Security Target

McAfee Policy Auditor 6.4 with ePolicy Orchestrator 5.10

Version 1.0

October 15, 2018

Prepared For:

McAfee LLC

2821 Mission College Blvd.

Santa Clara, CA 95054

www.mcafee.com

Prepared By:

Primasec Ltd

Le Domaine de Loustalviel

11420 Pech Luna, France

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Policy Auditor 6.4 with McAfee ePolicy Orchestrator 5.10. 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

1 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 6.4 with ePolicy Orchestrator 5.10
ST Revision	1.0
ST Publication Date	October 15, 2018
Author	Primasec Ltd

1.2 TOE Reference

TOE Reference	McAfee Policy Auditor 6.4 with McAfee ePolicy Orchestrator 5.10
TOE Type	Security Management

1.3 Document Organization

2 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
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

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

3 The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1, Revision 5 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.

4 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

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

TERM	DEFINITION
AD	Active Directory
AHA	Advanced Host Assessment
CC	Common Criteria version 3.1, R5 (ISO/IEC 15408)
CPE	Common Platform Enumeration
CPU	Central Processing Unit
DBMS	DataBase Management System
DNS	Domain Name System
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
GUI	Graphical User Interface
I&A	Identification & Authentication
IP	Internet Protocol
IT	Information Technology
JSON	JavaScript Object Notation
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
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
PDC	Primary Domain Controller
PP	Protection Profile

TERM	DEFINITION
RAM	Random Access Memory
SCAP	Security Content Automation Protocol
SF	Security Function
SFR	Security Functional Requirement
SNMP	Simple Network Mail Protocol
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
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

6 McAfee Policy Auditor 6.4 is an agent-based, purpose-built IT policy audit solution that automates the processes required for system compliance audits and inventory scans.

7 Policy Auditor measures compliance by comparing the actual configuration of a system to the defined wanted state of a system. When a system is audited Policy Auditor returns a score indicating how well the system complied with the audit, supporting the four scoring models described in the Extensible Configuration Checklist Description Format (XCCDF) 1.2 specifications.

8 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 XCCDF and the Open Vulnerability Assessment Language (OVAL). XCCDF describes what to check while OVAL specifies how to perform the check.

9 The Advanced Host Assessment (AHA) feature provides core functionality to create inventory scan tasks. Inventory scan tasks collect information from managed systems, such as installed applications, operating systems details, services, registered extensions, network interfaces, system information, CPE and ports in use. Scan results can then be managed via ePO.

10 File integrity monitoring provides notification of changes to specified text files on managed systems.

11 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.

12 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. Plug-Ins executing on the managed systems perform the policy audit and inventory scans and return the results to Policy Auditor. Policy Auditor allows policy audits and inventory scans to be conducted on various releases of operating systems detailed in the McAfee Knowledge Centre Technical Article ID KB72961, at the following link: https://kc.mcafee.com/corporate/index?page=content&id=KB72961.

13 The platforms covered in the evaluated configuration are as follows:

Managed systems:

- Windows 2012 Server R2 Update
- Windows Server 2016
- Windows 10 1709
- Red Hat Enterprise Linux 7

ePO Server:

- Windows Server 2016 with MS SQL Server 2016

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

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

1.7 TOE Description

16 The TOE helps organizations monitor policy compliance on their assets by performing policy audits and inventory scans on those assets. This solution allows managers to continuously monitor the state of their assets. McAfee Policy Auditor utilizes the Security Content Automation Protocol (SCAP) standard and the JavaScript Object Notation standard (JSON) to specify computer security configuration information and inventory checks, respectively.

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

1.7.1 Physical Boundary

18 The TOE is a software TOE and includes:

On the dedicated server platform -

1. The ePO application
2. The Policy Auditor extension
3. The Benchmark Editor extension
4. Advanced Host Assessment
5. The AHA Content Distributor
6. Agent Handler

On each managed system to be audited -

1. McAfee Agent
2. The Policy Auditor Agent Plug-In
3. The Audit Content Plug-In
4. The AHA Plug-In
5. The AHA Content Update Plug-In

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

20 The following documentation provided to end users is included in the TOE boundary (all in .pdf format):

1. *McAfee Policy Auditor 6.4.0 Installation Guide*
2. *McAfee Policy Auditor 6.4.0 Product Guide*
3. *McAfee Policy Auditor 6.4.0 Interface Reference Guide*
4. *Installation Guide McAfee ePolicy Orchestrator 5.10.0*
5. *Product Guide McAfee ePolicy Orchestrator 5.10.0*
6. *McAfee Policy Auditor 6.4.0 For use with ePolicy Orchestrator 5.10.0 Common Criteria Evaluated Configuration Guide*
7. *McAfee Agent 5.5.1 Product Guide*
8. *McAfee Agent 5.5.1 Installation Guide*

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

TOE COMPONENT		FILE DESCRIPTION	Filke Name
TOE Software	Policy Auditor 6.4	Policy Auditor 6.4 Product Package	6_4_0_173_PA.zip
		Policy Auditor 6.4 Agent for Windows	6_4_0_252_PAA_WIN.zip
		Policy Auditor 6.4 Agent for Linux	6_4_0_252_PAA_Linux.zip
	ePolicy Orchestrator 5.10	ePO 5.10.0.2428	EPO510_2428_5_LR2.zip
		McAfee Agent 5.5.1.342	MA551WIN.zip MA551LNX.zip
		MA ePO policy and reporting extension 5.5.1.342	EPOAGENTMETA.zip
		McAfee Agent Help 5.5.1.342	help_ma_551.zip

TOE COMPONENT		FILE DESCRIPTION	Filke Name
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

22 All TOE software and documentation is available for download from the McAfee website. Download of software requires a current Grant Number.

23 The evaluated configuration consists of a single instance of the management system (with ePO plus Policy Auditor, Benchmark Editor, Advanced Host Assessment and AHA Content Distributor extensions, and the Agent Handler) and one or more instances of managed systems (with McAfee Agent, Policy Auditor Agent Plug-in, Audit Content Plug-in, AHA Plug-in and AHA Content Update Plug-in).

24 ePO supports both ePO authentication and Windows authentication of user account credentials.

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

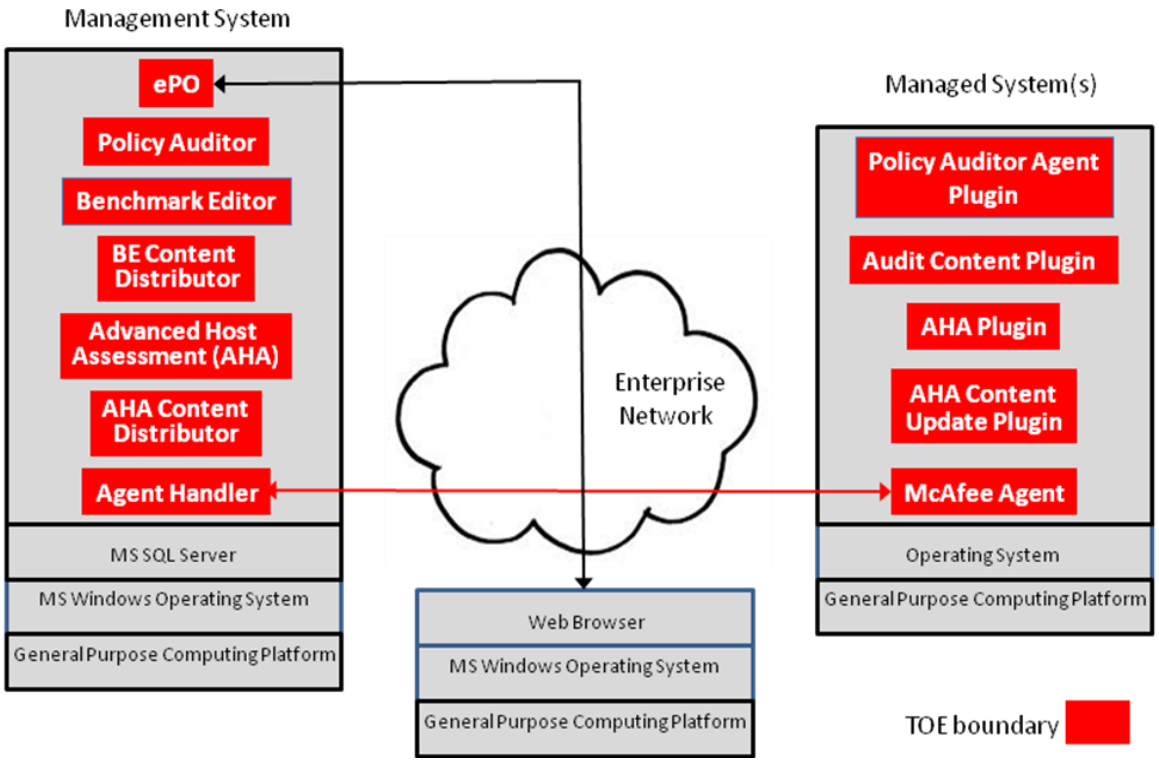


Figure 1 – TOE Boundary

26 The following specific configuration options apply to the evaluated configuration:

1. McAfee Agent wake-up calls are enabled.

2. Incoming connections to McAfee Agents are only accepted from the configured address of the ePO server.
3. The only repository supported is the ePO server.
4. Updates to the TOE software are not permitted in the evaluated configuration.

27 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

28 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.

29 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	64-bit Intel Pentium D or higher 2.66 GHz or higher
Memory	8 GB available RAM recommended minimum
Free Disk Space	20 GB — Recommended minimum
Monitor	1366x768, 256-color, VGA monitor or higher
Operating System	Windows Server 2016
DBMS	Microsoft SQL Server 2016
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
Miscellaneous	Microsoft updates Microsoft Visual C++ 2010 Redistributable Package. Required — Installed automatically. MSXML3.0 and 6.0

Table 4 – Management System Component Requirements

30 McAfee Agent, Policy Auditor Agent Plug-In, Audit Content Plug-in, AHA Plug-in and AHA Content Update Plug-in execute on one or more systems whose policy settings are to be audited, or inventories scanned. The supported platforms for these components in the evaluated configuration are:

SUPPORTED AGENT OS
Windows 10 1709
Windows 2012 Server R2
Windows Server 2016

SUPPORTED AGENT OS
Red Hat Enterprise Linux 7

Table 5 – Supported Agent Platforms

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

COMPONENT	MINIMUM HARDWARE REQUIREMENTS
Memory	512MB RAM
Free Disk Space	50MB, excluding log files
Processor speed	1 GHz or higher
Network Card	Ethernet, 10Mb or higher

Table 6 – Agent Platform Hardware Requirements

32 The management system is accessed from remote systems via a browser, and the evaluated configuration uses Microsoft Internet Explorer 11 Web browser.

33 The TOE authenticates user credentials during the logon process through the ePolicy Orchestrator or via Windows. User accounts must be defined within ePO in order to associate permissions with the users.

1.7.3 Logical Boundary

34 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 and Inventory Scans	The TOE audits managed systems to determine policy compliance on those systems. The TOE can also specify and run inventory scans. Results of the policy audits and inventory scans 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.
Cryptographic Support	The TOE protects transmissions between the ePO and the McAfee Agent from disclosure and undetected modification by encrypting the transmissions. The TOE makes use of the cryptographic services provided by RSA BSAFE Crypto-C Micro Edition v4.0.1 (for McAfee Agent), and OpenSSL v1.0.2p library with FIPS module v2.0.16 (for ePO). These services include encryption/decryption, key generation and key destruction. The TOE checks the integrity and authenticity of data received from McAfee servers, making use of digital signature verification provided by RSA BSAFE Crypto-C Micro Edition v4.1.2 on ePO.
Identification & Authentication	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 either by ePO or 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).

TSF	DESCRIPTION
Management	The TOE's Management Security Function provides support functionality that enables users to configure and manage TOE components. Management of the TOE is done 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). This functionality ensures that all the defined systems in the enterprise network are known to the TOE and may be configured to be managed.
Data Exchange	The TOE is 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. The TOE is also able to import Advanced Host Assessment data in JSON format for inventory scans.

Table 7 – Logical Boundary Descriptions

1.7.4 TOE Data

35 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.			✓
ePO User Accounts	ePO user name, authentication configuration, enabled status, Administrator status and permission sets for each user authorized to access TOE functionality on the management system.	✓		
Administrator Status	Users assigned to the "administrator" permission set, which is a superset of all other permission sets. This includes the default "admin" user account created when ePO is installed. Users assigned to this permission set are known as "Administrator"		✓	
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.			✓

TSF Data	Description	AD	UA	GE
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.			✓
Inventory Scan	Causes inventory reports to be generated for managed systems.			✓
Product Policy	A collection of settings created, configured, then enforced 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 1.2 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

36 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 the IT Environment supplied operating systems.

37 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 ensure 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.

38 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.

39 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.

40 The TOE consists of distributed components. Communication between the components relies upon cryptographic functionality provided by the TOE to protect the information exchanged from disclosure or modification.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

41 The TOE is Common Criteria Version 3.1 Revision 5 (April 2017) 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

42 The TOE does not claim conformance to a Protection Profile.

3 Security Problem Definition

43 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.

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

3.1 Threats

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

46 The TOE addresses the following threats:

THREAT	DESCRIPTION
T.SCNCFG	Improper security configuration settings may exist in a managed system, allowing an unauthorized user to access the assets that it holds, possibly without detection.
T.SCNMLC	A user could execute malicious code on a managed system causing modification of the system protected data or undermining the system security functions.
T.SCNVUL	Vulnerabilities may exist in a managed system that could result in access by an unauthorized user to the assets that it holds.

Table 9 – Threats in the TOE Environment

THREAT	DESCRIPTION
T.COMDIS	An unauthorized user may attempt to bypass a security mechanism, and hence disclose the data collected and produced by the TOE.
T.COMINT	An unauthorized user may attempt to bypass a security mechanism, and hence compromise the integrity of the data collected and produced by the TOE.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE, causing inappropriate configurations to go undetected.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE, causing inappropriate configurations to go undetected.

THREAT	DESCRIPTION
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the TOE'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, resulting in potential compromise of managed systems.
T.FALREC	An administrator may fail to recognize vulnerabilities or inappropriate activity when reviewing data acquired from managed systems, resulting in potential compromise of those managed systems and the assets that they hold.

Table 10 – Threats against the TOE

3.2 Organizational Security Policies

47 An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section describes the Organizational Security Policies that the TOE is designed for use with.

POLICY	DESCRIPTION
P.COMPLY	System compliance with policy within the organization shall be determined, and records maintained.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.IMPORT	The TOE shall be able to import data about managed systems from LDAP servers.
P.DATAX	The TOE shall be able to exchange SCAP Benchmark Assessment data with external systems, and to import Advanced Host Assessment data.
P.CRYPTO	When carrying out cryptographic functions to protect the integrity of data in transit the TOE shall use cryptographic modules that have been validated to FIPS 140.

Table 11 – Organizational Security Policies

3.3 Assumptions

48 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 appropriate access to the systems it is intended to monitor.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to authorized users.

ASSUMPTION	DESCRIPTION
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.PROTECT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.[1]
A.PLATFORM	The hardware, operating system, and other software on which the TOE depends, operate correctly.

Table 12 – Assumptions

[1] Whilst this would be considered normal practice for server components of the TOE in an enterprise environment, it should be acknowledged that managed systems may not have the same level of protection.

4 Security Objectives

4.1 Security Objectives for the TOE

49 The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.PA	The TOE must be able to audit the configuration of computers on a network, and provide notification of deviations from a defined configuration.
O.IS	The TOE must be able to scan the inventories of computers on a network, and provide reports on system configuration.
O.INT	The TOE must be able to detect and report changes to designated files on computers on a network.
O.ACCESS	The TOE must restrict user access to only authorized TOE functions and data.
O.AUDIT	The TOE must generate audit records for data accesses and use of the TOE functions on the management system.
O.AUDIT_PROTECT	The TOE must provide the capability to protect the confidentiality and integrity of PA records and audit information generated by the TOE.
O.AUDIT_REVIEW	The TOE must provide the capability for authorized administrators to review PA records and audit information generated by the TOE.
O.CRYPTO	The TOE must provide cryptographic functionality and protocols required for the TOE to securely transfer information between distributed portions of the TOE, and must use only cryptographic modules that have been validated to FIPS 140.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data on the management system.
O.IMPORT	The TOE must provide mechanisms to import system data from Active Directory (LDAP servers).
O.DATAX	The TOE must provide mechanisms to exchange SCAP Benchmark Assessment data, and to import JSON Advanced Host Assessment data.

Table 13 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

50 The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE. PHYSICAL	Those responsible for the TOE must ensure that the hardware on which the TOE and IT environment software are installed is protected from any physical attack.

OBJECTIVE	DESCRIPTION
OE.PLATFORM	The hardware, operating system, and other software on which the TOE depends, must operate correctly.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner that is consistent with IT security.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.
OE.INTROP	The TOE must be interoperable with the managed systems that it monitors.
OE.PERSON	Personnel working as authorized administrators must be carefully selected and trained for proper operation of the System.
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.STORAGE	The IT Environment must manage the storage and retrieval of TOE data in the databases as directed by the TOE.
OE.TIME	The IT Environment will provide reliable timestamps to the TOE
OE.LDAP	The IT environment must maintain confidentiality and integrity for data transferred between the TOE and the LDAP server.

Table 14 – Operational Environment Security Objectives

Application Note: With regard to OE.PHYSICAL it should be noted that different levels of protection will be appropriate for different hardware platforms. Whereas, to avoid large scale compromise of the TOE, it may be appropriate to protect the ePO server and DBMS hardware in server rooms with limited access, this may not be appropriate for managed computers. For such managed computers network users should provide protection appropriate to the data being stored and processed, and no special measures would be expected.

4.3 Security Objectives Rationale

51 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.PA	O.IS	O.INT	O.ACCESS	O.AUDIT	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.CRYPTO	O.EADMIN	O.IDAUTH	O.IMPORT	O.DATAX	OE.PHYSICAL	OE.PLATFORM	OE.CREDEN	OE.INSTALL	OE.INTROP	OE.PERSON	OE.DATABASE	OE.STORAGE	OE.TIME	OE.LDAP
A.ACCESS																	✓					
A.DATABASE																			✓			

OBJECTIVE / THREAT / ASSUMPTION	O.PA	O.IS	O.INT	O.ACCESS	O.AUDIT	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.CRYPTO	O.EADMIN	O.IDAUTH	O.IMPORT	O.DATAX	OE.PHYSICAL	OE.PLATFORM	OE.CREDEN	OE.INSTALL	OE.INTROP	OE.PERSON	OE.DATABASE	OE.STORAGE	OE.TIME	OE.LDAP
A.NOEVIL													✓		✓	✓		✓				
A.PROTECT													✓									✓
A.PLATFORM														✓						✓		
P.COMPLY	✓	✓				✓	✓														✓	
P.ACCACT					✓	✓	✓			✓											✓	
P.IMPORT											✓											
P.DATAX												✓										
P.CRYPTO								✓								✓						
T.SCNCFG	✓	✓	✓				✓															
T.SCNMLC	✓	✓	✓				✓															
T.SCNVUL	✓	✓	✓				✓															
T.COMDIS				✓	✓	✓	✓	✓		✓			✓	✓							✓	
T.COMINT				✓	✓	✓	✓	✓		✓			✓	✓							✓	
T.IMPCON				✓	✓	✓	✓	✓	✓	✓						✓					✓	
T.LOSSOF				✓	✓	✓	✓			✓											✓	
T.NOHALT				✓						✓			✓									
T.PRIVIL				✓	✓	✓	✓			✓											✓	✓
T.FALREC	✓	✓					✓											✓				

Table 15 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

52 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 OE.INTROP objective ensures the TOE has the needed access.
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.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 OE.INSTALL objective ensures that the TOE is properly installed and operated and the OE.PHYSICAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data. The OE. PERSON supports this assumption by requiring careful selection and training of authorized administrators.
A.PROTECT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. The OE.PHYSICAL objective provides for the physical protection of the TOE hardware and software. OE.LDAP specifies that communications with the LDAP server must be protected.
A.PLATFORM	The hardware, operating system, and other software on which the TOE depends, operate correctly. The OE.PLATFORM objective supports this assumption by requiring that the hardware, operating system, and other software on which the TOE depends operate correctly. The OE.STORAGE objective supports this assumption by requiring management of the storage and retrieval of TOE data in the databases is correctly managed.
P.COMPLY	System compliance with policy within the organization shall be determined, and records maintained. The O.PA objective calls for the audit of systems within the organization for compliance with defined policy configurations. The O.IS objective calls for inventory scans of systems within the organization to facilitate the detection of unwanted objects or system configurations. The O.AUDIT_PROTECT and O.AUDIT_REVIEW objectives support this by requiring that the records generated from policy audits be protected and available for review by authorized administrators. OE.TIME supports this by calling for reliable time stamps for the audit data.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE. The O.AUDIT objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.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. The O.AUDIT_PROTECT objective requires that the confidentiality and integrity of the audit records be protected. OE.TIME supports this by calling for reliable time stamps for the audit data.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
P.IMPORT	The TOE shall be able to import system data from Active Directory (LDAP servers). The O.IMPORT objective addresses this policy by requiring the TOE to provide functionality to import data about managed systems from LDAP servers.
P.DATAX	The TOE shall be able to exchange SCAP Benchmark Assessment data with external systems, and to import Advanced Host Assessment data. The O.DATAX objective addresses this policy by requiring the TOE to provide mechanisms to exchange SCAP data with external sources, and to import JSON data.
P.CRYPTO	When carrying out cryptographic functions to protect the integrity of data in transit the TOE shall use cryptographic modules that have been validated to FIPS 140. The TOE addresses this through O.CRYPTO, and the requirement that where options exist the correct modes are chosen on installation is addressed through OE.INSTALL.
T.SCNCFG	Improper security configuration settings may exist in a managed system, allowing an unauthorized user to access the assets that it holds, possibly without detection. The O.PA objective addresses this through audit of the configuration of computers on a network, and the O.IS objective works towards a similar goal through use of inventory scans. The O.INT objective calls for the ability to monitor changes to specified files. The O.AUDIT_REVIEW objective deals with the need to review the data gathered.
T.SCNMLC	A user could execute malicious code on a managed system causing modification of the system protected data or undermining the system security functions. The O.PA objective addresses this through audit of the configuration of computers on a network, and the O.IS objective allows for the detection of system content or configurations that could be exploited. The O.INT objective calls for the ability to monitor changes to specified files. The O.AUDIT_REVIEW objective deals with the need to review the data gathered from managed systems.
T.SCNVUL	Vulnerabilities may exist in a managed system that could result in access by an unauthorized user to the assets that it holds. The O.PA objective addresses this through audit of the configuration of computers on a network, and the O.IS objective allows for the detection of system content or configurations that could introduce vulnerabilities into the systems. The O.INT objective calls for the ability to monitor changes to specified files. The O.AUDIT_REVIEW objective deals with the need to review the data gathered from managed systems.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.COMDIS	An unauthorized user may attempt to bypass a security mechanism, and hence disclose the data collected and produced by the TOE. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.CRYPTO objective requires the TOE to provide cryptographic functionality and protocols to protect the data during transit. The OE.PLATFORM and OE.PHYSICAL objectives support the TOE through protection within the IT Environment. The audit objectives (O.AUDIT, O.AUDIT_PROTECT, O.AUDIT_REVIEW and OE.TIME) call for user activity to be audited, helping to detect attempted attacks.
T.COMINT	An unauthorized user may attempt to bypass a security mechanism, and hence compromise the integrity of the data collected and produced by the TOE. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.CRYPTO objective requires the TOE to provide cryptographic functionality and protocols to protect the data during transit. The OE.PLATFORM and OE.PHYSICAL objectives support the TOE through protection within the IT Environment. The audit objectives (O.AUDIT, O.AUDIT_PROTECT, O.AUDIT_REVIEW and OE.TIME) call for user activity to be audited, helping to detect attempted attacks.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE, causing potential intrusions to go undetected. The OE.INSTALL 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.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.CRYPTO objective requires the TOE to provide cryptographic functionality and protocols to protect the data during transit. Unauthorized modification of policy data being transferred to managed systems could affect the configuration of the TOE. The audit objectives (O.AUDIT, O.AUDIT_PROTECT, O.AUDIT_REVIEW and OE.TIME) call for user activity to be audited, helping to detect attempted attacks.

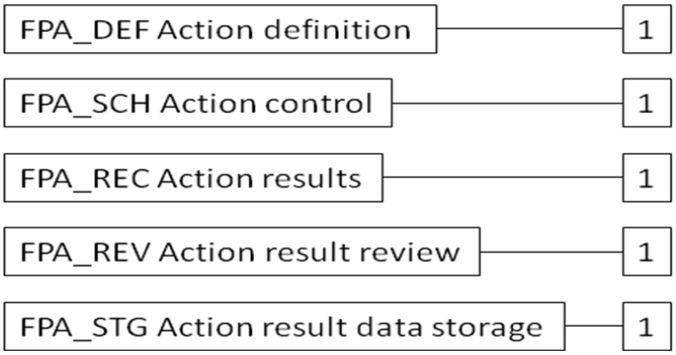
THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE, causing inappropriate configurations to go undetected. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The audit objectives (O.AUDIT, O.AUDIT_PROTECT, O.AUDIT_REVIEW and OE.TIME) call for user activity to be audited, helping to detect attempted attacks.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the TOE's collection and analysis functions by halting execution of the TOE. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.PHYSICAL objective calls for physical protection of the TOE within the IT environment, addressing attempts to halt the TOE through access to TOE physical components.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data, resulting in potential compromise of managed systems. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The audit objectives (O.AUDIT, O.AUDIT_PROTECT, O.AUDIT_REVIEW and OE.TIME) call for user activity to be audited, helping to detect attempted attacks. OE.LDAP specifies that communications with the LDAP server must be protected.
T.FALREC	An administrator may fail to recognize vulnerabilities or inappropriate activity when reviewing data acquired from managed systems, resulting in potential compromise of those managed systems and the assets that they hold. O.PA addresses the collection of policy audit data, based on defined configurations, and O.IS deals with inventory scans. OE.AUDIT_REVIEW requires functions to allow the presentation and review of this data. OE. PERSON supports these functions by requiring careful selection and training of TOE administrators in the use of these functions.

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

5 Extended Components Definition

5.1 Introduction

53 A new Policy Audit class (FPA) is required to help express clearly the functionality provided by Policy Auditor. Five families of requirements are included in the new class specifically to address the data collected and analysed by the TOE, each containing one component. These families of requirements address system data and provide for requirements about collecting, reviewing and managing this data.



5.2 FPA_DEF Action definition

Management: FPA_DEF.1

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

a) Control of access to the action definition functions.

Audit: FPA_DEF.1

55 There are no auditable events foreseen.

FPA_DEF.1 Action definition

Hierarchical to: No other components

Dependencies: No dependencies

FPA_DEF.1.1 **The TSF shall provide [assignment: *list of users*] with the capability to [assignment: *list of actions*] that determine [selection, choose one of: *the compliance of managed systems to defined standards, the presence of [assignment: list of objects or information] on managed systems*].**

5.3 FPA_SCH Action control

Management: FPA_SCH.1

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

a) Control of access to the action distribution functions.

Audit: FPA_SCH.1

57 There are no auditable events foreseen.

FPA_SCH.1 Action control

Hierarchical to: No other components

Dependencies: FPA_DEF.1* Action definition

FPA_SCH.1.1 **The TSF shall provide [assignment: *list of users*] with the capability to schedule [assignment: *list of actions*] to be executed on [assignment: *list of objects*] at defined intervals.**

5.4 FPA_REC Action results

Management: FPA_REC.1

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

There are no management actions foreseen

Audit: FPA_REC.1

59 There are no auditable events foreseen.

FPA_REC.1 Policy audit results

Hierarchical to: No other components

Dependencies: FPA_DEF.1* Action definition
FPA_SCH.1* Action control

FPA_REC.1.1 **The TSF shall record [assignment: *list of data attributes to be recorded*] when [assignment: *list of actions*] is carried out on [assignment: *list of objects*].**

5.5 FPA_REV Action result review

Management: FPA_REV.1

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

There are no management actions foreseen

Audit: FPA_REV.1

61 There are no auditable events foreseen.

FPA_REV.1 Action result review

Hierarchical to: No other components

Dependencies: FPA_DEF.1* Action definition
FPA_SCH.1* Action control

FPA_REV.1.1 **The TSF shall provide [assignment: *list of users*] with the capability to [assignment: *list of operations*] the results of [assignment: list of actions].**

FPA_REV.1.2 **The TSF shall provide the [assignment: *list of actions*] results in a manner suitable for the user to interpret the information.**

5.6 FPA_STG Action result data storage

Management: FPA_STG.1

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

There are no management actions foreseen

Audit: FPA_STG.1

63 There are no auditable events foreseen.

FPA_STG.1 Action result data storage

Hierarchical to: No other components

Dependencies: FPA_DEF.1* Action definition
FPA_SCH.1* Action control

FPA_STG.1.1 **The TSF shall protect the stored [assignment: *list of actions*] results from unauthorized modification and deletion.**

6 Security Requirements

64 The security requirements that are levied on the TOE are specified in this section of the ST. Extended components are identified using an asterisk (*).

6.1 Security Functional Requirements

65 The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and the extended components defined in section 5 of this ST, 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_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
Policy Audit	FPA_DEF.1*(1)	Action definition
	FPA_DEF.1*(2)	
	FPA_SCH.1*(1)	Action control
	FPA_SCH.1*(2)	
	FPA_REC.1*(1)	Action results
	FPA_REC.1*(2)	
	FPA_REV.1*	Action result review
	FPA_STG.1*	Action result data storage
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_SDI.2	Stored data integrity monitoring and action
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	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_ITT.1	Basic internal TSF data transfer protection
	FPT_TDC.1(1)	Inter-TSF Basic TSF data consistency
	FPT_TDC.1(2)	Inter-TSF Basic TSF data consistency

Table 17 – 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*].

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
FIA_ATD.1	All changes to TSF data (including password changes) result in an audit record being generated.	
FIA_UAU.2	Use of the user authentication mechanism	User identity, location
FIA_UID.2	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

Table 18 – Audit Events and Details

6.1.1.2 FAU_GEN.2 User Identity Association

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

6.1.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [*an ePO Administrator or user assigned to the Global reviewer permission set*] 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_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to apply [*sorting and filtering*] of audit data based on [*the fields listed in the table below*].

Event type	Field	Filter/Sort
ePO Operational Events	Action	Sort
	Completion time	Filter, Sort
	Details	Sort
	Priority	Sort
	Start Time	Filter, Sort
	Success	Filter, Sort
	User Name	Sort

Table 19 – Selectable audit review fields

6.1.1.6 FAU_STG.1 Protected Audit Trail Storage

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

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

6.1.2 Policy Audit (FPA)*

6.1.2.1 FPA_DEF.1 Action definition (1)*

FPA_DEF.1.1(1) The TSF shall provide [*an ePO Administrator or a user with permissions*] with the capability to [*create, edit, delete, import and activate policy audit benchmarks*] that determine [the compliance of *managed systems* to defined standards].

6.1.2.2 FPA_DEF.1 Action definition (2)*

FPA_DEF.1.1(2) The TSF shall provide [*an ePO Administrator or a user with permissions*] with the capability to [*create, edit, delete, import and activate inventory scans*] that determine [the presence of [installed *applications*[2], *services, open ports, operating systems, network related information*[3], *system information*[4], *registered file name extensions*] on managed systems].

6.1.2.3 FPA_SCH.1 Action control (1)*

FPA_SCH.1.1(1) The TSF shall provide [*an ePO Administrator or a user with permissions*] with the capability to schedule [*policy audits*] to be executed on [*managed systems*] at defined intervals.

6.1.2.4 FPA_SCH.1 Action control (2)*

FPA_SCH.1.1(2) The TSF shall provide [*an ePO Administrator or a user with permissions*] with the capability to schedule [*inventory scans*] to be carried out on [*managed systems*] at defined intervals.

6.1.2.5 FPA_REC.1 Action results (1)*

FPA_REC.1.1(1) The TSF shall record [*the following results:*

a) Benchmark ID;

b) Profile ID (if any);

c) Audit date;

d) Expiration date;

e) Score;

f) System group;

g) System name;

h) System tags;

[2] Applications also include patches, Windows applications, Windows features, package manager applications, browser extensions and plug-ins.
[3] Network related information includes IPv4 or IPv6 addresses, MAC address, DHCP enabled, Default gateway, primary and secondary DNS.
[4] System information includes FQDN, system manufacturer and model, GUID, BIOS, BIOS vendor, BIOS version, BIOS release date, system or motherboard serial number.

i) No. of rules passed;

j) *No. of rules failed*]

when [*a policy audit*] is carried out on [*a managed system*].

6.1.2.6 FPA_REC.1 Action results (2)*

FPA_REC.1.1(2) The TSF shall record [*the results of the scan*[5]] when [*an inventory scan*] is carried out on [*a managed system*].

6.1.2.7 FPA_REV.1 Action result review*

FPA_REV.1.1 The TSF shall provide [*an ePO Administrator or a user with permissions*] with the capability to [*read, collate and export*] the results of [*policy audits and inventory scans*].

FPA_REV.1.2 The TSF shall provide the [*policy audit and inventory scan*] results in a manner suitable for the user to interpret the information.

6.1.2.8 FPA_STG.1 Action result data storage*

FPA_STG.1.1 The TSF shall protect the stored [*policy audit results and inventory scan results*] from unauthorized modification and deletion.

6.1.3 Cryptographic Support (FCS)

6.1.3.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*see table below*] and specified cryptographic key sizes [*see table below*] that meet the following [*list of standards -see table below*].

Component	Purpose	Algorithm	Key size	Standard
ePO	TLS	*CTR_DRBG for deterministic random bit generation*	256 (AES), 2048 (RSA)	*NIST Special Publication 800-90 (CAVP DRBG algorithm certificate #1451)*
MA	TLS	*HMAC_DRBG for random number generation*	256 (AES), 2048 (RSA)	*NIST Special Publication 800-90A (CAVP DRBG algorithm certificate #191)*

Table 20 - Key generation

[5] Results of the scan may be in the form of a list of objects present on the scanned system, or information related to those objects, according to the scan definition.

6.1.3.2 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2 level 1*].

6.1.3.3 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [*list of cryptographic operations – see table below*] in accordance with a specified cryptographic algorithm [*cryptographic algorithm – see table below*] and cryptographic key sizes [*cryptographic key sizes – see table below*] that meet the following: [*list of standards – see table below*].

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards
Key Transport	RSA encrypt/decrypt	2048	Allowed in FIPS mode
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (operating in CBC mode)	256	FIPS 197
Secure Hashing	SHA-256	Not Applicable	FIPS 180-3
Signature verification	RSA	2048	FIPS 186-4

Table 21 - Cryptographic Operations

6.1.4 User Data Protection (FDP)

6.1.4.1 FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [*modifications to file content or ownership*] on all objects, based on the following attributes: [*file designated for monitoring by an ePO Administrator or a user with permissions*].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [*generate an event on the managed system and send it to the ePO server*].

6.1.5 Identification and Authentication (FIA)

6.1.5.1 FIA_ATD.1 User Attribute Definition

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

a) ePO User name;

b) Authentication configuration;

c) *Permission Sets*].

6.1.5.2 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.5.3 FIA_UID.2 User Identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.5.4 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) ePO user name; and

b) Permission sets].

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 during a 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 login.

6.1.6 Security Management (FMT)

6.1.6.1 FMT_MTD.1 Management of TSF Data

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

PERMISSION SET/CATEGORY	ASSOCIATED PERMISSION[6]
Agent Handler	View Agent Handlers (query)
	Edit (modify) Agent Handlers, Create and Edit (modify) Agent Handler Groups, Create and Edit Agent Handler Assignments (query), create, modify, delete)
Audit Log	View audit log (query)
	View and purge (delete) audit log
Dashboards	Use public dashboards (query)
	Use (view) public dashboards; create and edit (modify) private dashboards
	Use (view) public dashboards; create and edit (modify) private dashboards; make private dashboards public (modify)
ePO User Accounts	n/a (only allowed by an ePO Administrator) (query, create, delete, modify)
File Integrity Monitoring	View File Integrity Monitoring (query)
	Manage File Integrity Monitoring (create, use, query, modify, delete)
LDAP	Browse (query, modify, delete) registered servers
McAfee Agent	View (query) Policy Settings
	View and Change (modify) Policy Settings
	View (query) Task Settings
	View and Change (query, modify) Task Settings
Multi-Server Roll-Up Data	Run and Edit (use, query) Queries Based on Roll-Up Data
	Run and Edit (use, query) Queries Based on Roll-Up Data, Schedule Roll-Up Data Tasks (use), Purge Roll-Up Data (delete)
PA Admin: Benchmark Editor	Activate benchmarks (use)
	Edit benchmark tailoring (query, modify)
	Create, delete and apply (query, use, delete) labels
	Create, delete, modify, import and unlock benchmarks
	Create, delete and import checks
PA Admin: Findings	View and hide/unhide findings (query)
PA Admin: Issue Management	Create, edit, view, and purge assigned issues (create, modify, delete)
PA Admin: Policy Assignment Rule	View and Edit Rules (create, query, modify, delete)
PA Admin: Policy Auditor	Accept and delete events, and reset system baseline (query, delete)
	Allow access to Enterprise Manager (use)
	Grant and modify waivers (use)
	Allow access to File Entitlement (use)
	Add, remove and change audits and assignments (create, modify, delete)

[6] This column provides the name of the permission. The brackets show how this relates to the assignment in the FMT_MTD.1.

PERMISSION SET/CATEGORY	ASSOCIATED PERMISSION[6]
PA Admin: McAfee Policy Auditor Agent	View and change settings (query, modify)
PA Admin: McAfee Policy Auditor Rollup	View McAfee Policy Auditor rollup reports (query)
PA Agent Admin: McAfee Policy Auditor Agent	View and change settings (query, modify)
PA Agent Admin: Advanced Host Assessment	View and change Advanced Host Assessment policy (query, modify)
	View and change Advanced Host Assessment task (query, modify)
PA Audit Admin: Benchmark Editor	View and export checks (query, export)
	View and export benchmarks (query, export)
PA Audit Admin: Findings	View and hide/unhide findings (query)
PA Audit Admin: Issue Management	Basic Create issues and edit, view and purge issues created by or assigned to me (create, query, modify, delete)
PA Audit Admin: Policy Auditor	View waivers (query)
	Allow access to Enterprise Manager (use)
	Add, remove and change audits and assignments (create, modify, delete)
PA Benchmark Activator: McAfee Benchmark Editor	Activate benchmarks (use)
	View and export checks (query, export)
	View and export benchmarks (query, export)
PA Benchmark Editor: McAfee Benchmark Editor	Edit benchmark tailoring (modify)
	Create, delete and apply labels (create, delete, apply)
	Create, delete and import checks (create, delete, import)
	Create, delete, change and import benchmarks (create, delete, import)
PA Scan Admin: Advanced Host Assessment Agent	View scans and assignments (query)
	Add, remove and change scans and assignments (create, modify, delete)
PA Scan Admin: Advanced Host Assessment	View Advanced Host Assessment policy settings (query)
	View and change Advanced Host Assessment policy settings (query, modify)
PA Scan Admin: Server Tasks	Create, edit, view, run and end Scheduler tasks (create, modify, query, use)
	View the Scheduler tasks results in the Server Task Log (query)
PA Scan Admin: Systems	View the System Tree tab (query)
PA Scan Admin: System Tree access	Can search on the following nodes and portions of the system tress: My Organization (query)
	Can access the following nodes and portions of the system tree: My Organization (query, modify, delete)

PERMISSION SET/CATEGORY	ASSOCIATED PERMISSION[6]
PA Viewer: McAfee Benchmark Editor	View and export checks (query, export)
	View and export benchmarks (query, export)
PA Viewer: Findings	View findings (query)
PA Viewer: Policy Auditor	View waivers (query)
	View audits and assignments (query)
PA Viewer: Advanced Host Assessment Agent	View scans and assignments (query)
	Add, remove and change scans and assignments (query, create, modify, delete)
PA Viewer: Advanced Host Assessment	View and change Advanced Host Assessment policy (query, modify)
	View and change Advanced Host Assessment task (query, modify)
PA Waiver Granter: McAfee Benchmark Editor	View and export checks (query, export)
	View and export benchmarks (query, export)
PA Waiver Granter: Findings	View findings (query)
PA Waiver Granter: Issue Management	Create, edit, view and purge assigned issues (create, modify, query, delete)
PA Waiver Granter: Policy Auditor	View audits and assignments (query)
	Grant and change waivers (query, modify)
Policy Assignment Rule	View Rules (query)
	View and Edit Rules (create, query, modify, delete)
Product Investment Program	View Policy and Task Settings (query)
	View and Change Policy and Task Settings (query, modify)
Queries and Reports	Use public groups (query, use)
	Use public queries(query, use); create and edit private queries (create, query, modify, delete)
	Edit public groups (create, query, modify, delete); create and edit private groups (create, query, modify, delete); make private queries/reports public (modify)
Registered Servers	Database Server: View Registered Servers, View, Create and Edit Registered Servers (create, query, modify, delete)
	LDAP Server: View, Create and Edit Registered Servers (create, query, modify, delete)
	View Registered Servers: View, Create and Edit Registered Servers (create, query, modify, delete)
	ePO: View Registered Servers, View, Create and Edit Registered Servers (create, query, modify, delete)

PERMISSION SET/CATEGORY	ASSOCIATED PERMISSION[6]
	SNMP Server: View Registered Servers, View, Create and Edit Registered Servers (create, query, modify, delete)
Server Tasks	View Scheduler Tasks, View Scheduler Task Results in the Server Log (query)
	Create, Edit, Run, View and End Scheduler Tasks, View Scheduler Task Results in the Server Log (create, query, modify, use, delete)
Software	Master Repository: View Packages, Add, Remove and Change Packages, Perform Pull Tasks (create, query, delete)
Software Manager	View List of Available Products (query)
Systems	System Tree: View "System Tree" Tab, Wake Up Agents, View Agent Activity Log, Edit System Tree Groups and Systems, Deploy Agents (query, modify, delete)
System Tree access	My Organization (query, modify, delete)

Table 22 – TSF Data Access Permissions

6.1.6.2 FMT_SMF.1 Specification of Management Functions

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

a) ePO User Account management,

b) Permission Set management,

c) Audit Log management,

d) Policy Audit Event Log management,

e) Systems and System Tree access,

f) Registered Servers management,

g) Product Policy management,

h) Query and report management,

i) Dashboard management,

j) Benchmark management,

k) Policy Auditor management,

l) Policy Audit management,

m) Inventory Scan management,

n) Waiver management, and

o) File Integrity Monitoring management].

6.1.6.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles: [*Administrator and User with Selected Permissions*].

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

Application Note: In ePO a role is called a permission set.

6.1.7 Protection of the TSF (FPT)

6.1.7.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

6.1.7.2 FPT_TDC.1(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) When conflicting information is received from different sources, highest priority is given to information learned from the McAfee Agent, then to Active Directory,].

6.1.7.3 FPT_TDC.1(2) Inter-TSF Basic TSF Data Consistency

FPT_TDC.1.1(2) The TSF shall provide the capability to consistently interpret [*SCAP Benchmark Assessments and JSON Advanced Host Assessment data*] when shared between the TSF and another trusted IT product.

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

6.2 Security Assurance Requirements

66 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
ASE: Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements

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

Table 23 – Security Assurance Requirements at EAL2

6.3 CC Component Hierarchies and Dependencies

67 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_SAR.3	No other components	FAU_SAR.1	Satisfied
FAU_STG.1	No other components	FAU_GEN.1	Satisfied
FPA_DEF.1* (1)&(2)	No other components	None	n/a
FPA_SCH.1* (1)&(2)	No other components	FPA_DEF.1*	Satisfied

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FPA_REC.1* (1)&(2)	No other components	FPA_DEF.1*, FPA_SCH.1*	Satisfied
FPA_REV.1*	No other components	FPA_DEF.1*, FPA_SCH.1*	Satisfied
FPA_STG.1*	No other components	FPA_DEF.1*, FPA_SCH.1*	Satisfied
FCS_CKM.1	No other components	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	Satisfied by FCS_COP.1 and FCS_CKM.4
FCS_CKM.4	No other components	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FCS_CKM.1
FCS_COP.1	No other components	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FCS_CKM.1 and FCS_CKM.4
FDP_SDI.2	FDP_SDI.1	None	n/a
FIA_ATD.1	No other components	None	n/a
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UID.2	FIA_UID.1	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 by FIA_UID.2
FPT_ITT.1	No other components	None	n/a
FPT_TDC.1(1) &(2)	No other components	None	n/a

Table 24 – 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:

SFR \ OBJECTIVE	O.PA	O.IS	O.INT	O.ACCESS	O.AUDIT	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.CRYPTO	O.EADMIN	O.IDAUTH	O.IMPORT	O.DATAX
FAU_GEN.1					✓							
FAU_GEN.2					✓							
FAU_SAR.1							✓					
FAU_SAR.2				✓								
FAU_SAR.3							✓					
FAU_STG.1					✓	✓						
FPA_DEF.1*(1)	✓											
FPA_DEF.1*(2)		✓										
FPA_SCH.1*(1)	✓											
FPA_SCH.1*(2)		✓										
FPA_REC.1*(1)	✓											
FPA_REC.1*(2)		✓										
FPA_REV.1*	✓	✓					✓					
FPA_STG.1*	✓	✓				✓						
FCS_CKM.1								✓				
FCS_CKM.4								✓				
FCS_COP.1								✓				
FDP_SDI.2			✓									
FIA_ATD.1										✓		
FIA_UAU.2				✓						✓		
FIA_UID.2				✓						✓		
FIA_USB.1				✓						✓		
FMT_MTD.1				✓					✓		✓	✓
FMT_SMF.1				✓					✓			
FMT_SMR.1				✓					✓			
FPT_ITT.1						✓						
FPT_TDC.1(1)											✓	
FPT_TDC.1(2)												✓

Table 25 – Mapping of TOE SFRs to Security Objectives

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

OBJECTIVE	RATIONALE
O.PA	*The TOE must be able to audit the configuration of computers on a network, and provide notification of deviations from a defined configuration.* The TOE is required to support the definition [FPA_DEF.1*(1)}, distribution and scheduling [FPA_SCH.1*(1)] of policy audits for managed computers on a network. Results of these policy audits are recorded [FPA_REC.1*(1)] and stored securely [FPA_STG.1*]. The results can be reviewed by authorized users [FPA_REV.1*].
O.IS	*The TOE must be able to scan the inventories of computers on a network, and provide reports on system configuration.* The TOE is required to support the definition [FPA_DEF.1*(2)}, distribution and scheduling [FPA_SCH.1*(2)] of inventory scans for managed computers on a network. Results of these inventory scans are recorded [FPA_REC.1*(2)] and stored securely [FPA_STG.1*]. The results can be reviewed by authorized users [FPA_REV.1*].
O.INT	*The TOE must be able to detect and report changes to designated files on computers on a network.* The TOE is required to monitor and report changes to monitored objects within systems [FDP_SDI.2].
O.ACCESS	*The TOE must restrict user access to only authorized TOE functions and data.* Users authorized to access the TOE are determined using an identification process [FIA_UID.2] and authentication [FIA_UAU.2]. 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.2].
O.AUDIT	*The TOE must generate audit records for data accesses and use of the TOE functions on the management system*. 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]. 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 must provide the capability to protect the confidentiality and integrity of PA records and audit information generated by the TOE.* The TOE is required to protect the stored PA records and audit information from unauthorized deletion or modification, including during transmission between separate parts of the TOE [FAU_STG.1, FPA_STG.1*, FPT_ITT.1].
O.AUDIT_REVIEW	*The TOE must provide the capability for authorized administrators to review PA records and audit information generated by the TOE.* The TOE is required to provide functions for the review of audit data [FAU_SAR.1, FAU_SAR.3] and PA records [FPA_REV.1*].

OBJECTIVE	RATIONALE
O.CRYPTO	*The TOE must provide cryptographic functionality and protocols required for the TOE to securely transfer information between distributed portions of the TOE, and must use only cryptographic modules that have been validated to FIPS 140.* The cryptographic SFRs, [FCS_CKM.1, FCS_CKM.4 and FCS_COP.1] describe key generation and cryptographic operation for encryption between end points of the distributed TOE.
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.IDAUTH	*The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data on the management system*. 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.2] and authentication process [FIA_UAU.2]. 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].
O.IMPORT	*The TOE must provide mechanisms to import system information from Active Directory (LDAP servers)*. 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.DATAX	*The TOE must provide mechanisms to exchange SCAP Benchmark Assessment data, and to import JSON Advanced Host Assessment data.* The TOE includes mechanisms to exchange SCAP Benchmark Assessment data with external systems, and to import JSON Advanced Host Assessment data [FPT_TDC.1(2)]. Access to this functionality is restricted [FMT_MTD.1].

Table 26 – Rationale for Mapping of TOE SFRs to Objectives

6.4.2 Security Assurance Requirements Rationale

69 EAL2 was chosen to provide a moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the TOE environment. While the TOE may monitor a hostile environment, the servers on which it is located are assumed to provide protection by employing measures appropriate to that environment. At EAL2, the TOE will have incurred a search for obvious flaws to support its introduction into the protected environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

6.5 TOE Summary Specification Rationale

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

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

SFR \ TSF	Policy Audits	Inventory Scans	TSF Data Protection	Identification & Authentication	Management	Audit	System Information Import	Data Exchange
FAU_GEN.1						✓		
FAU_GEN.2						✓		
FAU_SAR.1						✓		
FAU_SAR.2						✓		
FAU_SAR.3						✓		
FAU_STG.1						✓		
FPA_DEF.1*(1)	✓							
FPA_DEF.1*(2)		✓						
FPA_SCH.1*(1)	✓							
FPA_SCH.1*(2)		✓						
FPA_REC.1*(1)	✓							
FPA_REC.1*(2)		✓						
FPA_REV.1*	✓	✓						
FPA_STG.1*	✓	✓						
FCS_CKM.1			✓					
FCS_CKM.4			✓					
FCS_COP.1			✓					
FDP_SDI.2	✓							
FIA_ATD.1					✓			
FIA_UAU.2				✓				
FIA_UID.2				✓				
FIA_USB.1				✓				
FMT_MTD.1					✓			
FMT_SMF.1					✓			
FMT_SMR.1					✓			
FPT_ITT.1			✓					
FPT_TDC.1(1)							✓	
FPT_TDC.1(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.

SFR	SF AND RATIONALE
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_SAR.3	**Audit** – Audit data can be sorted and filtered.
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.
FPA_DEF.1*(1)	**Policy Audits –** Benchmarks can be defined within the TOE or imported.
FPA_DEF.1*(2)	**Inventory scans** – Inventory scans can be defined within the TOE.
FPA_SCH.1*(1)	**Policy Audits** – Policy audits can be transferred to managed systems and scheduled.
FPA_SCH.1*(2)	**Inventory scans** – Inventory scans can be transferred to managed systems and scheduled.
FPA_REC.1*(1)	**Policy Audits –** The results of policy audits are stored and returned to ePO for analysis
FPA_REC.1*(2)	**Inventory scans** - The results of inventory scans are stored and returned to ePO for analysis
FPA_REV.1*	**Policy Audits –** Authorized users can display and analyse the results of policy audits. **Inventory scans** - Authorized users can display and analyse the results of inventory scans.
FPA_STG.1*	**Policy Audits –** The results of policy audits are held securely against unauthorized modification or deletion. **Inventory scans** - The results of inventory scans are held securely against unauthorized modification or deletion.
FCS_CKM.1	**TSF Data Protection –** Cryptographic keys are generated on the Manager Agent or the ePO for encrypted communications between the MA and the ePO.
FCS_CKM.4	**TSF Data Protection –** Keys used for encrypted communications between MA and ePO are zeroized when communication is complete.
FCS_COP.1	**TSF Data Protection –** Encrypted communications between the ePO and MA use cryptographic algorithms and key sizes specified in ST Table 21 – Cryptographic Operations.
FDP_SDI.2	**Policy Audits –** File integrity scans are used to detect unauthorised changes to important files on a system.
FIA_ATD.1	**Management** – User security attributes are associated with the user account via ePO User Account management.
FIA_UAU.2	**Identification & Authentication** - The TSF requires users to 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 authentication.

SFR	SF AND RATIONALE
FIA_UID.2	**Identification & Authentication**- The TSF requires users to identify 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.
FIA_USB.1	**Identification & Authentication** - Upon successful login, the TOE binds the 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 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 one or more ePO permission sets for the user.
FPT_ITT.1	**TSF Data Protection –** Traffic between MA on a managed system and ePO is protected.
FPT_TDC.1(1)	**System Information Import** – The TOE provides the functionality to import asset data information from Active Directory (LDAP servers) and correctly interpret the information.
FPT_TDC.1(2)	**Data Exchange** – The TOE can import SCAP Benchmark Assessment data and export reports in SCAP-conformant XML files. The TOE can import JSON Advanced Host Assessment data.

Table 28 – SFR to TSF Rationale

7 TOE Summary Specification

7.1 Policy Audits

72 The TOE evaluates the status of managed systems relative to audits that contain user defined or industry standard 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.

Rules

73 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. 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.

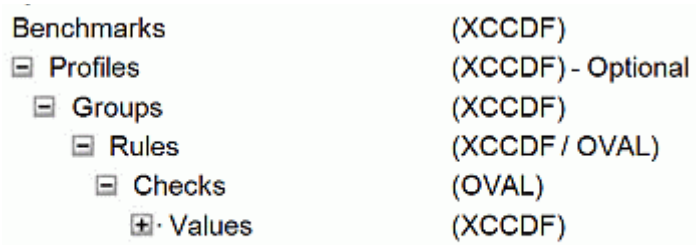


Figure 2 – Benchmark Structure

Benchmarks

74 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.

75 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.

Audits

76 Audits are composed of benchmarks that are generally supplied by McAfee, but may be imported from third-party sources or defined by a user with Benchmark Editor. Received or imported benchmarks must be activated in Benchmark Editor before they can be used in audits.

Scoring

77 Policy Auditor provides the means to score audits according to four different scoring models (all of the scoring models described in the XCCDF 1.2 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

78 Waivers provide a way to temporarily affect audit scoring for managed systems. Waivers can be useful when a managed system that is non-compliant with a rule or a benchmark, but is permitted to remain so 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.

79 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.

80 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.

81 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

82 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.

83 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 and MD5 digest to represent the file.

84 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

85 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 by an ePO Administrator.

86 Queries can be private 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.

87 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

88 Dashboards are an alternative mechanism for viewing the collected policy audit data. Individual users with the "Permission to use public dashboards" or an Administrator 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.

Data retention

89 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. Scan data older than a specified number of days can also be removed by an ePO Administrator or user assigned the Group Admin permission set.

Policy Auditor Agent

90 The Policy Auditor Agent is a plug-in to McAfee Agent. It extends the features of McAfee Agent to support Policy Auditor. When audits are deployed to the McAfee Agent from Policy Auditor, the Policy Auditor Agent Plug-in controls when the audits are to 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.

Related SFRS: FPA_DEF.1*(1), FPA_SCH.1*(1), FPA_REC.1*(1), FPA_REV.1*, FPA_STG.1*, FDP_SDI.2

7.2 Inventory scans

91 Policy Auditor can be used to scan inventory items on a managed system. Supported inventory scan items are applications, services, ports, operation system, network interfaces, system information and registered extensions.

92 The list of inventory items to be used in a scan can be defined using ePO. The scans can then be assigned to managed systems and scheduled for running, run manually from ePO using the command line, or can be run locally.

93 The results of inventory scans can be viewed using ePO, and scan data can be purged when no longer required.

Queries

94 Queries are configurable objects that retrieve and display collected event records from inventory scans 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 scans may be viewed by users with the "View System Tree" permission or by an ePO Administrator.

95 Queries can be private 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.

96 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. Scan History — Retrieves information on inventory scans 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 Scan History query, the time unit must match the schedule interval for the server task. McAfee recommends creating the Boolean pie chart query first, followed by the server task that generates the scan events, and finally the Scan History query.
2. Managed Systems — Retrieves information about systems running the McAfee Security Agent.

Dashboards

97 Dashboards are an alternative mechanism for viewing the collected inventory scan data. Individual users with the "Permission to use public dashboards" or an Administrator 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.

Data retention

98 Inventory scan 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 inventory scan data. Scan data older than a specified number of days can also be removed by an ePO Administrator or user assigned the Group Admin permission set.

Related SFRS: FPA_DEF.1*(2), FPA_SCH.1*(2), FPA_REC.1*(2), FPA_REV.1*, FPA_STG.1*

7.3 TSF Data Protection

99 Communications between McAfee Agents and ePO take the form of XML messages. Communications can include policies to implement, or audit data gathered by Policy Auditor. The messages are transferred via HTTPS. The TOE protects these transmissions between the ePO and the McAfee Agent from disclosure and modification by encrypting the transmissions under TLS, using AES operating in CBC mode, with 256 bit key size (by default the cipher used by ePO and McAfee Agent is TLS_DHE_RSA_WITH_AES_256_CBC_SHA256).

100 In FIPS mode, ePO uses OpenSSL v1.0.2p with FIPS module v2.0.16 (FIPS 140-2 certificate #2398) for TLS 1.2. Key generation uses CTR_DRBG for deterministic random bit generation, following NIST Special Publication 800-90 (CAVP DRBG algorithm certificate #1451). Zeroization of cryptographic keys and other sensitive data is carried out before memory is deallocated.

101 For verification of the authenticity and integrity of content downloaded from McAfee servers (Benchmarks and AHA data) ePO makes use of the RSA Crypto-C ME 4.1.2 cryptographic library (FIPS 140-2 certificate #2294). The data is signed by McAfee using the McAfee private key (RSA 2048), and verified by ePO. If the signature is not valid the data is rejected.

102 McAfee Agent uses RSA BSAFE Crypto-C Micro Edition v4.0.1 (FIPS 140-2 certificate #2097) to provide cryptographic services for this link. Key generation uses HMAC_DRBG for deterministic random bit generation, following NIST special Publication 800-90 (CAVP DRBG algorithm certificate #191). Zeroization of cryptographic keys and other sensitive data is carried out before memory is deallocated.

103 McAfee affirms that the cryptographic modules have been implemented in accordance with their FIPS 140 security policies, and when the TOE is configured in FIPS mode the cryptographic functions operate as intended.

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards	CAVP Cert #
Key Transport	RSA encrypt/decrypt	2048	Allowed in FIPS mode	OpenSSL #2444 BSAFE #1046
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (operating in CBC mode)	256	FIPS 197	OpenSSL #4469 BSAFE #2017
Secure Hashing	SHA-256	Not Applicable	FIPS 180-3	OpenSSL #3681 BSAFE #1767
Signature verification	RSA	2048	FIPS 186-4	RSA Crypto-C ME #1850

Table 29 - Cryptographic operations ePO/MA

Related SFRs: FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FPT_ITT.1

7.4 Identification & Authentication

104 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.

105 If Windows authentication is enabled, the supplied password is passed to Windows for validation, otherwise it is validated against ePO's internal password store. If authentication 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.

106 Upon successful login, the union of all the permissions from the permission sets from the user account configuration is 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 user logs out and logs back in again.

Related SFRs: FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1

7.5 Management

107 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-ePO user.

108 The TOE provides functionality to manage the following:

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

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

7.5.1 ePO User Account Management

109 Each user authorized for login to ePO must be defined with ePO. Only an Administrator 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 authentication for all users)
4. Permission sets granted to the user.

110 One or more permission sets may be associated with an account. ePO Administrators are only granted permission as “Administrator” and have access to everything in ePO.

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

1. Create and delete user accounts.
2. Create, delete, and assign permission sets.

7.5.2 Permission Set Management

111 A permission set is a group of permissions that can be granted to any users by assigning it to those users’ accounts. ePO provides the following predefined permission sets:

- Executive Reviewer

- Global Reviewer
- Group Admin
- Group Reviewer

112 When a user account is created, the user can be assigned to either a permission set (pre-defined or administrator defined) or assigned as an “Administrator”. If the new user account is assigned to a permission set they are considered to be an “ePO user”, whereas if they are assigned to “Administrator” they are considered to be an “Administrator”.

113 One or more permission sets can be assigned to any users who are not ePO administrators (ePO administrators can only be assigned as an Administrator).

114 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 registered servers, but another permission set applied to the same account grants all permissions to registered servers, that account has all permissions to registered servers.

115 When a new ePO product extension (e.g., PA) is installed into ePO 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 Administrators can then grant permissions to users through existing or new permission sets.

116 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.

117 When a permission set is created or modified, the permissions granted via the permission set may be specified by an Administrator.

7.5.3 Audit Log Management

118 An ePO Administrator may view and purge events in the audit log. A user with the appropriate permissions may view only, or view and purge events in the audit log.

7.5.4 Registered Servers

119 Registered servers allows for integration of ePO with other external servers. For example an LDAP server may be registered to facilitate connection to an Active Directory server for synchronization of active directory system and user data with ePO. ePO Administrators may create, view, modify and delete registered servers. Servers may be registered as:

- McAfee ePO – additional McAfee ePO servers for use with the main ePO server to collect or aggregate data,
- LDAP – as above, to synchronize directory system and user data,
- SNMP – to receive SNMP traps,
- Database servers – to retrieve data from a database server.

120 ePO Users can only be granted permission to view registered server settings by assigning the “View registered servers” permission from the Registered Servers permission set.

7.5.5 Systems and System Tree Management

121 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 organization of systems within units called groups.

122 Groups have these characteristics:

1. Groups can be created by ePO 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 an ePO administrator or user with both the “View "System Tree" tab” and “Edit System Tree groups and systems” permissions.

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

1. It can't be deleted.
2. It can't be renamed.
3. Its sorting criteria can't be changed (although sorting criteria for subgroups can be created)
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.

124 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 are added to the System Tree. Inheritance may be disabled for individual groups or systems by an ePO 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.

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

7.5.6 Product Policy Management

126 A product policy is a collection of settings that is created, configured, and then enforced. 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 product policy settings are reconfigured, the new settings are delivered to, and enforced on, the managed systems at the next agent-server communication.

127 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.

128 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 this inheritance is broken 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. An ePO Administrator can assign any product policy in the Policy Catalog to any group or system. Assignment allows product policy settings to be defined once for a specific need, and then applied to multiple locations.

129 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 an ePO Administrator. When a product policy is deleted, all groups and systems where it is currently applied inherit the product policy of their parent group.

130 Once associated with a group or system, enforcement of individual product policies may be enabled and disabled by an ePO Administrator.

7.5.7 Query and Report Management

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

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

7.5.8 Policy Audit Event Log Management

132 An ePO Administrator can configure the length of time policy audit event records are to be saved. Entries beyond that time are automatically purged.

133 The policy audit event records may also be purged manually by an ePO 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.

7.5.9 Dashboard Management

134 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.

7.5.10 Benchmark Management

135 A user can create benchmarks. Benchmark Editor contains a Check Catalog that allows selection of any check that the system contains. New checks can also be created. Operations on benchmarks and checks can be performed according to the following permissions that may be granted to users (an ePO Administrator can 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.

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

137 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. McAfee-provided benchmarks can be tailored.

138 Profiling allows the creation of 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.

139 A benchmark will have one of these status types:

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

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

141 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. Labels can be created, deleted or applied to benchmarks or checks.

7.5.11 Policy Auditor Management

142 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.

143 Policy Auditor allows an ePO 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 a system should achieve.

144 An ePO Administrator may modify the Data Retention parameters to set how long Policy Auditor retains its audit data. The Data Retention Unit Type setting offers a choice from days, weeks, months or years. The Data Retention Units setting allows the units of time to be specified in conjunction with the Data Retention Unit Type setting.

145 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 an ePO Administrator.

7.5.12 Policy Audit Management

146 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).

147 Operations on policy audits (create, delete, view and modify) can be performed according to the following permissions that can be granted to users (an ePO Administrator can perform all operations):

1. Add, remove, and change Audits and Assignments;

2. View Audits and Assignments.

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

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

7.5.13 Waiver Management

149 An ePO 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.

150 An ePO 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.

151 An ePO 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.

152 An ePO 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.

7.5.14 File Integrity Management

153 Users may create, view, modify, apply and delete File Integrity Monitoring policies based upon their permissions. To use File Integrity monitoring feature, the user is required to first create a policy that details the files to monitor or exclude from monitoring, and assign the same to the agent on the target system. Management actions associated with File Integrity Monitoring are as follows:

> 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, modify the policy to include/exclude files, and delete the policy. Pre-built queries and reports are available to the user for viewing the results of File Integrity Monitoring, or the user can create new queries and a report dashboard for analysis of results.

Related SFRs: FPA_DEF.1*(1), FPA_SCH.1*(1), FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

7.5.15 Inventory Scan Management

154 Users may create, view, modify, apply and delete Advanced Host Assessment Scan policies based upon their permissions. To use Advanced Host Assessment Scan feature, the user is required to first create a Client Task of type Inventory Scan. The task can then be assigned to a managed system or group of systems to be run in accordance with the defined schedule. Alternatively, the inventory scan task can be run on an individual system immediately using the Host Inventory "Scan Now" action in the System Tree view.

155 Management actions associated with Advanced Host Assessment Scan policies are:

1. The user defines what to which managed systems/group of systems the scan is to be applied.
2. The user can choose whether to reset the baseline scan data. By design, the scan result includes only the difference in baseline from the last scan results, if this option is not enabled.

3. The user can choose whether to synchronize the scan results. Synchronize scan option populates the latest data from the previous scan.
4. The user can select the inventory items to be scanned. The available inventory items are applications, services, ports, operation system, network interfaces, system information and registered extensions.
5. The user can define the scan schedule.

Related SFRs: FPA_DEF.1*(2), FPA_SCH.1*(2), FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

7.6 Audit

156 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.

157 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.

158 Audit Log entries can be queried against by an ePO Administrator or users with the “View Audit Log” permission. The Audit Log entries are automatically purged based upon an ePO 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.

Related SFRs: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1

7.7 System Information Import

159 ePO offers integration with Active Directory as a source for systems, and even as a source for the structure of the System Tree.

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

161 There are two types of Active Directory synchronization (systems only and systems and structure). Which one to be used depends on the level of integration required with Active Directory.

With each type, the synchronization is controlled 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.

162 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.

163 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 sorting criteria on groups is changed, 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.

Related SFRs: FPT_TDC.1(1)

7.8 Data Exchange

7.8.1 Benchmark data

164 Benchmark Editor provides several ways to bring benchmarks into a system.

165 The primary means for obtaining benchmark content is through the standard ePO content delivery mechanism. An ePO server task allows McAfee-supplied benchmarks and checks to be downloaded to the master repository, and added to the Benchmark Catalog and the Check Catalog, according to the schedule that has been set. The relevant ePO permission is “Create, Edit, Run, View and End Scheduler Tasks, View Scheduler Task Results in the Server Log”.

166 A number of benchmarks have been developed by third-party vendors. These can be downloaded as single archive (ZIP) or XML files, and then imported into the Benchmark Catalog.

167 Benchmarks can be exported from the Benchmark Catalog as single archive (ZIP) files. Users can then share these benchmarks within their organization or with others.

168 Imported benchmarks may be used by an ePO Administrator or a user with either the “Create, delete, change and import benchmarks” or “Create, delete, modify, import, and unlock benchmarks” permission.

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

170 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.

171 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.

7.8.2 AHA data

172 Advanced Host Assessment data is obtained through the standard ePO content delivery mechanism. An ePO server task allows the AHA content to be downloaded, according to the schedule that has been set. The relevant ePO permission is “Create, Edit, Run, View and End Scheduler Tasks, View Scheduler Task Results in the Server Log”.

173 The data can then be used in inventory scans by a user with the “View and change Advanced Host Assessment policy settings” permission.

Related SFRs: FPA_DEF.1*, FPT_TDC.1(2)