Received benchmark, it is assigned the Edit status.
3. Tailor — When you tailor a Received benchmark, it is assigned the Tailor status.
4. Edit_Tailor — a benchmark may be assigned the Edit_Tailor status when you tailor a benchmark that is already in Edit status or when you edit a benchmark that is already in Tailor status.
5. Activated — Activation is the final step in making a benchmark available to other applications.
6. Archived — when you activate a bookmark, the original Received benchmark is given the status of Archived.

Only activated benchmarks are used when performing policy audits on managed systems.

Labels are a method for classifying a benchmark or check for aid in future searches. Each benchmark or check can have zero or more labels attached to it. You may create, delete or apply labels to benchmarks or checks.

7.3.12 Policy Auditor Management

Settings may be configured in the Policy Auditor extension that influence the audits performed on the managed systems or the reporting of the results of those audits.

Policy Auditor allows a global administrator to modify the score that constitutes passing an audit or failing an audit. A score equal to or less than the Maximum Low Score is considered to be below the desired level that you want a system to achieve.

A global administrator may modify the Data Retention parameters to set how long Policy Auditor retains its audit data. The Data Retention Unit Type setting offers you to choose from days, weeks, months or years. The Data Retention Units setting allows you to specify the units of time in conjunction with the Data Retention Unit Type setting.

Policy Auditor calculates a score for managed systems based upon the results of policy audits. The scoring model used for this calculation may be configured by a global administrator.

7.3.13 Policy Audit Management

An audit gathers data about managed systems to determine whether they are in compliance with corporate and industry security standards. An audit consists of:

1. A benchmark or a selected profile within a benchmark
2. Managed Systems assigned to this policy audit
3. A frequency (how often the data should be gathered)

Operations on policy audits (create, delete, view and modify) may be performed according to the following permissions that may be granted to users (a global administrator may perform all operations):

1. Add, remove, and change Audits and Assignments
2. View Audits and Assignments

Policy Auditor provides two methods for assigning systems to a policy audit. The first method allows you to include managed systems by specifying a system, group or tag. The second method allows you to include managed systems by specifying Criteria. Criteria can be defined by selecting properties and using comparison operators and values to represent managed systems. You can select one or more of the following properties:

1. CPU Serial Number
2. CPU Type
3. CPU Speed
4. Default Language
5. Description
6. DNS Name

7. Domain Name
8. Free Disk Space (MB)
9. Free Memory (bytes)
10. IP Address
11. IPX Address
12. Is 64 bit OS
13. Is Laptop
14. MAC Address
15. Number of CPUs
16. OS Build Number
17. OS OEM Identifier
18. OS Platform
19. OS Service Pack Version
20. OS Type
21. OS Version
22. Subnet Address
23. Subnet Mask
24. System Name
25. Time Zone
26. Total Disk Space (MB)
27. Total Physical Memory (bytes)
28. User Name

7.3.14 Waiver Management

A global administrator or user with the “View Waivers” permission may request a waiver. The user specifies the managed system to which the waiver applies, the benchmark and rule (if applicable), and the time period for which the waiver is applicable. The waiver is not in effect until the waiver has been granted.

A global administrator or user with the “Grant and modify Waivers” permission may grant a waiver that has been requested. The same user may request and grant a waiver if that user has the required permissions. Once granted, the waiver is in effect according to the time period specified in the request or until it is expired.

A global administrator or user with the “Grant and modify Waivers” permission may expire a waiver that is in effect. This effectively changes the time period specified when the waiver was requested.

A global administrator or user with the “Grant and modify Waivers” permission may delete a waiver that has been requested (but not granted) or a waiver that has been granted but whose associated time period has not yet commenced.

7.3.15 File Integrity Management

Users may create, view, modify, apply and delete File Integrity Monitoring policies based upon their permissions. Management actions associated with File Integrity Monitoring are as follows:

1. Query — The user specifies the managed system to which the File Integrity Monitoring policy applies, the benchmark and rule (if applicable), and the time period for which the policy is applicable. The policy is not in effect until the waiver has been granted.
2. Create, apply, query, modify, and delete – The user can create a File Integrity Monitoring policy (including specific files and subfolders of the file’s directory), apply the policy to an agent, query policies as stated above, modify the policy to include/exclude files, and delete the policy.

7.4 Audit

The Audit Log maintains a record of ePO user actions. The auditable events are specified in the Audit Events and Details table in the FAU_GEN.1 section.

The Audit Log entries display in a sortable table. For added flexibility, you can also filter the log so that it only displays failed actions, or only entries that are within a certain age. The Audit Log displays seven columns:

1. Action — The name of the action the ePO user attempted.
2. Completion Time — The 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 Global Administrator or users with the “View Audit Log” permission. The Audit Log entries are automatically purged based upon a Global Administrator-configured age. Other than automatic purging, no mechanisms are provided for users to modify or delete entries. The audit log entries are stored in the database; if space is exhausted, new entries are discarded.

7.5 System Information Import

ePO offers integration with both Active Directory and NT domains as a source for systems, and even (in the case of Active Directory) as a source for the structure of the System Tree.

If your network runs Active Directory, you can use Active Directory synchronization to create, populate, and maintain part or all of the System Tree with Active Directory synchronization. Once defined, the System Tree is updated with any new systems (and subcontainers) in your Active Directory.

There are two types of Active Directory synchronization (systems only and systems and structure). Which one you use depends on the level of integration you want with Active Directory.

With each type, you control the synchronization by selecting whether to:

1. Deploy agents automatically to systems new to ePolicy Orchestrator.
2. Delete systems from ePolicy Orchestrator (and remove their agents) when they are deleted from Active Directory.
3. Prevent adding systems to the group if they exist elsewhere in the System Tree.
4. Exclude certain Active Directory containers from the synchronization. These containers and their systems are ignored during synchronization.

Use may also your NT domains as a source for populating your System Tree. When you synchronize a group to an NT domain, all systems from the domain are put in the group as a flat list. You can manage those systems in the single group, or you can create subgroups for more granular organizational needs.

When systems are imported, their placement in the System Tree may be automatically determined by criteria-based sorting of two forms. IP address sorting may be used if IP address organization coincides with your management needs for the System Tree. Tag based sorting may be used to sort systems based on tags associated with them.

The server has three modes for criteria-based sorting:

1. Disable System Tree sorting
2. Sort systems on each agent-server communication — Systems are sorted again at each agent-server communication. When you change sorting criteria on groups, systems move to the new group at their next agent-server communication.
3. Sort systems once — Systems are sorted at the next agent-server communication and marked to never be sorted again.

7.5.1 SCAP Data Exchange

Benchmark Editor provides several ways to bring benchmarks into your system. These provide the flexibility to develop an updating strategy to ensure that your benchmarks stay up-to-date.

The primary means for obtaining benchmark content is through the standard ePO content delivery mechanism. If you have configured ePO to use Custom Benchmarks and Checks Synchronization, then McAfee-supplied benchmarks and checks are automatically added to the Benchmark Catalog and the Check Catalog, respectively, according to the schedule you have set.

A number of benchmarks have been developed by third-party vendors. You can download these benchmarks as single archive (ZIP) or XML files and import them into the Benchmark Catalog.

You can export benchmarks from the Benchmark Catalog as single archive (ZIP) files. Users can then share these benchmarks within your organization or with others.

Benchmarks may be imported by a global administrator or a user with either the “Create, delete, modify, and import benchmarks” or “Create, delete, modify, import, and unlock benchmarks” permission.

Policy audits and policy audit results may be exported in two different formats: XCCDF and OVAL. Benchmarks may be exported by a global administrator or a user with the “View and Export benchmarks” permission.

Export in XCCDF format creates a file that conforms to the XCCDF results schema, as defined in the XCCDF specification. It contains the latest results for all of the systems and benchmarks in the policy audit. The results file can be consumed by any tool that understands the XCCDF results schema.

Export in OVAL format creates an OVAL results file that conforms to the OVAL results schema. This file can be consumed by any tool that understands the OVAL results schema.