National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme Validation Report

McAfee MOVE 2.5 and McAfee ePolicy Orchestrator 4.6

Report Number: CCEVS-VR-VID10500-2012

Dated: 14 September 2012

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

Jerome F. Myers
Jean Petty

Common Criteria Testing Laboratory
COACT CAFE Laboratory
Columbia, Maryland 21046-2587

Table of Contents

List of Figures

List of Tables

1 Executive Summary

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the McAfee MOVE 2.5 and McAfee ePolicy Orchestrator 4.6 at EAL2 augmented with ALC_FLR.2. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by the CAFE Laboratory of COACT Incorporated, located in Columbia, Maryland. The evaluation was completed on 31 August 2012. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by COACT and submitted to the Validators. The evaluation determined the product conforms to the CC Version 3.1, Revision 3, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.2 resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is the McAfee MOVE 2.5 and McAfee ePolicy Orchestrator 4.6.

McAfee MOVE Antivirus is an anti-virus solution for virtual environments that removes the need to install an anti-virus application on every virtual machine (VM).

A traditional security solution for virtual environments uses an anti-virus application running on every VM on a hypervisor. This requirement reduces VM density per hypervisor and causes high disk, CPU, and memory usage. McAfee MOVE Antivirus solves this issue by offloading all on-access scanning to a dedicated VM that runs an offload scan server to improve performance related to anti-virus scanning. This results in increased VM density per hypervisor.

The management capabilities for MOVE are provided by ePO through the MOVE ePO Extension and McAfee Agent ePO manages McAfee Agents and MOVE Software that reside on client systems. By using ePO you can manage a large enterprise network from a centralized system. ePO through the McAfee Agent provides capabilities to distribute updated MOVE Security policies, DAT files to the Offload Scan Server. ePO also centrally manages Event and Log records.

Communication between the distributed components of the TOE is protected from disclosure and modification by cryptographic functionality provided by the FIPS approved components of the McAfee ePO and the McAfee Agent. It is assumed that the IT environment will provide a secure line of communications between the TOE and remote administrators.

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, security evaluations are conducted by 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.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire 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 CCEVS' 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 organizations and individuals participating in the evaluation.

Table 1 - Evaluation Identifier

McAfee MOVE 2.5 and McAfee ePolicy Orchestrator 4.6	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	McAfee MOVE 2.5 and McAfee ePolicy Orchestrator 4.6
Protection Profile	N/A
Security Target	Security Target McAfee MOVE 2.5 and ePolicy Orchestrator 4.6, Document Version 1.4, August 14, 2012
Evaluation Technical Report	Evaluation Technical Report for the McAfee MOVE 2.5 and ePolicy Orchestrator 4.6, August 31, 2012 Document No. E2-0412-014
Conformance Result	Part 2 extended and EAL2 Part 3 conformant
Version of CC	CC Version 3.1 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on May 1, 2012.
Version of CEM	CEM Version 3.1 and all applicable NIAP and International Interpretations effective on May 1, 2012.
Sponsor	McAfee, Inc. 3965 Freedom Circle

McAfee MOVE 2.5 and McAfee ePolicy Orchestrator 4.6	
	Santa Clara, CA 95054
Developer	McAfee, Inc. 3965 Freedom Circle Santa Clara, CA 95054
Evaluator(s)	**COACT Incorporated** Greg Beaver Jonathan M. Alexander Rory Saunders
Validator(s)	**NIAP CCEVS** Jerome F. Myers Jean Petty

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 TOE Description

The TOE includes these components:

- McAfee MOVE Antivirus Agent for Windows — Allows virtual desktops and servers to communicate with ePolicy Orchestrator.
- McAfee MOVE Antivirus Offload Server — Provides offloaded scanning support for virtual servers, minimizing the impact on virtual desktops.
- McAfee MOVE Antivirus ePolicy Orchestrator extension — Provides policies and controls for configuring McAfee MOVE Antivirus behavior.
- ePolicy Orchestrator – provides management capabilities for the TOE.
- McAfee Agent – provides common communication functionality between ePO and all of McAfee's product-specific software (such as MOVE).

Note specifically that the hardware, operating systems and third party support software (such as the Microsoft SQL Server database) on each of the systems that TOE software executes on are excluded from the TOE boundary.

4 Assumptions

The assumptions listed below are assumed to be met by the environment and operating conditions of the system.

Table 2 - Assumptions

ASSUMPTION	DESCRIPTION
A.AUDIT_BACKUP	Administrators will back up audit records and monitor disk usage to ensure audit information is not lost.
A.NO_EVIL	Administrators are non-hostile, appropriately trained, and follow all administrative guidance.
A.PHYSICAL	It is assumed that the appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
A.SECURE_COMMS	It is assumed that the IT environment will provide a secure line of communications between the TOE and remote administrators.
A.SECURE_UPDATES	Administrators will implement secure mechanisms for receiving and validating updated signature files from the Anti-Virus vendors, and for distributing the updates to the central management systems.

5 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:

Table 3 - Threats Addressed By the TOE

THREAT	DESCRIPTION
T.AUDIT_ COMPROMISE	A user or process may gain unauthorized access to the audit trail and cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a security relevant event.

THREAT	DESCRIPTION
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of memory used by the TOE to scan files or process administrator requests.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted)
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.
T.UNIDENTIFIED_ACTIONS	Failure of the authorized administrator to identify and act upon unauthorized actions may occur.
T.VIRUS	A malicious agent may attempt to introduce a virus onto a workstation to compromise data on that workstation, or use that workstation to attack additional systems.

6 Organizational Security Policies

The following Organizational Security Policies apply to the TOE:

POLICY	DESCRIPTION
P.ACCESS_BANNER	The system shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHY	Only NIST FIPS validated cryptography (methods and implementations) are acceptable for cryptographic hashing of DAT files.
P.ROLES	The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

7 Clarification of Scope

The McAfee MOVE 2.5 and ePolicy Orchestrator 4.6 TOE usage and major security features are listed below.

A) **Virus Scanning and Alerts** - The TOE provides for scanning and detection of file-based viruses. Users are alerted of actions on both the managed systems (via pop-up dialog) and the management system (via log). This functionality is supported in the VSE component of the Offload Scan Server.

B) **Audit** - Event information is concurrently generated for transmission to the ePO management databases. Event records for all clients can be reviewed from the ePO console.

C) **Management** - ePO enables the Global Administrator to centrally manage virus scan settings on workstations, configure and manage the actions the virus scan component takes when detection of an infection occurs, and manage the Event and Log records.

D) **Cryptographic Operation** - Anti-virus packages are distributed to the workstation with a SHA-1 hash value used to verify the integrity of the package. Communications between ePO and the McAfee Agent are encrypted using AES implemented by FIPS 140-2 validated modules.

8 Architecture 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 4 - TOE ePO Server 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 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

COMPONENT	MINIMUM REQUIREMENTS
Virtual Infrastructure	Citrix XenServer 5.5 Update 2 Microsoft Hyper-V Server 2008 R2 VMware ESX 3.5 Update 4 VMware ESX 4.0 Update 1
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 supported platforms for McAfee Agent and MOVE Agent are:

Table 5 - Managed System Platform Requirements

COMPONENT	MINIMUM REQUIREMENTS
Processor	One vCPU 2 GHz or higher
Memory	1 GB RAM
Free Disk Space	8 GB
Operating System	**Server Operating Systems:** Microsoft Windows Server 2008 SP2 (32-bit or 64-bit) Microsoft Windows Server 2008 R2 SP1 (64-bit) Microsoft Windows Server 2003 R2 SP2 (32-bit) **Workstation Operating Systems:** Microsoft Windows XP SP3 Microsoft Windows 7 Home Premium, Professional, and Ultimate (32 and 64 bit)

COMPONENT	MINIMUM REQUIREMENTS
Additional Software	Microsoft Windows Installer (MSI) version 3.1 or later
Network Card	Ethernet, 10Mb or higher

The supported platforms for McAfee Offload Scan Server are:

Table 6 - Offload Scan Server Platform Requirements

COMPONENT	MINIMUM REQUIREMENTS
Processor	One vCPU 2 GHz or higher
Memory	1 GB RAM
Free Disk Space	8 GB
Operating System	**Server Operating Systems:** Microsoft Windows Server 2008 SP2 (64-bit) Microsoft Windows Server 2008 R2 SP1 (64-bit)
Additional Software	Microsoft Windows Installer (MSI) version 3.1 or later
Network Card	Ethernet, 10Mb or higher

The management system is accessed from remote systems via a browser. The supported browsers are Microsoft Internet Explorer 6.0 with Service Pack 1 or later or Microsoft Internet Explorer 7.0.
Identification and authentication services for ePO users and workstation users are provided by the operational environment. Windows services are invoked by the TOE to validate user credentials. Windows may be integrated with a credential store to perform the credential validation.

9 Product Delivery

Once a purchase of the McAfee MOVE 2.5 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 MOVE 2.5 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 MOVE 2.5 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 MOVE 2.5 and ePolicy Orchestrator 4.6:

Download	Notes
EPO462L.zip	ePolicy Orchestrator v4.6.2
MA460P1WIN.zip	McAfee Agent 4.6.0 (Patch 1)

Download	Notes
EPOAGENTMETA.zip	McAfee Agent 4.6.0 Patch 1 Extension
MOVE-AV_Agent_2500_WIN.zip	MOVE AntiVirus [Multi-Platform] 2.5 Agent Package
MOVE-AV_Ext_2.5.0.zip	MOVE AntiVirus [Multi-Platform] 2.5 Management Extension for McAfee ePO
MOVE-AV_Ext_2.5.0_License.zip	MOVE AntiVirus [Multi-Platform] 2.5 License Extension for McAfee ePO
MOVE-AV_Offload_Server_Setup_x86.exe	MOVE AntiVirus [Multi-Platform] 2.5 Offload Server Setup
VSE880LMLRP1.zip	VirusScan 8.8 Repost Patch 1

Selecting the documentation tab at the product download site allows the user to download the product documentation. Product documentation is available for each of the specific product downloads and versions. The documentation listed below was relevant to the evaluated versions and was downloaded and considered part of the evaluation.

A) Release Notes for McAfee ePolicy Orchestrator 4.6.2

B) Installation Guide McAfee ePolicy Orchestrator 4.6.0 Software

C) Product Guide McAfee ePolicy Orchestrator 4.6.0 Software

D) Release Notes - McAfee MOVE AntiVirus 2_5_0

E) MOVE Antivirus 2.5 Product Guide

F) VirusScan 8.8 Patch 1 Release Notes

G) VirusScan Enterprise 8.8 Release Notes

H) VirusScan Enterprise 8.8 Installation Guide

I) VirusScan Enterprise 8.8 Product Guide.

J) Product Guide McAfee Agent 4.6.0

K) Release Notes McAfee Agent 4.6.0 Patch 1 for Windows

9.1 Download Security Mechanisms

All software released to customers are developed by McAfee software engineers and tested by a dedicated Quality Assurance (QA) organization. When QA considers a release candidate package to be ready for customer release, the results of QA testing are presented to a Management Team for a final authorization to release to web (RTW). If the Management Team gives approval to release the final release candidate package, QA uploads the final product (software and documentation) to the McAfee download server.
QA posts the final, validated files on an internal secured server where the files are scanned for malware and stored. Access controls to this sever are management by McAfee Information Technology group and audited by McAfee Risk Management. QA verifies the integrity of the

package prior to posting. QA then uses a proprietary Posting Tool to post the product and documentation files from the internal secured server onto the McAfee download server. The download server is accessible from the Internet by customers who have been explicitly granted access via the Grant Code process. Each Grant Code is unique and only provides access to the products the customer is entitled to. Checksums are saved for all files posted to the download server so that unauthorized modifications may be detected. After posting new files, QA performs a test download and verifies that the checksums are correct.

As described above, Grant Codes are unique per customer and provide access to the software the customer has purchased. Grant Codes are sent directly to the named contact on the customer's order and are valid for 30 days before they expire. The McAfee download server uses HTTPS (or SSL encryption) to secure the link between the customer and the download server. After entering the appropriate Grant Code, the customer is presented with a page permitting them to select the available versions of the product they are entitled to download. The customer shall select the appropriate product version (as specified in the TOE Security Target) and associated documentation to download the Common Criteria evaluated product.

9.2 Configuring the TOE according to the requirements of the Security Target

Communications between ePO and the McAfee Agent are encrypted using AES implemented by FIPS 140-2 validated modules.
This section outlines the required steps for entering FIPS Mode for ePO and the McAfee Agent.

To install ePO in FIPS mode:

1. The installation must be a new install. Upgrading from a previous version of ePO is not valid.
2. During the installation process, enter the following command at the command line interface: C:\> <ePO 4.6 install package>\setup.exe ENABLEFIPSMODE=1
3. After installation, edit <ePO install dir>\server\conf\orion\logs\logconfig.xml. Change the priority value parameter of the root logger level from warn to info.

To install McAfee Agent in FIPS mode:

1. The installation must be a new install. Upgrading from a previous version of McAfee Agent is not valid.
2. The module is included with McAfee Agent 4.6 and is not separately purchased or Installed.
3. McAfee Agent 4.6 (and subsequently the module) can be installed either via deployment from ePO Server or downloading and executing framepkg.exe from the ePO server.

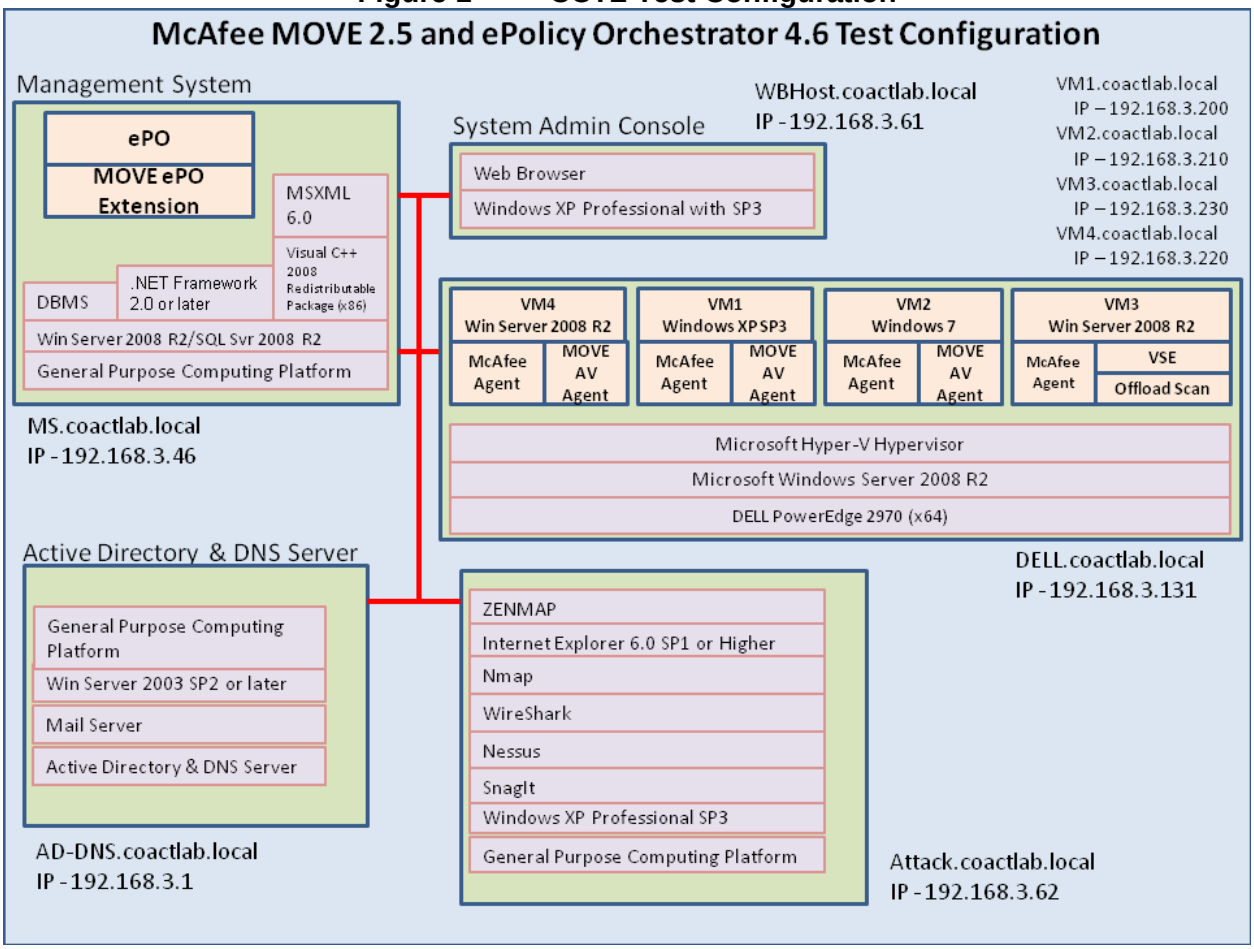
10 Evaluator Functional Test Environment

Testing was completed on August 31, 2012 at the COACT CCTL in Columbia, Maryland. COACT employees performed the tests.

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



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

Table 7 - Test Configuration Overview

System	Purpose
Management System (ePO Server)	The ePolicy Orchestrator server provides a scalable platform for centralized policy management and enforcement of your security products and systems on which they reside. The system should be configured per the figure above, with the Active Directory and DNS server configured as coactlab.local. The Management System maps to address 192.168.3.46.
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.
Managed System	Test computer with MOVE and the VMs installed.
System Admin Console	This system that provides remote access to the

System	Purpose
	Management System.
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 8 - Management System Platform Requirements

Management System Minimum Requirements	
Processor	Intel Pentium D 3 GHz
Memory	2 GB RAM
Free Disk Space	2.5 GB
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	Windows Server 2008 R2 Standard
DBMS	Microsoft SQL Server 2008 R2
Browser	Internet Explorer 8.0
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.
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) Outlook Express MSXML 6.0 Adobe Reader
TOE	McAfee ePO 4.6 McAfee MOVE ePO Extension 4.6
Configuration	Static IP address 192.168.3.46 FQDN: MS.CoactLab.local
Updates	All third party vendor security and product updates

Table 9 - Attack PC Details

Item	Purpose
Installed software	Windows XP Professional SP3 (x32 - Including all updates and patches) Internet Explorer 8.0 ZENMAP GUI 5.21 Nmap 5.21 SnagIt 8 WireShark 1.8.0 Nessus Version 4.4
Configuration	Static IP address 192.168.3.62 FQDN: Attack.CoactLab.local

Table 10 - Active Directory & DNS Server Details

Item	Purpose
Operating System	Microsoft Windows Server 2003 SP2
Installed software	MailEnable 5.51 Internet Explorer 8.0
Configuration	Static IP address 192.168.3.1 FQDN: AD-DNS.CoactLab.local Primary Domain Controller for CoactLab.local DNS Server for CoactLab.local with records for all systems identified in the test configuration
Updates	All third party vendor security and product updates

Table 11 - System Admin Console Details

Item	Purpose
Installed software	Windows XP Professional SP3 (x32 - Including all updates and patches) Internet Explorer 8.0 Snag It 8 Adobe Reader
Configuration	Static IP address 192.168.3.61 FQDN: WBHost.CoactLab.local
Updates	All third party vendor security and product updates

Table 12 - Dell Server Details

Item	Purpose
Processor	Dell PowerEdge 2970 (x64)

Operating System	**Server Operating System:** Windows Server 2008 R2 SP1 (64-bit)
Installed software	Internet Explorer 8.0 Snag It 8 Microsoft Hyper-V Server 2008 R2 Hypervisor
Additional software	Microsoft Windows Installer (MSI) version 3.1 or later
Network Card	10Mb Ethernet or higher
Configuration	Static IP address 192.168.3.131 FQDN: Dell.CoactLab.local
Updates	All third party vendor security and product updates

Table 13 - VM1 Virtual System Details

Item	Purpose
Operating System	**Hyper-V Image** Windows XP SP3
Installed software	Internet Explorer 8.0 Snag It 8 McAfee Agent, v4.6.0 McAfee MOVE Agent 2.5
Additional software	Microsoft Windows Installer (MSI) version 3.1 or later
Network Card	10Mb Ethernet or higher
Configuration	Static IP address 192.168.3.200 FQDN: VM1.CoactLab.local
Updates	All third party vendor security and product updates

Table 14 - VM2 Virtual System Details

Item	Purpose
Operating System	**Hyper-V Image** Windows 7 Professional (64-bit)
Installed software	Internet Explorer 8 Snag It 8 McAfee Agent, v4.6.0 McAfee MOVE Agent 2.5
Additional software	Microsoft Windows Installer (MSI) version 3.1 or later
Network Card	10Mb Ethernet or higher
Configuration	Static IP address 192.168.3.210 FQDN: VM2.CoactLab.local
Updates	All third party vendor security and product updates

Table 15 - VM3 Virtual System Details

Item	Purpose
Operating System	**Hyper-V Image** Windows Server 2008 R2 SP1 (64-bit)
Installed software	Internet Explorer 8.0 Snag It 8 McAfee Agent, v4.6.0 McAfee MOVE Antivirus Offload Server VSE 8.8
Additional software	Microsoft Windows Installer (MSI) version 3.1 or later
Network Card	10Mb Ethernet or higher
Configuration	Static IP address 192.168.3.230 FQDN: VM3.CoactLab.local
Updates	All third party vendor security and product updates

Table 16 - VM4 Virtual System Details

Item	Purpose
Operating System	**Hyper-V Image** Windows Server 2008 R2 SP1 (64-bit)
Installed software	Internet Explorer 8.0 Snag It 8 McAfee Agent, v4.6.0 McAfee MOVE Agent 2.5
Additional software	Microsoft Windows Installer (MSI) version 3.1 or later
Network Card	10Mb Ethernet or higher
Configuration	Static IP address 192.168.3.220 FQDN: VM4.CoactLab.local
Updates	All third party vendor security and product updates

10.1 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 McAfee MOVE Antivirus 2.5 with McAfee ePolicy Orchestrator 4.6 Test Report, Dated August 20, 2012. Document No. E2-0412-013.

10.2 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.

10.3 Evaluator Penetration Tests

The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below.

A) http://osvdb.org/

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

C) http://secunia.com/

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

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

A) McAfee

B) McAfee, Inc.

C) Virus Scan Enterprise

D) McAfee Virus Scan

E) McAfee Agent

F) McAfee MOVE

G) MOVE Agent

H) ePolicy

I) ePolicy Orchestrator

J) ePolicy Orchestrator extension

K) McAfee ePolicy Orchestrator 4.6

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

A) Citrix XenServer 5.5 Update 2

B) Microsoft Hyper-V Server 2008 R2

C) VMware ESX 3.5 Update 4

D) VMware ESX 4.0 Update 1

The identified vulnerabilities for the TOE were for earlier versions of the TOE. The evaluator contacted the vendor concerning these findings and the vendor confirmed that all of the identified vulnerabilities were mitigated and included in the evaluated version of the TOE. No additional patches or updates are required by the end user for the present version of the TOE in order to mitigate these vulnerabilities.

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

10. Validator Comments

The TOE was successfully evaluated in the defined evaluated configuration and scope described in Security Target. The validation team recommends certification of the TOE at EAL 2 augmented with ALC_FLR.2.

11. Security Target

McAfee Endpoint Encryption for PC with McAfee ePolicy Orchestrator Common Criteria EAL2+ Security Target, Rev 014, June 22, 2012

12. List of Acronyms

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
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
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 following list of standards was used in this evaluation:

- Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model, Version 3.1, Revision 3, dated July 2009
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 3.1, Revision 3, dated July 2009
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 3.1, Revision 3, dated July 2009
- Common Methodology for Information Technology Security Evaluation Methodology Version 3.1, Revision 3, July 2009
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000