Security Target

McAfee Enterprise Mobility Management 12.0

Document Version 1.16

September 24, 2014

Prepared For:

McAfee, Inc.

2821 Mission College Blvd.

Santa Clara, CA 95054

Prepared By:

Primasec Ltd

Le Domaine de Loustalviel

11420 Pech Luna, France

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the McAfee Enterprise Mobility Management 12.0. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1 Introduction

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

1.1 ST Reference

ST Title	Security Target: McAfee Enterprise Mobility Management 12.0
ST Revision	1.16
ST Publication Date	July 20, 2014
Author	Primasec

1.2 TOE Reference

TOE Reference	McAfee Enterprise Mobility Management 12.0
TOE Type	Mobile Security

1.3 Document Organization

This Security Target follows the following format:

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

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

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

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by *italicized* text.
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by underlined text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FIA_UAU.1.1 (1) and FIA_UAU.1.1 (2) refer to separate instances of the FIA_UAU.1 security functional requirement component.

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

1.5 Document Terminology

The following table describes the terms and acronyms used in this document:

TERM	DEFINITION
CC	Common Criteria version 3.1 (ISO/IEC 15408)
CPU	Central Processing Unit
DBMS	DataBase Management System
EAL	Evaluation Assurance Level
EMM	Enterprise Mobility Management
GUI	Graphical User Interface
I&A	Identification & Authentication
IIS	Internet Information Services
IP	Internet Protocol
IT	Information Technology
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
RAM	Random Access Memory
SF	Security Function

TERM	DEFINITION
SFP	Security Function Policy
SFR	Security Functional Requirement
SQL	Structured Query Language
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
VGA	Video Graphics Array

Table 2 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

The McAfee EMM platform provides secure management of mobile devices. McAfee EMM allows the integration of smart mobile devices into enterprise networks with the same level of security protection enabled on laptops and desktops. With McAfee EMM, System Administrators have the tools and capabilities needed to effectively secure mobile devices in the enterprise network, seamlessly manage them in a scalable architecture, and efficiently assist users when problems arise.

McAfee EMM is a web-based solution that helps manage the entire life cycle of the mobile device. McAfee EMM's combination of device management, network control and compliance reporting delivers a powerful mobile device security solution. Note that the scope of the TOE covers the management element only, and does not include software on the mobile devices themselves.

The following sections provide a summary of the specific TOE sub-components. Note that communication between the distributed components of the TOE is protected from disclosure and modification by cryptographic functionality provided by the operational environment.

1.6.1 McAfee EMM Hub

The McAfee EMM Hub component manages communication between components. The Hub allows secure communication across the firewall (between the DMZ and the internal network) and eliminates the need to open custom firewall ports. SSL communication is established between the components. The EMM Hub interacts with both ePO and the EMM database to extract details of policies for managed mobile devices.

1.6.2 McAfee EMM Portal

The McAfee Client Application (out of scope) connects to the EMM Portal to request the policy for the device. The McAfee EMM Portal (EMM Portal) allows device users to initiate wipe requests via a browser in the event their device is lost or stolen. This component should be installed in the DMZ.

1.6.3 McAfee EMM Proxy

The EMM Proxy is an IIS (Internet Information Services) application that controls access to enterprise resources on the DMZ server before reaching the internal network. The McAfee EMM Proxy proxies ActiveSync traffic between mobile device email clients and the internal email servers. This component should be installed in the DMZ.

1.6.4 McAfee EMM Push Notifier

The Push Notifier sends notifications to the managed mobile devices, prompting the device to connect back to the EMM Portal. This is done via the Apple and Google push notification services in the cloud. This component should be installed in the DMZ.

1.6.5 ePolicy Orchestrator

ePO provides the central management interface and functionality for the administrators of the TOE. It also provides reporting and policy storage capabilities, all through a single point of control. An extension to ePO provides EMM specific management features. Mobile ePO provides communication between ePO and the EMM Hub.

1.7 TOE Description

1.7.1 Physical Boundary

The TOE is a software TOE and includes the EMM Server components listed below executing on general purpose computing platforms:

a. McAfee EMM Hub
b. McAfee EMM Portal
c. McAfee EMM Proxy
d. McAfee EMM Push Notifier
e. McAfee ePO with EMM extension and MePO

Note specifically that the hardware, operating systems and third party support software (e.g. DBMS) on each of the systems are excluded from the TOE boundary.

The Portal, Proxy and Push Notifier can operate on a single platform in the DMZ. The Hub, ePO and database servers would normally be on separate platforms within the internal network.

In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	EMM Server Version 12.0.780.52882 McAfee ePO 5.1.0 build 509 with hotfixes 1, 960279-2, 962156 and 973112 McAfee EMM 12.0 build 12.0.0.1073 McAfee EMM help 12.0.0.022
Operational Environment	McAfee EMM App (iOS and Android devices) Version 4.9.1 McAfee EMM Secure Container (Android devices) App Version 2.3.93 Hardware specified in the following: • Table 4 – Management System Component Requirements • Table 5 – Supported Mobile Platforms

Table 3 – Evaluated Configuration for the TOE

The evaluated configuration consists of a single instance of the management system (comprised of the EMM Server, EMM Hub and EMM DMZ Server) and one or more instances of managed systems running the McAfee EMM Client App.

The following figure presents an example of an operational configuration.

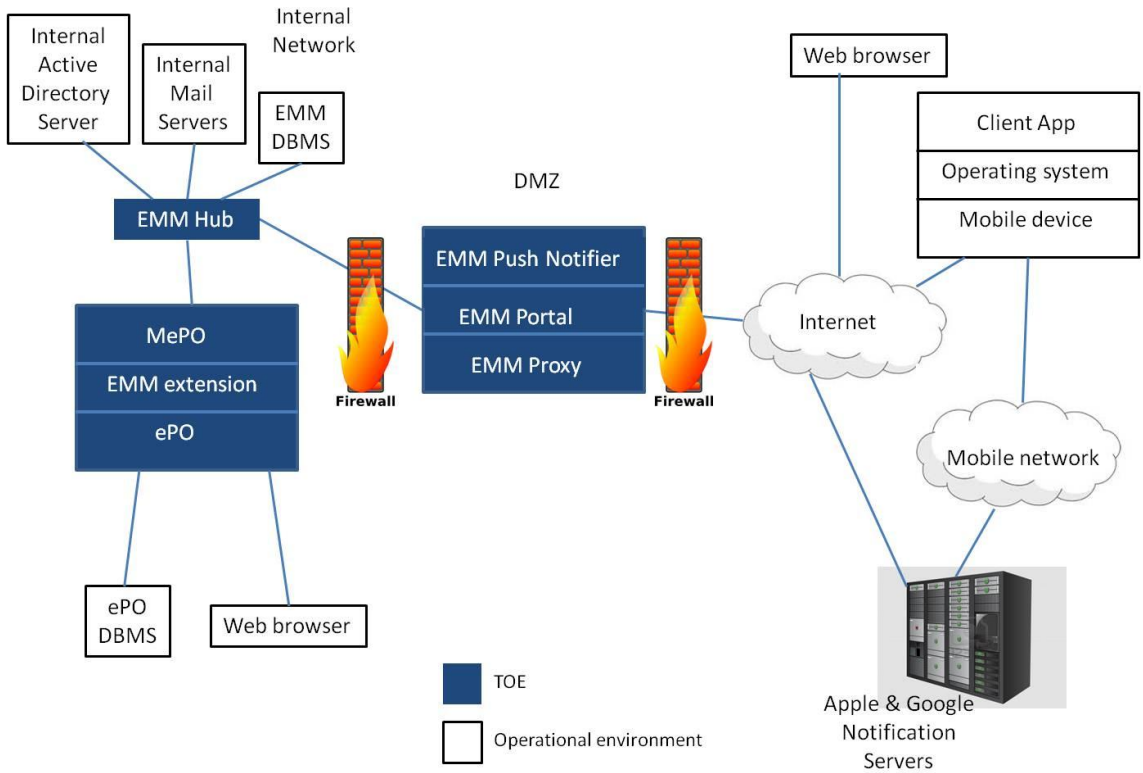

Figure 1 – TOE Boundary

1.7.2 Hardware and Software Supplied by the Operational Environment

The TOE is a software TOE. The hardware, operating systems and all third party support software (e.g., DBMS) on the systems on which the TOE executes are excluded from the TOE boundary.

The platforms on which the EMM Server software is installed must be dedicated to functioning as the management system. EMM Server operates as a distribution system and management system for a client-server architecture offering components for the server part of the architecture (not the clients). The TOE requires the following hardware and software configuration on these management platforms:

COMPONENT	MINIMUM REQUIREMENTS
Processor	Dual core CPU
Memory	4 GB RAM
Free Disk Space	1 GB
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	• Windows Server 2008 64-bit with Service Pack 2 (Standard or Enterprise Edition) • Windows Server 2008 R2 64-bit with Service Pack 1 (Standard or Enterprise Edition)
DBMS	• Microsoft SQL Server 2005 with Service Pack 3 or later (Enterprise, Standard, or Workgroup Edition) • Microsoft SQL Server 2008 R2 32- and 64-bit with Service Pack 1 or later (Enterprise, Standard, or Workgroup Edition)
Web Browser	• Internet Explorer 8.0 or later • Firefox 10.0 or later • Chrome 17 or later

Table 4 – Management System Component Requirements

The McAfee EMM Client App executes on one or more systems whose policy settings are to be audited and enforced by the operating system. The supported platforms are:

TYPE	PLATFORM
Apple iOS	iOS versions 5, 6 and 7
Google Android	Android versions 2.3 – 4.4

Table 5 – Supported Mobile Platforms

1.7.2.1 TOE Guidance Documentation

The following guidance documentation is provided as part of the TOE:

- *Product Guide: McAfee Enterprise Mobility Management® (McAfee EMM®) 12.0*
- *Installation Guide: McAfee Enterprise Mobility Management® (McAfee EMM®) 12.0*
- *Operational User Guidance and Preparative Procedures Supplement: McAfee Enterprise Mobility Management 12.0*
- *Installation Guide: McAfee ePolicy Orchestrator 5.1.0 Software*
- *Product Guide: McAfee ePolicy Orchestrator 5.1.0 Software*

1.7.3 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

TSF	DESCRIPTION
Identification and Authentication	On the management system, the TOE requires administrators to identify and authenticate themselves before accessing the ePO software. No action can be initiated before proper identification and authentication. Each TOE administrator has security attributes associated with their user account that define the functionality the user is allowed to perform. On the user portal, the TOE requires users to identify and authenticate themselves before accessing the Portal software. No action can be initiated before proper identification and authentication.
Management	The TOE's Management Security Function provides support functionality that enables users to configure and manage TOE components. Management of the TOE is performed via the ePO GUI. Management privileges are defined per-user.
Audit	The TOE's Audit Security Function provides auditing of management actions performed by administrators. Authorized users may review the audit records via ePO Audit.
Policy Management	The TOE pushes policies to managed systems (i.e., mobile devices). These policies dictate allowed features and functions and are specified by an administrator through an access control policy.

Table 6 – Logical Boundary Descriptions

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 4 (September 2012) Part 2 conformant and Part 3 conformant at Evaluation Assurance Level 2 and augmented by ALC_FLR.2 – Flaw Reporting Procedures.

2.2 Protection Profile Conformance Claim

The TOE does not claim conformance to a Protection Profile.

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organizational security policy statements or rules with which the TOE must comply.
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.COMDIS	An unauthorized person may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.COMINT	An unauthorized person may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.IMPCON	An unauthorized person may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.LOSSOF	An unauthorized person may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized person may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized person may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data
T.MOBILE_POLICY	An unauthorized person may access features or functions of managed systems that may compromise the security infrastructure.

Table 7 – Threats Addressed by the TOE

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The following Organizational Security Policies apply to the TOE:

POLICY	DESCRIPTION
P.ACCACT	Persons using the TOE shall be accountable for their actions within the TOE.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.DETECT	Event audit logs that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.INTEGRITY	Data collected and produced by the TOE shall be protected from modification.
P.MANAGE	The TOE shall only be managed by those authorized to do so.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

Table 8 – Organizational Security Policies

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to authorized persons.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PROTCT	The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.
A.PKI	A public key infrastructure is in place that allows the TOE to verify the authenticity of communications with a mail server.

Table 9 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ACCESS	The TOE must allow only authorized access to TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions on the management system.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users and administrators prior to allowing access to TOE functions and data.
O.INTEGRITY	The TOE must ensure the integrity of all System data.
O.MOBILE_POLICY	The TOE must create policy data that may be used by the environment to enforce the access to and features available within a controlled mobile device.

Table 10 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users and administrators in a manner which is consistent with IT security.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.INTEROP	The TOE must be interoperable with the managed systems it monitors.
OE.PERSON	Personnel working as authorized administrators must be carefully selected and trained for proper operation of the system.
OE.AUDIT_REVIEW	The Operational Environment must provide the capability for authorized administrators to review audit information generated by the TOE.
OE.CRYPTO	The Operational Environment must provide the cryptographic functionality and protocols required for the TOE to securely transfer information between the TOE and the TOE environment.
OE.DATABASE	Those responsible for the TOE must ensure that access to the database via mechanisms outside the TOE boundary (e.g., DBMS) is restricted to authorized administrators only.
OE.PROTECT	The Operational Environment will protect itself and the TOE from external interference or tampering.

OBJECTIVE	DESCRIPTION
OE.STORAGE	The Operational Environment will store TOE data in the database and retrieve it when directed by the TOE.
OE.TIME	The Operational Environment will provide reliable timestamps to the TOE
OE.MOBILE_ACCESS	The TOE environment will supply the resources required to enforce access to and features available within a controlled mobile device.
OE.PKI	The operational environment must provide a public key infrastructure that allows mail server digital certificates to be verified.

Table 11 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies (if applicable). The following table provides a high level mapping of coverage for each threat, assumption, and policy:

OBJECTIVE / THREAT / ASSUMPTION	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.INTEGRITY	O.MOBILE_POLICY	OE.PHYCAL	OE.CREDEN	OE.INSTALL	OE.INTEROP	OE.PERSON	OE.AUDIT_REVIEW	OE.CRYPTO	OE.DATABASE	OE.PROTECT	OE.STORAGE	OE.TIME	OE.MOBILE_ACCESS	OE.PKI
A.ACCESS										✓									
A.DATABASE														✓					
A.DYNMIC										✓	✓								
A.LOCATE							✓												
A.MANAGE											✓								
A.NOEVIL							✓	✓	✓		✓								
A.PROTCT							✓												
A.PKI																			✓
P.ACCACT		✓		✓								✓							
P.ACCESS	✓			✓										✓					
P.DETECT		✓															✓		
P.INTEGRITY					✓								✓			✓			
P.MANAGE	✓		✓	✓				✓	✓		✓								
P.PROTCT	✓						✓						✓		✓	✓			
T.COMDIS	✓			✓											✓				
T.COMINT	✓			✓	✓										✓				
T.IMPCON	✓		✓	✓					✓										
T.LOSSOF	✓			✓										✓		✓			
T.NOHALT	✓			✓															
T.PRIVIL	✓			✓															
T.MOBILE_POLICY						✓												✓	

Table 12 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

The following table provides detailed evidence of coverage for each threat, policy, and assumption:

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions. The OE.INTEROP objective ensures the TOE has the needed access.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to authorized persons. The OE.DATABASE objective ensures that access to any mechanisms outside the TOE boundary that may be used to access the database is configured by the administrators such that only authorized users may utilize the mechanisms.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors. The OE.INTEROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will be managed appropriately.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The OE.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The OE.INSTALL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data. The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. The OE.PHYCAL objective provides for the physical protection of the TOE hardware and software.
A.PKI	A public key infrastructure is in place that allows the TOE to verify the authenticity of communications with a mail server. The OE.PKI objective ensures that the required public key infrastructure is in place so that the TOE can verify that the mail server certificate is signed by a recognized third party.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
P.ACCACT	Persons using the TOE shall be accountable for their actions within the TOE. The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this policy by ensuring each user and administrator is uniquely identified and authenticated. The OE.AUDIT_REVIEW objective provides the ability for administrators to review the audit records generated by the TOE so that accountability for administrator actions can be determined.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes. The O.IDAUTH objective provides for identification and authentication of users and administrators prior to any TOE function accesses via the EMM console web interface. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.PERSON objective helps to ensure that authorized users and administrators know their duties and behave appropriately. The OE.DATABASE objective addresses this policy for mechanisms outside the TSC via Operational Environment protections of the system data trail and the database used to hold TOE data. The O.ACCESS objective addresses this policy for mechanisms inside the TSC via TOE protections of the system data trail.
P.DETECT	Event audit logs that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected. The O.AUDITS objectives address this policy by requiring collection of audit and policy audit data. The OE.TIME objective supports this policy by providing a time stamp for insertion into the system data records.
P.INTEGRITY	Data collected and produced by the TOE shall be protected from modification. The O.INTEGRITY objective ensures the protection of System data from modification. The OE.CRYPTO objective requires the Operational Environment to provide cryptographic functionality and protocols that can be used by the TOE to protect the data during transit. The OE.STORAGE objective requires the Operational Environment to provide storage and retrieval mechanisms for System data for use by the TOE.
P.MANAGE	The TOE shall only be managed by those authorized to do so. The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTALL objective supports the OE.PERSON objective by ensuring administrators follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for identification and authentication of users and administrators prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized access to TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. The O.ACCESS objective only allows permitted authorized access to TOE functions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports the TOE protection from the Operational Environment. The OE.CRYPTO objective requires the Operational Environment to provide cryptographic functionality and protocols that can be used by the TOE to protect the data during transit. The OE.STORAGE objective requires the Operational Environment to provide storage and retrieval mechanisms for System data for use by the TOE.
T.COMDIS	An unauthorized person may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The OE.PROTECT objective supports the TOE protection from the Operational Environment.
T.COMINT	An unauthorized person may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized access to TOE data. The O.INTEGRITY objective ensures no System data will be modified. The OE.PROTECT objective supports the TOE protection from the Operational Environment.
T.MOBILE_POLICY	An unauthorized person may access features or functions of managed systems that may compromise the security infrastructure. The O.MOBILE_POLICY objective ensures that the appropriate policy is available to the environment where it may be enforced in accordance with OE.MOBILE_ACCESS.
T.IMPCON	An unauthorized person may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. The OE.INSTALL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized access to TOE functions.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.LOSSOF	An unauthorized person may attempt to remove or destroy data collected and produced by the TOE. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized access to TOE data. The OE.STORAGE ensures all system data will be stored in the database, while OE.DATABASE objective ensures no System data will be deleted from the database.
T.NOHALT	An unauthorized person may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized access to TOE functions.
T.PRIVIL	An unauthorized person may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. The O.IDAUTH objective provides for identification and authentication of users and administrators prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized access to TOE functions.

Table 13 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

This Security Target does not include any extended components.

6 Security Requirements

The security requirements that are levied on the TOE and the Operational Environment are specified in this section of the ST.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and those that were explicitly stated, all of which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
User Data Protection	FDP_ACC.1	Subset Access Control
	FDP_ACF.1	Security Attribute Based Access Control
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing of Identification
Security Management	FMT_MTD.1	Management of TSF Data
	FMT_MSA.3	Static Attribute Initialization
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles

Table 14 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

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

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

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

c) *The events identified in the following table*

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, *the information detailed in the following table*.

Application Note: The auditable events for the (not specified) level of auditing are included in the following table:

COMPONENT	EVENT	DETAILS
FAU_GEN.1	Start-up and shutdown of audit functions	
FDP_ACC.1	None	
FIA_ATD.1	All changes to TSF data related to ePO users (including passwords) result in an audit record being generated.	
FIA_UAU.1	All use of the user authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMF.1	Use of the management functions.	User identity, function used
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Table 15 – Audit Events and Details

6.1.1.2 FAU_GEN.2 User Identity Association

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

6.1.2 User Data Protection (FDP)

6.1.2.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the *iOS Mobile Access Control SFP and the Android Mobile Access Control SFP* on

Subjects: Client applications running on mobile devices registered with the server

Objects: Features on mobile devices

Operations: allow, block.

6.1.2.2 FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the *iOS Mobile Access Control SFP and the Android Mobile Access Control SFP* to objects based on the following:

Subjects: Client applications running on mobile devices registered with the server

Subject security attributes: Associated Policy

Objects: Features on mobile devices

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

The TSF provides a policy which enforces the operation (allow, block) on the client application attempting to access the mobile device feature.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *no additional rules*.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the *following explicit denial rules:*

Deny access to all features if the lock policy is set;

Wipe corporate data if the wipe corporate data policy is set;

Wipe the device if the wipe policy is set.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 User Attribute Definition

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

a) *Global Administrator & administrator-defined roles: User name, Role/permission set.*

b) *EMM Portal User: User name, locked status*

6.1.3.2 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow *no actions* on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.3 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow *no actions* on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to *perform the operation specified in the table below* the *data described in the table below* to *the role(s) specified in table below:*

TSF DATA	OPERATION	AUTHORIZED ROLES
Admin Account Attributes	Query, Modify, Delete	Global Administrator

TSF DATA	OPERATION	AUTHORIZED ROLES
Policy Configurations	Query	Global Administrator, administrator-defined roles with "McAfee Enterprise Mobility – Policies: View settings"
	Modify, Delete	Global Administrator, administrator-defined roles with "McAfee Enterprise Mobility – Policies: View and change settings"
Managed Device Actions	Execute Wipe Corporate Data	Global Administrator, administrator-defined roles with "Mobile Actions: Allow Wipe Corporate Data"
	Execute Locking devices	Global Administrator, administrator-defined roles with "Mobile Actions: Allow Locking devices"
	Execute Unlocking devices	Global Administrator, administrator-defined roles with "Mobile Actions: Allow Unlocking devices"
	Execute MDM Uninstall	Global Administrator, administrator-defined roles with "Mobile Actions: Allow uninstall"
	Execute Lock users	Global Administrator, administrator-defined roles with "Mobile Actions: Allow locking users"
	Execute Wipe	Global Administrator, administrator-defined roles with "Mobile Actions: Allow Wipe" EMM Portal user
Compliance Reports	Query	Global Administrator, administrator-defined roles with "Use public dashboards"

Table 16 – TSF Data Access Permissions

6.1.4.2 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the *iOS Mobile Access Control SFP and Android Mobile Access Control SFP* to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *System Administrator* to specify alternative initial values to override the default values when an object or information is created.

6.1.4.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

a) Manage administrator Accounts

b) Manage EMM portal user accounts

c) Set access policies for, and perform actions on, managed devices

d) Review policy compliance reports[1].

6.1.4.4 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles: *Global Administrator, administrator-defined roles, EMM Portal user*.

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

6.2 Security Assurance Requirements

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

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
ATE: Tests	ATE_COV.1	Evidence of Coverage

[1] Reports on the compliance of mobile devices with assigned policies.

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing – Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 17 – Security Assurance Requirements at EAL2

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN.1	No other components	FPT_STM.1	Satisfied by OE.TIME in the environment
FAU_GEN.2	No other components	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied
FDP_ACC.1	No other components	FDP_ACF.1	Satisfied by FDP_ACF.1
FDP_ACF.1	No other components	FDP_ACC.1 FMT_MSA.3	Satisfied by FDP_ACC.1
FIA_ATD.1	No other components	None	n/a
FIA_UID.1	No other components	None	n/a
FIA_UAU.1	No other components.	FIA_UID.1	Satisfied
FMT_MSA.3	No other components	FMT_MSA.1 FMT_SMR.1	Not Satisfied[2] Satisfied
FMT_MTD.1	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components	None	n/a
FMT_SMR.1	No other components	FIA_UID.1	Satisfied

Table 18 – TOE SFR Dependency Rationale

6.4 Security Requirements Rationale

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

[2]This dependency is not applicable because the iOS Mobile Access Control SFP and the Android Mobile Access Control SFP do not allow access to security attributes in order to change them. The TOE provides default policy settings for security attributes, but these SFPs do not permit any action on security attributes.

6.4.1 Security Functional Requirements for the TOE

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

SFR \ OBJECTIVE	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.INTEGRITY	O.MOBILE_POLICY
FAU_GEN.1		✓				
FAU_GEN.2		✓				
FDP_ACC.1						✓
FDP_ACF.1						✓
FIA_ATD.1				✓		
FIA_UID.1	✓			✓		
FIA_UAU.1	✓			✓		
FMT_MTD.1	✓		✓		✓	
FMT_MSA.3	✓					✓
FMT_SMF.1	✓		✓			
FMT_SMR.1	✓		✓			

Table 19 – Mapping of TOE SFRs to Security Objectives

The following table provides detailed evidence of coverage for each security objective:

OBJECTIVE	RATIONALE
O.ACCESS	The TOE must allow only authorized access to TOE functions and data. Access to the TOEis determined using an identification and authentication process (FIA_UID.1 and FIA_UAU.1) at either ePO or the EMM portal. The permitted access to TOE data and functions by authorized administrators at ePO is determined by the defined roles and permissions (FMT_MTD.1, FMT_SMF.1, FMT_SMR.1). The permitted access to TOE data and functions by EMM Portal users is determined by the assigned user access policy.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions. Security-relevant events must be defined and auditable for the TOE (FAU_GEN.1). The user associated with the events must be recorded (FAU_GEN.2).
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The functions and roles required for effective management are defined (FMT_SMF.1, FMT_SMR.1), and the specific access privileges for the roles and permissions is enforced (FMT_MTD.1).

OBJECTIVE	RATIONALE
O.IDAUTH	The TOE must be able to identify and authenticate users and administrators prior to allowing access to TOE functions and data. Security attributes of subjects used to enforce the security policy of the TOE must be defined (FIA_ATD.1). Users authorized to access the TOE are determined using an identification and authentication process (FIA_UID.1 and FIA_UAU.1).
O.INTEGRITY	The TOE must ensure the integrity of all System data. Only authorized administrators of the System may query or add System data (FMT_MTD.1).
O.MOBILE_POLICY	The TOE must create policy data that may be used by the environment to enforce the access to and features available within a controlled mobile device. The TOE shall create policies that are used by the environment to enforce access to and features available within a controlled mobile device. (FDP_ACC.1, FDP_ACF.1). The default values of security attributes are restrictive in nature (FMT_MSA.3).

Table 20 – Rationale for Mapping of TOE SFRs to Objectives

6.4.2 Security Assurance Requirements

This section identifies the Lifecycle , Development, Test, and Guidance measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Architecture Description: McAfee Enterprise Mobility Management 12.0
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: McAfee Enterprise Mobility Management 12.0
ADV_TDS.1: Basic Design	Basic Design: McAfee Enterprise Mobility Management 12.0
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: McAfee Enterprise Mobility Management 12.0
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: McAfee Enterprise Mobility Management 12.0
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: McAfee Enterprise Mobility Management 12.0
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: McAfee Enterprise Mobility Management 12.0
ALC_DEL.1: Delivery Procedures	Delivery Procedures: McAfee Enterprise Mobility Management 12.0
ALC_FLR.2: Flaw Reporting	Flaw Reporting: McAfee Enterprise Mobility Management 12.0
ATE_COV.1: Evidence of Coverage	Security Testing: McAfee Enterprise Mobility Management 12.0

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ATE_FUN.1: Functional Testing	Security Testing: McAfee Enterprise Mobility Management 12.0
ATE_IND.2: Independent Testing – Sample	Security Testing: McAfee Enterprise Mobility Management 12.0

Table 21 – Security Assurance Measures

6.4.2.1 Rationale for TOE Assurance Requirements Selection

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

The general level of assurance for the TOE is:

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

6.5 TOE Summary Specification Rationale

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE's Security Functions and the SFRs and the rationale.

TSF / SFR	Policy Management	Identification and Authentication	Management	Audit
FAU_GEN.1				✓
FAU_GEN.2				✓
FDP_ACC.1	✓			
FDP_ACF.1	✓			
FIA_ATD.1			✓	
FIA_UID.1		✓		

TSF / SFR	Policy Management	Identification and Authentication	Management	Audit
FIA_UAU.1		✓		
FMT_MSA.3			✓	
FMT_MTD.1			✓	
FMT_SMF.1			✓	
FMT_SMR.1			✓	

Table 22 – SFR to TOE Security Functions Mapping

SFR	SECURITY FUNCTION AND RATIONALE
FAU_GEN.1	**Audit –** User actions area audited according to the events specified in the table with the SFR.
FAU_GEN.2	**Audit –** The audit log records include the associated user name when applicable.
FDP_ACC.1	**Policy Management** – The TOE implements policy-based access control to restrict actions available on managed devices.
FDP_ACF.1	**Policy Management** – The TOE implements policy-based access control to restrict actions available on managed devices.
FIA_ATD.1	**Management** – User security attributes are associated with the administrative user/EMM Portal user upon successful login.
FIA_UID.1	**Identification and Authentication** – The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface. No action at either ePO or EMM portal can be initiated before proper identification and authentication.
FIA_UAU.1	**Identification and Authentication** – The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface. No action at either ePO or EMM portal can be initiated before proper identification and authentication.
FMT_MSA.3	**Management** – The TOE ensures the default values of security attributes are permissive in nature.
FMT_MTD.1	**Management** – The Systems Administrator and user permissions determine the access privileges of the user to TOE data.
FMT_SMF.1	**Management** – The management functions that must be provided for effective management of the TOE are defined and described.

SFR	SECURITY FUNCTION AND RATIONALE
FMT_SMR.1	**Management** – The TOE provides the roles specified in the SFR. When an administrator account is created or modified on ePO, the role is specified by setting or clearing the appropriate permission sets for the user. EMM portal accounts are created by synchronisation with the LDAP server to import the available mailbox accounts. The permissions associated with the account are then configured through the access control policy.

Table 23 – SFR to TSF Rationale

7 TOE Summary Specification

7.1 Policy Management

The TOE allows policies to be defined through the management interface provided by ePO and the EMM extension. These policies are then distributed to mobile devices for compliance to network security and usage restrictions. The access control policies determine whether user access to the mobile device feature is allowed or blocked. Each device type (i.e. iOS or Android) offers different features to the user, and so each policy is based on device type. Policies include settings for allowing or blocking the mobile user's permission to synchronize corporate data.

The following two tables show parameters contained in the device-dependent policies and actions.

CATEGORY	DESCRIPTION	OPTIONS	IOS	ANDROID
Mail and Compliance	General compliance	Block mail sync for all devices assigned this policy / Determine mail sync availability based on selected options	X	X
	Configuration	Configure an ActiveSync account	X	X
		Direct traffic through an EMM Proxy server	X	X
		ActiveSync endpoint	X	X
		McAfee VMS		X
		App protection		X
		Check jailbroken status at intervals (hours)	X	
		If ignored, number of notifications to resend	X	
		Notification resend interval	X	
	Compliance actions	Unencrypted devices	X	X
		Jailbroken/rooted devices	X	X
		Devices with unverified jailbreak status	X	
		Devices with blacklisted apps	X	X
		Devices running iOS versions earlier than	X	
		Devices that don't use McAfee Secure Container		X
		Devices that don't use McAfee VMS		X
		Devices overdue for McAfee VMS scan		X
		Devices overdue for McAfee VMS update		X
		Devices with malware		X
		Devices with malicious apps		X
		Devices with suspicious apps		X
Passcode (Passcode and Restrictions for Android	Power-on passcode	Require passcode to access the device	X	X
		Allow sequential or repeat characters	X	
		Maximum number of characters	X	X
		Alphanumeric with minimum number of special characters	X	X
		Lock the device after minutes of inactivity	X	X
		Remember previous passcodes	X	X
		Require a new passcode after number of days	X	X
		Wipe the device after failed passcode attempts	X	X

CATEGORY	DESCRIPTION	OPTIONS	IOS	ANDROID
	Secure Container Passcode	Require passcode to access the McAfee Secure Container		X
		Allow sequential or repeat characters		X
		Maximum number of characters		X
		Alphanumeric with minimum number of special characters		X
		Lock McAfee Secure Container after minutes of inactivity		X
		Remember previous passcodes		X
		Require a new passcode after number of days		X
		Wipe McAfee Secure Container after failed passcode attempts		X
	Restrictions(Android)	Block camera (Android v4 and later)		X
		Restrict untrusted TLS certificates		X
		Allow McAfee Secure Container to sync while roaming		X
		Allow opening attachments from McAfee Secure Container in other programs		X
Restrictions	Restrictions	iTunes explicit content	X	
		YouTube (iOS 5 only)	X	
		iTunes	X	
		Camera	X	
		Allow FaceTime	X	
		Screen capture	X	
		Automatic sync while roaming	X	
		In-App purchases	X	
		Multiplayer gaming	X	
		Voice dialing	X	
		Installing iTunes applications	X	
		Safari	X	
		Safari – Allow autofill	X	
		Safari – Display fraud warnings	X	
		Safari – Allow Javascript	X	
		Safari – Block pop-ups	X	
		Safari – Allow cookies	X	
	IOS 5 and later restrictions	iTunes store access without password	X	
		iCloud backup	X	
		iCloud document synch	X	
		iCloud key-value sync	X	
		Photo stream	X	
		Untrusted TLS certificates	X	
		Siri (voice assistant)	X	
		Allow Siri when device is locked	X	
		Sending diagnostic data	X	
		Moving, forwarding or replying to corporate email using other email accounts	X	
		Sending corporate email from third party apps	X	
	IOS 6 and later restrictions	Passbook when device is locked	X	
		Shared photo stream	X	

CATEGORY	DESCRIPTION	OPTIONS	IOS	ANDROID
	IOS 7 restrictions	Opening documents from managed apps and accounts in unmanaged apps and accounts	X	
		Opening documents from unmanaged apps and accounts in managed apps and accounts	X	
	Roaming restrictions	Roaming	X	
		Voice roaming	X	
		Data roaming	X	
Certificates	Client certificates	Add/delete	X	
	Server certificates	Add/delete	X	
VPN	VPN profiles	Add/delete/modify	X	
Wi-Fi	Wi-Fi profiles	Add/delete/modify	X	X
APN	APN settings	Use custom carrier APN	X	
		Name	X	
		User name	X	
		Password	X	
		Proxy server	X	
		Proxy port	X	
Supervised Devices	App lock (iOS 6 and later)	Enable app lock	X	
		App identifier	X	
		Device rotation	X	
		Auto-lock	X	
	Restrictions	Game Center	X	
		iBooks	X	
		iBooks adult content	X	
		Installing certificates or configuration profiles	X	
	HTTP proxy	Redirect traffic through an HTTP proxy server	X	
Web clips	Web clips	Add/delete	X	
Blacklist	Application list	Add/delete blacklisted apps	X	X
Whitelist	Application list	Add/delete whitelisted apps	X	X
Single sign-on	Single sign-on profiles	Add/delete/modify single sign-on profiles	X	

Table 24 – Device policy configuration options

The following actions are available for the authorized administrator to initiate through ePO.

	IOS	ANDROID
Lock	X	X
MDM uninstall	X	X
Unlock	X	X
Wipe	X	X
Wipe corporate data	X	X

Table 25 – Device action configuration options

In addition, the EMM Portal user is able to initiate a “Wipe device” action through the EMM portal.

7.2 Identification and Authentication

The TOE has the ability to authenticate all management users locally using a password. All users must enter a username and password into ePO, which is validated by the TOE against the user authentication information stored by the TOE. If the authentication succeeds, the user receives a session token that is used for identification of subsequent requests during that session. If not, the login process is terminated and the login GUI is redisplayed.

The TOE has the ability to identify and authenticate all EMM portal users using the user’s email address and password, which is verified by the LDAP server. If the LDAP server reports successful verification of the identification and authentication credentials, the user receives a session token that is used for identification of subsequent requests during that session. If not, the login process is terminated and the login GUI is redisplayed.

7.3 Management

The TOE provides support functionality that enables an authorized administrator to configure and manage TOE components. Management of the TOE is performed via the ePO GUI.

The TOE allows an authorized administrator to create, manage, and publish security policies. Available functions for administration of access policies include:

- Select device settings
- Assign policies to groups
- Reorder Policies
- Set device resource restrictions

Once the authorized administrator defines one or more security policies, those policies are assigned to devices, users and or groups via ePO.

The TOE provides functionality to allow authorized administrators to determine the security policy conformance of the mobile user community. ePO ensures the default values of security attributes are permissive in nature, enforcing the iOS Mobile Access Control SFP and Android Mobile Access Control SFP for the TOE. For example, the Starter Policy for iOS Mobile Access Control SFP will be default allow access to devices that are jailbroken.

The TOE provides functionality to allow authorized administrators to review compliance reports in ePO. The summary reports indicate which managed devices comply with the configured access policies and which do not. The detailed reports indicate the areas of compliance/non-compliance for a particular device.

The TOE provides functionality to allow authorized administrators to unlock EMM portal user accounts, which have become locked during attempts to configure a mobile device.

The table below demonstrates the roles available and the operations each role can perform on TSF data:

AUTHORIZED ROLES[3]	TSF DATA	OPERATION
Global Administrator	Admin Account Attributes	Query, Modify, Delete
Global Administrator, administrator-defined roles with "Mobile Actions: Allow unlocking users"	Unlock users	Execute
Global Administrator, administrator-defined roles with "McAfee Enterprise Mobility – Policies: View settings"	Policy Configurations	Query
Global Administrator, administrator-defined roles with "McAfee Enterprise Mobility – Policies: View and change settings"	Policy Configurations	Modify, Delete
Global Administrator, administrator-defined roles with "Mobile Actions: Allow Wipe Corporate Data"	Wipe Corporate Data	Execute
Global Administrator, administrator-defined roles with "Mobile Actions: Allow Locking devices"	Locking devices	Execute
Global Administrator, administrator-defined roles with "Mobile Actions: Allow Unlocking devices"	Unlocking devices	Execute
Global Administrator, administrator-defined roles with "Mobile Actions: Allow uninstall"	MDM Uninstall	Execute

[3] Global administrator is able to perform all operations.

AUTHORIZED ROLES[3]	TSF DATA	OPERATION
Global Administrator, administrator-defined roles with "Mobile Actions: Allow Wipe" EMM Portal user	Wipe	Execute
Global Administrator, administrator-defined roles with "Use public dashboards"	Compliance Reports	Query

Table 26 – Data Access Permissions

ePO management permissions are defined per authorized administrator . Global Administrator status to an ePO account implicitly grants all permissions to that authorized administrator. Upon successful authentication the administrator permissions remain fixed for the duration of the session (until the administrator logs off).

The TOE provides functionality to manage the following:

1. **ePO User Accounts** - Each authorized administrator for login to ePO must be defined with ePO (only administrative users are able to log in to ePO). Only Global Administrators may perform ePO user account management functions (create, view, modify and delete).
2. **Permission Sets** - A permission set is a group of permissions that can be granted to any authorized administrator by assigning it to those authorized administrators' accounts. One or more permission sets can be assigned to any authorized administrator who are not Global Administrators (Global Administrators have all permissions to all products and features). Global Administrators may create, view, modify and delete permission sets.
3. **Notifications** - Notifications sent by ePO may be specified in response to events generated by the TOE. Notifications cause email messages to be sent to the configured recipient(s) or SNMP traps to be generated.
4. **System tree** - The system tree organizes managed systems in units for monitoring, assigning policies, scheduling tasks, and taking actions. The system tree is a hierarchical structure that allows systems to be organized within units called groups.
5. **Queries** - Authorized administrators may create, view, modify, use and delete queries based upon their permissions.
6. **Dashboards** - Authorized administrator-specific dashboards (including EMM compliance reports) may be configured to display data of interest to each administrator. These chart-based displays are updated at a configured rate to keep the information current.
7. **EMM policies** - EMM policies are configured on ePO. The policies determine what operations can be performed on each managed mobile device.
8. **Mobile Actions** – EMM actions to control access to mobile devices and protect corporate dates with targeted wipe functions can be initiated from ePO, and the wipe action can additionally be initiated from the Portal UI.

9. **Deployment of policies** - Policies can be deployed from ePO to a managed mobile device, including the ability to wipe and lock a device.

7.4 Audit

The TOE maintains an audit log for ePO-based actions. The auditable events are specified in the Audit Events and Details table in the FAU_GEN.1 section. Fields available include:

- Action — The name of the action the McAfee EMM authorized administrator attempted.
- Completion Time — The time the action finished.
- Details — More information about the action.
- Priority — Importance of the action.
- Start Time — The time the action was initiated.
- Success — Whether the action was successfully completed.
- User Name —Name of the logged-on administrator account that was used to take the action.