National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

McAfee Endpoint Encryption for PC 6.2
with McAfee ePolicy Orchestrator 4.6

Report Number:	**CCEVS-VR-VID10486-2012**
Dated:	**10 September 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 6940
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 any restrictions are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the McAfee Endpoint Encryption for PC 6.2 with 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 Endpoint Encryption for PC 6.2 with 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 August 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 Rycombe Consulting Limited. 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.3 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 Endpoint Encryption for PC 6.2 with 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.3. All security functional requirements are derived from Part 2 of the Common Criteria.

The TOE is a Personal Computer (PC) security system that provides data at rest protection, preventing the data stored on a PC from being read or used by an unauthorized person. It combines single sign-on user access control with transparent full disk encryption of HDD/SSD storage media to offer effective security for PCs running the Microsoft Windows operating system.

Integration with McAfee ePolicy Orchestrator (ePO) eases agent deployment, management, and reporting.

Communication between the Endpoint and ePO is secured using McAfee Agent.

ePO provides the management user interface for the TOE via a GUI accessed from remote systems using web browsers. User and Machine policies can be created, edited and deployed from ePO. Manual recovery allows users who have lost or compromised their logon credentials to regain secure access to their Endpoint PC.

ePO requires users to identify and authenticate themselves before access is granted to any data or management functions.

Audit records from both ePO and the Endpoints managed by it may be reviewed via the ePO GUI using fully customizable reports of which there are many built into the product.

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 Endpoint Encryption for PC 6.2 with McAfee ePO 4.6.
Protection Profiles	None.
Security Target	*McAfee Endpoint Encryption for PC 6.2 with McAfee ePolicy Orchestrator 4.6 Security Target*, Version 015, June 22, 2012
Dates of evaluation	November 2011 through August 2012
Evaluation Technical Report	*Evaluation Technical Report for the McAfee Endpoint Encryption for PC 6.2*, July 6, 2012, Document No. E2-0312-008
Conformance Result	Part 2 extended conformant and EAL2 Part 3 augmented with ALC_FLR.3
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R3, July 2009 and all applicable NIAP and International Interpretations effective on November 8, 2011
Common Evaluation Methodology (CEM) version	CEM version 3.1R3 dated July2009and all applicable NIAP and International Interpretations effective on November 8, 2011
Sponsor	McAfee, Inc., 3965 Freedom Circle, Santa Clara, CA 95054
Developer	McAfee, Inc., 3965 Freedom Circle, Santa Clara, CA 95054
Common Criteria Testing Lab	COACT Inc. CAFÉ Labs, Columbia, MD
Evaluators	Greg Beaver, Jonathan Alexander and Rory Saunders
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 Endpoint Encryption for PC 6.2 with McAfee ePolicy Orchestrator 4.6 were designed based on the following overarching security policies:

3.1 Cryptographic Operations

The TOE Endpoint uses AES-256 and the System Key to secure the TOE Endpoint storage media. All data written to the storage media is encrypted and all data read from the storage media is decrypted.

3.2 Identification and Authentication

Both ePO and the TOE Endpoint provide identity based access control.

The ePO administrator logs on to ePO using a username and password. No access to ePO functionality is available before the administrator has been successfully identified and authenticated.

The TOE Endpoint provides token-based user authentication, for instance using PKI certificate smartcards, stored value smartcards or password-only tokens. No access to the encrypted data on the storage media is available is available before the user has been successfully identified and authenticated.

3.3 Audit

ePO has built-in querying and reporting capabilities. These are customizable, flexible and easy to use. Included is the Query Builder wizard, which creates and runs queries that result in user-configured data in user-configured charts and tables.

3.4 Management

The TOE supports two types of operators. Within the context of the TOE, ePO operators are administrators and TOE Endpoint operators are referred to as users.

All aspects of the TOE Endpoint systems can be managed from ePO. User details are downloaded from Active Directory, and user and machine configurations are configured using ePO are deployed to TOE Endpoints as User Policies and System Policies respectively. User policies determine the user token policy as well as whether a user account is enabled or not on a system. Similarly, system policies determine the storage media encryption policy and where and when users are forced to logon (Preboot, Windows, both or neither).

Users may also change their own password if they are permitted to as part of their user policy.

3.5 Protection of the TSF

The TOE Endpoint has a number of related functions that help to maintain its integrity under certain circumstances, such as hardware failure, or communications link failure.

If installed in FIPS mode, the TSF runs a suite of tests during initial start-up, and in the case of the random number generator test, continuously to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

After a user account has been disabled or the user has forgotten their logon password when they try to logon, the TSF enters a maintenance mode where the ability to recover the normal functionality of the TOE Endpoint is provided either online via a secure administration session, or offline using the offline recovery procedure..

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.MANAGEMENT	One or more proficient persons are assigned to administer the TOE and the security of its data.
A.NO_MALEVOLENCE	The system administrators are not careless, malicious or intentionally negligent, and can be expected to follow the administrative guidance given to them in the TOE administration documentation.
A.PROFICIENT_USERS	Authorized TOE users and administrators follow the guidance provided for the secure operation of the TOE. There is no formal user guidance; it is the responsibility of the administrator to ensure that the users are given appropriate guidance.
A.AUTHENTICATION_DATA_PRIVATE	Authentication data is kept private by authorized users of the TOE.
A.TIME_SOURCE	The TOE's IT environment provides a reliable time source to enable the TOE to timestamp audit records.
A.CRYPTOGRAPHIC_KEY_DESTRUCTION	The TOE's IT environment provides a means of deleting all cryptographic keys within the TOE.
A.SECURE_BACKUP	User's data backups are separately encrypted or physically protected to ensure data security is not compromised through theft of or unauthorized access to backup information.
A.AVAILABLE_BACKUP	Regular and complete backups are taken to enable recovery of user data in the event of loss or damage to data as a result of the actions of a threat agent.
A.DOMAIN_SEPARATION	The operating system is able to provide separate threads of execution to protect the TOE from interference from other software running on the TOE PC.
A.TRUSTED_SOFTWARE	The software environment runs only trusted software that has been approved by the network manager. This also presumes appropriate protections against malicious installation of non-approved software such as viruses and Trojan horses by the appropriate deployment of firewalls, bastion hosts, and anti-virus software as appropriate.
A.NON_TECHNICAL_IDENTITY_VERIFICATION	There is a database of authorized TOE-users along with user-specific authentication data for the purpose of enabling administrative personnel to verify the identity of a user over a voice-only telephone line before providing them with support.

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.ACCESS	An unauthorized user of the TOE may access information without having permission from the person who owns, or is responsible for, the information. This threat is applicable if the TOE is stolen or otherwise falls into the hands of an attacker who then attempts to gain unauthorized access to the assets protected by the TOE.
T.ALTERNATE_BOOT_PROCESS	An unauthorized user with physical access to the system may use a boot floppy or similar device to subvert the system's normal boot process in order to access information assets contained on the system.
T.CONFIG _MODIFICATION	Configuration data or other sensitive data (such as registry settings) may be modified by unauthorized users.
T. CORRUPT_AUDIT	Unauthorized users may modify audit data by gaining unauthorized access to the audit trail.
T.EASE_OF_USE_ADMIN	The administrator may unintentionally select insecure configuration parameters or insecure default configuration parameters for the user.
T.EASE_OF_USE_USER	The user may unintentionally select insecure configuration parameters, reducing the security of the TOE.
T.EAVESDROP_TRANSIT	An unauthorized user may listen in on communications (electronic or otherwise) between the TOE components, and so gain unauthorized access to information.
T.PASSWORD_LOSS	The user may forget their password, making data unavailable.
T.RECORD_ACTIONS	An unauthorized user may perform unauthorized actions that go undetected.
T.RECOVERY_MASQUERADE	An unauthorized user with physical access to the TOE may try and perform the recovery procedure in order to gain access to the information securely stored on the TOE.
T.REMOVE_DISK	An unauthorized user with physical access to the system may remove storage media such as a hard disk from the system in order to circumvent the authentication mechanisms of the TOE and gain access to information contained on the drive.
T.SYSTEM_ACCESS	An unauthorized user may gain unauthorized access to the system and act as an administrator or other authorized user.
T.UNAUTHORIZED_MODIFICATION	An unauthorized user may modify the TOE software (executable code), and so gain unauthorized access to system and user resources.

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.

- In order to be in the evaluated configuration, all third party products must be up to date with all security updates and patches installed.
- In order to be in the evaluated configuration, the TOE must be installed in the FIPS mode.
- ePO and McAfee Agent are both installed in FIPS mode according to the TOE administration documentation
- Invalidate user's password after ten or less successive unsuccessful logon attempts
- All hard disks are encrypted
- Users are forced to logon with Preboot Authentication
- The platform on which the ePO software is installed must be dedicated to functioning as the management system
- The installation of the ePO software must be a new install. Upgrading from a previous version of ePO is not valid.
- The installation of the McAfee agent software must be a new install. Upgrading from a previous version of McAfee agent is not valid. Under certain conditions, you may have to remove the McAfee Agent manually. Possible reasons include:
    a. A failed upgrade leaves mismatched files that stops the /Forceuninstall from removing the agent.
    b. Issues with the Prevent McAfee services from being stopped option in VirusScan Enterprise (VSE) 8.5i and later.
    c. Corruption of files in previously installed versions of McAfee Agent or Common Management Agent.
    d. Third-party software conflicts
- CAUTION: All installation and un-installation of the TOE is to be performed by knowledgeable personnel and may involve opening or modifying the registry. Registry modifications are irreversible and could cause system failure if done incorrectly.

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 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 2 - TOE ePO Server Requirements

COMPONENT	MINIMUM REQUIREMENTS
Processor	Intel Pentium III-class or higher; 1GHz or higher
Memory	1 GB RAM or higher
Free Disk Space	1 GB
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	Windows Server 2008 Enterprise with Service Pack 2 or later Windows Server 2008 Standard with Service Pack 2 or later Windows Server 2008 R2 Enterprise Windows Server 2008 R2 Standard
DBMS	Microsoft SQL Server 2005 Microsoft SQL Server 2008
Browser	Internet Explorer 7.0 or 8.0 browser or Firefox 3.0 browser
Network Card	100Mb Ethernet or higher
Disk partition format	NTFS
Domain Controllers	The system must have a trust relationship with the Primary Domain Controller (PDC) on the network.

The TOE Endpoint software can be run on Windows server-class operating systems. However, the evaluated IT environments are the following endpoint operating systems:

Table 3 - TOE Endpoint Systems Requirements

SYSTEMS	REQUIREMENTS
Processor	Intel Pentium III-class or higher; 1GHz or higher
Memory	1 GB RAM or higher
Free Disk Space	Minimum of 200 MB
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	Windows 7 (32-bit and 64-bit) with SP1 Windows Vista (32-bit and 64-bit) with SP2 Windows XP (32-bit) with SP3
Network Card	100Mb Ethernet or higher

6 Documentation

When the purchase of the McAfee EEPC v6.2 and ePolicy Orchestrator 4.6 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 McAfee EEPC v6.2 and ePolicy Orchestrator 4.6 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.

The final product is tested, authorized for release, and posted to a McAfee download server. Multiple versions of the McAfee EEPC v6.2 and ePolicy Orchestrator 4.6 product may be available on the server. The customer downloads the base version of the evaluated software and documentation. The documentation package includes installation instructions.

Download the following for the McAfee EEPC v6.2 and ePolicy Orchestrator 4.6:

A)	EPO462L.zip	ePolicy Orchestrator v4.6.2
B)	MA460P1WIN.zip	McAfee Agent 4.6.1
C)	EPOAGENTMETA.zip	McAfee Agent 4.6.0 Patch 1 Extension
D)	McAfeeEEPC62.Zip	McAfee EEPCv6.2

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

A) Release Notes: McAfee Endpoint Encryption for PC 6.2 For use with ePolicy Orchestrator 4.5, 4.6 Software

B) Product Guide McAfee Endpoint Encryption 6.2 For use with ePolicy Orchestrator 4.5, 4.6 Software

C) Scripting Guide McAfee Endpoint Encryption 6.2 For use with ePolicy Orchestrator 4.6 Software

D) Best Practices Guide McAfee Endpoint Encryption for PC 6.2 Software For use with ePolicy Orchestrator 4.5, 4.6 Software

E) EETech User Guide McAfee Endpoint Encryption for PC 6.2 For use with ePolicy Orchestrator 4.5, 4.6 Software

F) Migration Guide McAfee Endpoint Encryption for PC 6.2 For use with ePolicy Orchestrator 4.5, 4.6 Software

G) Release Notes for McAfee ePolicy Orchestrator 4.6.2

H) Hardware Sizing and Bandwidth Usage Guide McAfee ePolicy Orchestrator 4.6.0 Software

I) Installation Guide McAfee ePolicy Orchestrator 4.6.0 Software

J) Product Guide McAfee ePolicy Orchestrator 4.6.0 Software

K) Scripting Guide ePolicy Orchestrator 4.6.0

L) Product Guide McAfee Agent 4.6.0

M) Release Notes McAfee Agent 4.6.0 Patch 1 for Windows

The following documents were examined and considered part of the Common Criteria Evaluation:

A) Release Notes: McAfee Endpoint Encryption for PC 6.2 For use with ePolicy Orchestrator 4.5, 4.6 Software

B) Product Guide McAfee Endpoint Encryption 6.2 For use with ePolicy Orchestrator 4.5, 4.6 Software

C) Release Notes for McAfee ePolicy Orchestrator 4.6.2

D) Installation Guide McAfee ePolicy Orchestrator 4.6.0 Software

E) Product Guide McAfee ePolicy Orchestrator 4.6.0 Software

F) Product Guide McAfee Agent 4.6.0

G) Release Notes McAfee Agent 4.6.0 Patch 1 for Windows

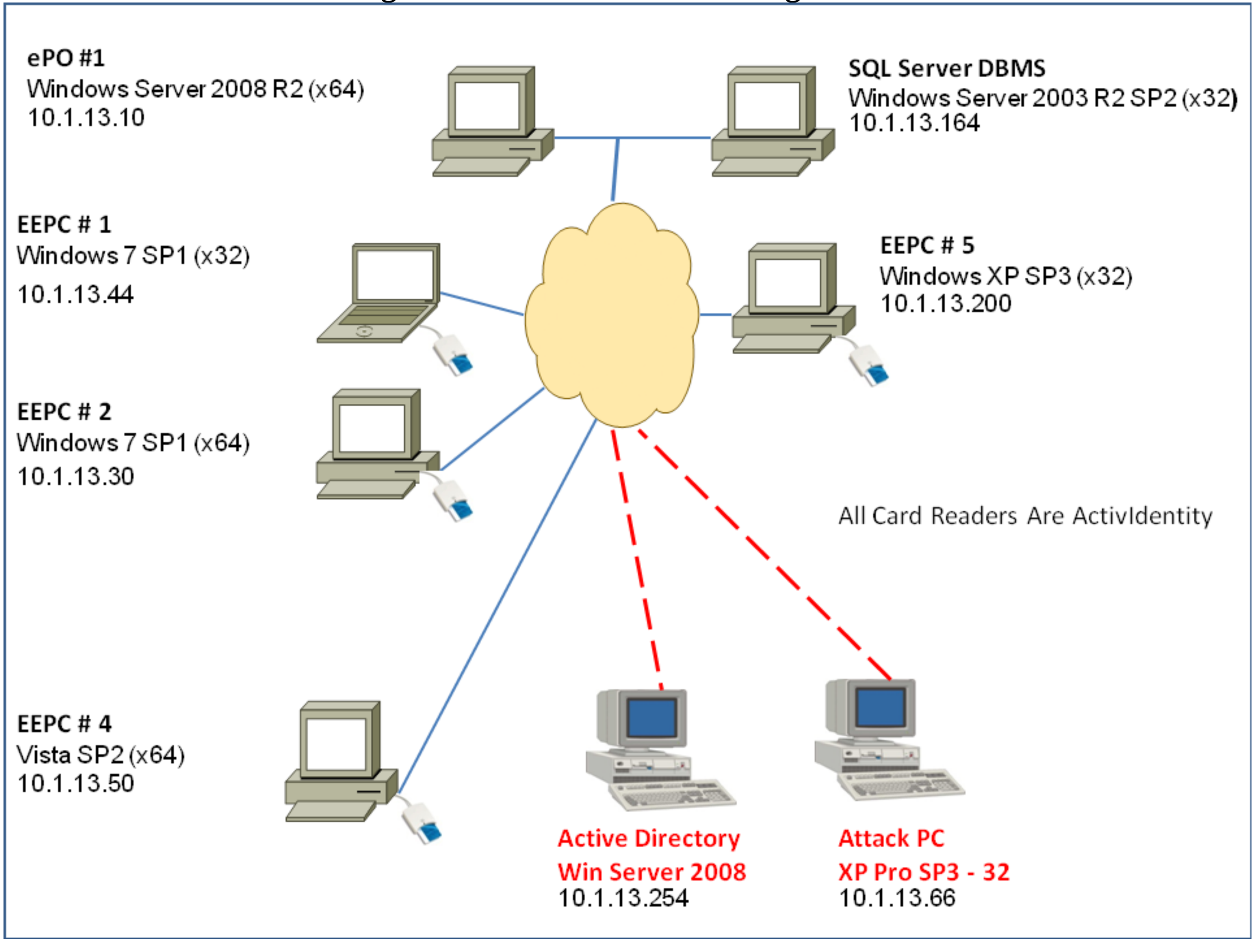
7 IT Product Testing

Testing was completed on July 6, 2012 at the COACT CCTL in Columbia, Maryland. COACT employees performed the tests.

7.1 Test 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



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

Table 4 - Test Configuration Overview

System	Purpose
ePO #1	The ePolicy Orchestrator server provides a scalable platform for centralized policy management and enforcement of your security products and systems on which they reside.
SQL Server DBMS	This system hosts the DBMS software. The system should be configured per the figure above, with the Active Directory and DNS servers both configured as coactlab.com
Active Directory & DNS Server	This system provides the Active Directory and Domain Name System (DNS) infrastructure for the testing.
Attack PC	Computer from which the penetration tests will be launched against the TOE.
EEPC #1	Test computer with Endpoint Encryption PC installed.
EEPC #2	Test computer with Endpoint Encryption PC installed.
EEPC #4	Test computer with Endpoint Encryption PC installed.
EEPC #5	Laptop Computer - Test computer with Endpoint Encryption PC installed.
NetGear 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 - ePO #1 Details

Management System Requirements	
Operating System	Windows Server 2008 R2 SP2 (x64)
Software	Internet Explorer 8.0 browser SnagIt 8 Adobe Reader Version X 10.1.1 ePO, v4.6.0 (+ patch 2) EEAdmin ePO extension, v1.2 EEPC ePO extension, v1.2 EEAdmin policy hook, v1.2 EEAdmin event parser, v1.2
Configuration	Static IP address 10.1.13.10 FQDN: EPO1.CoactLab.com
Updates	All third party vendor security and product updates

Table 6 - SQL Server DBMS Details

Management System Requirements	
Operating System	Windows Server 2003 R2 SP2 (x32)
Software	Internet Explorer 8.0 browser SnagIt 8 Adobe Reader Version X (10.1.1)
Configuration	Static IP address 10.1.13.164 FQDN: EPO2.CoactLab.com
Updates	All third party vendor security and product updates

Table 7 - Attack PC Details

Item	Purpose
Installed software	Windows XP Professional SP3 (x32 - Including all updates and patches) Internet Explorer 8.0 browser ZENMAP GUI 5.21 Nmap 5.21 SnagIt 8 WireShark 1.6.4 Nessus Version 3.0.6.1
Configuration	Static IP address 10.1.13.66 FQDN: Attack.CoactLab.com

Table 8 - Active Directory & DNS Server Details

Item	Purpose
Operating System	Microsoft Windows Server 2008 Server R2 SP2
Installed software	Internet Explorer 8.0 browser
Configuration	Static IP address 10.1.13.254 FQDN: AD-DNS.CoactLab.com Primary Domain Controller for CoactLab.com DNS Server for CoactLab.com with records for all systems identified in the test configuration
Updates	All third party vendor security and product updates

Table 9 - EEPC #1 PC Details

Item	Purpose
Installed software	Windows 7 SP1 (x32) Internet Explorer 9.0 Snag It 8 ActivClient 6.2 McAfee Agent, v4.6.0 SP1 McAfee EEPC Agent, MfeEEAgent, v1.2 McAfee EEPC Encryption Provider, MfeEEPC, v6.2
Configuration	Static IP address 10.1.13.44 FQDN: EEPC1.CoactLab.com
Card Reader	ActivIdentity Card Reader
Updates	All third party vendor security and product updates

Table 10 - EEPC #2 PC Details

Item	Purpose
Installed software	Windows 7 SP1 (x64) Internet Explorer 8.0 Snag It 8 ActivClient 6.2 McAfee Agent, v4.6.0 SP1 McAfee EEPC Agent, MfeEEAgent, v1.2 McAfee EEPC Encryption Provider, MfeEEPC, v6.2
Configuration	Static IP address 10.1.13.30 FQDN: EEPC2.CoactLab.com
Card Reader	ActivIdentity Card Reader
Updates	All third party vendor security and product updates

Table 11 - EEPC #4 PC Details

Item	Purpose
Installed software	Windows Vista SP2 (x64) Internet Explorer 7.0 Snag It 8 ActivClient 6.2 McAfee Agent, v4.6.0 SP1 McAfee EEPC Agent, MfeEEAgent, v1.2 McAfee EEPC Encryption Provider, MfeEEPC, v6.2
Configuration	Static IP address 10.1.13.50 FQDN: EEPC4.CoactLab.com
Card Reader	ActivIdentity Card Reader
Updates	All third party vendor security and product updates

Table 12 - EEPC #5 PC Details

Item	Purpose
Laptop Computer	
Installed software	Windows XP SP3 (x32) Internet Explorer 8.0 browser and Firefox 12.0 browser Snag It 8 ActivClient 6.2 McAfee Agent, v4.6.0 SP1 McAfee EEPC Agent, MfeEEAgent, v1.2 McAfee EEPC Encryption Provider, MfeEEPC, v6.2
Configuration	Static IP address 10.1.13.200 FQDN: EEPC5.CoactLab.com
Card Reader	ActivIdentity Card Reader
Updates	All third party vendor security and product updates

7.2 Functional Test Results

The repeated developer test suite includes all of the developer functional tests. Additionally, each of the Security Function and developer tested TSFI are included in the CCTL test suite. Results are found in the E2-0312-007 McAfee Endpoint Encryption for PC 6.2 with McAfee ePolicy Orchestrator 4.6 Test Report, dated March 30, 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 sources of the publicly available information examined are:

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

B) http://secunia.com/

C) http://www.securityfocus.com/

D) http://osvdb.org/

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

A) McAfee

B) Endpoint Encryption

C) EEPC

D) ePolicy Orchestrator

E) Safeboot

F) ePO

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

A) SQL Server 2005

B) SQL Server 2008

C) Active Directory

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 do 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 evaluation determined that the product meets the requirements for EAL 2 augmented with ALC_FLR.3. 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 Endpoint Encryption for PC 6.2 with 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.

- The user of this product should carefully review the restrictions on the evaluated configuration documented in the Clarification of Scope Section 4.3 of this report.
- CAUTION: All installation and un-installation of the TOE is to be performed by knowledgeable personnel and may involve opening or modifying the registry. Registry modifications are irreversible and could cause system failure if done incorrectly.

11 Security Target

The Security Target is identified as the McAfee Endpoint Encryption for PC 6.2 with McAfee ePolicy Orchestrator 4.6 Security Target, Rev 014, June 22, 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.3.

12 Glossary

The following abbreviations and definitions are used throughout this document:

TERM	DESCRIPTION
AES	Advanced Encryption Standard
Authorized Administrator	Any entity that is able to establish a secure management session with the TOE
Authorized User	Any entity that has logged on to the TOE Endpoint through the logon GUI
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CSP	Critical Security Parameters
DLL	Dynamic Link Library
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
IPC	Inter-process communication
IT	Information Technology
Machine	The TOE Endpoint PC
MBR	Master Boot Record
McAfee ePO	McAfee ePolicy Orchestrator: A McAfee software installation to allow configuration and management of a McAfee Endpoint Encryption for PC deployment
OS	Operating System
PKCS-5	Public Key Cryptography Standard 5 (Password-Based Cryptography Specification)
PP	Protection Profile
RSA	An algorithm for public-key cryptography. Named after Rivest, Shamir and Adleman who first publicly described it.
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SOF	Strength of Function
ST	Security Target
Storage Media	Any media for which TOE protection in the form of data encryption is required. Storage Media include internal hard drives and external SATA hard drives, but not external USB hard drives, USB memory sticks or floppy disks.
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TOE Endpoint	The McAfee Endpoint Encryption for PC client deployment

TOE Data	The encrypted contents of the TOE storage media.
TOE Manager	The McAfee ePolicy Orchestrator and McAfee Agent
TLS	Transport Layer Security
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
XML	Extensible Markup Language

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 R3, July 2009.
- Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 3.1 R3, July 2009.
- Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 3.1 R3, July 2009.
- Common Criteria Project Sponsoring Organisations. *Common Methodology for Information Technology Security Evaluation*, Version 3.1 R3, July 2009.
- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 2.0, September 8, 2008.
- McAfee Endpoint Encryption for PC 6.2 with McAfee ePolicy Orchestrator 4.6 Security Target, Version 015, June 22, 2012.
- Evaluation Technical Report for the McAfee Endpoint Encryption for PC 6.2, July 6, 2012, Document No. E2-0312-008.
- McAfee Endpoint Encryption for PC 6.2 with McAfee ePolicy Orchestrator 4.6 Test Report, March 30, 2012, Document No. E2-0312-007.