National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

McAfee Policy Auditor 6.0 and McAfee ePolicy Orchestrator 4.6

Report Number:	**CCEVS-VR-VID10484-2012**
Dated:	**10 May 2012**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Mike Allen (Lead Validator)
Jerome F. Myers (Senior Validator)
Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10 where the restrictions are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the McAfee Policy Auditor 6.0 and McAfee ePolicy Orchestrator 4.6. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of the McAfee Policy Auditor 6.0 and McAfee ePolicy Orchestrator 4.6 was performed by the CAFÉ Laboratory of COACT Incorporated, the Common Criteria Testing Laboratory, in Columbia, Maryland USA and was completed in February 2012.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by McAfee. The ETR and test report used in developing this validation report were written by COACT. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1 R2, dated September 2007 at Evaluation Assurance Level 2 (EAL 2) augmented with ALC_FLR.2 and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1 R2, dated September 2007. The product, when configured as specified in the installation guides, user guides, and Security Target satisfies all of the security functional requirements stated in the McAfee Policy Auditor 6.0 and McAfee ePolicy Orchestrator 4.6 Security Target. The evaluation team determined the product to be both Part 2 extended and Part 3 augmented compliant, and meets the assurance requirements of EAL 2 augmented by ALC_FLR.2. All security functional requirements are derived from Part 2 of the Common Criteria.

The McAfee Policy Auditor 6.0 is an agent-based, purpose-built IT policy audit solution that leverages the XCCDF and OVAL security standards to automate the processes required for internal and external IT audits. McAfee Policy Auditor evaluates the status of managed systems relative to audits that contain benchmarks. Benchmarks contain rules that describe the desired state of a managed system. Benchmarks are distributed with the TOE or imported into McAfee Benchmark Editor and, once activated, can be used by Policy Auditor. Benchmarks are written in the open-source XML standard formats Extensible Configuration Checklist Description

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

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

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

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

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

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

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (IT) products, desiring a security evaluation, contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant (if any); and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	**Identifier**
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	McAfee Policy Auditor 6.0 and McAfee ePolicy Orchestrator 4.6
Protection Profiles	None.
Security Target	*McAfee Policy Auditor 6.0 and McAfee ePolicy Orchestrator 4.6 Security Target*, Version 0.4, February 15, 2012
Dates of evaluation	November 2009 through February 2012
Evaluation Technical Report	*Evaluation Technical Report for the McAfee Policy Auditor 6.0 and McAfee ePolicy Orchestrator 4.6*, Document No. F2-0212-002, 6 April 2012
Conformance Result	Part 2 extended conformant and EAL2 Part 3 augmented with ALC_FLR.2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R2, September 2007 and all applicable NIAP and International Interpretations effective on November 8, 2011
Common Evaluation Methodology (CEM) version	CEM version 3.1R2 dated September 2007and all applicable NIAP and International Interpretations effective on November 8, 2011
Sponsor	McAfee, Inc., 2821 Mission College Blvd., Santa Clara, CA 95054
Developer	McAfee, Inc., 2821 Mission College Blvd. , Santa Clara, CA 95054
Common Criteria Testing Lab	COACT Inc. CAFÉ Labs, Columbia, MD
Evaluators	Greg Beaver and Jonathan Alexander
Validation Team	Dr. Jerome Myers and Mike Allen of the Aerospace Corporation

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

I-0418 – Evaluation of the TOE Summary Specification: Part 1 Vs Part 3
I-0426 – Content of PP Claims Rationale
I-0427 – Identification of Standards

International Interpretations

None

3 Security Policy

The security requirements enforced by the McAfee Policy Auditor 6.0 and McAfee ePolicy Orchestrator 4.6 were designed based on the following overarching security policies:

3.1 Audit

The TOE audits managed systems to determine policy compliance on those systems. Results of the policy audits are stored in the database (the DBMS is in the IT Environment and not part of this evaluation), 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.

The TOE's Audit Security Function provides auditing of management actions performed by administrators. Authorized users may review the audit records via ePO.

3.2 Identification and Authentication

The TOE requires users to identify and authenticate themselves before accessing the TOE software. User accounts must be defined within ePO, but authentication of the user credentials is performed by Windows. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with their user account that define the functionality the user is allowed to perform.

I&A for local login to the operating system (i.e., via a local console) is performed by the local OS (IT Environment) on the management system and all managed systems.

3.3 Management

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

3.4 Managed System Information

The TOE may be configured to import information about systems to be managed from Active Directory (LDAP servers) or NT domain controllers. This functionality ensures that all the defined systems in the enterprise network are known to the TOE and may be configured to be managed.

3.5 SCAP Data Exchange

The TOE must be able to import and export SCAP benchmark assessment data. This functionality ensures that the assessments remain current as new benchmarks are developed and allows custom-designed benchmarks in the TOE to be made available to other systems.

4 Assumptions and Clarification of Scope

The assumptions, threats and policies in the following paragraphs were considered during the evaluation of the McAfee Policy Auditor 6.0 and McAfee ePolicy Orchestrator 4.6.

4.1 Assumptions

ASSUMPTION	DESCRIPTION
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the IT Systems the TOE monitors.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

4.2 Threats

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

The TOE Addresses the following threats:

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

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

THREAT	DESCRIPTION
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on data acquired from managed systems.
T.SCNCFG	Improper security configuration settings may exist in the managed systems.
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.

4.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation and how the TOE needs to be configured to ensure it operates in the evaluated configuration.

- The assumptions about the underlying operating system and DBMS mean that to achieve true EAL 2 level of assurance for the complete McAfee Policy Auditor 6.0

and McAfee ePolicy Orchestrator 4.6 system, the operating system, DBMS and underlying hardware need to be evaluated at or above the EAL 2 level of assurance.

- Communications to and from the TOE and the managed systems is via a trusted path that is part of the environment and not part of this evaluation. Users must ensure the proper level of security is employed on this path.

- The administrator is responsible for updating all patches and security updates for the third party software components that are included on the McAfee installation downloads.

- Use of virtual machine architecture to implement the product is an optional feature.

- The process to track flaws and updates may require purchase of a Service Level Agreement (See the Validator's Comments, Section 10 below, for further details).

5 Architectural Information

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

The platform on which the ePO, Policy Auditor and Benchmark Editor software is installed must be dedicated to functioning as the management system. ePO operates as a distribution system and management system for a client-server architecture offering components for the server part of the architecture (not the clients). The TOE requires the following hardware and software configuration on this platform.

Table 1 - Management System Component Requirements

COMPONENT	MINIMUM REQUIREMENTS
Processor	Intel Pentium 4-class or higher 1.3 GHz or higher
Memory	2 GB available RAM minimum 4 GB available RAM recommended minimum
Free Disk Space	1.5 GB — First-time installation minimum 2 GB — Upgrade minimum 2.5 GB — Recommended minimum
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	Windows Server 2003 Enterprise with Service Pack 2 or later Windows Server 2003 Standard with Service Pack 2 or later Windows Server 2003 Datacenter with Service Pack 2 or later Windows Server 2008 Enterprise with Service Pack 2 or later Windows Server 2008 Standard with Service Pack 2 or later Windows Server 2008 Datacenter with Service Pack 2 or later Windows Server 2008 R2 Enterprise Windows Server 2008 R2 Standard Windows Server 2008 R2 Datacenter Windows 2008 Small Business Server Premium
Virtual Infrastructure (Optional)	Citrix XenServer 5.5 Update 2 Microsoft Hyper-V Server 2008 R2 VMware ESX 3.5 Update 4 VMware ESX 4.0 Update 1

COMPONENT	MINIMUM REQUIREMENTS
DBMS	Microsoft SQL Server 2005 (with Service Pack 3 or higher) Microsoft SQL Server 2008 SP1/SP2/R2
Network Card	Ethernet, 100Mb or higher
Disk Partition Formats	NTFS
Domain Controllers	The system must have a trust relationship with the Primary Domain Controller (PDC) on the network
Miscellaneous	Microsoft .NET Framework 2.0 or later (Required — You must acquire and install this software manually. This software is required if you select an installation option that automatically installs the SQL Server Express 2005 software bundled with this ePolicy Orchestrator software.) Microsoft updates Microsoft Visual C++ Required — Installed automatically. 2005 SP1 Redistributable Microsoft Visual C++ Required — Installed automatically. 2008 Redistributable Package (x86) MSXML 6.0

The administrator is responsible for updating all patches and security updates for the third party software components that are included on the McAfee installation downloads.

The McAfee Agent and Policy Auditor Agent Plug-In execute on one or more systems whose policy settings are to be audited. The supported platforms for these components are:

Table 2 - Supported Agent Platforms

SUPPORTED AGENT OS	PLATFORM
Windows 2000 Server	X86 platforms
Windows 2000 Advanced Server with SP 1, 2, 3, or 4	X86 platforms
Windows 2000 Professional with SP 1, 2, 3, or 4	X86 platforms
Windows XP Professional with SP1	X86 and X64 platforms
Windows Server 2003 Standard Edition	X86 and X64 platforms
Windows Server 2003 Enterprise Edition	X86 and X64 platforms
Windows Vista, 7	X86 and X64 platforms
Windows 2008 Server	X86 and X64 platforms
Mac OS X 10.4, 10.5, 10.6	X86 and X64 platforms, PowerPC

SUPPORTED AGENT OS	PLATFORM
HP-UX 11i v1, HP-UX 11i v2, HP-UX 11i v2 Itanium, HP-UX 11i v3, HP-UX 11i v3 Itanium	RISC
Solaris 8, 9, 10	SPARC
SuSE Linux 9, Enterprise Server 10, Enterprise Server 11	X86 and X64 platforms
Red Hat Linux AS, ES, WS 4.0	X86 and X64 platforms
Red Hat Enterprise Linux 5.0, 5.1, 6.0	X86 and X64 platforms
AIX 5.3 (TL8 SP5) and AIX 6.1 (TL2 SP0)	Power5, Power 6

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

Table 3 - Agent Platform Hardware Requirements

COMPONENT	MINIMUM HARDWARE REQUIREMENTS
Memory	20 MB RAM
Free Disk Space	300 MB
Processor	Intel Pentium---class, Celeron, or compatible processor; 166 MHz processor or higher.

The management system is accessed from remote systems via a browser. The supported browsers are Firefox 3.5, Firefox 3.6, Internet Explorer 7.0, Internet Explorer 8.0.

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

6 Documentation

Once a purchase of McAfee Policy Auditor has been processed through the McAfee order fulfillment system, a Grant Code is issued to the customer via email. The Grant Code provides access (for up to one month) to the Policy Auditor downloadable files on a McAfee download server. The URL of the server is communicated to the customer in the same email as the Grant Code.

During the installation process, the customer may retrieve updates from the McAfee download server and applies them to the base version. Application of these patches brings the TOE to the evaluated version (6.0.x).

Download the following for the McAfee Policy Auditor Server:

A) McAfee ePolicy Orchestrator v4.6.0

B) McAfee Agent 4.6.0

C) McAfee Policy Auditor v6.0

Selecting the documentation tab allows the user to download the following documents:

A) McAfee Benchmark Editor 6.0.0 Product Guide for use with ePolicy Orchestrator 4.5 and 4.6

B) Release Notes McAfee ePolicy Orchestrator 4.6.0

C) Installation Guide McAfee ePolicy Orchestrator 4.6.0 Software

D) Product Guide McAfee ePolicy Orchestrator 4.6.0 Software

E) Product Guide McAfee Agent 4.6.0

F) McAfee Policy Auditor 6.0.0 software Installation Guide

G) McAfee Policy Auditor 6.0 software Product Guide for ePolicy Orchestrator 4.6

H) McAfee Policy Auditor Content Creator 6.0.0 Product Guide

I) McAfee Benchmark Editor 6.0.0 Product Guide for use with ePolicy Orchestrator 4.5 and 4.6

All of the documents listed above were examined and evaluated during the course of the evaluation.

7 IT Product Testing

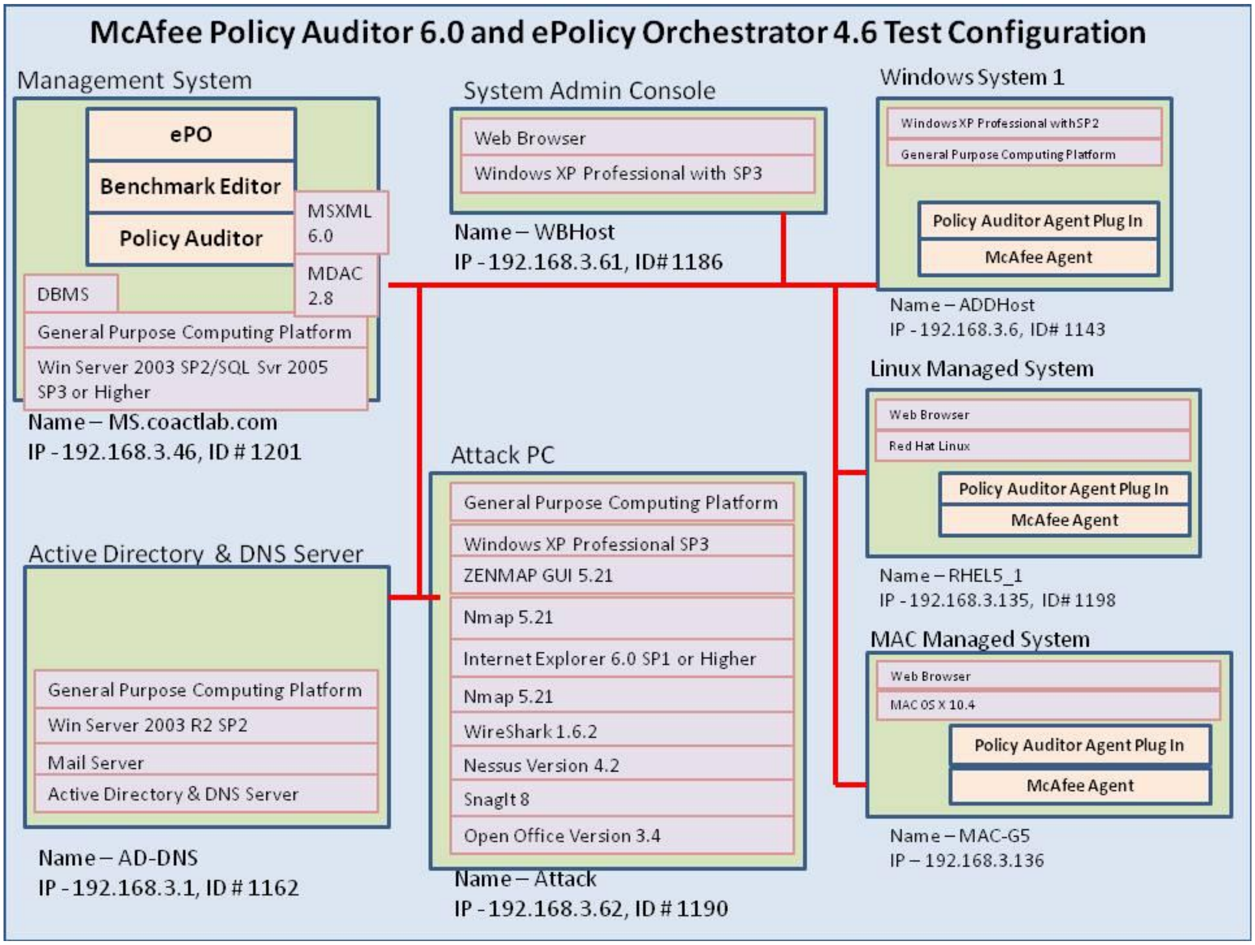
Testing was completed on February 29, 2012 at the COACT CCTL in Columbia, Maryland. COACT employees performed the tests.

7.1 Evaluator Functional Test Environment

Testing was performed on the following test bed configuration.

The following figure graphically displays the test configuration used for functional testing. The evaluator test configuration is equivalent to the vendor test setup. The evaluator test setup also includes the Active Directory/DNS.

Figure 1 - CCTL Test Configuration


McAfee Policy Auditor 6.0 and ePolicy Orchestrator 4.6 Test Configuration
Management System
ePO
Benchmark Editor
Policy Auditor
MSXML 6.0
MDAC 2.8
DBMS
General Purpose Computing Platform
Win Server 2003 SP2/SQL Svr 2005 SP3 or Higher
Name – MS.coactlab.com
IP - 192.168.3.46, ID # 1201
System Admin Console
Web Browser
Windows XP Professional with SP3
Name – WBHost
IP - 192.168.3.61, ID# 1186
Windows System 1
Windows XP Professional with SP2
General Purpose Computing Platform
Policy Auditor Agent Plug In
McAfee Agent
Name – ADDHost
IP - 192.168.3.6, ID# 1143
Linux Managed System
Web Browser
Red Hat Linux
Policy Auditor Agent Plug In
McAfee Agent
Name – RHEL5_1
IP - 192.168.3.135, ID# 1198
Attack PC
General Purpose Computing Platform
Windows XP Professional SP3
ZENMAP GUI 5.21
Nmap 5.21
Internet Explorer 6.0 SP1 or Higher
Nmap 5.21
WireShark 1.6.2
Nessus Version 4.2
SnagIt 8
Open Office Version 3.4
Name – Attack
IP - 192.168.3.62, ID # 1190
Active Directory & DNS Server
General Purpose Computing Platform
Win Server 2003 R2 SP2
Mail Server
Active Directory & DNS Server
Name – AD-DNS
IP - 192.168.3.1, ID # 1162
MAC Managed System
Web Browser
MAC OS X 10.4
Policy Auditor Agent Plug In
McAfee Agent
Name – MAC-G5
IP – 192.168.3.136

An overview of the purpose of each of these systems is provided in the following table.

Table 4 - Test Configuration Description

System	Purpose
Management System	This system provides the management functionality for the TOE. The system includes the ePO, Benchmark Editor, and Policy Auditor. The Microsoft SQL Server is installed to provide the database storage.
Windows System 1	This system hosts the Policy Auditor Agent Plugin and the McAfee Agent for the Windows OS environment. The agents will scan the system for vulnerabilities.
Linux Managed System	This system hosts the Policy Auditor Agent Plugin and the McAfee Agent for the Linux OS environment. The agents will scan the system for vulnerabilities.
MAC Managed System	This system hosts the Policy Auditor Agent Plugin and the McAfee Agent for the MAC OS environment. The agents will scan the system for vulnerabilities.
Attack PC	This system provides the attack and penetration test tools.
Active Directory & DNS Server	This system provides the Active Directory and Domain Name System (DNS) infrastructure for the testing. The mail server is also installed on this PC.
System Admin Console	The management system is accessed from the System Admin Console via a browser.
Switch	Not shown in the figure above, but included in the test configuration is a NetGear GS716T switch that will be used to connect the different systems on the network.

Specific configuration details for each of the systems are provided in the tables below.

Table 5 - Management System Requirements

Management System Requirements	
Operating System	Windows Server 2003 SP2
DBMS	Microsoft SQL Server 2005 SP3 or Higher
Additional Software	McAfee Policy Auditor 6.0 McAfee ePolicy Orchestrator 4.6 MDAC 2.8 (Installed automatically) Microsoft .NET Framework 2.0 or later Microsoft Visual C++ 2005 SP1 Redistributable (Installed automatically) Microsoft Visual C++ 2008 Redistributable Package (x86) (Installed automatically) MSXML 6.0 (Installed automatically)
Network Card	Ethernet

Disk Partition Formats	NTFS

Table 6 - Windows System 1 Requirements

Managed System 1 Requirements	
Operating System	Windows XP SP2
Additional Software	McAfee Agent Policy Auditor Agent Plugin
Network Card	Ethernet
Disk Partition Formats	NTFS

Table 7 - Attack PC Details

Item	Purpose
Installed software	Windows XP Professional SP3 Internet Explorer 6.0 SP1or later WinZip 10 ZENMAP GUI 5.21 Nmap 5.21 SnagIt 8 WireShark 1.6.2 Nessus Version 4.2 Open Office Version 3.2.1

Table 8 - Active Directory & DNS Server Details

Item	Purpose
Installed software	Microsoft Windows 2003 Server R2 SP2 Mail Enable Standard Edition Version 5.51

Table 9 - System Admin Console PC Details

Item	Purpose
Installed software	Windows XP Professional with SP3 Microsoft Internet Explorer 7 Open Office Version 3.4 Snagit Version 8 Adobe Reader Version 10.1.1

Table 10 - MAC Managed System

Item	Purpose
Installed software	MAC OS X 10.4.11 McAfee Agent Policy Auditor Agent Plugin

Table 11 - Linux Managed System

Item	Purpose
Installed software	Linux Red Hat 5.1 McAfee Agent Policy Auditor Agent Plugin

7.2 Functional Test Results

The repeated developer test suite included all of the developer functional tests. Additionally, each of the Security Functions and developer tested TSFI are included in the CCTL test suite. Results are found in the F2-0212-001 McAfee Policy Auditor Evaluation Test Report, dated April 13, 2012.

7.3 Evaluator Independent Testing

The tests chosen for independent testing allow the evaluation team to exercise the TOE in a different manner than that of the developer's testing. The intent of the independent tests is to give the evaluation team confidence that the TOE operates correctly in a wider range of conditions than would be possible purely using the developer's own efforts, given a fixed level of resource. The selected independent tests allow for a finer level of granularity of testing compared to the developer's testing, or provide additional testing of functions that were not exhaustively tested by the developer. The tests allow specific functions and functionality to be tested. The tests reflect knowledge of the TOE gained from performing other work units in the evaluation. The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests.

7.4 Evaluator Penetration Tests

The evaluator examined each of the obvious vulnerabilities identified during the developer's vulnerability analysis. After consulting the sources identified by the developer used during the initial vulnerability analysis, the evaluator examined sources of information publicly available to support the identification of possible potential vulnerabilities in the TOE. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.

A) http://web.nvd.nist.gov

B) http://osvdb.org/

C) http://securitytracker.com/

The evaluator performed the public domain vulnerability searches using the following key words.

A) McAfee
B) Policy Auditor
C) Security Management

D) Benchmarks
E) ePolicy Orchestrator 4.6
F) McAfee Agent 4.6

The following third party products required by the TOE were searched for vulnerabilities. The following search terms were used.

A) SQL Server 2005 (With SP3 or higher)
B) SQL Server 2008 (SP1/SP2/R2)
C) MSXML 6.0

After verifying that the developer's analysis approach sufficiently included all of the necessary available information regarding the identified vulnerabilities, the evaluator made an assessment of the rationales provided by the developer indicting that the vulnerability is non-exploitable in the intended environment of the TOE.

While verifying the information found in the developer's vulnerability assessment the evaluators conducted a search to verify if additional obvious vulnerabilities exist for the TOE. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerabilities.

The evaluator determined that the rationales provided by the developer indicate that the vulnerabilities identified are non-exploitable in the intended environment of the TOE.

8 Evaluated Configuration

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. See Section 5 for the supported hardware and operating systems for the TOE.

9 Results of the Evaluation

The evaluator devised a test plan and a set of test procedures to test the TOE’s mitigation of the identified vulnerabilities by testing the product for selected identified vulnerabilities.

The evaluation determined that the product meets the requirements for EAL 2 augmented with ALC_FLR.2. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by COACT Inc.

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the McAfee Policy Auditor 6.0 and McAfee ePolicy Orchestrator 4.6 meets the claims stated in the Security Target. The validation team also wishes to add the following clarification about the use of the product.

- For user's who wish to report or monitor flaws, a Knowledge Base (KB) article is posted to McAfee's public support website. Users may access the KB articles without purchasing a support agreement. For customers who chose to purchase a support agreement, proactive notification will be provided based on their paid support level and corresponding Service Level Agreement (SLA, i.e, Gold, Gold Select, Platinum, or Platinum Select). Note that Policy Auditor is an enterprise product and it is sold with a minimum of 12 months of Gold level support by default. Should the support agreement lapse beyond its term, the customer may at their discretion access the McAfee public support website to review relevant KB articles for their particular product(s).

11 Security Target

The Security Target is identified as the McAfee Policy Auditor 6.0 and McAfee ePolicy Orchestrator 4.6 Security Target, Version 0.4, February 15, 2012. The document identifies the security functional requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2 augmented with ALC_FLR.2.

12 Glossary

The following abbreviations and definitions are used throughout this document:

AD	Active Directory
ADO	ActiveX Data Objects
API	Application Program Interface
CC	Common Criteria
CCE	Common Configuration Enumeration
CM	Configuration Management
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DBMS	DataBase Management System
DNS	Domain Name System
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
FDCC	Federal Desktop Core Configuration
GUI	Graphical User Interface
I&A	Identification & Authentication
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IIS	Internet Information Services
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
KB	Knowledge Base
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MDAC	Microsoft Data Access Components
NTFS	New Technology File System
NTLM	NT LAN Manager
OS	Operating System
OVAL	Open Vulnerability Assessment Language
PP	Protection Profile
RAM	Random Access Memory
SCAP	Security Content Automation Protocol
SF	Security Function
SFR	Security Functional Requirement
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SP	Service Pack
SQL	Structured Query Language
SSL	Secure Socket Layer
ST	Security Target

TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TSF Interface
UDP	User Datagram Protocol
XCCDF	eXtensible Configuration Checklist Description Format

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1 R2, September 2007.
- Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 3.1 R2, September 2007.
- Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 3.1 R2, September 2007.
- Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 1, Version 3.1 R2, September 2007.
- Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1 R2, September 2007.
- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.
- Security Target McAfee Policy Auditor 6.0 and ePolicy Orchestrator 4.6, version 0.4, February 15, 2012
- Evaluation Technical Report for the McAfee Policy Auditor 6.0 and ePolicy Orchestrator 4.6, April 6, 2012, Document No. F2-0212-002
- McAfee Policy Auditor 6.0 and ePolicy Orchestrator 4.6Test Report, April 13, 2012, Document No. F2-0212-001