McAfee Endpoint Encryption 7.0 for PC with McAfee ePolicy Orchestrator 4.6 Common Criteria EAL2+ Security Target

Prepared for McAfee, Inc. by

Primasec Ltd

McAfee, Inc.
2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com

Contents

Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	McAfee, Inc. McAfee Endpoint Encryption for PC with McAfee ePolicy Orchestrator Security Target
ST Revision	018
ST Publication Date	02 May 2013
Author	Primasec Limited

1.2 TOE Reference

TOE Reference	McAfee Endpoint Encryption for PC 7.0 with McAfee ePolicy Orchestrator 4.6
TOE Type	Centrally Managed PC Access Control and Full Disk Encryption

1.3 Document Organization

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Figure 1 Document Organization

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement*, *selection*, *assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by underlined text.

- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).

- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *italicized* text.

- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FIA_UAU.1.1 (A) and FIA_UAU.1.1 (B) refer to separate instances of the FIA_UAU.1 security functional requirement component.

Outside the SFRs, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

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

Figure 2 Glossary

1.6 TOE Overview

McAfee Endpoint Encryption for PC 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.

Seamless 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.

1.7 TOE Description

McAfee Endpoint Encryption for PC is a Personal Computer (PC) security system that prevents the data stored on a PC's HDD/SSD storage media from being read or used by an unauthorized person. Non-removable and eSATA hard drives can be encrypted. USB, FireWire or PCMCIA connected media cannot be encrypted.

By necessity, the boot record and certain non-security relevant configuration data must remain in plaintext, but everything else on the storage media is encrypted. In simple terms, the McAfee Endpoint Encryption client software takes control of a user's storage media away from the operating system. The McAfee Endpoint Encryption client software encrypts data written to the storage media, and decrypts data read from it. If the storage media is read directly, one would find only encrypted data, even in the Windows swap file and temporary file areas.

ePO provides the functionality to securely deploy, configure and manage the McAfee Endpoint Encryption Client using policies. A policy is a set of rules that determine how the McAfee Endpoint Encryption Client software functions on the user's computer.

In order to operate in compliance with this Security Target, the TOE Endpoint must be installed and operated in a certain manner. This is referred to as its Common Criteria mode of operation, or CC mode for short. CC mode is defined as follows:

- Endpoint is installed in FIPS mode according to the TOE administration documentation
- 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
- Encryption of all hard disks
- Users forced to logon with Preboot Authentication

The client software is installed on the client system. After the installation, the system synchronizes with ePO and acquires the user data, token data, and Pre-Boot graphics. When this is complete, the user authenticates and logs on through the Pre-Boot environment, which loads the operating system, and uses the system as normal.

In this document, the McAfee Endpoint Encryption client software is also known as the TOE Endpoint or simply the Endpoint. If "TOE" is used, this refers to all of the software within the TOE, including the Endpoint, McAfee Agent and ePO. The full list of TOE software components is given in section 1.7.1 below.

1.7.1 Physical Boundary

The TOE is a software TOE and includes:

1. The ePO application executing on a dedicated server (which includes an ePO Agent Handler)
2. Optional additional ePO Agent Handler(s)
3. An EEPC specific ePO extension
4. The McAfee Agent application on each managed system
5. The Endpoint software installed on each client PC

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.

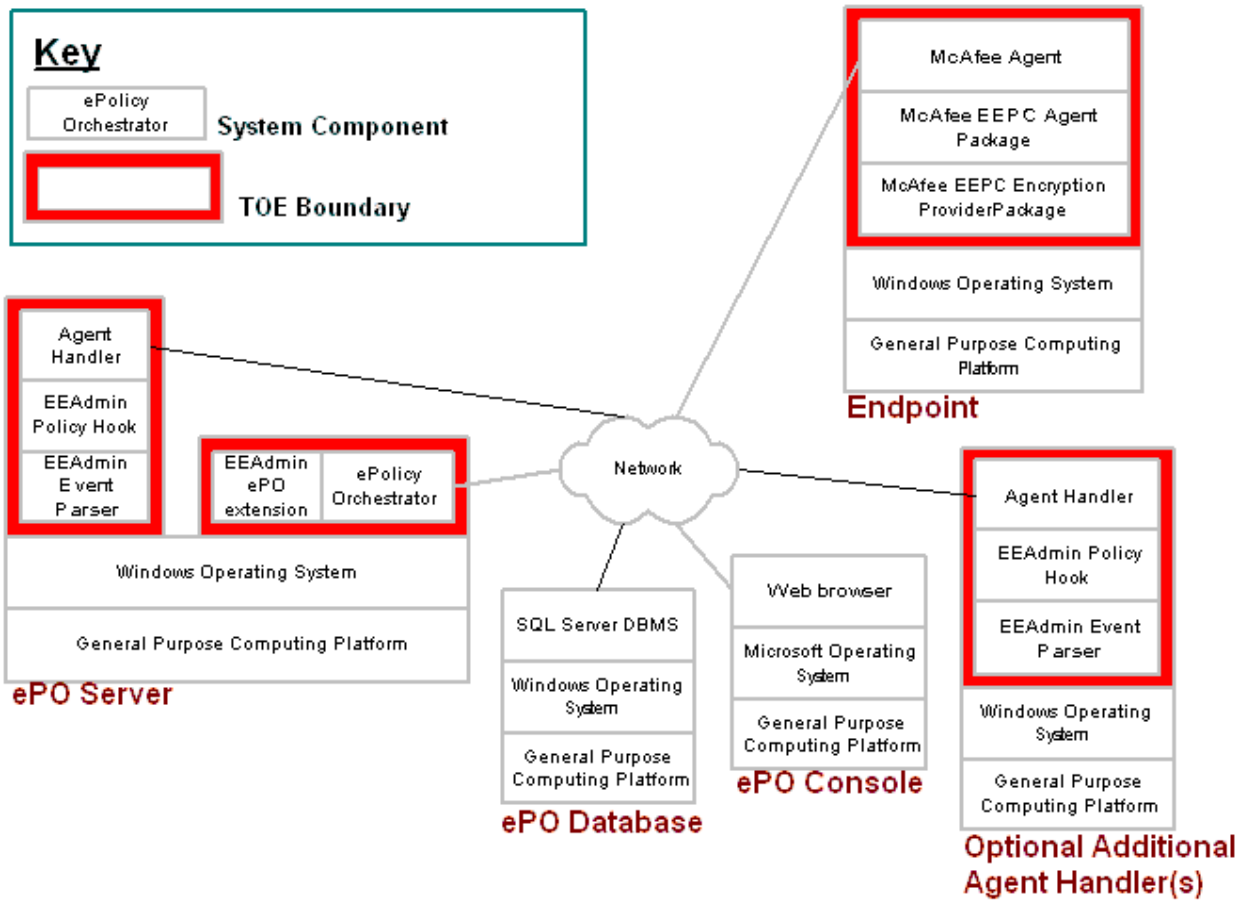


Figure 3 TOE Boundary

The TOE components communicate with each other as follows:

TOE COMPONENT	INTERCONNECTIONS
ePO Server	An administrator has access to the functionality of the ePO Server via the ePO console. Configuration data is stored on the ePO Database. Policies are deployed to Endpoints via Agent Handlers.
Endpoint	The Endpoint communicates with the ePO Server via an Agent Handler for the purpose of receiving policy updates and key archiving.

Figure 4 TOE Component Inter-communication

In order to comply with the evaluated configuration, the hardware and software components detailed in Figure 7 and Figure 8 should be used along with the following TOE components:

TOE COMPONENT	VERSION AND DETAILS
ePO	ePO, v4.6.4 EEAdmin ePO extension, v7.0.0.311 EEPC ePO extension, v7.0.0.311 EEAdmin policy hook, v7.0.0.311 EEAdmin event parser, v7.0.0.311
Endpoint	McAfee Agent, v4.6 McAfee EEPC Agent, MfeEEAgent, v7.0.0.311 McAfee EEPC Encryption Provider, MfeEEPC, v7.0.0.311[1]

Figure 5 TOE Components

1.7.1.1 ePO

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 ePolicy Orchestrator Administration console allows the administrator to manage the McAfee Endpoint Encryption policies in the client computer. It also allows you to deploy and manage the McAfee Endpoint Encryption products including EEPC. It provides comprehensive reporting and product deployment capabilities; all through a single point of control.

McAfee Endpoint Encryption is managed through ePolicy Orchestrator using a combination of user and product-based policies. The ePolicy Orchestrator console allows the administrator to enforce policies across groups of computers or on a single computer. Any new policy enforcement through McAfee ePO overrides the existing policy that is already set on the individual systems.

1.7.1.2 EEPC ePO extension

The EEPC extension installed in ePolicy Orchestrator defines the encryption algorithm, product settings, and server settings for the client system. The EEPC software package checked in to ePolicy Orchestrator defines the actual Endpoint Encryption software that is installed on the client system.

1.7.1.3 EEAdmin ePO extension

The EE Administration system (EE Admin) defines the generic endpoint encryption settings for product-based policies, user-based policies, and server settings for the users and provides the back-end processing required for EEPC management.

1.7.1.4 EEAdmin Policy Hook

The policy hook intercepts EEPC system policies sent from ePO to an endpoint, and injects user and timestamp metadata into them, before handing them off for delivery to the Endpoint. This mechanism is used to deliver user manifests to the Endpoint.

[1] When installed in FIPS mode, crypto v6.1.3 is installed on the endpoint workstation.

1.7.1.5 EEAdmin Event Parser

The Event Parser processes events sent from an Endpoint to the ePolicy Orchestrator, and posts appropriate data back to the Endpoint.

1.7.1.6 McAfee Agent

The McAfee Agent is the client-side component that provides secure communication between the Endpoint and ePolicy Orchestrator. The agent also provides local services to the Endpoint.

The McAfee Agent delivers services that include upgrading and installing software, logging, reporting events and properties, task scheduling, communication and policy deployment and storage.

1.7.1.7 EEPC Agent

The EEPC Agent is a flexible and generic host messaging service which provides the architecture to support multiple plugins. It interfaces to the McAfee Agent, and messages from EEPC Agent plugins are routed to and from McAfee Agent through the EEPC Agent. It contains no cryptography or encryption services.

1.7.1.8 EEPC Encryption Provider

The EEPC Encryption provider plugs in to the EEPC Agent provides and manages software encryption capabilities on a Windows TOE Endpoint system.

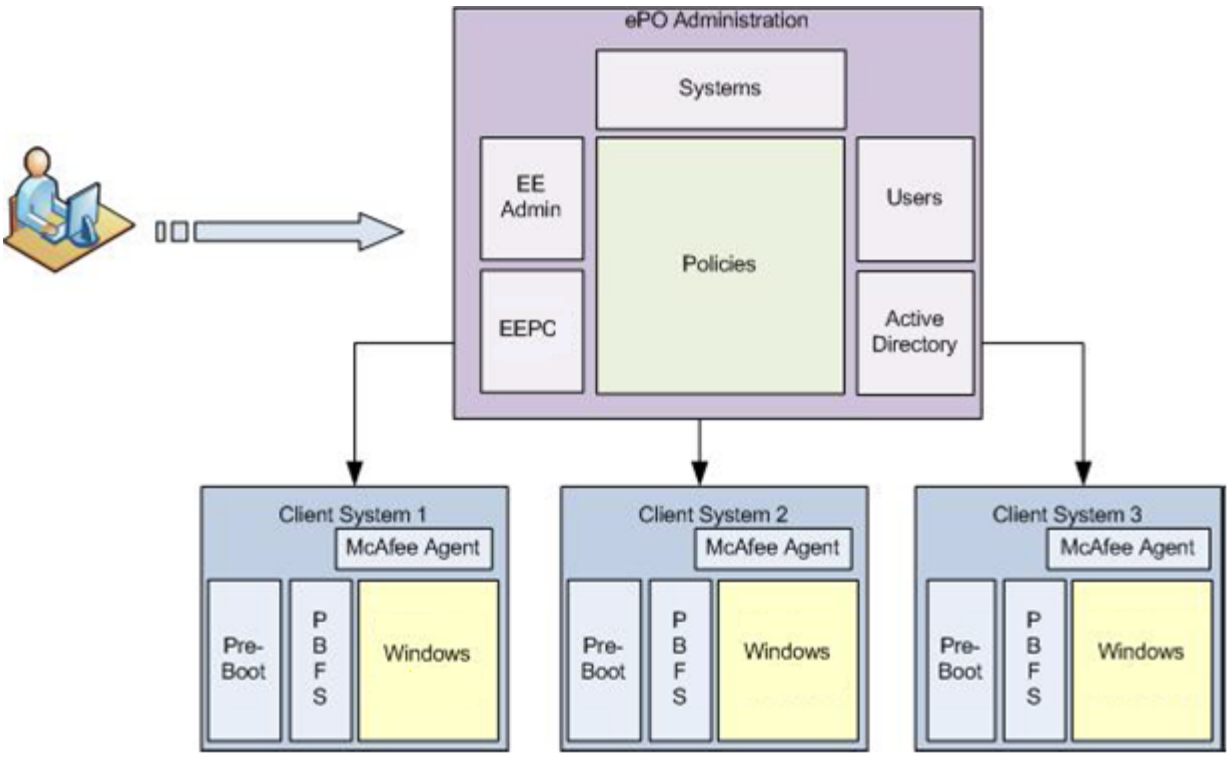


Figure 6 TOE Administration

1.7.2 Hardware and Software Supplied by the IT Environment

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.

1.7.2.1 ePO Server Systems

ePO can be installed on any supported Microsoft Windows server-class operating systems. These are:

- Windows Server 2008 (with Service Pack 2 or higher) Datacenter, Enterprise or Standard, 32 bit or 64-bit
- Windows Server 2008 R2 Datacenter, Enterprise or Standard, 64-bit
- Windows 2008 Small Business Server Premium edition, 64-bit

However, the evaluated IT environments are as follows:

COMPONENT	REQUIREMENTS
Processor	Intel Pentium 4-class or higher; 1.3GHz or higher
Memory	2 GB RAM or higher
Free Disk Space	1.5 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 SP3 or higher Microsoft SQL Server 2008 R2
Browser	Internet Explorer 7.0 or 8.0 browser or Firefox 3.5 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.

Figure 7 ePO Server Requirements

1.7.2.2 TOE Endpoint System requirements

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

SYSTEM	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 8 (32-bit and 64-bit) with legacy BIOS (MBR boot) Windows 7 (32-bit and 64-bit) with SP1, with legacy BIOS (MBR boot) Windows Vista (32-bit and 64-bit) with SP2 Windows XP (32-bit) with SP3
Network Card	100Mb Ethernet or higher

Figure 8 TOE Endpoint System Requirements

1.7.3 Logical Boundary

The logical boundary of the TOE is represented by the thick red line in Figure 3. All of the components within the red border are logically contained within the TOE.

The following features of McAfee Endpoint Encryption PC 7.0 are not part of the evaluated configuration:

a) Use of clients supporting UEFI boot mode as Endpoints;
b) UEFI platform crypto libraries for Windows 8 (the legacy BIOS preboot environment is required, such that the FIPS validated crypto libraries certified for EEPC 6.2 are used);
c) Out of band management;
d) Hardware entropy source;
e) Offline activation;
f) Preboot smart check.

1.7.4 TOE Data

The TOE Data is defined as the encrypted contents of the TOE Endpoint storage media.

1.8 Rationale for Non-bypassability and Separation of the TOE

The responsibility for non-bypassability and non-interference is split between the TOE and the IT Environment. TOE components are software only products and therefore the non-bypassability and non-interference claims are dependent upon hardware and OS mechanisms.

ePO and the TOE Endpoint execute on separate PCs and the rationale for non-bypassability and separation differ for each.

ePO and its extensions execute on a dedicated PC. They run on top of the IT Environment supplied operating systems.

ePO ensures that the security policy is applied and succeeds before further processing is permitted whenever a security relevant interface is invoked: the interfaces are well defined and insure that the

access restrictions are enforced. Security irrelevant interfaces do not interact with the security functionality of the TOE. The TOE depends upon OS mechanisms to protect TSF data such that it can only be accessed via the TOE.

The TOE Endpoint software executes on a PC and protects it from unauthorised access to TSF data

The TOE is implemented with well-defined interfaces that can be categorized as security relevant or security irrelevant. The TOE is implemented such that security irrelevant interfaces have no means of impacting the security functionality of the TOE. Unauthenticated users may not perform any actions within the TOE. The TOE tracks multiple users by sessions and ensures the access privileges of each are enforced.

The ePO server hardware provides virtual memory and process separation, which the server OS utilizes to ensure that other (non-ePO) processes may not interfere with ePO; all interactions are limited to the defined ePO interfaces. The OS and DBMS restrict access to TOE data in the database to prevent interference with the TOE via that mechanism.

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

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 extended and Part 3 conformant at Evaluation Assurance Level 2 and augmented by ALC_FLR.3 – Systematic Flaw remediation.

2.2 Protection Profile Conformance Claim

The TOE does not claim conformance to a Protection Profile.

3 Security Problem Definition

3.1 Threats

This section describes the threats to the assets of the TOE against which specific protection within the TOE or its environment is required.

This section describes the threat profile that the TOE addresses. This profile should be considered in the context of a global system security policy. The TOE is a PC access control and full disk encryption product and the threats it addresses are selected in order to fulfill these objectives.

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.

3.2 Organizational Security Policies

This section describes the complete set of organizational security policy statements or rules with which the TOE must comply.

P.AUTHORIZED_USERS
Only authorized users may use the system.

P.CRYPTOGRAPHIC_KEYS
Cryptographic keys will be generated, accessed, protected, and destroyed in a secure fashion.

P.CRYPTOGRAPHIC_OPERATIONS
All cryptographic operations performed using CAVP approved and certified algorithms.

P.EAVESDROP_TRANSIT
System data must be protected in transmission between the protected system client and server components.

P.USER_ACCOUNTABILITY
Users of the system shall be held accountable for their security relevant actions within the system.

3.3 Assumptions

This section describes the assumptions that have been made about the environment in which the TOE is used, including assumptions about personnel and the physical environment of the TOE. The TOE operates in a secure manner and provides its countermeasures as long as it is utilized in a manner that adheres to the intended environment, and method of delivery, installation and administration.

3.3.1 Personnel Assumptions

This section describes the assumptions about how the staff that are authorized to use the TOE behave.

A.MANAGEMENT
One or more proficient persons are assigned to administer the TOE and the security 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 that he is responsible for are given appropriate guidance.

A.AUTHENTICATION_DATA_PRIVATE
Authentication data is kept private by authorized users of the TOE.

3.3.2 Physical Assumptions

This section describes the assumptions made about the physical environment in which the TOE operates.

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.

3.3.3 System Assumptions

This section describes the assumptions made about the whole of the system of which the TOE forms a component. The assumptions are made in relation to the TOE.

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 Security Objectives

Security objectives address all of the security environment aspects identified. They reflect the intended method of use of the TOE and are suitable to counter all identified threats and cover all identified organizational security policies and assumptions.

4.1 Security Objectives for the TOE

O.AUTHORISATION
The TSF must ensure that only authorized users gain access to the TOE and its resources by uniquely identifying all users and authenticating their claimed identity before granting access to the TOE and its resources.

O.ACCESS_CONTROL
The TSF must control access to the TOE based on authenticating a user's identity.

O.ENCRYPTED_MEDIA
The TSF must provide encryption to protect the data and files kept on the TOE's storage media from unauthorized users that have gained physical access to that storage media.

O.EFFECTIVE_ADMINISTRATION
The TOE must allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

O.AUDIT
The TSF must record the security relevant actions of users of the TOE and have the ability to associate each action with an identified user where possible. The TSF must present this information in a comprehensible format to authorized users while preventing access to unauthorized users.

O.SECURE_RECOVERY
The TOE should allow the user with assistance from an administrator to regain access to his machine and set a new password after forgetting his password.

O.PROTECT
The TSF must protect its own data and resources. It must protect against external interference or tampering.

O.DATA_TRANSFER
The TSF must have the capability to protect system data in transmission between ePO and the TOE Endpoint component.

O.CRYPTOGRAPHIC_KEYS
The TSF must ensure that cryptographic keys are generated, accessed, and protected in a secure fashion.

O.CRYPTOGRAPHIC_OPERATIONS

The TSF must ensure that all cryptographic operations used to protect information and encryption keys are approved and certified by CAVP.

O.EASE_OF_USE_USER
The TSF must prevent the user from configuring the TOE in an insecure fashion. As an aid to this, the user must be allowed to change his password, as required.

4.2 Security Objectives for the Operational Environment

4.2.1 Security Objectives for the IT Environment

OE.TIME_SOURCE
The TOE IT environment must provide a reliable time source to enable the TOE to timestamp audit records.

OE.CRYPTOGRAPHIC_KEY_DESTRUCTION
In order to destroy all keys within the TOE, the operator should uninstall the TOE and then the hard drive on which it was installed should be reformatted and overwritten at least once. The operator should remain present during this process. Uninstallation will remove any plaintext keys from memory and from the hard disk. Reformatting the hard drive will remove any encrypted or public keys from the hard disk. In this way all key material is destroyed. There are no user-accessible plaintext keys in the TOE. Following the destruction process, all keys will have been erased and overwritten.

OE.SECURE_BACKUP
The TOE IT environment must create user data backups that are separately encrypted or physically protected to ensure data security is not compromised through theft of or unauthorized access to backup information.

OE.AVAILABLE_BACKUP
The TOE IT environment must take 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.

OE.DOMAIN_SEPARATION
The TOE IT environment must provide separate threads of execution for TOE processes.

OE.TRUSTED_SOFTWARE
The TOE IT environment must run 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.

4.2.2 Security Objectives for the Non-IT Environment

OE.MANAGED

Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains IT security objectives. These are competent, trained administrators who are not careless, negligent or hostile.

OE.AUTH
Those responsible for the TOE must ensure that users protect all access credentials, such as physical tokens and passwords or other authentication information in a manner that maintains IT security objectives.

OE.EASE_OF_USE_ADMIN
The administrator should ensure that the TOE is configured securely, that is that the TOE is operating in CC mode.

OE.EASE_OF_USE_USER
The user should ensure that his login credentials are not divulged to an unauthorized party and that the TOE is never left unattended while the user is logged onto it.

OE.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.

4.3 Security Objectives Rationale

The following table demonstrates that each threat identified in the TOE security environment is countered by one or more security objectives. Conversely, each security objective (either solely or in collection with other objectives) matches at least one assumption, threat or procedure.

SECURITY OBJECTIVES / THREAT/ ASSUMPTION	OE.MANAGED	OE.EASE_OF_USE_ADMIN	OE.EASE_OF_USE_USER	OE.AUTH	OE.TIME_SOURCE	OE.CRYPTOGRAPHIC_KEY_DESTRUCTION	OE.SECURE_BACKUP	OE.AVAILABLE_BACKUP	OE.DOMAIN_SEPARATION	OE.TRUSTED_SOFTWARE	OE.NON_TECHNICAL_IDENTITY_VERIFICATION
A.CRYPTOGRAPHIC_KEY_DESTRUCTION						X					
A.MANAGEMENT	X										
A.NO_MALEVOLENCE	X										
A.PROFICIENT_USERS		X	X								
A.AUTHENTICATION_DATA_PRIVATE			X	X							
A.TIME_SOURCE					X						
A.SECURE_BACKUP							X				
A.AVAILABLE_BACKUP								X			
A.DOMAIN_SEPARATION									X		
A.TRUSTED_SOFTWARE										X	
A.NON_TECHNICAL_IDENTITY_VERIFICATION											X
T.ACCESS											
T.ALTERNATE_BOOT_PROCESS											
T.CONFIG_MODIFICATION											
T. CORRUPT_AUDIT											
T.EASE_OF_USE_ADMIN		X									
T.EASE_OF_USE_USER											
T.EAVESDROP_TRANSIT											
T.PASSWORD_LOSS											X
T.RECORD_ACTIONS											
T.RECOVERY_MASQUERADE											X
T.REMOVE_DISK											
T.SYSTEM_ACCESS	X										
T.UNAUTHORISED_MODIFICATION	X		X								

SECURITY OBJECTIVES / THREAT/ ASSUMPTION	OE.MANAGED	OE.EASE_OF_USE_ADMIN	OE.EASE_OF_USE_USER	OE.AUTH	OE.TIME_SOURCE	OE.CRYPTOGRAPHIC_KEY_DESTRUCTION	OE.SECURE_BACKUP	OE.AVAILABLE_BACKUP	OE.DOMAIN_SEPARATION	OE.TRUSTED_SOFTWARE	OE.NON_TECHNICAL_IDENTITY_VERIFICATION
P.AUTHORISED_USERS											
P.CRYPTOGRAPHIC_KEYS						X					
P.CRYPTOGRAPHIC_OPERATIONS											
P.EAVESDROP_TRANSIT											
P.USER_ACCOUNTABILITY				X							

Figure 9 Matching Threats and Organizational Security Policies with Security Objectives for the IT Environment

SECURITY OBJECTIVES / THREAT/ ASSUMPTION	O.AUTHORISATION	O.ACCESS_CONTROL	O.AUDIT	O.ENCRYPTED_MEDIA	O.PROTECT	O.EFFECTIVE_ADMINISTRATION	O.EASE_OF_USE_USER	O.DATA_TRANSFER	O.SECURE_RECOVERY	O.CRYPTOGRAPHIC_KEYS	O.CRYPTOGRAPHIC_OPERATIONS
A.CRYPTOGRAPHIC_KEY_DESTRUCTION											
A.MANAGEMENT											
A.NO_MALEVOLENCE											

SECURITY OBJECTIVES / THREAT/ ASSUMPTION	O.AUTHORISATION	O.ACCESS_CONTROL	O.AUDIT	O.ENCRYPTED_MEDIA	O.PROTECT	O.EFFECTIVE_ADMINISTRATION	O.EASE_OF_USE_USER	O.DATA_TRANSFER	O.SECURE_RECOVERY	O.CRYPTOGRAPHIC_KEYS	O.CRYPTOGRAPHIC_OPERATIONS
A.PROFICIENT_USERS											
A.AUTHENTICATION_DATA_PRIVATE											
A.TIME_SOURCE											
A.SECURE_BACKUP											
A.AVAILABLE_BACKUP											
A.DOMAIN_SEPARATION											
A.TRUSTED_SOFTWARE											
A.NON_TECHNICAL_IDENTITY_VERIFICATION											
T.ACCESS	X	X	X								
T.ALTERNATE_BOOT_PROCESS				X							
T.CONFIG_MODIFICATION					X						
T.CORRUPT_AUDIT	X		X	X		X					
T.EASE_OF_USE_ADMIN											
T.EASE_OF_USE_USER							X				
T.EAVESDROP_TRANSIT								X			
T.PASSWORD_LOSS									X		
T.RECORD_ACTIONS	X		X								
T.RECOVERY_MASQUERADE	X										
T.REMOVE_DISK				X							
T.SYSTEM_ACCESS	X				X						
T.UNAUTHORISED_MODIFICATION	X			X	X						
P.AUTHORISED_USERS	X										
P.CRYPTOGRAPHIC_KEYS										X	

THREAT/ ASSUMPTION \ SECURITY OBJECTIVES	O.AUTHORISATION	O.ACCESS_CONTROL	O.AUDIT	O.ENCRYPTED_MEDIA	O.PROTECT	O.EFFECTIVE_ADMINISTRATION	O.EASE_OF_USE_USER	O.DATA_TRANSFER	O.SECURE_RECOVERY	O.CRYPTOGRAPHIC_KEYS	O.CRYPTOGRAPHIC_OPERATIONS
P.CRYPTOGRAPHIC_OPERATIONS											X
P.EAVESDROP_TRANSIT								X			
P.USER_ACCOUNTABILITY			X								

Figure 10 Matching Threats and Organizational Security Policies with Security Objectives

OE.MANAGED
Those responsible for the TOE ensure that it is managed securely. Specifically, one or more competent individuals are assigned management responsibility for the TOE (A.MANAGEMENT). These individuals are expected to behave professionally and are trusted to behave in a way that maintains the security of the TOE (A.NO_MALEVOLENCE). If the TSF is configured securely and its users and administrators act in accordance with their training in its correct use, then, if all other TSF security objectives are met, there should be no way for an unauthorized user to gain access to or modify the TOE, thus countering the threats T.SYSTEM_ACCESS and T.UNAUTHORISED_MODIFICATION.

OE.EASE_OF_USE_ADMIN
The TOE is managed by proficient administrators that have been trained in its use and follow the guidance laid down for its secure use (A.PROFICIENT_USERS). One measure of this proficiency is that administrators check their actions to ensure that they do not inadvertently configure the TSF in an insecure fashion, countering the threat T.EASE_OF_USE_ADMIN..

OE.EASE_OF_USE_USER
The TOE Endpoint is used by proficient users that have been trained in its use and follow the guidance laid down for its secure use (A.PROFICIENT_USERS). Specifically, users are expected to not leave the TOE Endpoint unattended in a logged in state, ensuring that it cannot be modified and so countering the threat T.UNAUTHORISED_MODIFICATION. Users are expected to keep their secure user credentials secret and so meet the assumption A.AUTHENTICATION_DATA_PRIVATE.

OE.AUTH
Users and administrators of the TOE are expected to keep their secure user credentials secret, and so meet the assumption A.AUTHENTICATION_DATA_PRIVATE. As an incentive, users may be held accountable for all security relevant actions carried out on the TSF (P.USER_ACCOUNTABILITY), and all such actions are audited, although this is covered by a separate objective, O.AUDIT.

OE.TIME_SOURCE
The IT environment provides a reliable source of time information to enable the TSF to timestamp its audit records (A.TIME_SOURCE).

OE.CRYPTOGRAPHIC_KEY_DESTRUCTION
The IT environment provides a means of deleting all of the cryptographic keys from the TOE (A.CRYPTOGRAPHIC_KEY_DESTRUCTION).

OE.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 (satisfying the assumption A.SECURE_BACKUP).

OE.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.AVAILABLE_BACKUP).

OE.DOMAIN_SEPARATION
Separate threads of execution for TOE processes enable the TOE to be protected from potential attack from malicious software processes (A.DOMAIN_SEPARATION).

OE.TRUSTED_SOFTWARE
Running only trusted software in the TOE IT environment and taking other relevant measures such as using anti-virus software and firewalls, etc. as appropriate protects the TOE against attack from malicious software and enables it to target its specific threat profile (A.TRUSTED_SOFTWARE).

OE.NON_TECHNICAL_IDENTITY_VERIFICATION
This objective, that there is a database of authorized TSF-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 directly addresses the assumption A.NON_TECHNICAL_IDENTITY_VERIFICATION. Ordinarily, recovery would take place using a secure management session, but there are times when this is not possible, such as when the use has no network connection to ePO. By allowing a user to be authenticated by non-technical means, it allows the administrator to reset the user's password in the event of password loss, thus countering the threat T.PASSWORD_LOSS. By providing a mechanism for the non-technical verification of the identity of a user, this objective counters the threat T.RECOVERY_MASQUERADE. There is a threat that this recovery mechanism can be subverted through an attacker overhearing the recovery process and impersonating

the user with the authentication information. This threat is addressed by the objective O.AUTHORISATION.

O.AUTHORISATION
This objective is at the heart of what McAfee Endpoint Encryption for PC does. McAfee Endpoint Encryption for PC provides access control and does not allow any user access until their credentials have been authenticated and so addresses the threats T.ACCESS, T.SYSTEM_ACCESS, T.RECORD_ACTIONS, T.UNAUTHORISED_MODIFICATION and T.CORRUPT_AUDIT. By implementing access control with authentication, this objective implements the policy P.AUTHORISED_USERS.

If a TOE Endpoint PC is stolen, this fact is used to allow it to be disabled by the ePO server. If the machine is connected to ePO, it can be disabled so that no user can logon to it. If it is not connected to ePO, and the thief tries to gain access to it via the offline recovery mechanism, he will be denied, even though he may be able to convincingly masquerade as a genuine user. This addresses the threat T.RECOVERY_MASQUERADE.

O.ACCESS_CONTROL
The TSF provides access control. This objective along with O.AUTHORISATION and O.AUDIT counters the threat T.ACCESS

O.AUDIT
The TSF audits certain events to allow authorized administrators to monitor how the TOE Endpoint is being used and potentially to detect any attempts to undermine its security. O.AUDIT implements the policy P.USER_ACCOUNTABILITY. By recording audit events and by requiring administrators to be authenticated before being able to view or clear audit information, this objective is partly responsible for countering the threats T.ACCESS, T.CORRUPT_AUDIT and T.RECORD_ACTIONS.

O.ENCRYPTED_MEDIA
Along with access control, the TSF encrypts its storage media so that any attempts to bypass access control will fail as the attacker will only have gained access to encrypted data that he will not be able to decrypt without also obtaining the hard disk encryption key. This objective therefore counters the threats T.ALTERNATE_BOOT_PROCESS and T.REMOVE_DISK. By encrypting the storage media, this also protects the audit trail and any other data or applications stored on the storage media against unauthorized modification, thus countering T.UNAUTHORISED_MODIFICATION and T.CORRUPT_AUDIT.

O.PROTECT
The TSF provides synchronization and self-test facilities to help it to detect any unauthorized modification or accidental corruption of its own configuration or resources. This counters the threat T.CONFIG_MODIFICATION, T.SYSTEM_ACCESS and T.UNAUTHORISED_MODIFICATION.

O.EFFECTIVE_ADMINISTRATION
This is in some ways an objective that is made up of aspects of other objectives (O.AUTHORISATION, OE.MANAGED, OE.EASE_OF_USE_ADMIN, O.DATA_TRANSFER, O.AUDIT) and is included to emphasize the

importance of administration to the TOE. It counters the threats T.SYSTEM_ACCESS, T.CORRUPT_AUDIT, T.RECOVERY_MASQUERADE, T.RECORD_ACTIONS, T.ACCESS and the assumption A.MANAGEMENT

O.EASE_OF_USE_USER
The only function that the user may perform at the client interface that affects the configuration of security is the ability to change his password. The administrator defines the password policy such that the user is not able to change his password to a value that contravenes this password policy. This objective thus counters the threat T.EASE_OF_USE_USER.

O.DATA_TRANSFER
This objective implements the policy P.EAVESDROP_TRANSIT using DSS and AES block encryption to authenticate and encrypt all transmissions between the TOE Endpoint and the ePO server. By doing so, it prevents unauthorized access to the information in the transmissions, thus countering the threat T.EAVESDROP_TRANSIT. The protocol for establishing a secure management session is a one-time authentication protocol, preventing an attacker from establishing a secure management session by replaying transmissions that he has recorded previously, and so countering the threat.

O.SECURE_RECOVERY
If a user forgets his password then there is the possibility that the TSF protected information will be lost. This objective counters the threat of T.PASSWORD_LOSS by providing a secure recovery mechanism to allow the user to regain authenticated access to the TOE Endpoint using a new password.

O.CRYPOTOGRAPHIC_KEYS
The TSF ensures that cryptographic keys are generated, accessed, and protected in a secure manner. O.CRYPTOGRAPHIC_KEYS contributes to the implementation of the security policy P.CRYPTOGRAPHIC_KEYS. The key destruction element of P.CRYPTOGRAPHIC_KEYS is provided by OE.CRYPTOGRAPHIC_KEY_DESTRUCTION.

O.CRYPTOGRAPHIC_OPERATIONS
The TSF must ensure that all cryptographic operations used to protect information and encryption keys use CAVP certified cryptographic algorithm implementations. O.CRYPTOGRAPHIC_OPERATIONS implements the security policy P.CRYPTOGRAPHIC_OPERATIONS.

5 Extended Components Definition

5.1.1 Class FDP: User Data Protection

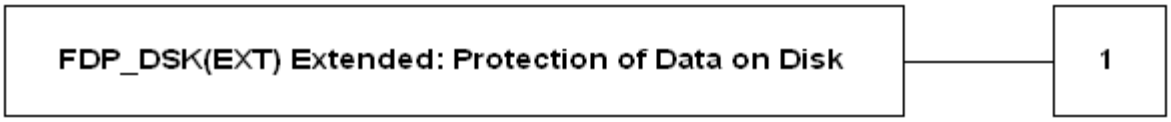
The FDP: User data protection class contains families specifying requirements related to protecting user data. FDP: User data protection is split into four groups of families that address user data within a TOE, during import, export, and storage as well as security attributes directly related to user data. This section defines an extended definition to address the requirement for encrypted user data storage.

Extended: Protection of Data on Disk (FDP_DSK(EXT))

Family behavior

This family relates to the secure storage of user data. It stipulates encryption of all user data. Encryption occurs using a suitable cryptographic algorithm and a suitable cryptographic key.

Component leveling



FDP_DSK(EXT).1 Extended: Protection of Data on Disk specifies that encryption of any critical file will not depend on a user electing to protect that file. The disk encryption specified in FDP_DSK(EXT).1 occurs transparently to the user and the decision to protect the data is outside the discretion of the user, which is a characteristic that distinguishes it from file encryption.

This requirement is addressing not just explicitly stored files containing user data but includes chunks of data that are stored in swap files, registries, and other IT Environment storage areas on the disk. It does not require encryption of all removable media. However, it does require encryption of all hard drives.
Management: FDP_DSK(EXT).1

There are no management activities foreseen.

Audit: FDP_DSK(EXT).1

There are no auditable events foreseen.

FDP_DSK(EXT).1 Extended: Protection of Data on Disk

Hierarchical to: No other components.

Dependencies: FCS_COP.1, FCS_CKM.1

FDP_DSK(EXT).1.1 The TSF shall perform Full Disk Encryption in accordance with FCS_COP.1.

FDP_DSK(EXT).1.2 The System Key can only exist on an unpowered laptop if it is encrypted with some other key (such as a User Key or Recovery Key) derived as specified in FCS_CKM.1.

FDP_DSK(EXT).1.3 The TSF shall encrypt all user data without user intervention.

Application Note: “Full Disk Encryption” is defined here as “the process of encrypting all the data on the hard drive of a computer, including the computer’s Operating System, and permitting access to the data

only after successful authentication to the TOE" with the exception of the MBR and associated bootable partition containing the code necessary to accept and process the authorization factors.

6 Security Requirements

6.1 Security Functional Requirements

FUNCTIONAL CLASS	FUNCTIONAL COMPONENTS
FAU: Security Audit	FAU_GEN.1 Audit data generation
	FAU_GEN.2 User identity association
	FAU_STG.1 Protected audit trail storage
	FAU_STG.3 Action in case of possible audit data loss (Endpoint)
	FAU_STG.4 Prevention of Audit Data Loss (ePO)
	FAU_SAR.1 Audit review
	FAU_SAR.3 Selectable audit review
FDP: User Data Protection	FDP_DSK(EXT).1 Extended: Protection of Data on Disk
FCS: Cryptographic Support	FCS_CKM.1 Cryptographic key generation
	FCS_COP.1(A) Cryptographic operation (data encryption and decryption)
	FCS_COP.1(B) Cryptographic operation (key encryption and decryption)
	FCS_COP.1(C) Cryptographic operation (authenticated administration)
FIA: Identification and authentication	FIA_ATD.1 User attribute definition
	FIA_UAU.2 User authentication before any action
	FIA_UAU.7 Protected authentication feedback
	FIA_UID.2 User identification before any action
FMT: Security Management	FMT_MTD.1(A) Management of TSF data (audit)
	FMT_MTD.1(B) Management of TSF data (password)
	FMT_REV.1 Revocation
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security roles
FPT: Protection of the TSF	FPT_TST.1 TSF testing
	FPT_RCV.1 Manual recovery

Figure 11 Security Functional Requirements of the TOE

6.1.1 Security Audit (FAU)

FAU_GEN.1 Audit data generation (TOE Endpoint)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *not specified* level of audit; and

c) All ePO and Endpoint events, specifically:
The following Endpoint events are audited:
- Logon events
- Password change
- Password invalidation
- Recovery events
- Disk Cryption events
- Policy change events
- Activation events

The ePO events audited are as follows:
- Recovery events
- User events
- Themes events
- V5 Audit events
- Server settings events
- Key re-use events
- Password events
- Clear SSO Details events

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, no other relevant information

Application Note: Auditing is always active in the TOE Endpoint. Audit entries are not created for the start-up and shutdown of the audit functions as these functions are never started up or shutdown. As long as the TOE Endpoint is operational, its audit functions are also operational.

FAU_GEN.2 User identity association
FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_STG.1 Protected audit trail storage
FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.
FAU_STG.1.2 The TSF shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.3 Action in case of possible audit data loss (TOE Endpoint)
FAU_STG.3.1 The TSF shall take the action of overwriting the oldest audit records first if the audit trail exceeds 1000 items.

FAU_STG.4 Prevention of Audit Data Loss (ePO)
FAU_STG.4.1 The TSF shall *ignore auditable events* and perform null action if the audit trail is full.

FAU_SAR.1 Audit review
FAU_SAR.1.1 The TSF shall provide authorized administrators with the capability to read all audit information from the audit records.
FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.3 Selectable audit review
FAU_SAR.3.1 The TSF shall provide the ability to apply sorting of audit data based on date and time, the event code, the object (device) or the description of the audited event.

Application Note: Audit Review and Selectable Audit Review are only accessible to an authorized administrator through the ePO Console.

6.1.2 User Data Protection (FDP)

FDP_DSK(EXT).1 Extended: Protection of Data on Disk
FDP_DSK(EXT).1.1 The TSF shall perform Full Disk Encryption in accordance with FCS_COP.1.
FDP_DSK(EXT).1.2 The System Key can only exist on an unpowered laptop if it is encrypted with some other key (such as a User Key or Recovery Key) derived as specified in FCS_CKM.1.
FDP_DSK(EXT).1.3 The TSF shall encrypt all user data without user intervention.

6.1.3 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic key generation
FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm HMAC Deterministic Random Bit Generator and specified cryptographic key sizes 256 bits for AES and 2048 bits for RSA that meet the following: SP 800-90.

Application Note: The TOE generates symmetric keys to use to encrypt the storage media and asymmetric keys to secure the symmetric keys.

Application Note: The cryptographic algorithms used within the TOE are provided by FIPS 140-2 cryptographic modules. These are the McAfee Endpoint Encryption Client Cryptographic Module (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2012.htm#1686) and the McAfee Endpoint Encryption Disk Driver Cryptographic Module (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2012.htm#1677). These modules have been successfully validated against the FIPS 140-2 criteria, and specifically their key generation and AES encryption functionality are approved to FIPS 140-2.

FCS_COP.1(A) Cryptographic operation (data encryption and decryption)
FCS_COP.1.1(A) The TSF shall perform data encryption and decryption in accordance with a specified cryptographic algorithm AES and cryptographic key sizes 256 bits that meet the following: FIPS 197.

Application Note: The TOE Endpoint uses AES for disk encryption.

FCS_COP.1(B) Cryptographic operation (key encryption and decryption)
FCS_COP.1.1(B) The TSF shall perform key encryption and decryption in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes 2048 bits that meet the following: PKCS#1.

FCS_COP.1(C) Cryptographic operation (authenticated administration)
FCS_COP.1.1(C) The TSF shall perform encrypted session based communication between Endpoint and ePO using McAfee Agent in accordance with a specified cryptographic algorithm TLS for key establishment and AES for encryption and cryptographic key sizes 256 bits for AES that meet the following: FIPS 197 for AES and RFC 5246 for TLS.

Application Note: The cryptographic algorithms used to provide authenticated administration are provided by two specific FIPS 140-2 cryptographic modules. These are the McAfee ePO Client Cryptographic Module (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm#1587) and the McAfee Agent Cryptographic Module (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm#1588). These modules have been successfully validated against the FIPS 140-2 criteria.

6.1.4 Identification and Authentication (FIA)

FIA_ATD.1 User attribute definition
FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) User Identitifier
b) Password policy
c) Token properties
d) System key
e) User public key
f) User secret key
g) User Group membership

FIA_UAU.2 User authentication before any action
FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.7 Protected authentication feedback
FIA_UAU.7.1 The TSF shall provide only [**assignment:** feedback consisting of a '*' for each character typed for all passwords] to the user while the authentication is in progress.

FIA_UID.2 User identification before any action
FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.5 Security Management (FMT)

The SFRs in this section refer to the TOE secure management of the TOE Endpoint.

FMT_MTD.1(A) Management of TSF data (audit)
FMT_MTD.1.1(A) The TSF shall restrict the ability to *query or clear* the TSF audit data to authorized administrators.

FMT_MTD.1(B) Management of TSF data (password)
FMT_MTD.1.1(B) The TSF shall restrict the ability to *modify* the a user's password to authorized administrators and a user may modify his own password if he successfully supplies his existing password first.

FMT_REV.1 Revocation
FMT_REV.1.1 The TSF shall restrict the ability to revoke user accounts associated with the *users* under the control of the TSF to authorized administrators.

FMT_REV.1.2 The TSF shall enforce the rules Revocation takes place the next time the user logs on.

FMT_SMF.1 Specification of Management Functions
FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: User: Changing password of current user. Administrator: Adding, modifying and deleting: user accounts, tokens and disk encryption policies.

FMT_SMR.1 Security roles
FMT_SMR.1.1 The TSF shall maintain the roles: Administrator, User
FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.6 Protection of the TSF (FPT)

FPT_TST.1 TSF testing
FPT_ TST.1.1 The TSF shall run a suite of self-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.
FPT_ TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of the TSF encryption algorithms, specifically AES-256, SHA-256 and RSA, and the random number generator.
FPT_ TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored executable code.

FPT_RCV.1 Manual recovery
FPT_RCV.1.1 After a user account has been disabled or the user has forgotten their logon password when they try to logon, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

6.2 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2) augmented by ALC_FLR.3. The assurance components are summarized in the following table:

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.3 Systematic flaw remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Figure 12 Security Assurance Requirements

6.3 CC Component Hierarchies and Dependencies

This section of the Security Target demonstrates that all of the SFRs hierarchical to or dependent on the identified SFRs are also included within the Security Target. Where there are dependencies outside of the TOE within the IT environment, a rationale as to how this dependency is satisfied is included.

SFR	Hierarchical to	Dependencies	Notes
FAU_GEN.1	No other components	FPT_STM.1	Satisfied by OE.TIME_SOURCE in the IT environment.
FAU_GEN.2	No other components	FAU_GEN.1 FIA_UID.1	
FAU_STG.1	No other components	FAU_GEN.1	

SFR	HIERARCHICAL TO	DEPENDENCIES	NOTES
FAU_STG.3	No other components	FAU_STG.1	
FAU_STG.4	FAU_STG.3	FAU_STG.1	
FAU_SAR.1	No other components	FAU_GEN.1	
FAU_SAR.3	No other components	FAU_SAR.1	
FDP_DSK(EXT).1	No other components	FCS_COP.1 FCS_CKM.1	
FCS_CKM.1	No other components	FCS_COP.1 FCS_CKM.4	FCS_CKM.4 satisfied by OE.CRYPTOGRAPHIC_KEY_DESTRUCTION in the IT environment.
FCS_COP.1(A)	No other components	FCS_CKM.1 FCS_CKM.4	
FCS_COP.1(B)	No other components	FCS_CKM.1 FCS_CKM.4	
FCS_COP.1(C)	No other components	FCS_CKM.1 FCS_CKM.4	
FIA_ATD.1	No other components	None	
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	The FIA_UID.1 requirement is a subset of the FIA_UID.2 requirement.
FIA_UAU.7	No other components	FIA_UAU.1	
FIA_UID.2	FIA_UID.1	None	
FMT_MTD.1(A)	No other components	FMT_SMR.1 FMT_SMF.1	
FMT_MTD.1(B)	No other components	FMT_SMR.1 FMT_SMF.1	
FMT_REV.1	No other components	FMT_SMR.1	
FMT_SMF.1	No other components	None	
FMT_SMR.1	No other components	FIA_UID.1	
FPT_TST.1	No other components	None	
FPT_RCV.1	No other components	AGD_OPE.1	See section 6.2

Figure 13 CC Component Hierarchies and Dependencies

6.4 Security Requirements Rationale

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

6.4.1 Security Functional Requirements for the TOE

The following table provides a high level mapping of coverage for each security objective:

SECURITY OBJECTIVES / SECURITY FUNCTIONAL REQUIREMENT	O.AUTHORISATION	O.ACCESS_CONTROL	O.AUDIT	O.ENCRYPTED_MEDIA	O.PROTECT	O.EFFECTIVE_ADMINISTRATION	O.EASE_OF_USE_USER	O.DATA_TRANSFER	O.SECURE_RECOVERY	O.CRYPTOGRAPHIC_KEYS	O.CRYPTOGRAPHIC_OPERATIONS
FDP_DSK(EXT).1				X							
FAU_GEN.1			X								
FAU_GEN.2			X								
FAU_STG.1					X						
FAU_STG.3					X						
FAU_STG.4					X						
FAU_SAR.1			X								
FAU_SAR.3			X								
FCS_CKM.1								X		X	
FCS_COP.1(A)				X							X
FCS_COP.1(B)										X	X
FCS_COP.1(C)								X			X
FIA_ATD.1				X							
FIA_UAU.2	X	X									
FIA_UAU.7	X										
FIA_UID.2	X										

SECURITY OBJECTIVES / SECURITY FUNCTIONAL REQUIREMENT	O.AUTHORISATION	O.ACCESS_CONTROL	O.AUDIT	O.ENCRYPTED_MEDIA	O.PROTECT	O.EFFECTIVE_ADMINISTRATION	O.EASE_OF_USE_USER	O.DATA_TRANSFER	O.SECURE_RECOVERY	O.CRYPTOGRAPHIC_KEYS	O.CRYPTOGRAPHIC_OPERATIONS
FMT_MTD.1(A)						X					
FMT_MTD.1(B)						X	X				
FMT_REV.1						X					
FMT_SMF.1						X	X				
FMT_SMR.1						X	X				
FPT_TST.1					X						
FPT_RCV.1									X		

Figure 14 Matching Security Functional Requirements to Security Objectives

OBJECTIVE	RATIONALE
O.AUTHORISATION	FIA_UAU.2 ensures that the TSF requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. FIA_UID.2 ensures that the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. FIA_UAU.7 helps to protect the Administrator and User credentials during authentication.
O.ACCESS_CONTROL	FIA_UAU.2 requires authentication of a user's identity before any TSF actions on behalf of that user are allowed.
O.ENCRYPTED_MEDIA	FDP_DSK(EXT).1 stipulates automatic full disk encryption. FCS_COP.1(A) specifies AES encryption using 256 bit keys and FIA_ATD.1 specifies the security attributes required for encrypting the media.
O.EFFECTIVE_ADMINISTRATION	FMT_SMR.1 provides two roles: user and administrator. This allows the management functions to be compartmentalized, so that some functions are available to users (such as the ability to change their own password, FMT_MTD.1(B)), while other functions necessary for

OBJECTIVE	RATIONALE
	effective administration of the TOE (FMT_MTD.1(A), FMT_SMF, FMT_REV.1) are restricted to authorized administrators.
O.AUDIT	The audit functionality generates audit records for security relevant actions and associates these with an identified user where possible (FAU_GEN.1, FAU_GEN.2). It presents this information in a comprehensible format to authorized users while preventing access to unauthorized users (FAU_SAR.1, FAU_SAR.3)
O.SECURE_RECOVERY	FPT_RCV.1 provides the ability for a user, with the assistance of an authorized administrator to regain access to his machine in the event of a lost token or forgotten password.
O.PROTECT	FPT_TST.1 provides cryptographic self-tests and component integrity testing to guard against corruption of executable code. The TOE protects the audit trail against possible audit data loss (FAU_STG.1, FAU_STG.3, FAU_STG.4).
O.DATA_TRANSFER	ePO and the TOE Endpoint establish a shared key from independently generated components (FCS_CKM.1) using TLS and use this key and AES-256 encryption to secure the management channel between ePO and the TOE Endpoint (FCS_COP.1(C)).
O.CRYPTOGRAPHIC_KEYS	Cryptographic keys are generated in accordance with an HMAC deterministic RBG (FCS_CKM.1). Secret keys are never transported in plaintext. Symmetric keys such as the System Key and System Recovery Key are encrypted first before being transported (FCS_COP.1(B)).
O.CRYPTOGRAPHIC_OPERATIONS	All of the cryptographic algorithms used by the cryptographic operations (FCS_COP.1(A), FCS_COP.1(B), FCS_COP.1(C)) have been tested and certified by the CAVP.
O.EASE_OF_USE_USER	FMT_SMR.1 provides two roles: user and administrator. This allows the management functions to be compartmentalized, so that only a limited set of functions is available to users (such as the ability to change their own password, FMT_MTD.1(B), FMT_SMF.1). The limited number of management functions available to users does not allow them to configure the TOE in an insecure manner.

Figure 15 Security Functional Requirements Rationale

6.4.2 Security Assurance Requirements

This section identifies the Configuration Management, Delivery/Operation, Development, Test, and Guidance measures applied to satisfy CC assurance requirements.

Assurance Class	Assurance Components	Assurance Measures
ADV: Development	ADV_ARC.1 Security architecture description	McAfee EEPC v6 ADV_ARC.1 Evidence
	ADV_FSP.2 Security-enforcing functional specification	McAfee EEPC v6 ADV_FSP.2 Evidence
	ADV_TDS.1 Basic design	McAfee EEPC v6 ADV_TDS.1 Evidence
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	McAfee Endpoint Encryption - 6.2 (EEPC) Product Guide
	AGD_PRE.1 Preparative procedures	McAfee Endpoint Encryption - 6.2 (EEPC) Product Guide
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system	Mcafee EEPC V6 ALC_CMC.2 And ALC_CMS.2 Evidence
	ALC_CMS.2 Parts of the TOE CM coverage	McAfee EEPC v6 Evidence
	ALC_DEL.1 Delivery procedures	McAfee EEPC v6 Evidence
	ALC_FLR.3 Systematic flaw remediation	McAfee EEPC v6 Evidence
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims	This document, section 2.
	ASE_ECD.1 Extended components definition	This document, section 5
	ASE_INT.1 ST introduction	This document, section 1
	ASE_OBJ.2 Security objectives	This document, section 4
	ASE_REQ.2 Derived security requirements	This document, section 6
	ASE_SPD.1 Security problem definition	This document, section 3
	ASE_TSS.1 TOE summary specification	This document, section 7
ATE: Tests	ATE_COV.1 Evidence of coverage	McAfee EEPC v6 ATE_FUN.1 and ATE_COV.1 Evidence
	ATE_FUN.1 Functional testing	McAfee EEPC v6 ATE_FUN.1 and ATE_COV.1 Evidence
	ATE_IND.2 Independent testing - sample	Evaluation support to replicate developer testing
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	Analysis performed during evaluation

Figure 16 Security Assurance Requirements Evidence

6.4.2.1 Rationale for TOE Assurance Requirements Selection

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

1. Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.
2. The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.
3. Consistent with current best practice for tracking and fixing flaws as well as providing fixes to customers.

The augmentation of ALC_FLR.3 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

7 TOE Summary Specification

The objective for the TOE summary specification is to provide potential consumers of the TOE with a description of how the TOE satisfies all the SFRs. The TOE summary specification provides the general technical mechanisms that the TOE uses for this purpose.

7.1 Installation

The EEPC client software is deployed from the McAfee ePO server and installed through McAfee Agent.

When ePO is installed, the Administrator selects a user name and password that are to be used as logon credentials for the ePO server. Once ePO is installed, there are a number of ePO-specific installation tasks that must be performed before the TOE Endpoint can be deployed.

Summary of installation steps to install TOE Endpoint using ePO:

1. The EEAdmin and EEPC extensions are installed into ePolicy Orchestrator.
2. The EEPC software packages (MfeEEPC.ZIP and MfeEEAgent.ZIP) are checked in to ePolicy Orchestrator.
3. The registered server (Windows Active Directory) is configured.
4. The automation task for LDAP Synchronization is configured and run.
5. The Endpoint Encryption Agent is deployed to the client.
6. The EEPC software package is deployed to the client.
7. When the TOE Endpoint system is restarted it will register with ePO.

8. ePO can then be used to add one or more of the users imported from Active Directory to a system or a group of systems.
9. A product settings policy can then be created or the default policy edited, then assigned to a system or a group of systems.
10. A user-based policy can then be created or the default policy edited, and then assigned to a user or a group of users on a system.

NOTE: The Endpoint Encryption System Status changes from Inactive to Active only after adding the user and enforcing the policies correctly.

11. The Endpoint Encryption System Status can be verified by right-clicking McAfee Agent System Tray on the client system, then clicking Quick Settings… Endpoint Encryption Status.

When the TOE Endpoint deployment is activated on the Endpoint PC, it EEPC creates the Pre-Boot File System (PBFS) in the client system and communicates with the ePolicy Orchestrator server to pull down the assigned Endpoint Encryption policies and encrypts the system as per the defined polices. After the subsequent restart, the Preboot logon screen appears and an assigned user can present his user name and token-based credentials in order to be authenticated.

The summary of the client installation process is depicted in Figure 2.

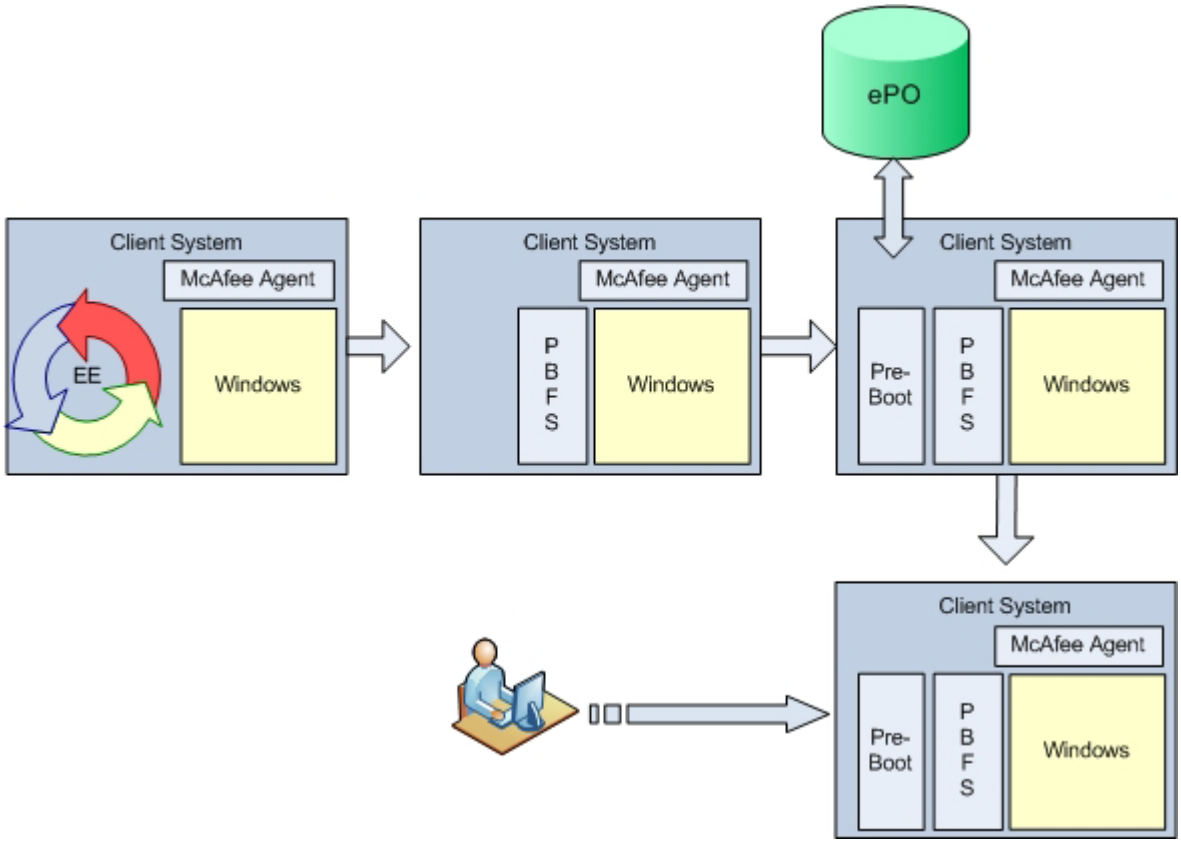


Figure 17 Client installation overview

7.2 Cryptographic Operations

When the TOE Endpoint is activated, it generates a number of cryptographic keys using its key generation algorithm that incorporates an SP 800-90 random bit generator. The TOE Endpoint generates a System key (AES-256) that it uses to encrypt the TOE Data and a System Recovery Key (AES-256) used for administrative recovery.

For uninitialized user accounts, the system key is stored encrypted with a hash of the default password. This is changed as soon as the user logs on for the first time.

In addition, for users that have certificates from Active Directory and an associated smart card containing the matching private key, the TOE Endpoint also generates an RSA key pair (2048 bits) for each system user for which the client has not yet received initialized user token data.

The System Key is only stored persistently in its encrypted form. It is stored in the PBFS encrypted by the User Public Key, one copy for each user. It is also stored wrapped with the System Recovery key. The User Secret Key is stored encrypted in the TOE Endpoint and during the logon process is decrypted by the user's token to enable it to be used to secure the hard disk during normal operation of the TOE Endpoint.

The link between ePO and the TOE Endpoint is secured by McAfee Agent. This uses TLS to establish a shared secret and then uses this as an AES-256 key to encrypt subsequent session-based traffic between the ePO server and the TOE Endpoint.

The System Key and System Recovery Key are encrypted by the Key Server Public Key (a 2048 bit RSA key) and sent to ePO after they are generated where they are stored in the Key Server for archiving purposes. The User Public Key of each system user is also sent to ePO after generation, as is the User Private Key, encrypted by the user's token (password, physical (biometric) token or smartcard).

The Key Server is an ePO component that stores a copy of the System Key from each activated Endpoint. The Key Server data is stored in an SQL Server. The Key Server is only used for out of bound emergency recovery of an Endpoint or the forensic decryption of Endpoint storage

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.

To summarize, the following are the keys used by the TOE:

Key	Purpose
System Key	To encrypt hard disk contents.
User Public Key	To encrypt system key and user attributes. One key pair per user.
User Secret Key	To decrypt system key and user attributes
System Recovery Key	To allow for administrative recovery. One key per module. Used to encrypt the system key on the client machine for recovery.
Challenge Key	Encrypts the system recovery key during the administrative

Key	Purpose
	recovery process. One per system. Client then uses Challenge Key to decrypt this response and so get access to the System Recovery Key
User Certificate Public Key	Certificate-based smart cards. Used to encrypt the system key on the client.
Key Server Public Key	Used to encrypt keys on the client prior to sending them to the key server database (ePO)

Figure 18 TOE Cryptographic Keys

7.3 Identification and Authentication

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

An ePO Administrator must logon successfully before being granted access to the ePO functionality. Authentication is provided in one of three ways, the specific mechanism used is determined when the user account is created. The available authentication types are ePO authentication (ePO user name and password), Windows authentication and certificate based authentication. The ePO administrator logs on to ePO as appropriate to their configured authentication type, by default, 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 smartcards. No access to the encrypted data on the storage media is available is available before the user has been successfully identified and authenticated.

With password-only tokens, the administrator can define and edit user policies with ePO and deploy these to Endpoint systems via policy updates. This allows the administrator to administer ePO connected endpoints. In this way, user accounts can be enabled or disabled, new accounts created, user password policies set (maximum and/or minimum password length and enforced password content defining the number of Alpha, Numeric, Alphanumeric, and Symbols characters required to form a password) or user passwords reset.

For physical tokens, it may be possible to change the token's PIN or biometric properties either locally in the Endpoint Pre-boot environment or using proprietary middleware. They are not managed by ePO.

For all authentication methods, there is obscured feedback, consisting of a '*' for each character typed for all passwords, to protect the authentication data from accidental disclosure during the logon process.

7.4 Audit

The audit log maintains a record of TOE Administrator (ePO user) actions and a set of events relating to the TOE User. These events are defined in FAU_GEN.1 above.

The audit log is accessed from ePO. Administrator actions can be reviewed from the **Menu→User Management→Audit Log**. TOE Endpoint events are generated on the TOE Endpoint and then sent to ePO by the McAfee Agent periodically according to a defined schedule. Such User audit events can be reviewed from **Menu→Reporting→Queries & Reports** and running the **EE: Product Client Events** report.

Each entry of the Administrator audit log is associated with an identified Administrator. With the User audit log, if an action is performed by an identified user, then the audit log entry is associated with that identified user. However, some audit events result from system actions rather than user actions and these are associated with the system that they relate to.

Audit records are only available from ePO and so are only available to Administrators. In order to view the audit logs, an Administrator must have first successfully logon to ePO using his logon credentials.

7.4.1 Administrator Audit Log

Columns that can be included when displaying the audit log are: “User Name”, “Action”, “Details”, “Start Time”, “Priority”, “Success”, “Completion Time”. The columns are displayed in the order defined by the user.

The audit log can only be viewed or cleared by authorized Administrators, and he can choose to view the entries ordered by any of the chosen columns in either ascending or descending order.

If the audit log becomes full, new entries are ignored.

7.4.2 User Audit Log

The columns of the “EE: Product Client Events” report are: “Event Generated (time)”, “Event ID”, “Event Description”, “Event Type”, “Severity”, “User Name”, “Error Code”, “Initiator ID”, “Host Name”.

The User audit log can only be viewed or cleared by authorized Administrators, and he can choose to view the entries ordered by any of the chosen columns in either ascending or descending order.

The User audit log can only hold 1000 entries. When it is full, each new entry added results in the oldest entry in the log becoming overwritten.

7.5 Management

The TOE supports two types of operator. 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 password policy (see section 7.3), 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).

Audit events are periodically uploaded from TOE Endpoints to ePO so that there is a central store of audit data that an administrator can use to aggregate audit data into reports to aid the management of a managed network of Endpoint Encryption for PC client machines. Audit is described in section 7.4.

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

To ensure that the Endpoint remains synchronized with ePO policies, McAfee Agent is used to periodically upload events from the Endpoint to ePO and also to download policy updates from ePO and enforce them on the Endpoint.

7.6 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.

When installed in CC mode as required to meet the requirements of this Security Target, 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 TOE Endpoint performs RSA, AES and SHA-256 known answer tests at startup and also performs an integrity test on the executable code of the TOE cryptographic algorithm components. In addition, the TOE Endpoint continuously monitors the output of the Random Bit Generator to ensure that the mechanism is operating correctly.

An administrator may disable a user account, preventing that user from logging on to a machine within the network of protected TOE Endpoint machines.

By default, and when operating in CC mode, a user account is disabled after ten successive logon failures.

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.

The online recovery mechanism allows an ePO authorized administrator to modify user security attributes to allow a user to recover access to the TOE Endpoint machine. However this mechanism requires synchronization between the ePO Server Database and the TOE Endpoint and Windows needs to be running for this to be possible. Online recovery is not possible from the pre-boot environment.

There are two types of offline recovery: Administrator offline recovery and self recovery. Both types of offline recovery are options that can be enabled or disabled on a user by user and machine by machine basis.

Administrator offline recovery allows a TOE Endpoint user to pass a TOE Endpoint recovery code request to the ePO administrator an independent means of verifying the identity of the TOE Endpoint user is required by the ePO administrator is required, A.NON_TECHNICAL_IDENTITY_VERIFICATION. The ePO administrator can then provide a recovery response code to allow the TOE Endpoint user to regain access to the TOE Endpoint.

Self-recovery allows the user to reset a forgotten password by answering a set of security questions. The full list of security questions is set by the administrator using ePO. (Note: Endpoint Encryption contains a generic set of questions by default that may be used or replaced with a set chosen by the authorized administrator).

A user account may be revoked from ePO by an authorized administrator. This change is deployed to an Endpoint via a policy update and so requires the Endpoint machine to be connected to the ePO server via a network connection. Once the updated policy is enforced, the user with the revoked account will no longer be able to logon to the Endpoint.

The TSF ensures that normal operation continues when the link to ePO is lost, by maintaining a local copy of its policies in the Preboot File System.