Protect what you value.

McAfee, Inc.

McAfee Endpoint Encryption for PC

with McAfee Endpoint Encryption Manager

Common Criteria

Security Target

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

Table of Contents

Table of Figures

References

CC	Common Criteria for Information Technology Security Evaluation, Version 3.1 revision 3, July 2009.
FIPS-PUB 180	Federal Information Processing Standard Publication (FIPS-PUB) 180-1, Secure Hash Standard, 17 April 1995
FIPS-PUB 186	Federal Information Processing Standard Publication (FIPS-PUB) 186-2, Digital Signature Standard (DSS), 5 October 2001
FIPS-PUB 197	Federal Information Processing Standard Publication (FIPS-PUB) 197, Advanced Encryption Standard (AES), 26 November 2001
FIPS-PUB 140	Federal Information Processing Standard Publication (FIPS-PUB) 140-2, Including Change Notices, Security Requirements for Cryptographic Modules, 3 December 2002
McAfee Endpoint Encryption Managers Guide	Device Encryption 5 PC Administrators Guide Version: 2006/09
RFC 2631	Diffie-Hellman Key Agreement Method, June 1999
RFC 2898	PKCS #5: Password-Based Cryptography Specification Version 2.0, September 2000

Glossary

AES	Advanced Encryption Standard
Authorised Administrator	Any entity that is able to establish a secure management session with the TOE
Authorised User	Any entity that has logged on to the TOE Client 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 PC
MBR	Master Boot Record
McAfee Endpoint Encryption Manager	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)
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA-1	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 and external hard drives, memory sticks and floppy disks.

TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TOE Client	The McAfee Endpoint Encryption for PC client deployment
TOE Data	The encrypted contents of the TOE storage media.
TOE Manager	The McAfee Endpoint Encryption Manager
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

1 Security Target Introduction

1.1 Security Target Identification

Security Target Title: McAfee Endpoint Encryption for PC with McAfee Endpoint Encryption Manager Common Criteria Security Target.

Security Target Version: 1.23.

TOE Identification: McAfee Endpoint Encryption for PC version 5.2.6 with McAfee Endpoint Encryption Manager version 5.2.6.

Evaluation Assurance Level (EAL): EAL4+ALC_FLR.3.

Common Criteria Identification: Common Criteria for Information Technology Security Evaluation, Version v3.1, Revision 3, July 2009.

Protection Profile Conformance: None

Keywords: disk encryption, access control, security target, EAL4+, McAfee, Inc., McAfee Endpoint Encryption.

1.2 Security Target Overview

McAfee Endpoint Encryption for PC is a Personal Computer (PC) security system that prevents 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 encryption of storage media to offer effective security for PCs running the Microsoft Windows™ operating system.

Management, deployment and user recovery are handled by a centralised McAfee Endpoint Encryption Manager and communication between the McAfee Endpoint Encryption Client and this administrative server is via TCP/IP using a cryptographically secure proprietary protocol.

1.3 Common Criteria Conformance Claim

The identified TOE conforms to the following specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 3, July 2009.
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, Revision 3, July 2009.
    - Part 3 Conformant
    - Evaluation Assurance Level 4 (EAL4) augmented with ALC_FLR.3.

2 TOE Description

McAfee Endpoint Encryption for PC is a Personal Computer (PC) security system that prevents the data stored on a PC’s storage media (hard drive(s) or external media, including floppy disks, external hard drives, memory sticks, etc., as appropriate) from being read or used by an unauthorized person. In simple terms, the McAfee Endpoint Encryption Client takes control of a user’s storage media away from the operating system. The McAfee Endpoint Encryption Client encrypts data written to 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. The McAfee Endpoint Encryption Manager provides the functionality to securely deploy, configure and manage the McAfee Endpoint Encryption Client.

In this document, the McAfee Endpoint Encryption Client is also known as the TOE Client, and the McAfee Endpoint Encryption Manager is also known as the TOE Manager. If "TOE" is used, this refers to both the TOE Client and TOE Manager.

Communication between the TOE Client and the TOE Manager is via a secure management session.

2.1 Scope and boundaries of the TOE

The components of the TOE are installed on general-purpose computers. The McAfee Endpoint Encryption for PC client and McAfee Endpoint Encryption Manager are installed on two separate PCs connected via a network. The physical boundary of the TOE is/are the software applications themselves and the APIs that they expose.

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

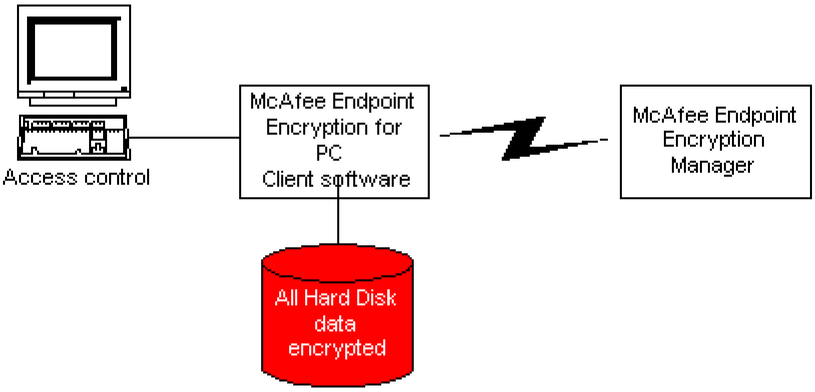
Access control
McAfee Endpoint Encryption for PC Client software
McAfee Endpoint Encryption Manager
All Hard Disk data encrypted

Figure 1 TOE logical boundary

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

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

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

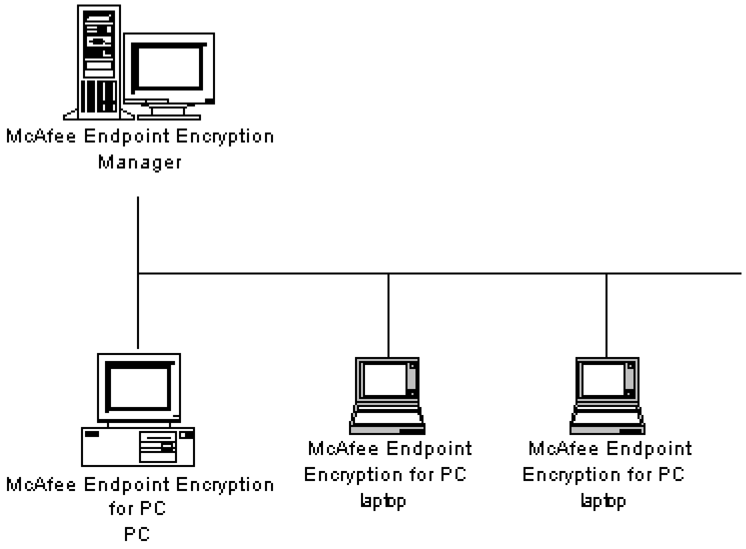
McAfee Endpoint Encryption Manager
McAfee Endpoint Encryption for PC PC
McAfee Endpoint Encryption for PC laptop
McAfee Endpoint Encryption for PC laptop

Figure 2 TOE IT environment

2.2 McAfee Endpoint Encryption for PC Family Functional Overview

McAfee Endpoint Encryption for PC replaces the boot sector of the hard disk to provide effective access control and optionally encrypts part or all of the hard disk drive. The TOE is a collection of software components running on one or more standard PCs.

McAfee Endpoint Encryption for PC supports centralized management of McAfee Endpoint Encryption for PC protected machines. McAfee Endpoint Encryption for PC components include the McAfee Endpoint Encryption Manager (including McAfee Endpoint Encryption Server, McAfee Endpoint Encryption Object Directory and McAfee Endpoint Encryption Connector Manager), and the McAfee Endpoint Encryption Client. Every time a McAfee Endpoint Encryption for PC protected machine boots, and optionally every time the user initiates a connection with the administration server, or after a set period of time, the McAfee Endpoint Encryption Client tries to contact its "Object Directory". This is a central store of configuration information for both machines and users, and is managed by McAfee Endpoint Encryption Managers. The Object Directory could be on the user’s local hard disk (if the user is working completely stand-alone), or could be in some remote location and accessed over Transmission Control Protocol/Internet Protocol (TCP/IP) via a secure McAfee Endpoint Encryption Server (in the case of a centrally managed enterprise).

The McAfee Endpoint Encryption for PC protected machine queries the Object Directory for any updates to its configuration, and if needed downloads and applies them. Typical updates could be a new user assigned to the machine by an administrator, a change in password policy, or a new file specified by the administrator. At the same time the McAfee Endpoint Encryption Client uploads details like the latest audit information, any user password changes, and security breaches to the Object Directory. In this way, transparent synchronization of the enterprise becomes possible.

The TOE Client is the McAfee Endpoint Encryption for PC Client software, as deployed from the TOE Manager as an “installation set”.

The TOE Manager is made up of the following items:

- McAfee Endpoint Encryption Manager (Administrator GUI application)
- McAfee Endpoint Encryption Server (Database server handling connections to the configuration database)
- McAfee Endpoint Encryption Object Directory (The configuration database, a proprietary database wholly contained within the TOE Manager)
- McAfee Endpoint Encryption Connector Manager (An application to allow users of third party products such as Microsoft Active Directory to be imported into the TOE).

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

CC mode is defined as:

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

In order to provide a TOE that is CC mode compliant, the TOE must be configured appropriately. This requires the McAfee Endpoint Encryption Manager to be used in a "CC mode" to deliver a CC-compliant TOE. Details of the method of use to achieve this are provided in the McAfee Endpoint Encryption Managers Guide.

2.3 McAfee Endpoint Encryption Client

The McAfee Endpoint Encryption Client consists of a boot Operating System (OS) (the McAfee Endpoint Encryption Client OS), a Basic Input Output System (BIOS) hook, Windows drivers, a system tray application and a set of Windows Dynamic Link Libraries (DLLs). McAfee Endpoint Encryption for PC installs a mini-operating system on the user's hard drive, this is what the user sees when they switch on the TOE Client. McAfee Endpoint Encryption for PC looks and feels like Microsoft Windows, with mouse and keyboard support, moveable windows etc. The McAfee Endpoint Encryption Client OS is completely self-contained and does not need to access any other files or programs on the hard disk(s), and is responsible for allowing the user to authenticate.

Once the user has entered the correct authentication information, the McAfee Endpoint Encryption Client operating system starts a driver in memory and boots the protected machine's original operating system. From this point on the machine will look and behave as if McAfee Endpoint Encryption for PC was not installed.

2.4 Token-based access control

The TOE supports several different types of token to provide identity based authentication for users, both for the TOE Client and TOE Manager.

Within the scope of the TOE are the password-only token and the CAC and PIV tokens.

With the password-only token, a password is used to identify the user with the user name provided during login. The password is used to decrypt the token key. The Token key structure includes a check value. If this check value matches the expected value, then the identity of the user is verified.

The CAC and PIV smartcards are PKI tokens. User identity is verified again via a user name and a password. The token is password protected. Following successful logon to the token, the certificate on the token is used to decrypt an encrypted user key, which is then used to decrypt the machine key. Each user is assigned a unique user name. Possession of the physical token, the ability to login to it using a secret password and then to decrypt the user key matching the user name of the user provides identity based authentication of that user.

The McAfee Endpoint Encryption Connector Manager allows security information to be synchronised between McAfee Endpoint Encryption and other systems, such as Microsoft Active Directory. It enables data from PKI infrastructures to propagate to the McAfee Endpoint Encryption Management Database.

Using this mechanism, it is possible to replicate details such as user identities and associated tokens (including CAC and PIV) from such third party systems.

The CAC and PIV physical tokens and Microsoft Active Directory are required to be in the IT environment of the TOE in order to provide the token-based access control functionality of the TOE.

The removal of the CAC and PIV tokens lock the TOE Client versions running the Windows XP operating system but not later Microsoft OS versions.

2.5 TOE Interfaces

2.5.1 TOE Client Interfaces

McAfee Endpoint Encryption for PC provides a logical interface via an Application Programming Interface (API) and a Graphical User Interface (GUI). This logical interface exposes services (described in section 2.8) that the User, the operating system and McAfee Endpoint Encryption Client applications may utilize directly.

The logical interfaces provided by the McAfee Endpoint Encryption Client are: data input, data output, control input, and status output as follows:

- Data Input – Input to all driver functions
- Data Output – Output from all driver functions
- Control Input – Input from TCP/IP interface, IPC interface, GUI
- Status Output – Return codes from driver functions, Show Status GUI option

The Data Input and Data Output interfaces are the interfaces through which data is encrypted with the chosen algorithm (more information found in section 2.10) prior to being written to a disk and encrypted data is decrypted when read from a disk.

The Control Input interface is the means by which the client is configured. This is the secure management interface between the TOE components. All configuration information is applied via synchronization operations with the associated Object Directory. Synchronization can be initiated by several means, including: TCP/IP connections to/from the management software, IPC (inter-process communications) functions and GUI options on the system tray application.

The Status Output interface consists of text information displayed in a dialog box when the “Show Status” option is selected on the system tray application menu.

2.5.2 TOE Manager Interfaces

The TOE Manager is a tool used to configure the TOE Client. An Administrator can add, modify and delete security attributes via a Graphical User Interface (GUI). This logical interface exposes the services (described in section 2.8) that the Administrator may use.

The logical interfaces provided by the McAfee Endpoint Encryption Client are: data input, data output, control input, and status output as follows:

- Data Input – GUI
- Data Output – GUI
- Control Input – Input from TCP/IP interface, IPC interface, GUI
- Status Output –GUI

The Data Input and Data Output interfaces are the interfaces through which configuration data is written to and read from the TOE Manager.

The Control Input interface is the means by which the client configuration is deployed to the TOE Client. This is the secure management interface between the TOE components. All configuration information is applied via synchronization operations. Synchronization can be initiated by several means, including: TCP/IP connections to/from the management software, IPC (inter-process communications) functions and GUI options for machine control.

The Status Output interface is synonymous with the Data Output interface for the TOE Manager.

2.6 TOE Client Operational Environment

The TOE Client runs on a standard IBM-compatible personal computer running a variant of the Windows operating system (the TOE is being evaluated on the Windows XP Professional (32-bit) with Service Pack 3, Windows Vista (32-bit and 64-bit) with Service Pack 1 and Windows 7 (32-bit and 64-bit) with no Service Pack.

The TOE Client runs in its own operating system threads. This provides it with protection from all other processes, preventing access to all keys, intermediate key generation values and other CSPs.

The task scheduler and architecture of the operating system maintain the integrity of the TOE.

The TOE Client is protected using token-based access control. The driver files are themselves encrypted on the storage media of the PC. So, any attacker would either need to possess the appropriate password, or would need to be able to decrypt the storage media to gain access to the executable code of the TOE Client. The source code is not included as part of the TOE Client, and the keys and CSPs are not stored in a plaintext form on the TOE Client.

There is no upper limit to the number of Users of the TOE Client, although only one operator can have access to the PC that contains the TOE Client at a time.

2.7 TOE Manager Operational Environment

The TOE Manager runs on a standard IBM-compatible personal computer and running a server variant of the Windows operating system. Specifically for this evaluation any of the 64-bit variants of Windows Server 2008 with Service Pack 1 and any variant of Windows Server 2003 with Service Pack 2.

The TOE Manager runs in its own operating system threads. This provides it with protection from all other processes, preventing access to all keys, intermediate key generation values and other CSPs.

The task scheduler and architecture of the operating system maintain the integrity of the TOE.

The TOE Manager is protected using token-based access control. The source code is not included as part of the TOE Manager, and the keys and CSPs are not stored in a plaintext form on the TOE Manager.

There is no upper limit to the number of Administrators of the TOE Manager, although only one operator can have access to the PC that contains the TOE Manager at a time.

2.8 Roles and Services

The TOE implements two roles: an Administrator role and a User role.

The following table, Figure 3, summarizes the services available to each role.

Role	Purpose	Services
Administrator	TOE Client configuration	- Connect to TOE Client using the TOE Manager, via an encrypted session to transmit control data
User	Usage of TOE Client functionality	- Utilize storage media encryption services - Initiate synchronization with management software - View status

Figure 3 Roles

The User role is assumed when a McAfee Endpoint Encryption for PC protected machine is booted and proper username and password is entered into the login prompt displayed by the boot McAfee Endpoint Encryption Client OS. Once authenticated, user specific information and key material are loaded from the PBFS (McAfee Endpoint Encryption Preboot File System) and the original operating system (with McAfee Endpoint Encryption for PC drivers installed) is launched. The necessary key material and machine state information is loaded into the drivers and the transparent encryption/decryption of disk-based information begins. A system tray application, which may be configured to start automatically, may be used to view the status of the TOE Client or to initiate a synchronization operation.

The Administrator role may be assumed by establishing an authenticated encrypted session with the TOE Client for purposes of configuring this TOE Client component. The user interface is provided by the McAfee Endpoint Encryption Manager. All communications between the management software and the client are encrypted using AES (with a session key generated using Diffie-Hellman key agreement). DSA is also used during the Diffie-Hellman key agreement to authenticate the server to prevent server spoofing.

Figure 4 summarizes the authentication mechanism for each of these roles, and Figure 5 describes the strength of these mechanisms.

Role	Type of Authentication	Authentication Data
User	Identity-based	Password (and possession of token.)
Administrator	Identity-based	Password (and possession of token.) DSS authenticated challenge-response mechanism to connect authenticated Administrator to module

Figure 4 Roles and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism
Password	It is possible to configure the minimum password length and the type of characters that can be used in a password. It is also possible to configure the client to lock up after a specified number of unsuccessful password entry attempts. McAfee, Inc. recommends a minimum password length of five characters, giving a random chance of success of 1 in 2.18 x 10^{14} (using a password made up of only lower case letters, upper case letters and numbers). The software is configured to lock up after 10 unsuccessful attempts; this gives a chance of successfully guessing the password at 1 in 2.18 x 10^{15}.
DSS authenticated challenge-response mechanism	Given that the key size is 1024 bits, that amounts to 2^{1024} (approximately 1.8 x 10^{308} possible keys).

Figure 5 Strength of Authentication Mechanisms

2.9 Access to Services

The following table, Figure 6, lists the authorized services linked to each of the Roles offered by the TOE. For an explanation of the various services listed, the reader should consult the McAfee Endpoint Encryption Managers Guide.

Role	Authorized Services
User (via TOE Client UI)	Synchronization
	Encryption/Decryption
	Show Status Functions
	TOE Client Self-test Functions
	Change User Password
	Activate the secure screensaver
Administrator (via TOE Manager UI driving the TOE management interface)	Synchronization
	Show Status Functions
	User/machine recovery requests
	Configuration
	File Updates
	Manage McAfee Endpoint Encryption for PC (Cryptographic & Key Management Functions)
	Software Updates
	User/machine recovery
	Set User Attributes (passwords, access rights, etc.)
	Change User Attributes
	Create User Groups
	Modify User Groups
	Delete User Groups
	Create Users
	Modify Users
	Delete Users
	TOE Manager Self-test Functions
	Lock workstation
	Reboot workstation

Figure 6 Services Authorized for Roles

2.10 Cryptographic Key Management

The TOE uses a variety of keys, including: hard disk encryption key, user encryption keys, session keys, recovery keys, database key (TOE Manager only), integrity check keys and server public key. The following table, Figure 7, lists all keys. Currently, AES is the only approved encryption algorithm in the McAfee Endpoint Encryption Client product and all encryption keys are AES keys. The server public key is a DSA key.

Key type	Purpose
Hard disk encryption key	To encrypt storage media contents; to authenticate client to the Object Directory; to encrypt database key (when local Object Directory is used)
Token key	To encrypt the token data, which contains the user key
User encryption keys	To encrypt secure user attributes
Server public key	To authenticate the Administrator communications
Machine recovery key	Encryption key used to recover the hard disk encryption key
User recovery keys	To recover user encryption keys
Database key	Used by the TOE Manager to protect certain attributes
Integrity check key	Used to perform TOE integrity check
Session keys	To encrypt traffic between client and remote server
Diffie-Hellman Keys	Used to establish session keys

Key type	Purpose
SHA-1 Known Answer Test (KAT) parameters	A fixed set of parameters used to validate the SHA-1 functionality during the SHA-1 known answer test performed at power-up
DSA Test KAT parameters	A fixed set of parameters used to validate the DSA functionality during the DSA known answer test performed at power-up
AES KAT data	Test data is taken from NIST Special Publication 800-38A 2001 Edition "Recommendations for Block Cipher Modes of Operation" This uses fixed parameters to generate cipher text and plain text which is then verified against expected values
PRNG seed values and seed keys	These are used to prevent the output from the PRNG from being predictable to an attacker. Knowledge of the seed values and seed keys is required to predict key values.
PRNG KAT data	Used to test the pseudo-random number generator to verify that it is operating correctly

Figure 7 Keys used by McAfee Endpoint Encryption Client

2.10.1 Key generation

Both the McAfee Endpoint Encryption Client and Manager generate symmetric key material (and the Diffie-Hellman public/private key pair used in session key establishment,) using a FIPS 186-2 Appendix 3.1 compliant pseudo-random number generator. The TOE Client generates the Hard Disk Encryption Key, the Machine Recovery Key and Session Keys, while the TOE Manager generates the Database Key, User Keys, User Recovery Keys and Session Keys.

2.10.2 Key entry and output

The TOE does not export any key material or pass any secret keys in plaintext from one TOE subject to another.

The Diffie-Hellman public key is passed between TOE subjects in plaintext, all other keys that may be passed from one TOE subject to another are passed in encrypted form.

The Machine key and Machine recovery key are generated by the TOE Client during the installation process. The User keys are generated by the TOE Manager.

The only key that is passed from one TOE subject to another manually is the recovery key, when it is required to recover a user or machine at the TOE client. A human administrator will pass this key from the TOE Manager to the human user of the TOE Client in response to a challenge from the TOE Client. The recovery key is encrypted and is entered manually by the TOE Client user. An offline authentication mechanism is required by the Administrator to verify the identity of the user."

2.10.3 Key storage

Key material is stored in the McAfee Endpoint Encryption File System (SBFS). All key material is encrypted using AES prior to storage. All sectors of the SBFS feature a checksum to guard against modification.

2.10.4 Protection of key material

Both the McAfee Endpoint Encryption Client and Manager securely manages key material for the lifetime of the key. All key material is encrypted with AES prior to storage in the SBFS and prior to export.

2.10.5 Zeroization of key material

All key material mentioned in Figure 7 above (the complete list of unprotected critical security parameters - CSPs), associated with a machine is zeroized when the McAfee Endpoint Encryption Client is uninstalled. All user encryption key material associated with users is zeroized when the user is deleted. All keys stored in the McAfee Endpoint Encryption Manager are stored in Operating System files and are deleted when they are no longer required.

2.11 Cryptographic Algorithms

The McAfee Endpoint Encryption Client supports the following algorithms:

- AES,
- DSA
- SHA-1.
- Diffie-Hellman

2.12 Self-Tests

Both the McAfee Endpoint Encryption Client and Manager implement power-up and conditional self tests. That is, both components perform their own self-tests. The following two sections outline the tests that are performed.

2.13 Power-up self-tests

The following table, Figure 8, lists the power-up self-tests performed by each of the TOE components:

SHA-1 known answer test
DSA known answer test
AES known answer test
Critical Functions (Configuration file signature verification test)
Software/Firmware integrity test (Signature verification)
Pseudo-Random Number Generator Known Answer Test

Figure 8 Power-up self-tests

Each of these tests is executed when the computer is turned on and the TOE component first executes. If any of these tests fail, the TOE component will not load. The TOE component must be reset to re-execute these tests.

2.13.1 Conditional self-tests

There are three conditional tests that are run by the TOE component. A continuous random number generator test is run every time the TOE requests a random number. Failure of this test may result in keys not being generated and an appropriate error message will be given. A test is also done when a software update occurs. All files are digitally signed and this signature is checked prior to any update of the software. There is also a manual key entry test that verifies correct entry of the user recovery keys and machine recovery key. More information on this test can be found in the Administrator’s Guide.

3 TOE Security Environment

3.1 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 utilised in a manner that adheres to the intended environment, and method of delivery, installation and administration.

3.1.1 Personnel Assumptions

This section describes the assumptions about how the staff that are authorised 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
Authorised 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 authorised users of the TOE.

3.1.2 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.SECURE_BACKUP
User’s data backups are separately encrypted or physically protected to ensure data security is not compromised through theft of or unauthorised 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.

3.1.3 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 authorised 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.

3.2 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 fulfil these objectives.

T.ACCESS
An unauthorised 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 unauthorised access to the assets protected by the TOE.

T.ALTERNATE_BOOT_PROCESS
An unauthorised 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 unauthorised users.

T. CORRUPT_AUDIT
Unauthorised users may modify audit data by gaining unauthorised 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 unauthorised user may listen in on communications (electronic or otherwise) between the TOE components, and so gain unauthorised access to information.

T.OBJECT_REUSE
Using expired authentication data, users may gain unauthorised access to information.

T.PASSWORD_LOSS
The user may forget their password, making data unavailable.

T.RECORD_ACTIONS
An unauthorised user may perform unauthorised actions that go undetected.

T.RECOVERY_PROCEDURE_INTERCEPT
An unauthorised user may eavesdrop on telephone communications between user of the TOE and the help desk when a user is performing the recovery procedure, and so gain unauthorised access to information.

T.RECOVERY_MASQUERADE
An unauthorised 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 unauthorised 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.SPOOF
A hostile entity may impersonate the TOE in order to gain unauthorised access to authentication data, such as by presenting a look-alike logon screen and asking for the user's password.

T.SYSTEM_ACCESS
An unauthorised user may gain unauthorised access to the system and act as an administrator or other authorised user.

T.UNAUTHORISED_MODIFICATION

An unauthorised user may modify the TOE software (executable code), and so gain unauthorised access to system and user resources.

3.3 Organisational Security Policies

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

P.AUTHORISED_USERS
Only authorised 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.FAULT_TOLERANCE
Access control functions must be able to continue to operate if systems lose communications with central McAfee Endpoint Encryption Managers.

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

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 organisational security policies and assumptions.

4.1 Objectives for the TOE

O.AUTHORISATION
The TSF must ensure that only authorised 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 user identity. The TSF must provide the ability to limit each user’s access.

O.ENCRYPTED_MEDIA
The TSF must provide encryption to protect designated information assets from unauthorised users that have gained physical access to the TOE’s storage media.

O.EFFECTIVE_ADMINISTRATION
The TOE must allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorised 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 authorised users while preventing access to unauthorised 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.TRUSTED_PATH
The TSF must provide the capability to allow users to ensure that they are communicating with the TOE during initial authentication and not with another entity impersonating the TOE.

O.DATA_TRANSFER
The TSF must have the capability to protect system data in transmission between any McAfee Endpoint Encryption Manager and the McAfee Endpoint Encryption for PC component.

O.CRYPTOGRAPHIC_KEYS
The TSF must ensure that cryptographic keys are generated, accessed, protected, and destroyed 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.FAULT_TOLERANCE
The TSF must continue to enforce access control policies if communications are lost with the central McAfee Endpoint Encryption Manager.

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.

O.NO_OBJECT_REUSE
The TSF must prevent users gaining unauthorised access to information using expired authentication data.

4.2 Objectives for the 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.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 unauthorised 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 unauthorised 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 authorised 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.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

This section defines the functional requirements for the TOE in terms of functional components drawn from Part 2 of the Common Criteria. Text contained within square brackets “[]” occurs where selection or assignment operations have been performed within the component.

Note regarding terminology used in assignment operations: For the purposes of this document, an **authorised administrator** is any entity that is able to establish a secure management session with the TOE, and an **(authorised) user** is any entity that is logged on to the TOE Client through the logon GUI.

A McAfee Endpoint Encryption Manager allows an authorised administrator to establish a secure session with the TOE Client. The existence of this secure session exposes a configuration and control interface to the TOE Client and the McAfee Endpoint Encryption Manager provides a GUI to enable the authorised administrator to make use of this interface. So, when the phrase “authorised administrator” is used with respect to the TOE it refers to an authenticated user of a TOE Manager.

The TOE is comprised of two distinct components, The McAfee Endpoint Encryption Manager (TOE Manager) and the McAfee Endpoint Encryption for PC client (TOE Client). For the purpose of clarity, the Security Functional Requirements for each of these components is listed here separately.

Where assignments or selections have been made in the SFR, this is indicated by the operator **assignment** or **selection** as appropriate.

Where more than one instance of an SFR is used, an alphabetic suffix is appended to indicate this iteration. For example, for the two iterations of FAU_GEN.1, the first is referred to as FAU_GEN.1(a) and the second as FAU_GEN.1(b).

Where a refinement is made to an SFR, this is indicated by the operator **refinement**.

5.1.1 TOE Client Security Functional Requirements

Functional Class	Functional Components
FAU: Security Audit	FAU_GEN.1(a) Audit data generation (TOE Client)
	FAU_GEN.2(a) User identity association (TOE Client)
	FAU_STG.1(a) Protected audit trail storage (TOE Client)
	FAU_STG.3(a) Action in case of possible audit data loss (TOE Client)
FCS: Cryptographic Support	FCS_CKM.1(a) Cryptographic key generation (symmetric)
	FCS_CKM.1(b) Cryptographic key generation (asymmetric)
	FCS_CKM.4 Cryptographic key destruction
	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)
FDP: User data protection	FDP_ACC.2(a) Complete access control (user)
	FDP_ACF.1(a) Security attribute based access control (user)
FIA: Identification and authentication	FIA_AFL.1 Authentication failure handling (user logon)
	FIA_ATD.1 User attribute definition
	FIA_UAU.2(a) User authentication before any action (Client)
	FIA_UAU.4(a) Single-use authentication mechanisms (secure management)
	FIA_UAU.7(a) Protected authentication feedback (Client)
	FIA_UID.2(a) User identification before any action (Client)
FMT: Security Management	FMT_MSA.1(a) Management of security attributes (secure management)
	FMT_MTD.1(a) Management of TSF data (audit)
	FMT_MTD.1(b) Management of TSF data (password)
	FMT_MTD.2(a) Management of limits on TSF data (authentication failure)
	FMT_REV.1(a) Revocation
	FMT_SMF.1 Specification of Management Functions
	FMT_SAE.1(a) Time-limited authorisation (secure management)
	FMT_SMR.1(a) Security roles
FPT: Protection of the TSF	FPT_TST.1 TSF testing
	FPT_FLS.1 Failure with preservation of secure state
	FPT_RCV.1 Manual recovery
FRU: Resource utilisation	FRU_FLT.1 Degraded fault tolerance
FTA: TOE access	FTA_SSL.2 User-initiated locking
	FTA_TSE.1 TOE session establishment
FTP: Trusted path/channels	FTP_TRP.1 Trusted path

Figure 9 Functional components of the TOE Client

5.1.1.1 FAU: Security Audit

FAU_GEN.1(a) Audit data generation (TOE Client)

FAU_GEN.1.1(a) 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 [**selection:** not specified] level of audit; and
c) [**assignment:** All try events, resulting from:
   - Expiry and timeouts
d) All success events, such as
   - Changes to passwords

- Logon
- Recovery

e) All failure events.

- Password change failures
- Logon failures
- Recovery failures]

FAU_GEN.1.2(a) 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, [**assignment:** no other relevant information]

Note: Auditing is always active in the TOE Client. 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 Client is operational, its audit functions are also operational.

FAU_GEN.2(a) User identity association (TOE Client)

FAU_GEN.2.1(a) 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(a) Protected audit trail storage (TOE Client)

FAU_STG.1.1(a) The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2(a) The TSF shall be able to [**selection:** prevent] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.3(a) Action in case of possible audit data loss (TOE Client)

FAU_STG.3.1(a) The TSF shall take [**assignment:** the action of overwriting the oldest audit records first] if the audit trail exceeds [**assignment:** 3000 items].

5.1.1.2 FCS: Cryptographic Support

The cryptographic algorithms used by the TOE were tested and approved by CAVP. As a result, the TOE contains a number of FIPS-approved algorithms: DSA (CAVP certificate #446), AES (certificates #1366, #893), RNG (certificates #752, #514) and SHA-1 (certificates #1247).

The TOE generates symmetric keys to use to encrypt the storage media and asymmetric keys to secure the TOE management protocol and in the process of doing so also generates symmetric key to encrypt these protocol messages once a secure management session has been established.

FCS_CKM.1(a) Cryptographic key generation (symmetric)

FCS_CKM.1.1(a) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**assignment:** DSA Random number generation] and specified cryptographic key sizes [**assignment:** 256 bits] that meet the following: [**assignment:** FIPS 186-2, Appendix 3.1].

FCS_CKM.1(b) Cryptographic key generation (asymmetric)

FCS_CKM.1.1(b) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**assignment:** Diffie-Hellman key exchange algorithm] and specified cryptographic key sizes [**assignment:** 1024 bits] that meet the following: [**assignment:** RFC 2631].

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**assignment:** zeroing] that meets the following: [**assignment:** FIPS 140-2, Section 4.7.6 Key Destruction].

FCS_COP.1(a) Cryptographic operation (data encryption and decryption)
The TOE Client uses AES for disk encryption

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

FCS_COP.1(b) Cryptographic operation (key encryption and decryption)

FCS_COP.1.1(b) The TSF shall perform [**assignment:** key encryption and decryption] in accordance with a specified cryptographic algorithm [**assignment:** AES] and cryptographic key sizes [**assignment:** 256 bits] that meet the following: [**assignment:** FIPS 197].

FCS_COP.1(c) Cryptographic operation (authenticated administration)

FCS_COP.1.1(c) The TSF shall perform [**assignment:** encrypted and authenticated session based communication with a McAfee Endpoint Encryption Manager] in accordance with a specified cryptographic algorithm [**assignment:** AES for encryption and DSA and SHA-1 for authentication] and cryptographic key sizes [**assignment:** 256 bits for AES and 1024 bits for DSA] that meet the following: [**assignment:** FIPS 197 for AES and FIPS 186-2 for DSA and SHA-1].

5.1.1.3 FDP: User data protection

FDP_ACC.2(a) Complete access control (user)

FDP_ACC.2.1(a) The TSF shall enforce the [**assignment:** machine access control SFP] on [**assignment:** all users and the TOE data] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2(a) The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1(a) Security attribute based access control (user)

FDP_ACF.1.1(a) The TSF shall enforce the [**assignment:** machine access control SFP] to objects based on the following: [**assignment:** user identity as defined in the McAfee Endpoint Encryption for PC Object Directory and each user's associated login credentials and keys].

FDP_ACF.1.2(a) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**assignment:** If a user identity has been verified via authentication of the user identity using a supplied token and login credentials, the derived keys will be used to give the user access to the assets protected by the TSF. Authentication failure will result in the user failing to gain access to the TSF assets].

FDP_ACF.1.3(a) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**assignment:** none].

FDP_ACF.1.4(a) The TSF shall explicitly deny access of subjects to objects based on the [**assignment:** none].

5.1.1.4 FIA: Identification and authentication

FIA_AFL.1 Authentication failure handling (user logon)

FIA_AFL.1.1 The TSF shall detect when [**selection: assignment:** "an administrator configurable positive integer within the range 1 to 20"] unsuccessful authentication attempts occur related to [**assignment:** user logon].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [**selection:** met or surpassed], the TSF shall [**assignment:** disable the user account].

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**assignment:**

a) User Identitifier
b) Password policy
c) Token properties
d) Hard disk encryption key
e) User encryption keys
f) User Group membership].

FIA_UAU.2(a) User authentication before any action (Client)

FIA_UAU.2.1(a) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4(a) Single-use authentication mechanisms (secure management)

FIA_UAU.4.1(a) The TSF shall prevent reuse of authentication data related to [**assignment:** the secure management mechanism and the offline recovery mechanism].

FIA_UAU.7(a) Protected authentication feedback (Client)

FIA_UAU.7.1(a) The TSF shall provide only [**assignment:** feedback consisting of a '*' for each character typed for all passwords and no feedback in the case of the secure management mechanism] to the user while the authentication is in progress.

FIA_UID.2(a) User identification before any action (Client)

FIA_UID.2.1(a) The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.1.5 FMT: Security Management

The SFRs in this section refer to the TOE secure management interface. This is the interface that electronically connects the TOE Manager to the TOE Client component using the secure management protocol.

FMT_MSA.1(a) Management of security attributes (secure management)

FMT_MSA.1.1(a) The TSF shall enforce the [**assignment:** machine access control SFP] to restrict the ability to [**selection:** assign, change_default, query, modify, delete] the security attributes [**assignment:** all McAfee Endpoint Encryption for PC Machine properties and User properties as defined in section 9] to [**assignment:** authorised administrators].

FMT_MSA.2(a) Secure security attributes (secure management)

FMT_MSA.2.1(a) The TSF shall ensure that only secure values are accepted for [**assignment:** the security attributes defined in section 9].

FMT_MSA.3(a) Static attribute initialisation (secure management)

FMT_MSA.3.1(a) The TSF shall enforce the [**assignment:** machine access control SFP] to provide [**selection:** restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(a) The TSF shall allow the [**assignment:** authorised administrators] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1(a) Management of TSF data (audit)

FMT_MTD.1.1(a) The TSF shall restrict the ability to [**selection:** query orclear] the [**assignment:** TSF audit data] to [**assignment:** authorised administrators].

FMT_MTD.1(b) Management of TSF data (password)

FMT_MTD.1.1(b) The TSF shall restrict the ability to [**selection:** modify] the [**assignment:** a user's password] to [**assignment:** authorised administrators and a user may modify his own password if he successfully supplies his existing password first].

FMT_MTD.2(a) Management of limits on TSF data (authentication failure)

FMT_MTD.2.1(a) The TSF shall restrict the specification of the limits for [**assignment:** successive logon authentication failures] to [**assignment:** authorised administrators].

FMT_MTD.2.2(a) The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [**assignment:** disable the user account until enabled again by an authorised administrator (as specified by an authorised administrator)].

FMT_REV.1(a) Revocation (secure management)

FMT_REV.1.1(a) The TSF shall restrict the ability to revoke [**assignment:** user accounts] associated with the [**selection:** users] under the control of the TSF to [**assignment:** authorised administrators].

FMT_REV.1.2(a) The TSF shall enforce the rules [**assignment:** Revocation can either take place the next time the user logs on, or the user can be revoked immediately, with their machine rebooted and their account disabled or deleted, as specified by the administrator].

FMT_SAE.1(a) Time-limited authorisation (secure management)

FMT_SAE.1.1(a) The TSF shall restrict the capability to specify an expiration time for [**assignment:** user passwords] to [**assignment:** authorised administrators].

FMT_SAE.1.2(a) For each of these security attributes, the TSF shall be able to [**assignment:** give the user a warning that the password is about to expire a specified time before expiry, but also prevent the user from logging on until he has changed the password] after the expiration time for the indicated security attribute has passed.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [**assignment:** User: Changing password of current user. Administrator: Modification of security attributes listed in section 9.]

FMT_SMR.1(a) Security roles (TSF)

FMT_SMR.1.1(a) The TSF shall maintain the roles [**assignment:** Administrator, User].

FMT_SMR.1.2(a) The TSF shall be able to associate users with roles.

5.1.1.6 FPT: Protection of the TSF

FPT_TST.1 TSF testing

FPT_ TST.1.1 The TSF shall run a suite of self-tests [**selection:** during initial start-up, and in the case of the random number generator test, continuously] to demonstrate the correct operation of the [**assignment:** security assumptions provided by the abstract machine that underlies the TSF].

FPT_ TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [**assignment:** the TSF encryption algorithms, specifically AES-256, SHA-1 and DSA, and the random number generator]

FPT_ TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored executable code.

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [**assignment:** unexpected termination of communications with McAfee Endpoint Encryption Manager or power failure to TOE PC].

FPT_RCV.1 Manual recovery

FPT_RCV.1.1 After [**assignment:** 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.

5.1.1.7 FRU: Resource utilisation

FRU_FLT.1 Degraded fault tolerance

FRU_FLT.1.1 The TSF shall ensure the operation of [**assignment:** uninterrupted user access to the TOE Client if this is allowed within the user configuration] when the following failures occur: [**assignment:** the link to the McAfee Endpoint Encryption Manager is lost].

5.1.1.8 FTA: TOE access

FTA_SSL.2 User-initiated locking

FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user’s own interactive session, by

a) Clearing or overwriting display devices, making the current contents unreadable;
b) Disabling any activity of the user’s data access/display devices other than unlocking the session.

FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: [**assignment:** a user to be successfully authenticated via a logon screen by presenting his user identity and password for authentication].

FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [**assignment:** user status. A user whose account is disabled will not be permitted to establish a session].

5.1.1.9 FTP: Trusted path/channels

FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [**selection:** local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [**assignment:** modification or disclosure].

FTP_TRP.1.2 The TSF shall permit [**selection:** local users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [**selection:** initial user authentication].

5.1.2 McAfee Endpoint Encryption Manager

For the purposes of this document, the McAfee Endpoint Encryption Manager is a required component of the TOE and is required to effectively realise the administrator role of the TOE.

The SFRs of the McAfee Endpoint Encryption Manager satisfy the objective O.EFFECTIVE_ADMINISTRATION.

Functional Class	Functional Components
FAU: Security Audit	FAU_GEN.1(b) Audit data generation (McAfee Endpoint Encryption Manager)
	FAU_GEN.2(b) User identity association (McAfee Endpoint Encryption Manager)
	FAU_STG.1(b) Protected audit trail storage (McAfee Endpoint Encryption Manager)
	FAU_STG.3(b) Action in case of possible audit data loss (McAfee Endpoint Encryption Manager)
	FAU_SAR.1 Audit review
	FAU_SAR.3 Selectable audit review
FDP: User data protection	FDP_ACC.2(b) Complete access control (Admin user)
	FDP_ACF.1(b) Security attribute based access control (Admin user)
FCS: Cryptographic Support	FCS_COP.1(d) Cryptographic operation (McAfee Endpoint Encryption Manager)
FIA: Identification and authentication	FIA_UAU.4(b) Single-use authentication mechanisms (McAfee Endpoint Encryption Manager)
	FIA_UAU.2(b) User authentication before any action (Manager)
	FIA_UAU.7(b) Protected authentication feedback (Manager)
	FIA_UID.2(b) User identification before any action (Manager)
FMT: Security Management	FMT_MSA.1(b) Management of security attributes (McAfee Endpoint Encryption Manager)
	FMT_MSA.2(b) Secure security attributes (McAfee Endpoint Encryption Manager)
	FMT_MSA.3(b) Static attribute initialisation (McAfee Endpoint Encryption Manager)
	FMT_MTD.1(e) Management of TSF data (audit)
	FMT_REV.1(b) Revocation (McAfee Endpoint Encryption Manager)
	FMT_SAE.1(b) Time-limited authorisation (McAfee Endpoint Encryption Manager)
	FMT_SMR.1(b) Security roles (McAfee Endpoint Encryption Manager)

Figure 10 Functional components of the TOE Manager

5.1.2.1 FAU: Security Audit

FAU_GEN.1(b) Audit data generation (McAfee Endpoint Encryption Manager)

FAU_GEN.1.1(b) 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 [**selection:** not specified] level of audit; and
- [**assignment:** Logon attempts
- Logon success
- Logon failure
- Administrator initiated security attribute (as detailed in section 9) changes
- Attempts to lock a client machine
- Attempts to reboot a client machine
- Attempts to force synchronise a client machine]

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, [**assignment:** no other relevant information]

FAU_GEN.2(b) User identity association (McAfee Endpoint Encryption Manager)

FAU_GEN.2.1(b) 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(b) Protected audit trail storage (McAfee Endpoint Encryption Manager)

FAU_STG.1.1(b) The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2(b) The TSF shall be able to [**selection:** prevent] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.3(b) Action in case of possible audit data loss (McAfee Endpoint Encryption Manager)

FAU_STG.3.1(b) The TSF shall take [**assignment:** the action of not creating new audit records] if the audit trail exceeds [**assignment:** Available space on the TOE Manager hard drive].

FAU_SAR.1 Audit review

FAU_SAR.1.1 The [**refinement:** McAfee Endpoint Encryption Manager] shall provide [**assignment:** authorised administrators] with the capability to read [**assignment:** all audit information] from the audit records.

FAU_SAR.1.2 The [**refinement:** McAfee Endpoint Encryption Manager] 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 [**refinement:** McAfee Endpoint Encryption Manager] shall provide the ability to apply [**assignment:** sorting] of audit data based on [**assignment:** date and time, the event code, the object (device) or the description of the audited event].

5.1.2.2 FDP: User data protection

FDP_ACC.2(b) Complete access control (Admin user)

FDP_ACC.2.1(b) The TSF shall enforce the [**assignment:** secure management SFP] on [**assignment:** all users of the McAfee Endpoint Encryption Manager and the Device properties] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2(b) The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1(b) Security attribute based access control (Admin user)

FDP_ACF.1.1(b) The TSF shall enforce the [**assignment:** secure management SFP] to objects based on the following: [**assignment:** users in possession of valid login credentials].

FDP_ACF.1.2(b) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**assignment:** If a user has been authenticated using login credentials, the derived keys will be used to give the user access to the assets protected by the TSF. Authentication failure will result in the user failing to gain access to the TSF assets].

FDP_ACF.1.3(b) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**assignment:** none].

FDP_ACF.1.4(b) The TSF shall explicitly deny access of subjects to objects based on the [**assignment:** none].

5.1.2.3 FCS: Cryptographic Support

FCS_COP.1(d) Cryptographic operation (McAfee Endpoint Encryption Manager)

FCS_COP.1.1(d) The [**refinement:** McAfee Endpoint Encryption Manager] shall perform [**assignment:** encrypted and authenticated session based communication with the TOE Client] in accordance with a specified cryptographic algorithm [**assignment:** AES for encryption and DSA and SHA-1 for authentication] and cryptographic key sizes [**assignment:** 256 bits for AES and 1024 bits for DSA] that meet the following: [**assignment:** FIPS 197 for AES and FIPS 186-2 for DSA and SHA-1].

5.1.2.4 FIA: Identification and authentication

FIA_UAU.2(b) User authentication before any action (Manager)

FIA_UAU.2.1(b) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4(b) Single-use authentication mechanisms (McAfee Endpoint Encryption Manager)

FIA_UAU.4.1(b) [**refinement:** The McAfee Endpoint Encryption Manager shall prevent reuse of authentication data related to [**assignment:** the secure management mechanism and the offline recovery mechanism].

FIA_UAU.7(b) Protected authentication feedback (Manager)

FIA_UAU.7.1(b) The TSF shall provide only [**assignment:** feedback consisting of a '*' for each character typed for all passwords and no feedback in the case of the secure management mechanism] to the user while the authentication is in progress.

FIA_UID.2(b) User identification before any action (Manager)

FIA_UID.2.1(b) The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.2.5 FMT: Security Management

FMT_MSA.1(b) Management of security attributes (McAfee Endpoint Encryption Manager)

FMT_MSA.1.1(b) [**refinement:** The McAfee Endpoint Encryption Manager] shall enforce the [**assignment:** secure management SFP] to restrict the ability to [**assignment:** assign, change_default, query, modify, delete] the security attributes [**assignment:** all McAfee Endpoint Encryption for PC Machine properties and User properties as defined in section 9] to [**assignment:** authorised administrators].

FMT_MSA.2(b) Secure security attributes (McAfee Endpoint Encryption Manager)

FMT_MSA.2.1(b) [**refinement:** The McAfee Endpoint Encryption Manager] shall ensure that only secure values are accepted for [**assignment:** the security attributes defined in section 9].

FMT_MSA.3(b) Static attribute initialisation (McAfee Endpoint Encryption Manager)

FMT_MSA.3.1(b) [**refinement:** The McAfee Endpoint Encryption Manager] shall enforce the [**assignment:** secure management SFP] to provide [**selection:** restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(b) The [**refinement:** McAfee Endpoint Encryption Manager] shall allow the [**assignment:** authorised administrators] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1(e) Management of TSF data (audit)

FMT_MTD.1.1(e) The [**refinement:** McAfee Endpoint Encryption Manager] shall restrict the ability to [**selection:** query, clear] the [**assignment:** TSF audit data] to [**assignment:** authorised administrators].

FMT_MTD.1(f) Management of TSF data (password)

FMT_MTD.1.1(f) The [**refinement:** McAfee Endpoint Encryption Manager] shall restrict the ability to [**selection:** modify] the [**assignment:** a user's password] to [**assignment:** authorised administrators and a user may modify his own password if he successfully supplies his existing password first].

FMT_REV.1(b) Revocation (McAfee Endpoint Encryption Manager)

FMT_REV.1.1(b) [**refinement:** The McAfee Endpoint Encryption Manager] shall restrict the ability to revoke [**assignment:** user accounts] associated with the [**selection:** users] under the control of the TSF to [**assignment:** authorised administrators].

FMT_REV.1.2(b) The [**refinement:** McAfee Endpoint Encryption Manager] shall enforce the rules [**assignment:** Revocation can either take place the next time the user logs on, or the user can be revoked immediately, with their machine rebooted and their account disabled or deleted, as specified by the administrator].

FMT_SAE.1(b) Time-limited authorisation (McAfee Endpoint Encryption Manager)

FMT_SAE.1.1(b) The [**refinement:** McAfee Endpoint Encryption Manager] shall restrict the capability to specify an expiration time for [**assignment:** user passwords] to [**assignment:** authorised administrators].

FMT_SAE.1.2(b) For each of these security attributes, the [**refinement:** McAfee Endpoint Encryption Manager] shall be able to [**assignment:** give the user a warning that the password is about to expire a specified time before expiry, but also prevent the user from logging on until he has changed the password] after the expiration time for the indicated security attribute has passed.

FMT_SMR.1(b) Security roles (McAfee Endpoint Encryption Manager)

FMT_SMR.1.1(b) The [**refinement:** McAfee Endpoint Encryption Manager] shall maintain the roles [**assignment:** Administrator].

FMT_SMR.1.2(b) The [**refinement:** McAfee Endpoint Encryption Manager] shall be able to associate users with roles.

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level (EAL) 4 components as specified in Part 3 of the Common Criteria. The EAL4 assurance components have been augmented with the addition of ALC_FLR.3. The table below provides a listing of all Security Assurance Requirements met by the TOE. For a detailed description of these components, please refer to the Common Criteria documentation directly.

Assurance class	Assurance components
Class ADV: Development	ADV_FSP.4 Complete functional specification ADV_ARC.1 Security architecture description ADV_IMP.1 Implementation representation of the TSF ADV_TDS.3 Basic modular design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
Class ALC: Life Cycle Support	ALC_CMS.4 Problem tracking CM coverage ALC_FLR.3 Systematic Flaw remediation ALC_CMC.4 Production support, acceptance procedures and automation ALC_DEL.1 Delivery procedures ALC_DVS.1 Identification of security measures ALC_LCD.1 Developer defined life-cycle model ALC_TAT.1 Well-defined development tools
Class ATE: Tests	ATE_COV.2 Analysis of coverage ATE_DPT.2 Testing: security enforcing modules ATE_FUN.1 Functional testing ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Figure 11 Assurance Components

5.3 Security Requirements for the IT Environment

This section identifies the IT security requirements that are to be met by the IT environment of the TOE. In this case, the requirements in this part of the Security Target are drawn from Common Criteria Part 2 and as such have been rephrased to clearly indicate that the IT environment, not the TOE, must meet the requirement. Such rephrasing is a special case of refinement and not subject to the assessment requirements associated with modified CC components.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The [**refinement:** IT environment] shall be able to provide reliable time stamps [**refinement:** for the use of the TSF].

This SFR maps to the assumption A.TIME_SOURCE.

6 TOE Summary Specification

This section defines the instantiation of the security requirements for the TOE. This specification provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

6.1 TOE Security Functions

This section specifies the IT security functions of the TOE and how these functions satisfy the TOE security functional requirements. This includes a bi-directional mapping between functions and requirements that clearly shows which functions satisfy which requirements and that all requirements are met. Each security function contributes to the satisfaction of at least one TOE security functional requirement.

The table below maps these security functions to the security functional requirements already identified in section 5.1. Each function is given an identifier to enable unambiguous cross-referencing through the assurance documentation.

This section is presented in an informal style, and for ease of narrative and conciseness does not reproduce verbatim the text of the security functional requirements drawn from CC part 2 and mapped to the TOE in section 5.1. If in some cases it is not obvious from the description that a security function embodies the security functional requirements expected from the table below, the mapping table (Figure 12) should be taken as indicating that the requirement is included in the function, although for the purpose of the description in this document that may be implicit.

IT Security Function	TOE Security Functional Requirement
TSF.USER_ACCESS_CONTROL	FDP_ACC.2(a) Complete access control (user)
	FDP_ACF.1(a) Security attribute based access control (user)
	FTA_SSL.2 User-initiated locking
	FTA_TSE.1 TOE session establishment
TSF.MGR_USER_ACCESS_CONTROL	FDP_ACC.2(b) Complete access control (Admin user)
	FDP_ACF.1(b) Security attribute based access control (Admin user)
TSF.USER_AUTHENTICATION	FTP_TRP.1 Trusted path
	FIA_UAU.2(a) User authentication before any action (Client)
	FIA_UAU.7(a) Protected authentication feedback (Client)
	FIA_UID.2(a) User identification before any action (Client)
	FIA_AFL.1 Authentication failure handling (user logon)
TSF.MGR_USER_AUTHENTICATION	FIA_UAU.2(b) User authentication before any action (Manager)
	FIA_UAU.7(b) Protected authentication feedback (Manager)
	FIA_UID.2(b) User identification before any action (Manager)
TSF.MANAGEMENT_BY_USER	FMT_MTD.1(b) Management of TSF data (password)
	FMT_SMF.1 Specification of Management Functions
TSF.HDD_ENCRYPTION	FCS_COP.1(a) Cryptographic operation (data encryption and decryption)
TSF.HDD_ENC_KEYMAN	FCS_CKM.1(a) Cryptographic key generation (symmetric)
	FCS_CKM.4 Cryptographic key destruction
	FCS_COP.1(b) Cryptographic operation (key encryption and decryption)
TSF.ADMIN_ACCESS_CONTROL	FIA_UAU.4(a) Single-use authentication mechanisms (secure management)
	FMT_MSA.1(a) Management of security attributes (secure management)
TSF.SECURE_MANAGEMENT	FCS_CKM.1(b) Cryptographic key generation (asymmetric)
	FCS_CKM.4 Cryptographic key destruction
	FCS_COP.1(c) Cryptographic operation (authenticated administration)
	FMT_MSA.1(a) Management of security attributes (secure management)
	FMT_MTD.1(a) Management of TSF data (audit)

IT Security Function	TOE Security Functional Requirement
	FMT_MTD.1(b) Management of TSF data (password)
	FMT_SMF.1 Specification of Management Functions
	FMT_MTD.2(a) Management of limits on TSF data (authentication failure)
	FMT_REV.1(a) Revocation
	FMT_SAE.1(a) Time-limited authorisation (secure management)
	FMT_SMR.1(a) Security roles
	FIA_ATD.1 User attribute definition
	FIA_UAU.4(a) Single-use authentication mechanisms (secure management)
	FCS_COP.1(d) Cryptographic operation (McAfee Endpoint Encryption Manager)
	FIA_UAU.4(b) Single-use authentication mechanisms (McAfee Endpoint Encryption Manager)
	FMT_MSA.1(b) Management of security attributes (McAfee Endpoint Encryption Manager)
	FMT_MSA.2(b) Secure security attributes (McAfee Endpoint Encryption Manager)
	FMT_MSA.3(b) Static attribute initialisation (McAfee Endpoint Encryption Manager)
	FMT_MTD.1(e) Management of TSF data (audit)
	FMT_REV.1(b) Revocation (McAfee Endpoint Encryption Manager)
	FMT_SAE.1(b) Time-limited authorisation (McAfee Endpoint Encryption Manager)
	FMT_SMR.1(b) Security roles (McAfee Endpoint Encryption Manager)
TSF.SECURITY_AUDIT	FAU_GEN.1(a) Audit data generation (TOE Client)
	FAU_GEN.2(a) User identity association (TOE Client)
	FAU_STG.1(a) Protected audit trail storage (TOE Client)
	FAU_STG.3(a) Action in case of possible audit data loss (TOE Client)
	FAU_GEN.1(b) Audit data generation (McAfee Endpoint Encryption Manager)
	FAU_GEN.2(b) User identity association (McAfee Endpoint Encryption Manager)
	FAU_STG.1(b) Protected audit trail storage (McAfee Endpoint Encryption Manager)
	FAU_STG.3(b) Action in case of possible audit data loss (McAfee Endpoint Encryption Manager)
	FAU_SAR.1 Audit review
	FAU_SAR.3 Selectable audit review
TSF.PROTECTION	FPT_TST.1 TSF testing
	FPT_FLS.1 Failure with preservation of secure state
	FPT_RCV.1 Manual recovery
	FRU_FLT.1 Degraded fault tolerance
TSF.ADMINISTRATION_SERVER	FCS_COP.1(d) Cryptographic operation (McAfee Endpoint Encryption Manager)
	FIA_UAU.4(b) Single-use authentication mechanisms (McAfee Endpoint Encryption Manager)
	FIA_UAU.2(b) User authentication before any action (Manager)
	FIA_UAU.7(b) Protected authentication feedback (Manager)
	FIA_UID.2(b) User identification before any action

IT Security Function	TOE Security Functional Requirement
	(Manager)
	FDP_ACC.2(b) Complete access control (Admin user)
	FDP_ACF.1(b) Security attribute based access control (Admin user)
	FMT_MSA.1(b) Management of security attributes (McAfee Endpoint Encryption Manager)
	FMT_MSA.2(b) Secure security attributes (McAfee Endpoint Encryption Manager)
	FMT_MSA.3(b) Static attribute initialisation (McAfee Endpoint Encryption Manager)
	FMT_MTD.1(e) Management of TSF data (audit)
	FMT_MTD.1(f) Management of TSF data (password)
	FMT_REV.1(b) Revocation (McAfee Endpoint Encryption Manager)
	FMT_SAE.1(b) Time-limited authorisation (McAfee Endpoint Encryption Manager)
	FMT_SMR.1(b) Security roles (McAfee Endpoint Encryption Manager)
	FAU_GEN.1(b) Audit data generation (McAfee Endpoint Encryption Manager)
	FAU_GEN.2(b) User identity association (McAfee Endpoint Encryption Manager)
	FAU_STG.1(b) Protected audit trail storage (McAfee Endpoint Encryption manager)
	FAU_STG.3(b) Action in case of possible audit data loss (McAfee Endpoint Encryption manager)
	FAU_SAR.1 Audit Review
	FAU_SAR.3 Selectable Audit Review

Figure 12 Mapping Security Functions to Security Functional Requirements

6.1.1 User Access Control – TSF.USER_ACCESS_CONTROL

The McAfee Endpoint Encryption Client replaces the master boot record on the bootable hard disk of the PC on which it is installed. So, when such a PC boots, the first code that gets loaded from the hard disk is the McAfee Endpoint Encryption Client and the user is presented with the McAfee Endpoint Encryption Client logon screen, and will be required to provide a valid user identifier and a valid, authenticated password before being granted access to the PC's data.

The storage media are encrypted and the hard disk encryption key must be loaded into the TOE Client before it can be decrypted. The user's logon credentials, that is, his user name and password/PIN, are presented to the token (password-only token, or CAC/PIV smartcard) to give the user access to the token key, via the logon process. This token key is used to access the key hierarchy and ultimately allows the TOE Client to access the hard disk encryption key and so decrypt the storage media.

If a user attempts to bypass the McAfee Endpoint Encryption Client logon by using a boot disk, for instance, they will be prevented from gaining access to the data stored on the storage media by virtue of the fact that the storage media is encrypted using AES and an encrypted key that cannot be subverted unless an attacker guesses the password or key or gains the password from a trusted individual.

Once a user has been granted access to the PC, they may choose to lock the PC, when leaving their desk for lunch, for instance, by activating the McAfee Endpoint Encryption Client screen saver, which will then present the user with the McAfee Endpoint Encryption Client logon screen when they try to use the PC again preventing unauthorised access.

A user whose account has been disabled will not be able to gain access to the TOE data, and if a user's account is disabled while he is using the TOE Client, he will be locked out and presented with the

McAfee Endpoint Encryption Client screen saver and not able to logon again until his account is enabled once again.

Additionally, optionally application control may be imposed by an Authorised Administrator. This provides the ability to restrict user access to specific applications or to restrict access to the whole PC to fixed times of day or to fixed days of the week, as appropriate. However, this functionality is only supported on the Microsoft Windows XP operating system and is not supported on later Windows operating systems.

This functionality constitutes the machine access control SFP.

6.1.2 Admin User Access Control – TSF.MGR_USER_ACCESS_CONTROL

The TOE Manager supports identity-based access control to protect its assets from unauthorised access. Users require valid credentials in the form of a user name, login credentials and a token (either a physical token, in the case of the CAC and PIV smartcards, or a logical token, in the form of the password-only token).

This functionality constitutes the TOE Manager access control SFP.

6.1.3 User Authentication – TSF.USER_AUTHENTICATION

The TOE Client supports token-based access control. Within the TOE Client boundary are the password-only token and the CAC and PIV tokens.

When a user boots up a PC protected by McAfee Endpoint Encryption for PC, they boot into the “McAfee Endpoint Encryption Client OS”, which is effectively what the TOE Client bootcode is, providing a trusted, secure and controlled environment in which the user may present his credentials (such as a user identity and a password, or a user identity and smartcard and PIN) to the McAfee Endpoint Encryption Client for authentication.

Before authentication can occur, the user must present the McAfee Endpoint Encryption Client with his identity (as assigned).

When the user logs on, the credentials that he supplies are authenticated.

Password-only token authentication
In the case of a password, this is checked against a securely stored value associated with the user using the PKCS-5 algorithm (RFC 2898).

This functionality contains the password authentication mechanism.

Authentication using CAC and PIV tokens
The CAC and PIV smartcards are PKI tokens. User identity is verified again via a user name and a password. The token is password protected. Following successful logon to the token, the certificate on the token is used to decrypt an encrypted user CSP which is then used to decrypt the machine key. Each user is assigned a unique user name. Possession of the physical token, the ability to login to it using a secret password and then to decrypt the user key matching the user name of the user provides identity based authentication of that user.

When a user presents his credentials to the McAfee Endpoint Encryption Client for authentication at logon, his identity may be displayed in plain text, but for password authentication, there will only be feedback consisting of a ‘*’ for each character typed while the authentication is in progress.

The user will be given a set number of opportunities to logon successfully, to cater for user error, but if the user exceeds the prescribed number of allowed consecutive failures, his account will be disabled.

6.1.4 TOE Manager User Authentication – TSF.MGR_USER_AUTHENTICATION

The TOE Manager supports token-based access control. Within the TOE Manager boundary are the password-only token and the CAC and PIV tokens.

When a user logs on to a TOE Manager, the user may present his credentials (such as a user identity and a password, or a user identity and smartcard and PIN) to the McAfee Endpoint Encryption Manager for authentication.

When the user logs on, the credentials that he supplies are authenticated.

Password-only token authentication
In the case of a password, this is checked against a securely stored value associated with the user using the PKCS-5 algorithm (RFC 2898).

This functionality contains the password authentication mechanism.

Authentication using CAC and PIV tokens
The CAC and PIV smartcards are PKI tokens. User identity is verified again via a user name and a password. The token is password protected. Following successful logon to the token, the certificate on the token is used to decrypt an encrypted user CSP which is then used to decrypt the machine key. Each user is assigned a unique user name. Possession of the physical token, the ability to login to it using a secret password and then to decrypt the user key matching the user name of the user provides identity based authentication of that user.

When a user presents his credentials to the McAfee Endpoint Encryption Manager for authentication at logon, there will only be feedback consisting of a '*' for each character typed while the authentication is in progress.

6.1.5 Management of TOE by User – TSF.MANAGEMENT_BY_USER

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

6.1.6 Hard Disk Encryption – TSF.HDD_ENCRYPTION

It is possible to subvert the logon process, for instance by using a bootable floppy disk, and so for this reason, the storage media of the TOE Client PC are encrypted to prevent unauthorised user access to the TOE data. This constitutes part of the machine access control SFP.

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

6.1.7 Hard Disk Encryption Key Management – TSF.HDD_ENC_KEYMAN

The TOE Client generates its hard disk encryption key using a pseudo-random number generator based on DSS with a key size of 256 bits.

The TSF destroys hard disk encryption keys by zeroing them when they are no longer in use, specifically when the TOE is uninstalled.

The hard disk encryption key is stored encrypted (using AES and a key length of 256 bits) under a key derived from the user's password. If the password changes, the hard disk encryption key is decrypted using the existing one and then encrypted for storage using the new password. The hard disk encryption key itself does not change in such circumstances.

The hard disk encryption key is decrypted as required when needed to access data on the TOE Client PC storage media. This can only occur once a user has successfully logged on to the TOE Client.

6.1.8 Administrative Access Control – TSF.ADMIN_ACCESS_CONTROL

Management of TOE Clients is via the administration secure management interface. Any administrator wishing to manage a TOE Client must first establish a secure management session with that TOE Client.

A proprietary protocol is used to establish a session key shared between the TOE Client and the TOE Manager. This is then used to encrypt a known value to authenticate the TOE Manager to the TOE Client and vice versa. This protocol incorporating the one-time session key and challenge-response mechanism, provides a single-use authentication mechanism.

Once a secure session has been established (using an authenticated message exchange), the administrators ability to modify TOE attributes is governed by the privilege level of the administrator on the TOE Manager machine.

An administrator sets up a machine configuration through the TOE Manager user interface. This is stored in the Object Directory and deployed to the TOE Client during a secure management session

Each user in the directory has a certain "administration privilege" with a range of between 1 (lowest) to 32 (root administrator), no user except the root administrator can change the attributes of a user of its privilege or above, but some attributes can be read regardless. This mechanism stops low privilege users from changing their own configuration, and protects high-level administrators from the activities of lower levels.

This function constitutes the secure management access control SFP.

6.1.9 Secure Management – TSF.SECURE_MANAGEMENT

The user may change his own password, however the bulk of the management of the TOE functionality must be performed by an administrator. All administrator configuration options relevant to the TOE machine and its users are detailed in section 9. This section discusses various aspects of secure management and some of the key configuration options in more detail.

The client and administrator create a secure session for allowing secure configuration to occur. This mutual authentication is performed using DSA signatures, and the session is then established using AES encryption of all link traffic using keys generated using Diffie-Hellman key. This is a single use authentication mechanism, it is not possible to create a new session by replaying old authentication data. No administration is permitted before an authenticated administration session has been established.

Users are assigned to groups. An administrator may add, modify or delete groups. The group provides a set of default initial values for a user configuration and allows easier allocation of users, as they can be assigned to a machine configuration by dint of being a group member rather than having to be assigned individually.

Only an authorised administrator may add, modify or delete users and their attributes on the TOE. For instance, set or reset a user’s password, and may also configure the password policy associated with that user, such as enforcing password length or content, password history, or lifetime. Also, the number of times that logon failure may consecutively occur before the user account is disabled may be set by the administrator.

For each user, the administrator creates a User Identifier, and defines a password policy. During installation a hard disk encryption key is generated along with user encryption keys that are stored in the McAfee Endpoint Encryption for PC Object Directory.

Each user will have a token associated with them in the management database. Within the boundary of the TOE are the CAC and PIV smartcards and the password-only token.

The McAfee Endpoint Encryption Connector Manager allows an administrator to import user identities and other security attributes from external systems

An authorised administrator can view and if required clear the audit data from a TOE.

If a user is deleted, his details will be removed from the TOE Manager immediately and from the TOE Client Object Directory once the TOE Client is resynchronised.

When the administrative session is terminated, all of the session keys that were created are then zeroed.

In addition, during an authorised administrative session, the administrator may:

- Synchronise the TOE Client with the TOE Manager database to invoke any configuration changes,
- Reboot the TOE Client,
- Lock the TOE Client to the screen saver,
- Disable the account of the current user,
- Deploy files to the TOE Client,
- Recover the TOE Client in the event of a lost password

This function constitutes the secure management SFP and contains the secure management mechanism.

6.1.10 Audit – TSF.SECURITY_AUDIT

6.1.10.1 TOE Client Audit

The TOE Client maintains an audit log. This contains a list of events that have occurred on the TOE Client, and each entry consists of a timestamp, type of event, user ID of the user logged on at the time and the result of the event. The audit functions are always active while the TOE Client is operational.

All of the following result in audit entries:

All try events, resulting from:

- Expiry and timeouts

All success events, such as

- Changes to passwords
- Logon
- Recovery

All failure events.

- Password change failures
- Logon failures
- Recovery failures

The audit log can only hold 3000 entries. When it is full, each new entry added results in the oldest entry in the log becoming overwritten.

The audit log can only be viewed or cleared by authorised administrators, and he can choose to view the entries ordered on a number of factors, specifically: date and time, the event code, the object (machine or user) or the description of the audited event.

As the TOE employs access control, access to the audit trail of the TOE Client is restricted, and protected from unauthorised modification or deletion.

6.1.10.2 TOE Manager Audit

The TOE Manager maintains an audit log. This contains a list of events that have occurred on the TOE Manager, and each entry consists of a timestamp, type of event, user ID of the user logged on at the time and the result of the event.

All of the following result in audit entries:

- Start-up and shutdown of the audit functions;
- Logon attempts
- Logon success
- Logon failure
- Administrator initiated security attribute (as detailed in section 9) changes
- Attempts to lock a client machine
- Attempts to reboot a client machine
- Attempts to force synchronise a client machine

The size (capacity) of the TOE Manager audit log is only limited by the available hard disk space. If the audit log becomes full, no new entries are added.

The audit log can only be viewed or cleared by authorised administrators, and he can choose to view the entries ordered on a number of factors, specifically: date and time, the event code, the object (machine or user) or the description of the audited event.

As the TOE employs access control, access to the audit trail of the TOE Manager is restricted, and protected from unauthorised modification or deletion.

6.1.11 Self-Protection of the TOE – TSF.PROTECTION

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

The TSF runs a suite of tests during initial start-up, and in the case of the random number generator test, continuously to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF. These tests are described in sections 2.12 and 2.13.

The TSF preserves a secure state when communications with the TOE Manager are unexpectedly terminated or when there is a power failure to the TOE Client.

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

The online recovery mechanism allows a TOE Manager authorised administrator to modify user security attributes to allow a user to recover access to the TOE Client machine. However this mechanism requires synchronisation between the TOE Manager Object Directory and the TOE Client copy 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: offline recovery and local recovery. Offline recovery is an option that can be enabled or disabled on a user by user and machine by machine basis.

Offline recovery allows a TOE Client user to pass a TOE Client recovery code request to the TOE Manager administrator An independent means of verifying the identity of the TOE Client user is required by the TOE Manager administrator is required, A.NON_TECHNICAL_IDENTITY_VERIFICATION. The TOE Manager administrator can then provide a recovery response code to allow the TOE Client user to regain access to the TOE Client.

Local 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 the TOE Manager. (Note: Endpoint Encryption contains a generic set of questions by default that may be used or replaced with a set chosen by the authorised administrator). When the user first sets up their local recovery feature they will be prompted to select a number of questions and provide the answers to them. These form the basis for their local self recovery feature. When performing self-recovery, the user will have to correctly answer a number of questions in order to regain access to the TOE Client.

The TSF ensures that normal operation continues when the link to the TOE Manager is lost, by maintaining a local copy of the Object Directory. The TOE Client can be configured such that if this link is lost and the TOE Client remains unsynchronised for a specified amount of time, then the TOE Client is locked.

6.1.12 McAfee Endpoint Encryption Manager – TSF.ADMINISTRATION_SERVER

This function gives an authorised administrator access to a GUI that allows him to configure and manage the TOE. TSF.ADMINISTRATION_SERVER allows the McAfee Endpoint Encryption Manager side of the functions TSF.ADMIN_ACCESS_CONTROL, TSF.SECURE_MANAGEMENT and TSF.SECURITY_AUDIT.

It also provides a user interface through which an authorised administrator may view or selectively review audit data from the TOE.

6.2 Assurance Measures

The requirements of the assurance components that the TOE must satisfy in order to achieve certification at EAL4+ are each addressed by a document specifically written for the purpose. The following table names each of these assurance documents.

Assurance components	Assurance Measures
ADV_FSP.4 Complete functional specification	McAfee Endpoint Encryption for PC Functional Specification
ADV_ARC.1 Security architecture description	McAfee Endpoint Encryption for PC Security Architecture
ADV_IMP.1 Implementation representation of the TSF	McAfee Endpoint Encryption for PC Low-Level Design Deliverables Package
ADV_TDS.3 Basic modular design	McAfee Endpoint Encryption for PC Low-Level Design Deliverables Package
AGD_OPE.1 Operational user guidance	McAfee Endpoint Encryption Quickstart Guide
AGD_PRE.1 Preparative procedures	McAfee Endpoint Encryption Managers Guide
ALC_CMS.4 Problem tracking CM coverage	McAfee Endpoint Encryption for PC Configuration Management Deliverables Package
ALC_FLR.3 Systematic Flaw remediation	McAfee Endpoint Encryption for PC Configuration Management Deliverables Package
ALC_CMC.4 Production support, acceptance procedures and automation	McAfee Endpoint Encryption for PC Configuration Management Deliverables Package
ALC_DEL.1 Delivery procedures	McAfee Endpoint Encryption for PC Delivery and Operation Deliverables Package
ALC_DVS.1 Identification of security measures	McAfee Endpoint Encryption for PC Life Cycle Deliverables Package
ALC_LCD.1 Developer defined life-cycle model	McAfee Endpoint Encryption for PC Life Cycle Deliverables Package
ALC_TAT.1 Well-defined development tools	McAfee Endpoint Encryption for PC Life Cycle Deliverables Package
ATE_COV.2 Analysis of coverage	McAfee Endpoint Encryption for PC Testing Deliverables Package
ATE_DPT.2 Testing: security enforcing modules	McAfee Endpoint Encryption for PC Testing Deliverables Package
ATE_FUN.1 Functional testing	McAfee Endpoint Encryption for PC Testing Deliverables Package

Assurance components	Assurance Measures
ATE_IND.2 Independent testing - sample	McAfee Endpoint Encryption for PC Testing Deliverables Package
AVA_VAN.3 Focused vulnerability analysis	McAfee Endpoint Encryption for PC Vulnerability Assessment Deliverables Package

Figure 13 Mapping of Assurance Components to Assurance Measures

7 Protection Profile Claims

This Security Target does not include any claims that the TOE conforms to any named Protection Profile.

8 Rationale

The purpose of this section is to demonstrate that the threats, assumptions and organisational security policies identified in the TOE security environment (see section 3) are satisfied by the security objectives described in section 4. Further, this section also demonstrates that these objectives are satisfied by the security functional requirements identified in section 5.

8.1 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.

Threats, assumptions and organisational security policies	Corresponding security objectives
A.MANAGEMENT	OE.MANAGED
A.NO_MALEVOLENCE	OE.MANAGED
A.PROFICIENT_USERS	OE.EASE_OF_USE_ADMIN OE.EASE_OF_USE_USER
A.AUTHENTICATION_DATA_PRIVATE	OE.EASE_OF_USE_USER OE.AUTH
A.TIME_SOURCE	OE.TIME_SOURCE
A.SECURE_BACKUP	OE.SECURE_BACKUP
A.AVAILABLE_BACKUP	OE.AVAILABLE_BACKUP
A.DOMAIN_SEPARATION	OE.DOMAIN_SEPARATION
A.TRUSTED_SOFTWARE	OE.TRUSTED_SOFTWARE
A.NON_TECHNICAL_IDENTITY_VERIFICATION	OE.NON_TECHNICAL_IDENTITY_VERIFICATION
T.ACCESS	O.AUTHORISATION O.ACCESS_CONTROL O.AUDIT
T.ALTERNATE_BOOT_PROCESS	O.ENCRYPTED_MEDIA
T.CONFIG _MODIFICATION	O.PROTECT
T. CORRUPT_AUDIT	O.AUTHORISATION O.ENCRYPTED_MEDIA O.EFFECTIVE_ADMINISTRATION O.AUDIT
T.EASE_OF_USE_ADMIN	OE.EASE_OF_USE_ADMIN
T.EASE_OF_USE_USER	O.EASE_OF_USE_USER
T.EAVESDROP_TRANSIT	O.DATA_TRANSFER
T.OBJECT_REUSE	O.NO_OBJECT_REUSE
T.PASSWORD_LOSS	O.SECURE_RECOVERY OE.NON_TECHNICAL_IDENTITY_VERIFICATION
T.RECORD_ACTIONS	O.AUTHORISATION O.AUDIT
T.RECOVERY_PROCEDURE_INTERCEPT	O.NO_OBJECT_REUSE
T.RECOVERY_MASQUERADE	O.AUTHORISATION

Threats, assumptions and organisational security policies	Corresponding security objectives
	OE.NON_TECHNICAL_IDENTITY_VERIFICATION
T.REMOVE_DISK	O.ENCRYPTED_MEDIA
T.SPOOF	O.TRUSTED_PATH O.DATA_TRANSFER
T.SYSTEM_ACCESS	O.AUTHORISATION O.PROTECT OE.MANAGED
T.UNAUTHORISED_MODIFICATION	O.AUTHORISATION O.ENCRYPTED_MEDIA O.PROTECT OE.MANAGED OE.EASE_OF_USE_USER
P.AUTHORISED_USERS	O.AUTHORISATION
P.CRYPTOGRAPHIC_KEYS	O.CRYPOTOGRAPHIC_KEYS
P.CRYPTOGRAPHIC_OPERATIONS	O.CRYPTOGRAPHIC_OPERATIONS
P.EAVESDROP_TRANSIT	O.DATA_TRANSFER
P.FAULT_TOLERANCE	O.FAULT_TOLERANCE
P.USER_ACCOUNTABILITY	OE.AUTH O.AUDIT

Figure 14 Mapping Threats, Assumptions and Policies to Objectives

Security Objectives	Corresponding threats, assumptions and organisational security policies
OE.MANAGED	A.MANAGEMENT A.NO_MALEVOLENCE T.SYSTEM_ACCESS T.UNAUTHORISED_MODIFICATION
OE.EASE_OF_USE_ADMIN	A.PROFICIENT_USERS T.EASE_OF_USE_ADMIN
OE.EASE_OF_USE_USER	A.PROFICIENT_USERS A.AUTHENTICATION_DATA_PRIVATE T.UNAUTHORISED_MODIFICATION
OE.AUTH	A.AUTHENTICATION_DATA_PRIVATE P.USER_ACCOUNTABILITY
OE.TIME_SOURCE	A.TIME_SOURCE
OE.SECURE_BACKUP	A.SECURE_BACKUP
OE.AVAILABLE_BACKUP	A.AVAILABLE_BACKUP
OE.DOMAIN_SEPARATION	A.DOMAIN_SEPARATION
OE.TRUSTED_SOFTWARE	A.TRUSTED_SOFTWARE
OE.NON_TECHNICAL_IDENTITY_VERIFICATION	A.NON_TECHNICAL_IDENTITY_VERIFICATION T.PASSWORD_LOSS T.RECOVERY_MASQUERADE
O.AUTHORISATION	T.ACCESS T. CORRUPT_AUDIT T.RECORD_ACTIONS T.RECOVERY_MASQUERADE T.SYSTEM_ACCESS T.UNAUTHORISED_MODIFICATION P.AUTHORISED_USERS
O.ACCESS_CONTROL	T.ACCESS
O.AUDIT	T.ACCESS T. CORRUPT_AUDIT T.RECORD_ACTIONS P.USER_ACCOUNTABILITY

Security Objectives	Corresponding threats, assumptions and organisational security policies
O.ENCRYPTED_MEDIA	T.ALTERNATE_BOOT_PROCESS T.CORRUPT_AUDIT T.UNAUTHORISED_MODIFICATION T.REMOVE_DISK
O.PROTECT	T.CONFIG _MODIFICATION T.SYSTEM_ACCESS T.UNAUTHORISED_MODIFICATION
O.TRUSTED_PATH	T.SPOOF
O.EFFECTIVE_ADMINISTRATION	T.CORRUPT_AUDIT
O.EASE_OF_USE_USER	T.EASE_OF_USE_USER
O.DATA_TRANSFER	T.EAVESDROP_TRANSIT P.EAVESDROP_TRANSIT
O.NO_OBJECT_REUSE	T.OBJECT_REUSE T.RECOVERY_PROCEDURE_INTERCEPT
O.SECURE_RECOVERY	T.PASSWORD_LOSS
O.TRUSTED_PATH	T.SPOOF
O.CRYPOTOGRAPHIC_KEYS	P.CRYPTOGRAPHIC_KEYS
O.CRYPTOGRAPHIC_OPERATIONS	P.CRYPTOGRAPHIC_OPERATIONS
O.FAULT_TOLERANCE	P.FAULT_TOLERANCE

Figure 15 Mapping Security Objectives to Threats, Assumptions and Policies

8.1.1.1 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.

8.1.1.2 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..

8.1.1.3 OE.EASE_OF_USE_USER

The TOE Client 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 Client 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.

8.1.1.4 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.

8.1.1.5 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).

8.1.1.6 OE.SECURE_BACKUP

User’s data backups are separately encrypted or physically protected to ensure data security is not compromised through theft of or unauthorised access to backup information (satisfying the assumption A.SECURE_BACKUP).

8.1.1.7 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).

8.1.1.8 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).

8.1.1.9 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).

8.1.1.10 OE.NON_TECHNICAL_IDENTITY_VERIFICATION

This objective, that there is a database of authorised 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 the McAfee Endpoint Encryption Manager. 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.

8.1.1.11 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 Client PC is stolen, this fact is used to allow it to be disabled by the TOE Manager. If the machine is connected to the TOE Manager, it can be disabled so that no user can logon to it. If it is not connected to the TOE Manager, 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.

8.1.1.12 O.ACCESS_CONTROL

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

8.1.1.13 O.AUDIT

The TSF audits certain events to allow authorized administrators to monitor how the TOE Client 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.

8.1.1.14 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.

8.1.1.15 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

8.1.1.16 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 emphasise 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

8.1.1.17 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.

8.1.1.18 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 TSF and the McAfee Endpoint Encryption Manager. 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.

8.1.1.19 O.NO_OBJECT_REUSE

The TSF uses one-time authentication mechanisms for both secure management and offline recovery. This counters the threats T.OBJECT_REUSE and T.RECOVERY_PROCEDURE_INTERCEPT. T.OBJECT_REUSE could also be a threat if the password mechanism allowed expired passwords to persist, but this is not the case. When a password is changed, the password that it replaces is no longer valid and cannot be used to gain access to the information stored on the TOE.

8.1.1.20 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 Client using a new password.

8.1.1.21 O.TRUSTED_PATH

This objective counters the threat that an attacker may impersonate the TSF in an attempt to gain the user's logon credentials, T.SPOOF. This objective along with others (O.UNATHORISED_MODIFICATION and O.AUTHORISED) counters this threat by providing a secure and reliable link between the user and the TSF.

8.1.1.22 O.CRYPOTOGRAPHIC_KEYS

The TSF ensures that cryptographic keys are generated, accessed, protected, and destroyed in a secure manner. O.CRYPTOGRAPHIC_KEYS implements the security policy P.CRYPTOGRAPHIC_KEYS.

8.1.1.23 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.

8.1.1.24 O.FAULT_TOLERANCE

This objective implements the policy P.FAULT_TOLERANCE.

8.2 Security Requirements Rationale

The Security Requirements for the TOE have been chosen to meet its Security Objectives effectively. All Functional Requirements have been selected directly from CC part 2 (where a requirement is dependent on one or more other SFRs, all dependencies have been selected), and all Assurance Requirements directly from CC part 3.

The figure below demonstrates that each TOE Security Objective is satisfied by one or more SFRs.

Security Objectives	TOE Security Functional Requirement
O.ACCESS_CONTROL	FDP_ACC.2(a) Complete access control (user) FDP_ACF.1(a) Security attribute based access control (user) FTA_SSL.2 User-initiated locking FTA_TSE.1 TOE session establishment FDP_ACC.2(b) Complete access control (Admin user) FDP_ACF.1(b) Security attribute based access control (Admin user)
O.FAULT_TOLERANCE	FRU_FLT.1 Degraded fault tolerance
O.TRUSTED_PATH	FTP_TRP.1 Trusted path
O.AUTHORISATION	FIA_UAU.2(a) User authentication before any action (Client) FIA_UAU.7(a) Protected authentication feedback (Client) FIA_UID.2(a) User identification before any action (Client) FIA_UAU.2(b) User authentication before any action (Manager) FIA_UAU.7(b) Protected authentication feedback (Manager) FIA_UID.2(b) User identification before any action (Manager) FIA_AFL.1 Authentication failure handling (user logon)
O.CRYPTOGRAPHIC_OPERATIONS	FCS_COP.1(a) Cryptographic operation (data encryption and decryption)

Security Objectives	TOE Security Functional Requirement
	FCS_COP.1(b) Cryptographic operation (key encryption and decryption) FCS_COP.1(c) Cryptographic operation (authenticated administration)
	FCS_COP.1(d) Cryptographic operation (McAfee Endpoint Encryption Manager)
O.CRYPTOGRAPHIC_KEYS	FCS_CKM.1(a) Cryptographic key generation (symmetric) FCS_CKM.4 Cryptographic key destruction
O.ENCRYPTED_MEDIA	FCS_COP.1(a) Cryptographic operation (data encryption and decryption) FIA_ATD.1 User attribute definition
O.NO_OBJECT_REUSE	FIA_UAU.4(a) Single-use authentication mechanisms (secure management)
O.EASE_OF_USE_USER	FMT_MTD.1(b) Management of TSF data (password) FMT_SMF.1 Specification of Management Functions FMT_SMR.1(a) Security roles

O.EFFECTIVE_ADMINISTRATION	FCS_CKM.1(b) Cryptographic key generation (asymmetric)
	FCS_CKM.4 Cryptographic key destruction
	FMT_MSA.1(a) Management of security attributes (secure management)
	FMT_MSA.2(a) Secure security attributes (secure management)
	FMT_MSA.3(a) Static attribute initialisation (secure management)
	FMT_MTD.1(a) Management of TSF data (audit)
	FMT_MTD.1(b) Management of TSF data (password)
	FMT_MTD.2(a) Management of limits on TSF data (authentication failure)
	FMT_SAE.1(a) Time-limited authorisation (secure management)
	FMT_REV.1(a) Revocation
	FMT_SMR.1(a) Security roles
	FIA_UAU.4(a) Single-use authentication mechanisms (secure management)
	FIA_UAU.7(a) Protected authentication feedback
	FCS_COP.1(d) Cryptographic operation (McAfee Endpoint Encryption Manager)
	FIA_UAU.4(b) Single-use authentication mechanisms (McAfee Endpoint Encryption Manager)
	FMT_MSA.1(b) Management of security attributes (McAfee Endpoint Encryption Manager)
	FMT_MSA.2(b) Secure security attributes (McAfee Endpoint Encryption Manager)
	FMT_MSA.3(b) Static attribute initialisation (McAfee Endpoint Encryption Manager)
	FMT_MTD.1(e) Management of TSF data (audit)
	FMT_MTD.1(f) Management of TSF data (password)
	FMT_REV.1(b) Revocation (McAfee Endpoint Encryption Manager)
	FMT_SAE.1(b) Time-limited authorisation (McAfee Endpoint Encryption Manager)
	FMT_SMR.1(b) Security roles (McAfee Endpoint Encryption Manager)

O.DATA_TRANSFER	FCS_CKM.1(b) Cryptographic key generation (asymmetric)
	FCS_CKM.4 Cryptographic key destruction
	FIA_UAU.4(a) Single-use authentication mechanisms (secure management)

Security Objectives	TOE Security Functional Requirement
	FIA_UAU.7(a) Protected authentication feedback (Client)
O.SECURE_RECOVERY	FIA_UAU.4(a) Single-use authentication mechanisms (secure management)
O.AUDIT	FAU_GEN.1(a) Audit data generation (TOE Client) FAU_GEN.2(a) User identity association (TOE Client) FAU_STG.1(a) Protected audit trail storage (TOE Client) FAU_STG.3(a) Action in case of possible audit data loss (TOE Client) FAU_GEN.1(b) Audit data generation (McAfee Endpoint Encryption Manager) FAU_GEN.2(b) User identity association (McAfee Endpoint Encryption Manager) FAU_STG.1(b) Protected audit trail storage (McAfee Endpoint Encryption Manager) FAU_STG.3(b) Action in case of possible audit data loss (McAfee Endpoint Encryption Manager) FAU_SAR.1 Audit review FAU_SAR.3 Selectable audit review

OE.TIME_SOURCE	FAU_GEN.1(a) Audit data generation (TOE Client)
	FAU_GEN.1(b) Audit data generation (McAfee Endpoint Encryption Manager)

O.PROTECT	FPT_TST.1 TSF testing FPT_FLS.1 Failure with preservation of secure state FPT_RCV.1 Manual recovery
OE.SECURE_BACKUP	AGD_OPE.1 Operational user guidance
OE.AVAILABLE_BACKUP	AGD_OPE.1 Operational user guidance
OE.MANAGED	AGD_OPE.1 Operational user guidance
OE.EASE_OF_USE_USER	AGD_OPE.1 Operational user guidance
OE.AUTH	AGD_OPE.1 Operational user guidance
OE.EASE_OF_USE_ADMIN	AGD_OPE.1 Operational user guidance

Figure 16 Mapping of Security Objectives to Functional and Assurance Requirements

Security Objectives	TOE Security Functional Requirement	Rationale
O.ACCESS_CONTROL	FDP_ACC.2(a)	O.ACCESS_CONTROL is the access control policy objective. This maps directly onto FDP.ACC.2(a).
	FDP_ACF.1(a)	FDP_ACF.1(a) states that the access control policy should be implemented with respect to the user's identity and password
	FTA_SSL.2	FTA_SSL.2 covers user-initiated locking of the TOE Client, invoking access control before any user can regain access to the TOE Client.
	FTA_TSE.1	Part of the access control policy is that user accounts may be disabled and users thereby denied access. This is provided by FTA_TSE.1.
	FDP_ACC.2(b)	O.ACCESS_CONTROL is the access control policy objective. This maps directly onto FDP.ACC.2(b)
	FDP_ACF.1(b)	FDP_ACF.1(b) states that the access control policy should be implemented with respect to the user's identity and password
O.FAULT_TOLERANCE	FRU_FLT.1	FRU_FLT.1 stipulates that normal operation of the TSF shall continue when communication is lost

Security Objectives	TOE Security Functional Requirement	Rationale
		with the McAfee Endpoint Encryption Manager. This matches the objective O.FAULT_TOLERANCE.
O.TRUSTED_PATH	FTP_TRP.1	There is a trusted path to enable users to be confident of the security of the link between the user and the TSF. FTP_TRP.1 matches O.TRUSTED_PATH.
O.AUTHORISATION	FIA_UAU.2(a)	O.AUTHORISATION ensures that users are authenticated before they are permitted access to the TOE Client. FIA_UAU.2(a) stipulates that users are required to be authenticated before they can use the TOE Client.
	FIA_UAU.7(a)	FIA_UAU.7(a) describes the user feedback given during user authentication.
	FIA_UID.2(a)	As part of the authentication process, users must be identified. This functionality is described in FIA_UID.2(a).
	FIA_UAU.2(b)	O.AUTHORISATION ensures that users are authenticated before they are permitted access to the TOE Manager. FIA_UAU.2(b) stipulates that users are required to be authenticated before they can use the TOE Manager.
	FIA_UAU.7(b)	FIA_UAU.7(b) describes the user feedback given during user authentication.
	FIA_UID.2(b)	As part of the authentication process, users must be identified. This functionality is described in FIA_UID.2.
	FIA_AFL.1	FIA_AFL.1 describes how user authentication failure is handled.
O.CRYPTOGRAPHIC_OPERATIONS	FCS_COP.1(a)	FCS_COP.1(a) states that AES is used for data encryption and decryption.
	FCS_COP.1(b)	FCS_COP.1(b) states that AES shall be used for key encryption by the TSF.
	FCS_COP.1(c)	FCS_COP.1(c) states that DSS is used to establish secure management communications and AES is used for encrypting communication data blocks.
	FCS_COP.1(d)	FCS_COP.1(d) states that AES for encryption and DSA and SHA-1 for authentication in the session base secure management.
O.CRYPTOGRAPHIC_KEYS	FCS_CKM.1(a)	O.CRYPTOGRAPHIC_KEYS states that cryptographic keys are generated, accessed, protected, and destroyed in a secure manner. FCS_CKM.1(a) states that keys will be generated using mechanisms that are compliant with FIPS 186-2, Appendix 3.1.
	FCS_CKM.4	FCS_CKM.4 states that keys will be destroyed using mechanisms that are compliant with FIPS 140-2.
O.ENCRYPTED_MEDIA	FCS_COP.1(a)	FCS_COP.1(a) states that data is encrypted and decrypted using AES, providing the encrypted media called for by O.ENCRYPTED_MEDIA.
	FIA_ATD.1	A number of user attributes are stored securely on the TSF.

Security Objectives	TOE Security Functional Requirement	Rationale
O.NO_OBJECT_REUSE	FIA_UAU.4(a)	FIA_UAU.4(a) stipulates that the single-use authentication mechanisms (offline recovery and secure management session establishment) operate in a way that prevents reuse of authentication data as a means of attack. This satisfies the objective O.NO_OBJECT_REUSE
O.EASE_OF_USE_USER	FMT_MTD.1(b)	O.EASE_OF_USE_USER stipulates that an authorised user should be permitted to change his password. FMT_MTD.1(b) satisfies that objective.
	FMT_SMF.1	FMT_SMF.1 specifies that the only security management function available to an authorised user is to change his password.
	FMT_SMR.1(a)	FMT_SMR.1(a) specifies that there is a user role.
O.EFFECTIVE_ADMINISTRATION	FCS_CKM.1(b)	FCS_CKM.1(b) specifies the means by which the key material used to secure the management of the TSF is generated.
	FCS_CKM.4	FCS_CKM.4 specifies how these keys are to be destroyed once they are no longer required
	FMT_MSA.1(a)	FMT_MSA.1(a) specifies that secure management is realised by implementing the secure management SFP.
	FMT_MSA.2(a)	FMT_MSA.2(a) stipulates that only secure attributes can be used to configure the TSF.
	FMT_MSA.3(a)	FMT_MSA.3(a) specifies that default values may be assigned by the secure management SFP and that these may be overridden by an authorised administrator to provide alternative values.
	FMT_MTD.1(a)	FMT_MTD.1(a) specifies that authorised administrators may view or clear the TSF audit data.
	FMT_MTD.1(b)	FMT_MTD.1(a) specifies that authorised administrators may set user passwords for the TSF.
	FMT_MTD.2(a)	FMT_MTD.2(a) allows authorised administrators to determine how repeated user logon failures are to be handled
	FMT_SAE.1(a)	FMT_SAE.1(a) allows only administrators to set the lifetime of a user password
	FMT_REV.1(a)	FMT_REV.1(a) allows authorised administrators to revoke user security attributes, that is disable user accounts.
	FMT_SMR.1(a)	FMT_SMR.1(a) specifies that there is an administrator role.
	FIA_UAU.4(a)	FIA_UAU.4(a) stipulates that the single-use secure management authentication mechanisms operates in a way that prevents reuse of authentication data as a means of attack.
	FIA_UAU.7(a)	FIA_UAU.7(a) stipulates that only success/Fail feedback is given in response to an attempt to establish a secure management session.
	FCS_COP.1(d)	FCS_COP.1(d) provides the secure management mechanism whereby only authenticated TOE Managers can deploy configuration changes to the TOE Client.

Security Objectives	TOE Security Functional Requirement	Rationale
	FIA_UAU.4(b)	FIA_UAU.4(b) provides the single-use authentication mechanism that contributes to the security of the secure management authentication
	FMT_MSA.1(b)	FMT_MSA.1(b) allows authorised administrators to change security attributes controlled by the TOE Manager
	FMT_MSA.2(b)	FMT_MSA.2(b) ensures that only secure values are possible for security attributes in the TOE Manager
	FMT_MSA.3(b)	FMT_MSA.3(b) ensures that restrictive default values are used for security attributes in the TOE Manager
	FMT_MTD.1(e)	FMT_MTD.1(e) states that only autorised administrators are allowed to query and clear the audit log.
	FMT_MTD.1(f)	FMT_MTD.1(f) states that only authorised administrators are able to change a user's password, or that a user may change their own password
	FMT_REV.1(b)	FMT_REV.1(b) states that only authorised administrators are able to revoke a user account.
	FMT_SAE.1(b)	FMT_SAE.1(b) states that only authorised administrators are allowed to change the lifetime of user passwords
	FMT_SMR.1(b)	FMT_SMR.1(b) defines the roles available to users of the TOE Manager. The use of roles allows the management of security functions to be restricted to authorised administrators
	FAU_SAR.1	FAU_SAR.1 states that audit review is restricted to authorised administrators.
	FAU_SAR.3	FAU_SAR.3 allows authorised administrators to selectively review audit information by sorting it. Only authorised administrators have access to audit information.
O.DATA_TRANSFER	FCS_CKM.1(b)	FCS_CKM.1(b) specifies the means by which the key material used to secure the management of the TSF is generated.
	FCS_CKM.4	FCS_CKM.4 states that keys will be destroyed using mechanisms that are compliant with FIPS 140-2.
	FIA_UAU.4(a)	FIA_UAU.4(a) stipulates that the single-use secure management authentication mechanisms operates in a way that prevents reuse of authentication data as a means of attack.
	FIA_UAU.7(a)	FIA_UAU.7(a) stipulates that only success/Fail feedback is given in response to an attempt to establish a secure management session.
O.SECURE_RECOVERY	FIA_UAU.4(a)	FIA_UAU.4(a) stipulates that the single-use secure management authentication mechanisms operates in a way that prevents reuse of authentication data as a means of attack.
O.AUDIT	FAU_GEN.1(a)	O.AUDIT requires that specific security relevant events be audited; that audit events are associated with identified users; that the audit log

Security Objectives	TOE Security Functional Requirement	Rationale
		is presented in a comprehensible format and that unauthorised access to the audit log is prohibited. FAU_GEN.1(a) describes the events that are audited by the TSF
	FAU_GEN.2(a)	FAU_GEN.2(a) associates each audit event with an identified user.
	FAU_STG.1(a)	FAU_STG.1(a) states that only authorised administrators may modify the audit trail.
	FAU_STG.3(a)	In order to maintain the audit trail, FAU_STG.3(a) states that in the event that the audit log becomes full, that new records may overwrite oldest ones
	FAU_GEN.1(b)	O.AUDIT requires that specific security relevant events be audited; that audit events are associated with identified users; that the audit log is presented in a comprehensible format and that unauthorised access to the audit log is prohibited. FAU_GEN.1(b) describes the events that are audited by the TSF
	FAU_GEN.2(b)	FAU_GEN.2(b) associates each audit event with an identified user.
	FAU_STG.1(b)	FAU_STG.1(b) states that only authorised administrators may modify the audit trail.
	FAU_STG.3(b)	In order to maintain the audit trail, FAU_STG.3(b) states that in the event that the audit log becomes full, that new records may overwrite oldest ones
	FAU_SAR.1	FAU_SAR.1 states that there must be a way for users to view the audit trail.
	FAU_SAR.3	FAU_SAR.3 states that the user can organise the audit trail to make it more comprehensible.
OE.TIME_SOURCE	FAU_GEN.1(a)	FAU_GEN.1(a) requires all audit events to be timestamped. OE.TIME_SOURCE provides such a timestamp.
	FAU_GEN.1(b)	FAU_GEN.1(b) requires all audit events to be timestamped. OE.TIME_SOURCE provides such a timestamp.
O.PROTECT	FPT_TST.1	O.PROTECT requires that the TSF protect itself against external interference and tampering FPT_TST.1 provides a suite of tests to monitor the correct functioning and integrity of the TSF
	FPT_FLS.1	In the event of failure of the power to the TSF or the connection to the McAfee Endpoint Encryption Manager, FPT_FLS.1 states that the TSF maintains a secure state.
	FPT_RCV.1	FPT_RCV.1 describes a method to return the TSF to an operational state in the event that a user forgets his password or has his account disabled for some other reason.
OE.SECURE_BACKUP	AGD_OPE.1	AGD_OPE.1 describes how to perform secure backups
OE.AVAILABLE_BACKUP	AGD_OPE.1	AGD_OPE.1 describes how to perform regular backups to enable recovery in the event of TSF

Security Objectives	TOE Security Functional Requirement	Rationale
		failure as a result of attack or some other cause.
OE.MANAGED	AGD_OPE.1	AGD_OPE.1 describes how the TSF should be used in order to fulfil its security objectives, and so provides all of the information required by the personnel responsible for administering the TSF.
OE.EASE_OF_USE_ADMIN	AGD_OPE.1	AGD_OPE.1 describes the administrative procedures required to ensure that the TSF remains secure.
OE.AUTH	AGD_OPE.1	AGD_OPE.1 describes the credentials that users must keep secure.
OE.EASE_OF_USE_USER	AGD_OPE.1	AGD_OPE.1 describes the procedures that users must follow in order to maintain the security of the TSF.

Figure 17 Justification of the mapping of security objectives to security functional requirements

8.3 TOE Summary Specification Rationale

The Security Objectives do not map directly to the IT Security Functions in a one-to-one fashion, and so a mapping table is included here.

IT Security Function	Security Objectives
TSF.USER_ACCESS_CONTROL	O.ACCESS_CONTROL O.FAULT_TOLERANCE
TSF.MGR_USER_ACCESS_CONTROL	O.ACCESS_CONTROL
TSF.USER_AUTHENTICATION	O.TRUSTED_PATH O.AUTHORISATION O.CRYPTOGRAPHIC_OPERATIONS O.NO_OBJECT_REUSE
TSF.MGR_USER_AUTHENTICATION	O.AUTHORISATION
TSF.MANAGEMENT_BY_USER	O.EASE_OF_USE_USER
TSF.HDD_ENCRYPTION	O.ENCRYPTED_MEDIA O.CRYPTOGRAPHIC_OPERATIONS
TSF.HDD_ENC_KEYMAN	O.CRYPTOGRAPHIC_KEYS
TSF.ADMIN_ACCESS_CONTROL	O.EFFECTIVE_ADMINISTRATION
TSF.SECURE_MANAGEMENT	O.DATA_TRANSFER O.EFFECTIVE_ADMINISTRATION O.CRYPTOGRAPHIC_KEYS O.CRYPTOGRAPHIC_OPERATIONS O.SECURE_RECOVERY O.NO_OBJECT_REUSE
TSF.SECURITY_AUDIT	O.AUDIT OE.TIME_SOURCE
TSF.PROTECTION	O.PROTECT

Figure 18 Mapping of Security Functions to Security Objectives

Where there is a one-to-many mapping of IT Security Functions to security objectives, the objectives are simply combined together to form the IT Security Functions, that is each the IT Security Functions is the sum of the security objectives that make it up. However, in a number of cases, security objectives contribute to more than one IT Security Function. In these cases, different aspects of the objective contribute to the different IT Security Functions, as follows:

8.3.1.1 O.CRYPTOGRAPHIC_KEYS

TSF.HDD_ENC_KEYMAN: Refers to the symmetric keys used by AES

TSF.SECURE_MANAGEMENT: Refers to the asymmetric keys used by DSS

8.3.1.2 O.CRYPTOGRAPHIC_OPERATIONS

TSF.USER_AUTHENTICATION: The password authentication mechanism
TSF.HDD_ENCRYPTION: Encryption of the storage media using AES.
TSF.SECURE_MANAGEMENT: Secure management using DSS

8.3.1.3 O.NO_OBJECT_REUSE

TSF.SECURE_MANAGEMENT: Refers to the single-use authentication used to establish a secure management session.
TSF.USER_AUTHENTICATION: Refers to the single-use authentication used during recovery.

The Security Objectives completely satisfy the assumptions, threats and policies, and these objectives in turn are realized by implementing the SFRs. Each objective matches a threat, assumption or policy, or combination of these. There is no security objective that does not address a threat, assumption or policy, or combination of these.

Similarly, each SFR corresponds to one or more security objective and no SFR does not have a matching security objective. Similarly each security objective is matched by one or more SFR.

Sections 8.1 and 8.2 described how the threats, assumptions and policies are addressed by security objectives and how these objectives are met by the SFRs of the TSF. The assurance measures have been shown to match the requirements, and evaluation is required to demonstrate that the measures in fact match the requirements.

8.4 PP Claims Rationale

There are no PP claims made in this Security Target.

8.5 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL4+ assurance package and is based on good rigorous commercial development practices. This ST has been developed for a generalized environment.

The TOE is used to protect information assets and it is assumed that possible attackers will have a low attack potential. The Security Objectives for the TOE were derived to resist this class of attacker, and CC EAL4+ was found to be sufficient to provide the assurance for the environment.

9 Appendix A – Administrative Options

The following options are available from the McAfee Endpoint Encryption Manager to configure the secure attributes of the TOE.

Object	Category	Options
Machine	Context menu (right click on machine in machine tree)	1. Force sync 2. Reboot machine 3. Lock machine
	General	Boot protection is any one of: 1. Disable 2. Enable 3. Remove 4. Remove and reboot

Object	Category	Options
	General – Options – each option may be enabled or disabled.	Windows Logon • Require McAfee Endpoint Encryption logon (must be set) • Attempt automatic Windows logon • Requires McAfee Endpoint Encryption re-logon • Automatically logon as boot user • McAfee Endpoint Encryption logon component always active • Set McAfee Endpoint Encryption password to Windows password Virus protection • Enable MBR virus protection Miscellaneous • Do not display previous user name at logon • Disable Power Fail Protection during encryption • Allow configuration manager to be closed • Reject suspend/hibernate requests (Note: this option is not supported in Microsoft Windows Vista or later operating systems[1].) • Disable checking for Autoboot
	Encryption	Only full encryption is supported in CC mode. Recovery key size (64, 128, 192 or 256 bits)
	Synch - the following options may be enabled or disabled:	• Automatically resynchronise every *nn* minutes • Allow local resynchronisation • Resynchronise when RAS connection is detected • Synchronise time with database • Disable synchronisation of files • Allow remote controlled resynchronisation, address *nnn.nnn.nnn.nnn*, port *nnnn* • Disable access if not synchronised for *nn* days • Delay synch at boot for *nn* minutes plus random up to *nn* minutes
	Screen saver	Options The following options may be enabled or disabled: • Allow user access to the Windows screen saver options • Run screen saver if token is removed (if supported) • Set McAfee Endpoint Encryption screen saver as default • Allow logon of administrators greater than level *n* • Set screen saver inactivity timeout (minutes) *n*

Object	Category	Options
User	Context menu (right click on user in the user tree)	The following options are available: • Create User • Rename • Delete • Create Token • Reset Token • Reset Local Recovery • Set SSO details • Force password change at next logon • View Audit • Reset to Group Configuration • Create copy • Properties (brings up all of the other user options – below)
	General	User accounts are either enabled or disabled and can be enabled indefinitely or for a fixed calendar period (from a start date to an end date).
	Passwords	The following options may be enabled: Password change • Force change if ‘12345’ • Prevent change • Enable password history *nn* • Require change after *nn* days warn *nn* days before Incorrect passwords • Timeout password entry after three invalid attempts Maximum disable time *nn* minutes • Invalidate password after *nn* attempts
	Password templates	McAfee Endpoint Encryption enforces minimum and maximum password lengths: • Minimum length *nn* • Maximum length *nn* Password content enforcement may be enabled (each type of control is optional, and all may be employed if required): • Password must have a minimum of *n* alpha characters • Password must have a minimum of *n* numeric characters • Password must have a minimum of *n* alphanumeric characters • Password must have a minimum of *n* symbol characters Password content restrictions may be enabled (each type of control is optional, and all may be employed if required): • No anagrams • No sequences • No palindromes • No simple words • Can’t be user name • Windows content rules

Notes:

[1] The Microsoft Windows Vista and Windows 7 operating systems do not support hibernation.