National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

McAfee Endpoint Encryption for PC version 5.2.6 with McAfee Endpoint Encryption Manager version 5.2.6

Report Number: CCEVS-VR-VID10400-2011
Dated: 4 October 2011
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 evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Validator Comments in Section 10.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Endpoint Encryption for PC version 5.2.6 with McAfee Endpoint Encryption Manager version 5.2.6. 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 Endpoint Encryption for PC version 5.2.6 with McAfee Endpoint Encryption Manager version 5.2.6 was performed by the CAFÉ Laboratory of COACT Incorporated, the Common Criteria Testing Laboratory, in Columbia, Maryland USA and was completed in August 2011.

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, Inc. 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 4 (EAL 4) 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 and user guides, satisfies all of the security functional requirements stated in the Endpoint Encryption for PC version 5.2.6 with McAfee Endpoint Encryption Manager version 5.2.6 Security Target. The evaluation team determined the product to be both Part 2 Conformant and Part 3 Augmented, and meets the assurance requirements of EAL 4 with 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 prevents the data stored on a PC from being read or used by an unauthorized person. In simple terms, the McAfee Endpoint Encryption Client takes control of a user's storage media away from the operating system. The McAfee Endpoint Encryption Client encrypts data written to storage media, and decrypts data read from the storage media. If the storage media is read directly, one would find only encrypted data, even in the Windows swap file and temporary file areas. The McAfee Endpoint Encryption Manager provides the functionality to securely deploy, configure and manage the McAfee Endpoint Encryption Client.

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	Endpoint Encryption for PC version 5.2.6 with McAfee Endpoint Encryption Manager version 5.2.6
Protection Profile	None
Security Target	*Endpoint Encryption for PC with McAfee Endpoint Encryption Manager Common Criteria Security Target*, version 1.23, July 27, 2011
Dates of evaluation	September 2009 through August 2011
Evaluation Technical Report	*Evaluation Technical Report for the Endpoint Encryption for PC 5.2.6 and McAfee Endpoint Encryption Manager 5.2.6*, Document No. E4-0111-005, August 1, 2011
Conformance Result	Part 2 conformant and EAL4 Part 3 augmented with ALC_FLR.3
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R2, September 2007 and all applicable NIAP and International Interpretations effective on December 17, 2008
Common Evaluation Methodology (CEM) version	CEM version 3.1R2 dated September 2007and all applicable NIAP and International Interpretations effective on December 17, 2008
Sponsor	McAfee, Inc., 2821 Mission College Blvd., Santa Clara, California 95054
Developer	McAfee, Inc., 2821 Mission College Blvd., Santa Clara, California 95054
Common Criteria Testing Lab	COACT Inc. CAFÉ Labs, Columbia, MD
Evaluators	Greg Beaver, Dave Cornwell 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

None

International Interpretations

None

3 Security Policy

The security requirements enforced by Endpoint Encryption for PC version 5.2.6 with McAfee Endpoint Encryption Manager version 5.2.6 were designed based on the following overarching security policies:

- **User Access Control**. The TOE Client replaces the master boot record on the bootable hard disk of the PC on which it is installed. Therefore, when a PC protected by the TOE boots, the first code that gets loaded from the hard disk is the McAfee Endpoint Encryption Client. The user is presented with the McAfee Endpoint Encryption Client logon screen. The Client supports token-based access control within the TOE Client boundary using a password-only token or the CAC and PIV tokens. When a user boots up a PC protected by the TOE, they boot into the "McAfee Endpoint Encryption Client OS", providing a trusted, secure and controlled environment in which the user may present his credentials for authentication.
  .
- **TOE Manager Access Control**. The TOE Manager supports token-based access control. Admin users require valid credentials in the form of a user name, login credentials and a token (either a physical token, in the case of the CAC and PIV smartcards, or a logical token in the form of the password-only token) before being granted access to the administrative functions.

- **Management of TOE by User.** It is possible for a user to change his password as part of the logon process or from the McAfee Endpoint Encryption Client screen saver, as long as they present their existing password for authentication as part of the process. This makes use of the password authentication mechanism.

- **Hard Disk Encryption.** The McAfee Endpoint Encryption Client operating system starts the crypt driver in memory once the user has entered the correct authentication information. From this point on the machine will look and behave as if the McAfee Endpoint Encryption Client was not installed, with all disk access going through the McAfee Endpoint Encryption Client, such that data read from storage media is decrypted and data written to storage media is encrypted, using the hard disk encryption key of the TOE Client.

- **Hard Disk Encryption Key Management.** The TOE Client generates its hard disk encryption key using a pseudo-random number generator based on DSS with a key size of 256 bits. The TSF destroys hard disk encryption keys by zeroing them when they are no longer in use, specifically when the TOE is uninstalled. The hard disk encryption key is stored encrypted (using AES and a key length of 256 bits) under a key derived from the user's password. If the password changes, the hard disk encryption key is decrypted using the existing one and then re-encrypted for storage using the new password. The hard disk encryption key itself does not change in such circumstances. The hard disk encryption key is decrypted as required when needed to access data on the TOE Client

PC storage media. This can only occur once a user has successfully logged on to the TOE Client.

- **Secure Management.** Management of TOE Clients is via the administration secure management interface. Any administrator wishing to manage a TOE Client must first establish a secure management session with that TOE Client. A proprietary protocol is used to establish a session key shared between the TOE Client and the TOE Manager. This is then used to encrypt a known value to authenticate the TOE Manager to the TOE Client and vice versa. This protocol incorporating the one-time session key and challenge-response mechanism provides a single-use authentication mechanism.

- **User TOE Management.** The user may change his own password, however the bulk of the management of the TOE functionality must be performed by an administrator.

- **TOE Client Audit.** The TOE Client maintains an audit log. This contains a list of events that have occurred on the TOE Client, and each entry consists of a timestamp, type of event, user ID of the user logged on at the time and the result of the event. The audit functions are always active while the TOE Client is operational. The audit log can only hold 3000 entries. When it is full, each new entry added results in the oldest entry in the log being overwritten. The audit log can only be viewed or cleared by authorized administrators. The administrator may choose to view the entries ordered on a number of factors, specifically: date and time, the event code, the object (machine or user) or the description of the audited event.

- **TOE Manager Audit.** The TOE Manager maintains an audit log. This contains a list of events that have occurred on the TOE Manager, and each entry consists of a timestamp, type of event, user ID of the user logged on at the time and the result of the event. The size (capacity) of the TOE Manager audit log is only limited by the available hard disk space. If the audit log becomes full, no new entries are added. The audit log can only be viewed or cleared by authorized administrators. The administrator may choose to view the entries ordered on a number of factors, specifically: date and time, the event code, the object (machine or user) or the description of the audited event.

- **Self-Protection of the TOE.** The TOE Client has a number of related functions that help to maintain its integrity under certain circumstances, such as hardware failure, or communications link failure. 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. The TSF preserves a secure state when communications with the TOE Manager are unexpectedly terminated or when there is a power failure to the TOE Client. 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 Client is provided either online via a secure administration session, or offline using the offline recovery procedure.

- **McAfee Endpoint Encryption Manager.** This function gives an authorized administrator access to a GUI that allows him to configure and manage the TOE. It also provides a user interface through which an authorized administrator may view or selectively review audit data from the TOE.

4 Assumptions and Clarification of Scope

The assumptions in the following paragraphs were made during the evaluation of Endpoint Encryption for PC version 5.2.6 with McAfee Endpoint Encryption Manager version 5.2.6.

4.1 Personnel Security Assumptions

- One or more proficient persons are assigned to administer the TOE and the security its data.
- 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.
- 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 that he is responsible for are given appropriate guidance.
- Authentication data is kept private by authorized users of the TOE.
- 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 Environmental Assumptions

- The TOE's IT environment provides a reliable time source to enable the TOE to timestamp audit records.
- 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.
- 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.
- 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.
- 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.

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. Note that:

- The assumptions about the underlying operating system mean that to achieve true EAL 4 level of assurance for the complete Endpoint Encryption for PC version 5.2.6 with McAfee Endpoint Encryption Manager version 5.2.6, the operating system and underlying hardware need to be evaluated at or above the EAL 4 level of assurance.

- There can be no other applications or servers running on the operating system or hardware platform used to support the McAfee Endpoint Encryption Manager version 5.2.6.

- The McAfee Endpoint Encryption Client consists of a boot Operating System (OS) (the McAfee Endpoint Encryption Client OS), a Basic Input Output System (BIOS) hook, Windows drivers, a system tray application and a set of Windows Dynamic Link Libraries (DLLs). McAfee Endpoint Encryption for PC installs a mini-operating system on the user's hard drive, this is what the user sees when they switch on the TOE Client. McAfee Endpoint Encryption for PC looks and feels like Microsoft Windows, with mouse and keyboard support, moveable windows etc. The McAfee Endpoint Encryption Client OS is completely self-contained and does not need to access any other files or programs on the hard disk(s), and is responsible for allowing the user to authenticate. Once the user has entered the correct authentication information, the McAfee Endpoint Encryption Client operating system starts a driver in memory and boots the protected machine's original operating system. From this point on the machine will look and behave as if McAfee Endpoint Encryption for PC was not installed.

- Although it is possible to install the McAfee Endpoint Encryption for PC client and McAfee Endpoint Encryption Manager on the same system, this feature was not tested nor is it considered part of the evaluated configuration.

- McAfee Endpoint Encryption for PC has the option of being configured in different ways. Details of the method of use to achieve the full CC evaluated configuration are provided in the McAfee Endpoint Encryption Managers Guide. At installation, the McAfee Endpoint Encryption Manager can specify how the fixed disks can be encrypted by choosing one of three encryption modes: full, partial, or none. Full encryption mode encrypts an entire partition. Partial encryption mode encrypts only a portion of a partition or hard disk. None encryption mode leaves the partition in plaintext with no encryption. Full encryption is the only valid mode that can be used if McAfee Endpoint Encryption for PC is to operate in a Common Criteria compliant mode (CC mode) and so comply with the requirements of the Security Target.

    - CC mode is defined as:
        - Password restrictions
            - Minimum password length of five characters

    - Invalidate user's password after ten or less successive unsuccessful logon attempts
- Full encryption of hard disk(s)
- Users forced to logon
- McAfee Endpoint Encryption client screen saver selected

5 Architectural Information

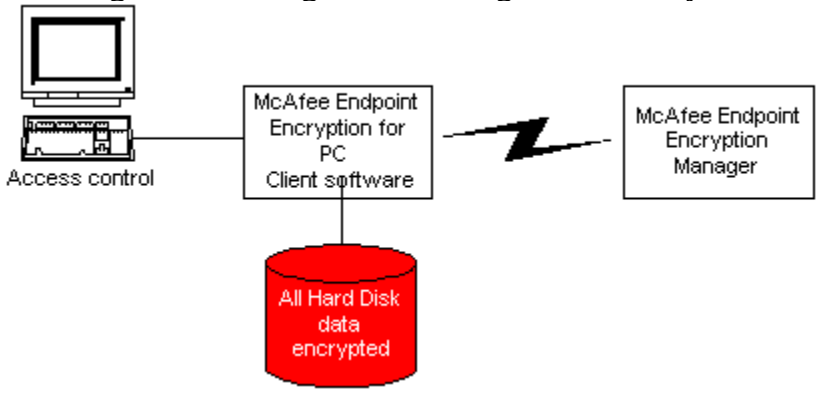
The components of the TOE are installed on general-purpose computers. The McAfee Endpoint Encryption for PC client and McAfee Endpoint Encryption Manager are installed on two separate PCs connected via a network.

Although it is possible to install the McAfee Endpoint Encryption for PC client and McAfee Endpoint Encryption Manager on the same system, this feature was not tested nor is it considered part of the evaluated configuration.

The physical boundary of the TOE is/are the software applications themselves and the APIs that they expose.

The logical boundary of the TOE is the application software that corresponds to version 5.2.6 of the McAfee Endpoint Encryption Client and v5.2.6 of the McAfee Endpoint Encryption Manager. See Figure 1 below.

Figure 1 - Figure 1 TOE logical boundary

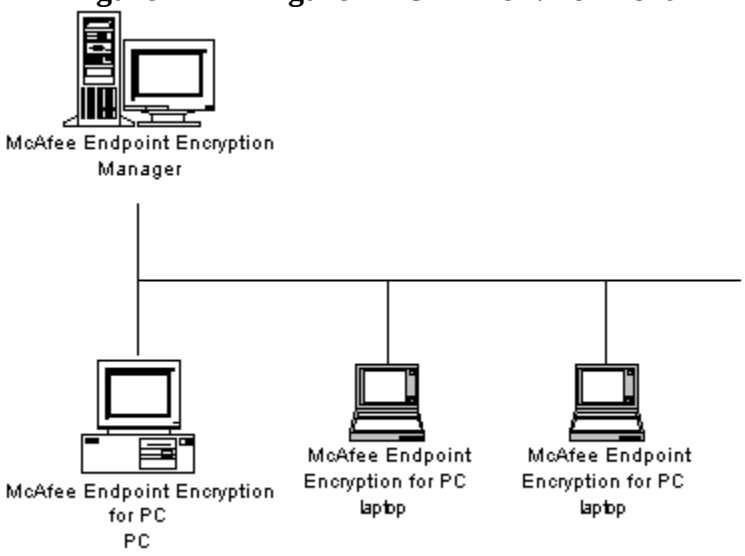


At the TOE boundary are its interfaces. There is a man-machine access control interface to allow a user to submit logon credentials for authentication. There is a disk drive interface to allow the contents of the disk drives to be secured through encryption, and there is a secure management interface to allow secure communication between McAfee Endpoint Encryption for PC and McAfee Endpoint Encryption Manager.

The IT environment of the TOE Client includes a PC running one of Microsoft Windows XP Professional with Service Pack 3, Windows Vista (32-bit or 64-bit) with service pack 1, or Windows 7 (32-bit or 64-bit) operating systems.

The IT environment of the TOE Manager includes a PC running one of the 64-bit variants of Microsoft Windows Server 2008 with Service Pack 1 and any variant of Microsoft Windows Server 2003 with Service Pack 2.

Figure 2 - Figure 2 TOE IT environment



6 Documentation

This section provides a listing of the IT product documentation provided with the Endpoint Encryption for PC version 5.2.6 with McAfee Endpoint Encryption Manager version 5.2.6 by the developer to the consumer or available from McAfee on their web site.

A Grant Code is provided to the customers that restricts access to relevant downloads (as opposed to other McAfee products). HTTPS is used for all downloads.

The customer is presented with a page permitting them to select the version to download. The customer selects the appropriate version (as specified in the appropriate Security Target document) and is then presented with options to download the software and/or documentation.

The evaluator downloaded the following material from the site:

A) McAfee Endpoint Encryption for PC / Quick Start Guide / Version 5.2.6
B) McAfee Endpoint Encryption for PC / Administration Guide / Version 5.2.6
C) McAfee Endpoint Encryption for PC / Product Release Notes / Version 5.2.6
D) McAfee Endpoint Encryption Manager / Product Release Notes / Version 5.2.6
E) McAfee Endpoint Encryption Manager / Administration Guide / Version 5.2.6
F) McAfee Endpoint Encryption for PC Version 5.2.6 installation file
G) McAfee Endpoint Encryption Manager Version 5.2.6 installation file

All of the documents listed above (A – E) are considered within the scope of the evaluation. NOTE: F & G above are the software files available from the McAfee site.

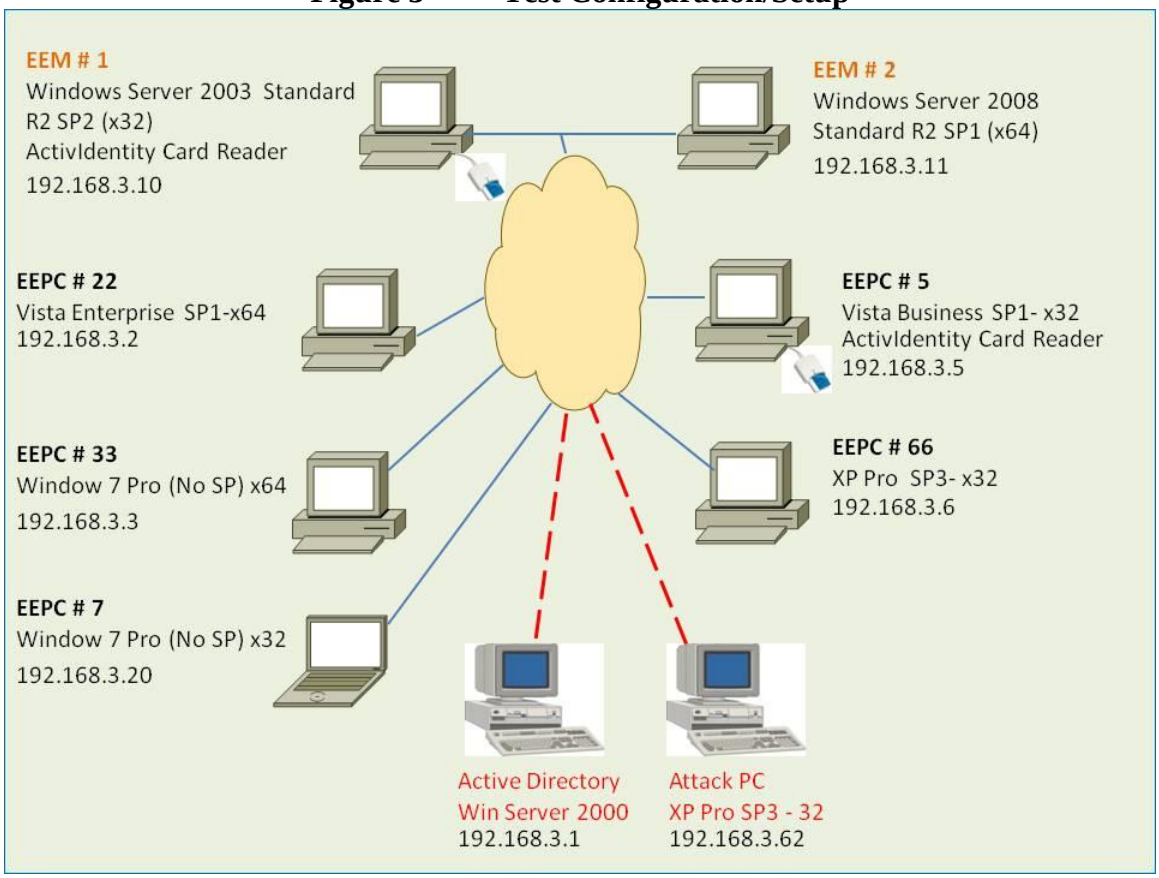
7 IT Product Testing

Testing was completed on August 1, 2011 at the COACT CCTL in Columbia, Maryland. COACT employees performed the tests.

7.1 Evaluator Functional Test Environment

Testing was performed on a test configuration consisting of the following test bed configuration.

Figure 3 - Test Configuration/Setup



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

Table 1 - Test Configuration Overview

System	Purpose
EEM #1	Endpoint Encryption Manager that controls the computers: EEPC #22, EEPC #33, EEPC #7 These three computers are managed in individual groups called: Machine22, Machine33, and Machine7 on EEM #1

System	Purpose
EEM #2	Endpoint Encryption Manager that controls the computers: EEPC #5, EEPC #66 These two machines are managed in a single group called Machines on EEM #2
EEPC #22	Test computer with Endpoint Encryption PC installed.
EEPC #33	Test computer with Endpoint Encryption PC installed.
EEPC #7	Test computer with Endpoint Encryption PC installed.
EEPC #5	Test computer with Endpoint Encryption PC installed.
EEPC #66	Test computer with Endpoint Encryption PC installed.
Active Directory & DNS Server	Computer to provide the Active Directory and DNS Server services.
Attack PC	Computer from which the penetration tests will be launched against the TOE.
NetGear Switch	10/100 M switch to provide the network connectivity.

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

Table 2 - EEM #1 Details

Management System Requirements	
Operating System	Windows Server 2003 R2 SP2 (x32)
Card Reader	ActivIdentity Card Reader
Software	Internet Explorer 6.0 SP1or later SnagIt 8 Libre Office 3.3
Configuration	Static IP address 192.168.3.10 FQDN: EEM1.CoactLab.com

Table 3 - EEM #2 Details

Managed System 1 Requirements	
Operating System	Windows Server 2008 Standard R2 SP1 (x64)
Software	Internet Explorer 6.0 SP1or later SnagIt 8

Managed System 1 Requirements	
	Libre Office 3.3
Configuration	Static IP address 192.168.3.11 FQDN: EEM2.CoactLab.com

Table 4 - EEPC #22 Details

Item	Purpose
Operating System	Vista Enterprise SP1 x64
Software	Internet Explorer 6.0 SP1or later SnagIt 8 Libre Office 3.3
Configuration	Static IP address 192.168.3.2 FQDN: EEPC2.CoactLab.com

Table 5 - EEPC #33 Details

Item	Purpose
Operating System	Windows 7 Pro (No SP) x64
Software	Internet Explorer 6.0 SP1or later SnagIt 8 Libre Office 3.3
Configuration	Static IP address 192.168.3.3 FQDN: EEPC3.CoactLab.com

Table 6 - EEPC #5 Details

Item	Purpose
Operating System	Vista Business SP1 x32
Card Reader	ActivIdentity Card Reader
Software	Internet Explorer 6.0 SP1or later SnagIt 8 Libre Office 3.3
Configuration	Static IP address 192.168.3.5 FQDN: EEPC5.CoactLab.com

Table 7 - EEPC #66 Details

Item	Purpose
Operating System	Windows XP Professional SP3 x32
Software	Internet Explorer 6.0 SP1or later SnagIt 8 Libre Office 3.3
Configuration	Static IP address 192.168.3.6 FQDN: EEPC6.CoactLab.com

Table 8 - Active Directory and DNS Server Details

Item	Purpose
Operating System	Windows Server 200
Software	Internet Explorer 6.0 SP1or later SnagIt 8 Libre Office 3.3
Configuration	Static IP address 192.168.3.1 FQDN: Attack.CoactLab.com Primary Domain Controller for CoactLab.com

Table 9 - Attack PC Details

Item	Purpose
Operating System	Windows XP Professional SP3
Software	ZENMAP GUI 5.21 Nmap 5.21 WireShark 1.4.0 Nessus Version 4.2 Internet Explorer 6.0 SP1or later SnagIt 8 Libre Office 3.3
Configuration	Static IP address 192.168.3.62 FQDN: Attack.CoactLab.com

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 McAfee Endpoint Encryption for PC version 5.2.6 with McAfee Endpoint Encryption Manager version 5.2.6 Test Report, dated August 1, 2011.

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 consulted vulnerability relevant sources of information to verify that the TOE did not have any obvious vulnerabilities. The sources consulted include:

A) http://cve.mitre.org

B) http://google.com

C) http://osvdb.org/

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

E) http://secunia.com/

F) http://www.us-cert.gov

G) http://securitytracker.com/

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

I) http://www.cvedetails.com/

Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerability.

7.5 Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any

undocumented interfaces or other security vulnerabilities in the final evaluated version. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Endpoint Encryption for PC version 5.2.6 with McAfee Endpoint Encryption Manager version 5.2.6 running the client on a PC running one of Microsoft Windows XP Professional with Service Pack 3, Windows Vista (32-bit or 64-bit) with service pack 1, or Windows 7 (32-bit or 64-bit) operating systems and the manager on a PC running one of the 64-bit variants of Microsoft Windows Server 2008 with Service Pack 1 and any variant of Microsoft Windows Server 2003 with Service Pack 2.

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 developer identified vulnerabilities.

The results of the testing activities were that all tests gave expected (correct) results. No vulnerabilities were found to be present in the evaluated TOE. The results of the penetration testing are documented in the vendor and CCTL proprietary report, McAfee Endpoint Encryption for PC version 5.2.6 with McAfee Endpoint Encryption Manager version 5.2.6 Test Report, dated August 1, 2011.

The evaluation determined that the product meets the requirements for EAL 4. 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 **Error! Unknown document property name.** Endpoint Encryption for PC version 5.2.6 with McAfee Endpoint Encryption Manager version 5.2.6 meet the claims stated in the Security Target. The validation team also wishes to add the following clarification about the use of the product.

1. Although it is possible to install the McAfee Endpoint Encryption for PC client and McAfee Endpoint Encryption Manager on the same system, this feature was not tested nor is it considered part of the evaluated configuration.
2. Various modes of operation are possible with the product. To operate the product in the evaluated configuration the below guidelines should be followed:
    - CC mode is defined as:
        - Password restrictions
            - Minimum password length of five characters
            - Invalidate user's password after ten or less successive unsuccessful logon attempts
        - Full encryption of hard disk(s)
        - Users forced to logon
        - McAfee Endpoint Encryption client screen saver selected

11 Security Target

The Security Target is identified as the **Error! Unknown document property name.** Endpoint Encryption for PC version 5.2.6 with McAfee Endpoint Encryption Manager version 5.2.6 Security Target, Version 1.23, July 27, 2011. 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 4 augmented with ALC_FLR.3.

12 Glossary

The following abbreviations and definitions are used throughout this document:

AES ..... Advanced Encryption Standard
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
MBR ..... Master Boot Record
EEM ..... McAfee Endpoint Encryption Manager
OS ..... Operating System
PKCS-5 ..... Public Key Cryptography Standard 5
SAR ..... Security Assurance Requirement
SFP ..... Security Function Policy
SFR ..... Security Functional Requirement
SHA-1 ..... Secure Hash Algorithm
SOF ..... Strength of Function
ST ..... Security Target
TCP/IP ..... Transmission Control Protocol/Internet Protocol
TOE ..... Target of Evaluation
TSC ..... TSF Scope of Control
TSF ..... TOE Security Functions
TSP ..... TOE Security Policy

13 Bibliography

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

1.) Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1 R2, September 2007.

2.) Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1 R2, September 2007.

3.) Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1 R2, September 2007.

4.) Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 1, Version 3.1 R2, September 2007.

5.) Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1 R2, September 2007.

6.) 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.

7.) McAfee Policy EEPC 5.2.6 with EEM 5.2.6 Test Report, August 1, 2011, Document No. E4-0111-004.

8.) Evaluation Technical Report for the McAfee Endpoint Encryption PC 5.2.6 and Endpoint Encryption Manager 5.2.6, Document No. E4-0111-005, August 1, 2011.

9.) **Error! Unknown document property name.** Endpoint Encryption for PC version 5.2.6 with McAfee Endpoint Encryption Manager version 5.2.6 Security Target, Version 1.23, July 27, 2011.