Security Target

McAfee Enterprise Mobility Management 9.7

Document Version 0.9

July 5, 2012

Prepared For:

McAfee, Inc.

2821 Mission College Blvd.

Santa Clara, CA 95054

www.mcafee.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Enterprise Mobility Management 9.7. 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 9.7
ST Revision	0.9
ST Publication Date	July 5, 2012
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	McAfee Enterprise Mobility Management 9.7
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
AD	Active Directory
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
MAC	Media Access Control
MDAC	Microsoft Data Access Components

TERM	DEFINITION
NTFS	New Technology File System
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
RAM	Random Access Memory
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength Of Function
SP	Service Pack
SQL	Structured Query Language
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
VGA	Video Graphics Array
XML	eXtensible Markup Language

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 to integration of smartphones 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 unique combination of device management, on-device security, network control, and compliance reporting delivers a powerful mobile device security solution.

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 (Hub) manages communications between McAfee EMM components. The McAfee EMM Hub allows secure communications between McAfee EMM modules across the firewall (between the DMZ and the internal network) and eliminates the need to open custom firewall ports. SSL

communications may be established between the components. Using a custom installation, the Hub can also communicate with the DMZ components via HTTP (non-secure).

1.6.2 McAfee EMM Console

The McAfee EMM Console (Console) is the application used to manage the McAfee EMM system and devices. It is an IIS application accessible via Internet Explorer or Firefox web browsers, with Microsoft Silverlight installed. Through the Console, administrative users configure system settings, change policies, manage devices and users, administer McAfee EMM roles, perform Helpdesk functions, and view reports.

1.6.3 McAfee EMM Portal

The McAfee EMM Portal (EMM Portal) allows device users to initiate requests for software downloads and to perform a few Helpdesk functions. The McAfee EMM Portal is an IIS application. Users access the EMM Portal from a browser on a PC or on a mobile device.

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 the same system:

a. McAfee EMM Hub including Cert Enroll
b. McAfee EMM Console
c. McAfee EMM Portal

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.

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

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	McAfee EMM 9.7.0.38202
IT Environment	McAfee iOS Client App Version 4.6 McAfee Android Client App Version 2.1 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 and one or more instances of managed systems running the McAfee EMM Client App.

The following figure presents an example of an operational configuration. The shaded elements in the boxes at the top of the figure represent the TOE components.

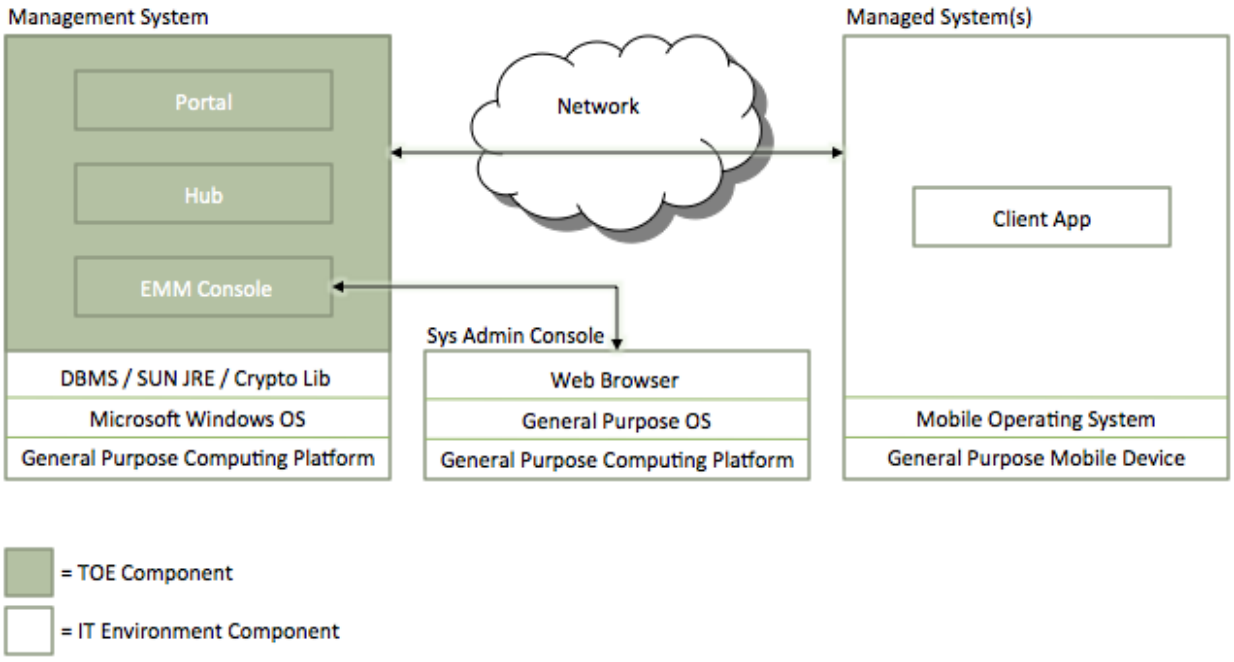

Figure 1 – TOE Boundary

1.7.2 Hardware and Software Supplied by the IT 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 platform 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 this management platform platform:

COMPONENT	MINIMUM REQUIREMENTS
Processor	Intel Pentium III-class or higher; 1GHz or higher
Memory	1 GB RAM
Free Disk Space	1 GB
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	Windows Server 2003 x86 or 64 bit Windows Server 2008 64 bit (Standard or Enterprise Versions) Windows Server 2008 R2 64 bit
DBMS	Microsoft SQL Server 2005 Microsoft SQL Server 2008

COMPONENT	MINIMUM REQUIREMENTS
Additional Software	Internet Explorer Firefox (Microsoft Silverlight must be installed on either browser)
Network Card	Ethernet, 100Mb or higher
Disk Partition Formats	NTFS
Domain Controllers	The system must have a trust relationship with the Primary Domain Controller (PDC) on the network

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 version 4 and 5
Google Android	Android version 2 and version 3

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®) 9.7*
- *Installation Guide: McAfee Enterprise Mobility Management® (McAfee EMM®) 9.6*[1]
- *Operational User Guidance and Preparative Procedures Supplement: McAfee Enterprise Mobility Management 9.7*

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 users to identify and authenticate themselves before accessing the TOE software. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with their user account that define the functionality the user is allowed to perform.
Management	The TOE's Management Security Function provides support functionality that enables users to configure and manage TOE components. Management of the TOE may be performed via the GUI. Management privileges are defined per-user.

[1] Note that the steps for installation of version 9.7 are the same as version 9.6; as such, no updated guide was developed.

TSF	DESCRIPTION
Audit	The TOE's Audit Security Function provides auditing of management actions performed by administrators. Authorized users may review the audit records via EMM Console.
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

1.8 Rationale for Non-bypassability and Separation of the TOE

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

The TOE ensures that the security policy is applied and succeeds before further processing is permitted whenever a security relevant interface is invoked: the interfaces are well defined and insure that the access restrictions are enforced. Non-security relevant interfaces do not interact with the security functionality of the TOE. The TOE depends upon OS mechanisms to protect TSF data such that it can only be accessed via the TOE. The system(s) on which TOE components execute is dedicated to that purpose.

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

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

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) 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 user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data
T.MOBILE_POLICY	An unauthorized user 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

POLICY	DESCRIPTION
P.ACCACT	Users of 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	Static configuration information 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 authorized users.
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.ASCOPE	The TOE is appropriately scalable to the IT Systems the TOE monitors.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.
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 hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

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 authorized users to access only authorized 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.AUDIT_PROTECT	The TOE will provide the capability to protect audit information generated by the TOE.
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 prior to allowing access to TOE functions and data on the management system.
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 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 is interoperable with the managed systems it monitors
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.AUDIT_PROTECT	The IT Environment will provide the capability to protect audit information generated by the TOE via mechanisms outside the TSC.
OE.AUDIT_REVIEW	The IT Environment will provide the capability for authorized administrators to review audit information generated by the TOE.
OE.CRYPTO	The IT Environment will provide the cryptographic functionality and protocols required for the TOE to securely transfer information between the TOE and the TOE environment.

OBJECTIVE	DESCRIPTION
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 users only.
OE.PROTECT	The IT environment will protect itself and the TOE from external interference or tampering.
OE.SD_PROTECTION	The IT Environment will provide the capability to protect system data via mechanisms outside the TSC.
OE.STORAGE	The IT Environment will store TOE data in the database and retrieve it when directed by the TOE.
OE.TIME	The IT 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.

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.EADMIN	O.ACCESS	O.IDAUTH	O.INTEGRITY	OE.INSTALL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTEROP	O.AUDITS	O.AUDIT_PROTECT	O.MOBILE_POLICY	OE.TIME	OE.PROTECT	OE.SD_PROTECTION	OE.DATABASE	OE.MOBILE_ACCESS	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW	OE.CRYPTO	OE.STORAGE
A.ACCESS									✓												
A.ASCOPE									✓												
A.DATABASE																✓					
A.DYNMIC								✓	✓												
A.LOCATE						✓															
A.MANAGE								✓													
A.NOEVIL					✓	✓	✓	✓													
A.PROTCT						✓															
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.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors. The OE.INTEROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users. 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 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 provides for the physical protection of the TOE hardware and software.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
P.ACCACT	Users of 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 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 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.SD_PROTECTION and OE.DATABASE objectives counter this threat for mechanisms outside the TSC via IT Environment protections of the system data trail and the database used to hold TOE data. The O.SD_PROTECTION and O.ACCESS objectives counter this threat for mechanisms inside the TSC via TOE protections of the system data trail and the database used to hold TOE data.
P.DETECT	Static configuration information 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 O.AUDIT_PROTECT and OE.AUDIT_PROTECT objectives ensure the integrity of audit records in the database generated by the TOE using access mechanisms inside and outside the TSC respectively. The OE.CRYPTO objective requires the IT 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 IT Environment to provide storage and retrieval mechanisms for System data for use by the TOE.
P.MANAGE	The TOE shall only be managed by authorized users. 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 administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access 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 OE.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports the TOE protection from the IT Environment. The OE.CRYPTO objective requires the IT 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 IT Environment to provide storage and retrieval mechanisms for System data for use by the TOE.
T.COMDIS	An unauthorized user 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 IT Environment.
T.COMINT	An unauthorized user 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 users to access TOE data. The O.INTEGRITY objective ensures no System data will be modified. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.MOBILE_POLICY	An authorized user 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 user 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 users to access TOE functions.
T.LOSSOF	An unauthorized user 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 users to access TOE data. The O.INTEGRITY objective ensures no System data will be deleted.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.NOHALT	An unauthorized user 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 users to access TOE functions.
T.PRIVIL	An unauthorized user 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 prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access 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 IT 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
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_STG.1	Protected Audit Trail Storage
User Data Protection	FDP_ACC.1(1) and FDP_ACC.1(2)	Subset Access Control
	FDP_ACF.1(1) and FDP_ACF.1(2)	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	
FAU_GEN.1	Access to the TOE and System data	Object IDs, Requested access
FAU_SAR.1	Reading of information from the audit records.	
FDP_ACF.1(1)	All decisions on policy management.	The presumed addresses of the source and destination subject.
FDP_ACF.1(2)	All decisions on policy management.	The presumed addresses of the source and destination subject.
FAU_SAR.2	Note: Unsuccessful attempts to read information from the audit records do not occur because the TOE does not present that capability to users that are not authorized to read the audit records.	
FIA_ATD.1	All changes to TSF data (including passwords) result in an audit record being generated. Note that passwords are not configured, so no audit records for rejection of a tested secret will be 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.

6.1.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *authorized users* with the capability to read *all information* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.5 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the audit records in the audit trail.

6.1.2 User Data Protection (FDP)

6.1.2.1 FDP_ACC.1(1) Subset Access Control

FDP_ACC.1.1(1) The TSF shall enforce the *iOS Mobile Access Control SFP* on

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

Objects: Features on mobile devices

Operations: allow, block, determine.

6.1.2.2 FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1(1) The TSF shall enforce the *iOS 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:

- *User Password for Login*
- *Password Length*
- *Password Expiration*
- *Require Alpha Numeric Password*
- *Password History*
- *Password Delay/Inactivity Timer*
- *Password Failure Action*

Allow Simple Password

Restrict iTunes

Restrict explicit content on iTunes

Remove YouTube App from home tiles

Restrict Use of Browser

Restrict Camera

Restrict Screen Capture

Restrict Automatic Sync While Roaming

Restrict In App Purchases

Restrict Multiplayer Gaming

Restrict Voice Dialing

Restrict Installing Applications

Allow Hands Free

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

If the mobile device has a valid policy and the policy contains an allow operation for the respective object.

FDP_ACF.1.3(1) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *no additional rules*.

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the *no additional explicit denial rules*.

6.1.2.3 FDP_ACC.1(2) Subset Access Control

FDP_ACC.1.1(2) The TSF shall enforce 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, determine

6.1.2.4 FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1(2) The TSF shall enforce 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:

Prompt user to enter a password when they login to the device

The minimum length in characters of the power-on passwords.

Require alpha and/or numeric characters in password.

Inactivity Timer

Monitor incorrect passwords and wipe the device upon reaching the configured threshold.

Allow a simple password

FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

If the mobile device has a valid policy and the policy contains an allowed operation for the respective object.

FDP_ACF.1.3(2) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *no additional rules*.

FDP_ACF.1.4(2) The TSF shall explicitly deny access of subjects to objects based on the *no additional explicit denial rules*.

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) User name;

b) *Role/permission set.*

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 **on the management system** before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated **on the management system** 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 **on the management system** 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 **on the management system**.

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	System Administrator
User Account Attributes	Query, Modify, Delete	System Administrator, Helpdesk Administrator
Policy Configurations	Query, Modify, Delete	System Administrator, Policy Administrator
Compliance Reports	Query	System Administrator, Reports Viewer, Helpdesk Administrator

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 *restrictive* 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) Set administrator password

b) Manage user accounts

c) Set access policies

d) Review policy compliance reports.

6.1.4.4 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles: *System Administrator, Policy Administrator, Helpdesk Administrator, and Reports Viewer*.

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
	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
FAU_SAR.1	No other components	FAU_GEN.1	Satisfied

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_SAR.2	No other components	FAU_SAR.1	Satisfied
FAU_STG.1	No other components	FAU_GEN.1	Satisfied
FDP_ACC.1(1)	No other components	FDP_ACF.1	Satisfied by FDP_ACF.1(1)
FDP_ACF.1(1)	No other components	FDP_ACC.1 FMT_MSA.3	Satisfied by FDP_ACC.1(1) Satisfied
FDP_ACC.1(2)	No other components	FDP_ACF.1	Satisfied by FDP_ACF.1(2)
FDP_ACF.1(2)	No other components	FDP_ACC.1 FMT_MSA.3	Satisfied by FDP_ACC.1(2) Satisfied
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

6.4.1 Security Functional Requirements for the TOE

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

[2]This dependency is not applicable because neither the iOS Mobile Access Control SFP nor the Android Mobile Access Control SFP allow access to security attributes. The TOE provides default policy settings for security attributes, but these SFPs do not permit any action on security attributes.

SFR \ OBJECTIVE	O.ACCESS	O.AUDITS	O.AUDIT_PROTECT	O.EADMIN	O.IDAUTH	O.INTEGRITY	O.MOBILE_POLICY
FAU_GEN.1		✓					
FAU_GEN.2		✓					
FAU_SAR.1	✓						
FAU_SAR.2	✓						
FAU_STG.1		✓	✓				
FDP_ACC.1(1) and FDP_ACC.1(2)							✓
FDP_ACF.1(1) and FDP_ACF.1(2)							✓
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 authorized users to access only appropriate TOE functions and data. Users authorized to access the TOE are determined using an identification and authentication process (FIA_UID.1 and FIA_UAU.1). The permitted access to TOE data by the roles and permissions is defined (FMT_MTD.1, FMT_SMF.1, FMT_SMR.1). The audit log records may only be viewed by authorized users (FAU_SAR.1, FAU_SAR.2). The default values of security attributes are restrictive in nature (FMT_MSA.3).
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). The TOE does not provide any mechanism for users to modify or delete audit records other than via configuration of the data retention timeframe, and that functionality is limited to administrators (FAU_STG.1).
O.AUDIT_PROTECT	The TOE will provide the capability to protect audit information generated by the TOE. The TOE is required to protect the stored audit records from unauthorized deletion or modification (FAU_STG.1).

OBJECTIVE	RATIONALE
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).
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data on the management system. 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(1), FDP_ACC.1(2), FDP_ACF.1(1), and FDP_ACF.1(2)).

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 9.7
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: McAfee Enterprise Mobility Management 9.7
ADV_TDS.1: Basic Design	Basic Design: McAfee Enterprise Mobility Management 9.7
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: McAfee Enterprise Mobility Management 9.7
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: McAfee Enterprise Mobility Management 9.7
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: McAfee Enterprise Mobility Management 9.7
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: McAfee Enterprise Mobility Management 9.7
ALC_DEL.1: Delivery Procedures	Delivery Procedures: McAfee Enterprise Mobility Management 9.7

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ALC_FLR.2: Flaw Reporting	Flaw Reporting: McAfee Enterprise Mobility Management 9.7
ATE_COV.1: Evidence of Coverage	Security Testing: McAfee Enterprise Mobility Management 9.7
ATE_FUN.1: Functional Testing	Security Testing: McAfee Enterprise Mobility Management 9.7
ATE_IND.2: Independent Testing – Sample	Security Testing: McAfee Enterprise Mobility Management 9.7

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.

SFR \ TSF	Policy Management	Identification and Authentication	Management	Audit
FAU_GEN.1				✓
FAU_GEN.2				✓

SFR \ TSF	Policy Management	Identification and Authentication	Management	Audit
FAU_SAR.1				✓
FAU_SAR.2				✓
FAU_STG.1				✓
FDP_ACC.1(1) and FDP_ACC.1(2)	✓			
FDP_ACF.1(1) and FDP_ACF.1(2)	✓			
FIA_ATD.1			✓	
FIA_UID.1		✓		
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.
FAU_SAR.1	**Audit –** Audit log records are displayed in a human readable table form from queries generated by authorized users.
FAU_SAR.2	**Audit –** Only authorized users have permission to query audit log records.
FAU_STG.1	**Audit –** The only mechanism provided by the TOE to cause audit records to be deleted is configuration of the data retention timeframe, which is restricted to administrators. The TOE does not provide any mechanism for users to modify audit records.
FDP_ACC.1(1) and FDP_ACF.1(2)	**Policy Management** – The TOE implements policy-based access control to restrict actions available on managed devices.
FDP_ACF.1(1) and FDP_ACF.1(2)	**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 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 can be initiated before proper identification and authentication.

SFR	SECURITY FUNCTION AND RATIONALE
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 can be initiated before proper identification and authentication.
FMT_MSA.3	**Management** – The TOE ensures the default values of security attributes are restrictive 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.
FMT_SMR.1	**Management** – The TOE provides the roles specified in the SFR. When a User Account is created or modified, the role is specified by setting or clearing the appropriate status for the user.

Table 23 – SFR to TSF Rationale

7 TOE Summary Specification

7.1 Policy Management

The TOE pushes policies to mobile devices for compliance to network security and usage restrictions. The available actions and usage restrictions associated with policies are as follows:

FUNCTIONALITY	SETTING	DESCRIPTION	VALID OPTIONS /FORMATS	IOS DEVICE	ANDROID
Security: Authentication Management	User Password for Login	Prompt user to enter a password when they login to the device	Should satisfy the password strength requirements	✓	✓
	Password Length	The minimum length in characters of the power-on passwords.	1 to 15	✓	✓
	Password Expiration	Monitor and set password age on the device.	ON, OFF, VALUE	✓	
	Require Alpha Numeric Password	Composition of password.	ON, OFF, VALUE	✓	✓
	Password History	Track the user passwords; restrict usage of previous passwords	ON, OFF, VALUE	✓	
	Password Delay/Inactivity Timer	Timeout for password inactivity on the device. Determines the password timeout on the device.	ON, OFF, VALUE	✓	✓
	Password Failure Action	Monitor incorrect passwords and wipe the device upon reaching the configured threshold. Wiping the device returns it to factory defaults.	ON, OFF, VALUE	✓	✓
	Allow Simple Password	Allow a simple password	ON, OFF	✓	✓
Security: Resource	Restrict iTunes	Restrict iTunes	ON, OFF	✓	

FUNCTIONALITY	SETTING	DESCRIPTION	VALID OPTIONS /FORMATS	IOS DEVICE	ANDROID
Management	Restrict explicit content on iTunes	Restrict explicit content on iTunes	ON, OFF	✓	
	Restrict Use of Browser	Restrict Browser	ON, OFF	✓	
	Remove YouTube App	Removes YouTube app from home tiles	ON, OFF	✓	
	Restrict Camera	Restrict Camera on the device	ON, OFF	✓	
	Restrict Screen Capture	Prevents screen captures on the device	ON, OFF	✓	
	Restrict Automatic Sync While Roaming	Prevents the device from syncing when roaming.	ON, OFF	✓	
	Restrict In App Purchases	Prevents In App Purchases	ON, OFF	✓	
	Restrict Multiplayer Gaming	Prevents the user from multiplayer gaming.	ON, OFF	✓	
	Restrict Voice Dialing	Prevents voice dialing capabilities.	ON, OFF	✓	
	Restrict Installing Applications	Prevents non-enterprise applications from being installed.	ON, OFF	✓	
	Allow Hands Free	Allow Bluetooth hands-free.	ON, OFF	✓	

Table 24 – Policy Controls for Device Types

7.2 Identification and Authentication

The TOE has the ability to authenticate users locally using a password or can integrate with a remote authentication server. Users enter a username and password, which is validated by the TOE against the user 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.

7.3 Management

The management of the security functions of the TOE are performed by the system administrator via the management console. The TOE allows an authorized user to create, manage, and publish security policies. Available functions include:

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

Once the system administrator defines one or more security policies, he/she assigns those policies to users and or groups via the management console.

The TOE provides functionality to allow system administrators to determine the security policy conformance of the mobile user community. The management console ensures the default values of security attributes are restrictive in nature as to enforce 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 restrict access to devices that are not jailbroken.

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

AUTHORIZED ROLES	TSF DATA	OPERATION
System Administrator	Admin Account Attributes	Query, Modify, Delete
System Administrator, Helpdesk Administrator	User Account Attributes	Query, Modify, Delete
System Administrator, Policy Administrator	Policy Configurations	Query, Modify, Delete
System Administrator, Reports Viewer, Helpdesk Administrator	Compliance Reports	Query

Table 25 – Data Access Permissions

7.4 Audit

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

- User Name

- Event Type
- Event Time
- Additional Information

The TOE provides the following Mobile Access Control SFP events:

NAME	DESCRIPTION
Audit Log Report	The Audit Log report provides a list of events; such as policy changes, logins, deleting devices, wiping devices, or uninstalling policy profiles. This provides an audit trail of action initiated by all Console users. Only the System Administrator can view the Audit Log.
Compliance Status Report	The Compliance Status report shows all registered mobile devices and information on whether those devices are compliant or non-compliant. You can view all users, compliant users, or non-compliant users by selecting an option from the Filter drop-down menu.
Package Deployment Report	The Package Deployment Report shows the status of packages being pushed to devices. You can view which packages are downloading, pending, been acknowledged, or that have completed downloading.
Pending Actions Report	The Pending Actions report lists any outstanding actions against devices. Pending actions include package updates, delete commands, uninstall commands, and wipe commands. This report shows which devices received commands and which devices did not.
Registered Users Report	The Registered Users report provides a list of all users that have provisioned mobile devices.
Software Status Report	The Software Status report lists each mobile device and it's versions of PDA Secure, Download Manager, and the security policy. The McAfee EMM app for iOS devices is not shown on this report.
Unregistered Devices Report	The Unregistered Devices Report lists those devices that attempt to sync to the ActiveSync server but do not have the McAfee EMM software installed. If compliance enforcement is enabled, these devices will be blocked from getting email, and if compliance enforcement is disabled, these devices can sync their email. In either case, this report will show when the device last synced.

Table 26 – Predefined EMM Event Reports