Extended Package for Mobile Device Management Agents

31 December 2014

Version 2.0

REVISION HISTORY

Version	Date	Description
1.0	21 October 2013	Initial Release
1.1	7 February 2014	Typographical changes and clarifications to front-matter
2.0	31 December 2014	Separation of MDM Agent SFRs. Updated cryptography, protocol, X.509 requirements. Added objective requirement for Agent audit storage. New requirement for unenrollment prevention. Initial Release of MDM Agent EP.

CONTENTS

TABLE OF TABLES

1. Introduction

This Extended Package (EP) describes security requirements for a Mobile Device Management (MDM) Agent and is intended to provide a minimal baseline set of requirements that are targeted at mitigating well defined and described threats. The Agent of an MDM system is only one component of an enterprise deployment of mobile devices. Other components, such as the mobile device platforms which enforce the security policies, and servers which host mobile application repositories, are out of scope. This introduction describes the features of a compliant Target of Evaluation (TOE) and discusses how this EP is to be used in conjunction with the MDM Protection Profile (PP) or the Mobile Device Fundamentals (MDF) PP.

1.1 Conformance Claims

This EP serves to complement the MDM PP v2.x or the MDF PP v2.x with additional SFRs and associated Assurance Activities specific to the MDM Agent. Assurance Activities are the actions that the evaluator performs in order to determine a TOE's compliance to the SFRs.

This EP conforms to Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3. It is CC Part 2 extended and CC Part 3 conformant.

1.2 How to Use This Extended Package

This EP extends the MDM PP v2.x when the MDM Agent is installed on a mobile device as an application that is developed by the MDM developer. This EP extends the MDF PP when the MDM Agent is built into the mobile device platform by the mobile device vendor.

As an EP of either the MDM PP v2.x or the MDF PP v2.x, it is expected that the content of this EP and the chosen PP be appropriately combined in the context of each product-specific Security Target. This EP has been specifically defined such that there should be no difficulty or ambiguity in doing so. When this EP is used with the MDM PP v2.x or the MDF PP v2.x, conformant TOEs are obligated to implement the functionality required in those PPs with the additional functionality defined in this EP in response to the threat environment discussed subsequently herein. An ST must identify the applicable versions of the PP chosen and this EP in its conformance claims.

1.3 Compliant Targets of Evaluation

The MDM system consists of two primary components: the MDM Server software and the MDM Agent.

The MDM operational environment consists of the mobile device on which the MDM Agent resides, the platform on which the MDM Server runs, and an untrusted wireless network over which they communicate, as pictured below.

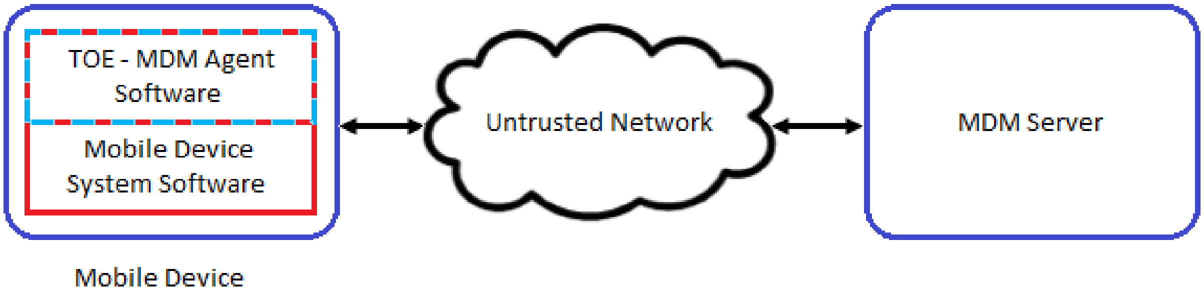

Figure 1: MDM System Operating Environment

The **MDM Agent**, which is the focus of this EP, is installed on a mobile device as an application or is part of the mobile device's OS. The MDM Agent establishes a secure connection back to the MDM Server controlled by an enterprise administrator. Optionally, the MDM Agent interacts with the Mobile Application Store (MAS) Server to download and install enterprise-hosted application.

The MDM Agent must closely interact with or be part of (as depicted by the dotted red/blue line in Figure 1) the mobile device's platform to establish policies and perform queries about device status. The mobile device, in turn, has its own security requirements specified in the MDF PP against which the mobile device must be evaluated either concurrently with or before the MDM Agent evaluation.

If the MDM Agent is part of the mobile device's OS, the agent may present multiple interfaces for configuring the mobile device, such as a local interface and a remote interface. Agents conforming to this profile must at least offer an interface with a trusted channel that serves as one piece of an MDM system. Compliant agents may also offer other interfaces, and the configuration aspects of these additional interfaces is in scope of this EP.

2. SECURITY PROBLEM DESCRIPTION

MDM Agents address a range of security threats from theft of sensitive data to unauthorized access to malicious application downloads. While many of these threats also apply to the MDM Server and the mobile device itself, the MDM Agent plays a key role in ensuring the integrity and confidentiality of data is maintained by interfacing directly with the OS of the device, either through a 3rd party application or as a part of the mobile device OS itself. Applicable threats addressed by the MDM Agent include malicious and flawed applications, network attacks, network eavesdropping, and physical access.

Appendix A presents the Security Problem Description (SPD) in a more “traditional” form. The following sections detail the problems that compliant TOEs will address; references to the “traditional” statements in Appendix A are included.

2.1 Threats

2.1.1 Malicious and Flawed Applications

Malicious or flawed application (app) threats exist because apps loaded onto a Mobile Device may include malicious or exploitable code. This code could be included unwittingly by its developer, perhaps as part of a software library. Malicious apps may attempt to exfiltrate data to which they have access. Malicious apps may be able to control the device's sensors (geolocation, camera, microphone, etc.) to gather intelligence about the user's surroundings even when those activities do not involve data resident or transmitted from the device. Flawed apps may give an attacker access to perform network-based or physical attacks that otherwise would have been prevented.

[T.MALICIOUS_APPS]

2.1.2 Network Attack

An attacker may position themselves on a wireless communications channel or elsewhere on the network infrastructure. From this vantage point, an attacker may initiate communication with the mobile device or alter communication between elements of the operating environment and other endpoints. By altering this communication, the attacker may be able to spoof the MDM Server.

[T.NETWORK_ATTACK]

2.1.3 Network Eavesdropping

In a similar manner to the network attack threat, an attacker may position themselves on a wireless communications channel or elsewhere on the network infrastructure. The attacker may then monitor or gain access to data being sent or received by the MDM Agent. By monitoring this data, the attacker may intercept security critical data including cryptographic keys and human-user authentication data.

[T.NETWORK_EAVESDROP]

2.1.4 Physical Access

Loss or theft of the underlying mobile device platform may give rise to loss of confidentiality of user data, including, most importantly, credentials. Physical access attacks involve attempts to access the device through external hardware ports, through its user interface, or through direct and possible destructive access to its storage media. Such attacks are intended to gain access to data from a lost or stolen mobile device that it is not expected to be returned to its owner. Although these attacks are primarily directed against the mobile device platform, the MDM Agent configures features which address this threat.

[T.PHYSICAL_ACCESS]

2.2 Assumptions

The assumptions for the MDM are defined in Appendix A.1.1.

2.3 Organizational Security Policy

The organization security policies for the MDM are defined in Appendix A.1.3.

3. Security Objectives

3.1 Security Objectives for the TOE

Compliant TOEs will provide security functionality and implement policies that address threats to the enterprise from inclusion of mobile devices. The following sections provide a description of this functionality in light of the threats previously discussed. The security functionality provided includes protected communications to and from the MDM Agent, configuration of security policies for mobile devices, and system reporting for detection of security relevant events.

3.1.1 Protected Communications

To address the issues concerning transmitting sensitive data to and from the MDM Agent described in Section 2.1.3, compliant TOEs will use a trusted communication path. The trusted channel to and from the MDM Agent is implemented using one (or more) of these standard protocols: DTLS, HTTPS, or TLS.

To address the threat of network attacks described in Section 2.1.2, the protocols described in this document provide encryption and mutual authentication to and from the MDM Agent in a cryptographically secure manner; thus, any attempt by a malicious attacker to represent himself to the MDM Agent as a MDM Server would be detected.

O.DATA_PROTECTION_TRANSIT -> (FCS_STG_EXT.4/FCS_STG_EXT.1(2), FTP_ITC_EXT.1/FPT_ITT_EXT.1, FCS_TLSC_EXT.1, FIA_ENR_EXT.2)

3.1.2 System Reporting

To ensure that information exists that allows administrators to discover unintentional issues with the configuration and operation of the mobile device, compliant TOEs have the capability of generating reports which may indicate such issues. Auditing of administrative activities provides information that may hasten corrective action.

O.ACCOUNTABILITY -> (FAU_ALT_EXT.2, FAU_GEN.1, FAU_SEL.1, FAU_STG_EXT.1)

3.1.3 Mobile Device Configuration

Mobile devices can accept security policies defined by the Enterprise in order to ensure protection of enterprise data that they may store or process. The MDM Agent is responsible for interacting with the mobile device platform to establish policies and execute commands from the MDM Server, and sending reports to the MDM Server.

O.APPLY_POLICY -> (FMT_SMF_EXT.3, FMT_UNR_EXT.1, FMT_POL_EXT.2)

3.2 Security Objectives for the Operational Environment

The objectives that are required to be met by the TOE's operational environment are defined in Appendix A.2.2.

4. Security Functional Requirements

The Security Functional Requirements (SFRs) included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4*, with additional extended functional components.

4.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Refinement made by PP author: Indicated by the word “Refinement” in **bold text** after the element number with additional text in **bold** text;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with *italicized and underlined* text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).
- Extended SFRs are identified by having a label ‘EXT’ after the requirement name for TOE SFRs.

4.2 Test Environment for Assurance Activities

The Test Environment for the assurance activities of the SFRs for MDM Agents differs based on whether the Agent EP extends the MDM PP or the MDF PP.

If the EP extends the MDM PP, the assurance activities shall be performed using the MDM Server in evaluation against the base MDM PP, and many of the assurance activities in this EP may be combined with the assurance activities in the MDM PP.

If the EP extends the MDF PP, the assurance activities shall be performed with a test MDM Server that is capable of exercising all of the functionality of the Agent. This test server is not required to be a commercial product and may be provided by the mobile device vendor as a tool for testing only. A number of the assurance activities in this EP may be combined with assurance activities in the MDF PP.

4.3 MDF PP Security Functional Requirement Direction

If this EP is extending the MDF PP, the Agent is expected to utilize a number of security functions implemented by the mobile device and evaluated against the base PP. This security functionality includes FCS_CKM.1, FCS_CKM.2, FCS_CKM_EXT.4, FCS_COP.1(*), FCS_RBG_EXT.1, FCS_TLSC_EXT.2, FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3, FPT_TST_EXT.2, FCS_DTLS_EXT.1, and FCS_HTTPS_EXT.1.

4.3.1 Cryptographic Support (FCS)

4.3.1.1 Cryptographic Key Storage

The following requirement is identical, except in name, to the Cryptographic Key Storage requirement for EPs extending the MDM PP. The names differ for clarity, and one must be added to the Agent’s ST depending on the base PP.

FCS_STG_EXT.4.1 The MDM Agent shall store persistent secrets and private keys when not in use in platform-provided key storage.

Application Note:

This requirement ensures that persistent secrets (credentials, secret keys) and private keys are stored securely when not in use by the mobile platform.

Assurance Activity:

TSS

The evaluator will verify that the TSS lists each persistent secret (credential, secret key) and private key needed to meet the requirements in the ST. For each of these items, the evaluator will confirm that the TSS lists for what purpose it is used, and, for each platform listed as supported in the ST, how it is stored. The evaluator shall verify that the Agent calls a platform-provided API to store persistent secrets and private keys.

4.3.2 Trusted Path/Channels (FTP)

4.3.2.1 Trusted Channel Communication

If the EP extends the MDF PP, the communication channel between the Agent and the Server is external to the TOE and FTP_ITC_EXT.1 in the MDF PP should be modified as below.

FTP_ITC_EXT.1.1 The TSF shall use 802.11-2012, 802.1X, and EAP-TLS and [selection, *at least one of: IPsec, TLS, DTLS, HTTPS protocol*] to provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels, provides assured identification of its end points, protects channel data from disclosure, and detects modification of the channel data.

Application Note:

This requirement is inherited from the base PP; the mobile device is required to perform the mandated cryptographic protocols as in the base PP for communication channels mandated in the MDF PP. The ST author must select one of TLS, DTLS, or HTTPS in order to establish and maintain a trusted channel between the TOE and the MDM Server. Only TLS, DTLS, or HTTPS are used in this trusted channel.

This requirement is to ensure that the transmission of any audit logs, mobile device information data (software version, hardware model, and application versions), and configuration data collected by the MDM Agent and sent from the MDM Agent to the MDM Server, when commanded, or at configurable intervals, is properly protected. This trusted channel also protects any commands and policies sent by the MDM Server to the MDM Agent. Either the MDM Agent or the MDM Server is able to initiate the connection.

This trusted channel protects both the connection between an enrolled MDM Agent and the MDM Server and the connection between an unenrolled MDM Agent and the MDM Server during the enrollment operation. Different protocols can be used for these two connections, and the description in the TSS should make this difference clear.

The trusted channel uses TLS, DTLS, or HTTPS as the protocol that preserves the confidentiality and integrity of MDM communications. The ST author chooses the mechanism or mechanisms supported by *the TOE, and then ensures the detailed requirements in Appendix C corresponding to their selection are copied to the ST if not already present.*

Protocol, RBG, Certificate validation, algorithm, and similar services may be met with platform provided services.

FTP_ITC_EXT.1.2 The TSF shall permit the TSF and the MDM Server and [selection: MAS Server, no other IT entities] to initiate communication via the trusted channel.

Application Note:

For all other use cases, the mobile device initiates the communication; however, for MDM Agents, the MDM Server may also initiate communication. This requirement replaces the requirement in the MDF PP.

FTP_ITC_EXT.1.3 The TSF shall initiate communication via the trusted channel for wireless access point connections, administrative communication, configured enterprise connections, and [selection: <u>OTA updates, no other connections</u>].

Application Note:

This element is inherited from the MDF PP; it is expected that Mobile Device will initiate the trusted channel between the MDM Agent and the MDM Server for administrative communication and may initiate other trusted channels to other trusted IT entities for other uses.

Assurance Activity:

The following additional assurance activities shall be performed.

TSS

The evaluator shall examine the TSS to determine that the methods of Agent-Server communication are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of remote TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.

GUIDANCE

The evaluator shall confirm that the operational guidance contains instructions for configuring the communication channel between the MDM Agent and the MDM Server and conditionally, the MAS Server for each supported method.

TEST

For a MDM Server and, conditionally, a MAS Server:

Test 1: The evaluators shall ensure that communications using each specified (in the operational guidance) Agent-Server communication method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.

Test 2: The evaluator shall ensure, for each method of Agent-Server communication, the channel data is not sent in plaintext.

Test 3: The evaluator shall ensure, for each communication channel with the MDM Server, that a protocol analyzer identifies the traffic as the protocol under testing.

Further assurance activities are associated with the specific protocols.

4.4 MDM PP Security Functional Requirement Direction

If this EP is extending the MDM PP, the Agent is part of the MDM TOE and any requirements on the MDM TOE also apply to the MDM Agent. These security functions includes FCS_CKM.1, FCS_CKM.2, FCS_CKM_EXT.4, FCS_COP.1(*), FCS_RBG_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3, FIA_X509_EXT.4, FPT_TST_EXT.2, FCS_DTLS_EXT.1, and FCS_HTTPS_EXT.1. The ST author should iterate the requirements in the MDM PP for each Agent in order to make the appropriate selections for each agent.

4.4.1 Cryptographic Support (FCS)

4.4.1.1 Cryptographic Key Storage

The following requirement is identical, except in name, to the Cryptographic Key Storage requirement for EPs extending the MDF PP. The names differ for clarity and one must be added to the Agent's ST depending on the base PP.

FCS_STG_EXT.1.1(2) The MDM Agent shall store persistent secrets and private keys when not in use in platform-provided key storage.

Application Note:

This requirement ensures that persistent secrets (credentials, secret keys) and private keys are stored securely when not in use by the mobile platform.

Assurance Activity:

TSS

The evaluator will verify that the TSS lists each persistent secret (credential, secret key) and private key needed to meet the requirements in the ST. For each of these items, the evaluator will confirm that the TSS lists for what purpose it is used, and, for each platform listed as supported in the ST, how it is stored. The evaluator shall verify that the Agent calls a platform-provided API to store persistent secrets and private keys.

4.4.1.2 TLS Client Protocol

The ST author shall include the FCS_TLSC_EXT.1 requirement from the Optional Requirements in the MDM PP.

4.4.2 Protection of the TSF (FPT)

If the EP extends the MDM PP, the communication channel between the Agent and the Server is internal to the TOE and is addressed by FPT_ITT.1 in the MDM PP.

4.5 TOE Security Functional Requirements

4.5.1 Security Audit (FAU)

4.5.1.1 Agent Alerts

FAU_ALT_EXT.2.1 The MDM Agent shall provide an alert via the trusted channel to the MDM Server in the event of any of the following:

a. successful application of policies to a mobile device;

b. [selection: receiving, generating] periodic reachability events;

[selection:

c. change in enrollment state,

d. failure to install an application from the MAS Server,

e. failure to update an application from the MAS Server,

f. [assignment: *other events*], no other events]

Application Note:

The trusted channel is defined in FPT_ITT.1. "Alert" in this requirement could be as simple as an audit record or a notification.

This requirement is to ensure that the MDM Agent shall notify the MDM Server whenever one of the events listed above occurs. Lack of receipt of a successful policy installation indicates the failure of the policy installation.

The periodic reachability events ensure that either the MDM Agent responds to MDM Server polls to determine device network reachability, or the MDM Agent can be configured to regularly notify the Server that it is reachable. The ST author must select "receiving" in the first case and "generating" in the second. The corresponding requirement for the MDM Server is FAU_NET_EXT.1 in the MDM PP.

The ST author must either assign further events or select the "no other events" option. Note that alerts may take time to reach the MDM Server, or not arrive, due to poor connectivity.

Assurance Activity:

TSS

The evaluator shall examine the TSS and verify that it describes how the alerts are implemented.

The evaluator ensures that the TSS describes how the candidate policy updates are obtained; and the actions that take place for successful (policy update installed) and unsuccessful (policy update not installed) cases. The software components that are performing the processing must also be identified in the TSS and verified by the evaluator.

The evaluator also ensures that the TSS describes how reachability events are implemented, and if configurable are selected in FMT_SMF_EXT.3.2. The evaluator verifies that this description clearly indicates who (MDM Agent or MDM Server) initiates reachability events.

TEST

Test 1: The evaluator shall perform a policy update from the test environment MDM server. The evaluator shall verify the MDM Agent accepts the update, makes the configured changes, and reports the success of the policy update back to the MDM Server.

Test 2: The evaluator shall perform each of the actions listed in FAU_ALT_EXT.1.1 and verify that the alert does in fact reach the MDM Server.

Test 3: The evaluator shall configure the MDM Agent to perform a network reachability test, both with and without such connectivity and ensure that results reflect each.

FAU_ALT_EXT.2.2 The MDM Agent shall queue alerts if the trusted channel is not available.

Assurance Activity:

TSS

The evaluator shall ensure that the TSS describes under what circumstances, if any, the alert may not be generated (e.g., the device is powered off or disconnected from the trusted channel), how alerts are queued, and the maximum amount of storage for queued messages.

TEST

The evaluator shall remove network connectivity from the MDM Agent and generate an alert/event in FAU_ALT_EXT.2.1. The evaluator shall restore network connectivity to the MDM Agent and verify that the alert generated while the TOE was disconnected is sent by the MDM Agent.

4.5.2 Identification and Authentication (FIA)

4.5.2.1 Enrollment of Mobile Device into Management

FIA_ENR_EXT.2.1 The MDM Agent shall record the reference identifier of the MDM Server during the enrollment process.

Application Note:

The reference identifier of the MDM Server may be the Distinguished Name, Domain Name, and/or the IP address of the MDM Server. This requirement allows the specification of the information to be to be used to establish a network connection and the reference identifier for authenticating the trusted channel between the MDM Server and MDM Agent (FPT_ITT.1).

Assurance Activity:

TSS

The evaluator shall examine the TSS to verify that it describes which types of reference identifiers are acceptable and how the identifier is specified (e.g. preconfigured in the MDM Agent, by the user, by the MDM server, in a policy).

GUIDANCE

The evaluator shall examine the operational guidance to verify that it describes how to configure reference identifier of the MDM Server's certificate and, if different than the reference identifier, the Domain Name or IP address (for connectivity) of the MDM Server.

TEST

The evaluator shall follow the operational guidance to establish the reference identifier of the MDM server on the MDM Agent and in conjunction with other Assurance Activities verify that the MDM Agent can connect to the MDM Server and validate the MDM Server's certificate.

4.5.3 Security Management (FMT)

4.5.3.1 Specification of Management Functions

FMT_SMF_EXT.3.1 The MDM Agent shall be capable of interacting with the platform to perform the following functions:

[selection:

a. <u>administrator-provided management functions in MDF PP;</u>

b. administrator-provided device management functions in MDM PP

]

c. Import the certificates to be used for authentication of MDM Agent communications
d. [selection: [assignment: *additional functions*], no additional functions].

Application Note:

This requirement captures all the configuration functionality in the MDM Agent to configure the underlying Mobile Device with the configuration policies sent from the MDM Server to the Agent. The ST author selects the base PP (MDF PP or MDM PP) as the source of the management functions.

The administrator-provided management functions in MDF PP are specified in Column 4 of Table 1 in MDF PPv2.x (reproduced in this EP as Table 8 in Appendix G) and in FPT_TUD_EXT.1 (for version queries). The administrator-provided device management functions in MDM PP are specified in FMT_SMF.1.1(1); the functions in the selection of FMT_SMF.1.1(1) in the MDM PP are required to correspond to the functions available on the platforms supported by the MDM Agent.

The ST author can add more commands and configuration policies by completing the assignment statement; these additional commands or configuration policies must be supported by the Mobile Device.

The agent must configure the platform based on the commands and configuration policies received from the MDM Server. The ST author shall not claim any functionality not provided by the supported Mobile Device(s). All selections and assignments performed by the ST author in this requirement should match the selections and assignments of the validated Mobile Device ST.

Assurance Activity:

This assurance activity may be performed in conjunction with other assurance activities in the base PP.

TSS

The evaluator shall verify that the any assigned functions are described in the TSS and that these functions are documented as supported by the platform. The evaluator shall examine the TSS to verify that any differences between management functions and policies for each supported Mobile Device are listed.

GUIDANCE

The evaluator shall verify the AGD guidance includes detailed instructions for configuring each function in this requirement.

If the MDM Agent is a component of the MDM system (i.e. MDM Server is the base PP), the evaluator shall verify, by consulting documentation for the claimed mobile device platforms, that the configurable functions listed for this Agent are supported by the platforms.

If the MDM Agent supports multiple interfaces for configuration (for example, both remote configuration and local configuration), the AGD guidance makes clear whether some functions are restricted to certain interfaces.

TEST

Test 1: In conjunction with the assurance activities in the base PP, the evaluator shall attempt to configure each administrator-provided management function and shall verify that the Mobile Device executes the commands and enforces the policies.

Test 2: The evaluator shall configure the MDM Agent authentication certificate in accordance with the configuration guidance. The evaluator shall verify that the MDM Agent uses this certificate in performing the tests for FPT_ITT.1.

Test 3: (conditional) The evaluator shall design and perform tests to demonstrate that the assigned function may be configured and that the intended behavior of the function is enacted by the mobile device.

FMT_SMF_EXT.3.2 The MDM Agent shall be capable of performing the following functions:

a. Enroll in management;
b. Configure whether users can unenroll the agent from management
c. [selection: configure periodicity of reachability events, [assignment: *other management functions*], no other functions].

Application Note:

This requirement captures all of the configuration in the MDM Agent for configuration of itself.

If the MDM Agent is a part of the mobile device, enrollment is a single function both of the Agent and of the mobile device (FMT_SMF_EXT.3.1).

If the MDM Agent is an application developed separately from the mobile device, the MDM Agent performs the function "enroll the mobile device in management" (per FMT_SMF_EXT.3.1) by registering itself to the mobile device as a device administrator. The Agent itself is enrolled in management by configuring the MDM Server to which the Agent answers.

If the Agent generates periodic reachability events in FAU_ALT_EXT.2.1 and the periodicity of these events is configurable, "configure periodicity of reachability events" must be selected.

Assurance Activity:

TSS

The evaluator shall verify that the TSS describes the methods in which the MDM Agent can be enrolled. The TSS description shall make clear if the MDM Agent supports multiple interfaces for enrollment and configuration (for example, both remote configuration and local configuration).

Additionally, the evaluator shall verify that the TSS describes any management functions of the MDM Agent.

GUIDANCE

The evaluator shall verify the AGD guidance includes detailed instructions for configuring each function in this requirement.

TEST

Test 1: In conjunction with other assurance activities, the evaluator shall attempt to enroll the MDM Agent in management with each interface identified in the TSS, and verify that the MDM Agent can manage the device and communicate with the MDM Server.

Test 2: (conditional) In conjunction with the assurance activity for FAU_ALT_EXT.2.1, the evaluator shall configure the periodicity for reachability events for several configured time periods and shall verify that the MDM Server receives alerts on that schedule.

Test 3: (conditional) The evaluator shall design and perform tests to demonstrate that the assigned function may be configured and that the intended behavior of the function is enacted by the mobile device.

4.5.3.2 User Unenrollment Prevention

FMT_UNR_EXT.1.1 The MDM Agent shall provide a mechanism to prevent users from unenrolling the mobile device from management.

Application Note:

Unenrolling is the action of transitioning from the enrolled state to the unenrolled state. If preventing the user from unenrolling is configurable, administrators configure whether users are allowed to unenroll through the MDM Server. For those configurations where unenrollment is allowed, the MDFPP describes configuration actions performed upon unenrollment in FMT_SMF_EXT.2.1; however, the MDM Agent is limited to those actions supported by the mobile device on which the Agent is operating.

Assurance Activity:

TSS

The evaluator shall ensure that the TSS describes the mechanism used to prevent users for enrolling. This description shall indicate if any configuration allows users to unenroll.

GUIDANCE

The evaluator shall ensure that the administrative guidance instructs administrators in configuring the unenrollment prevention in each available configuration interface. If any configuration allows users to unenroll, the guidance also describes the actions that unenroll the Agent.

TEST

Test 1: The evaluator shall configure the Agent according to the administrative guidance for each available configuration interface, shall attempt to unenroll the device, and shall verify that the attempt fails.

Test 2: (Conditional) If any configuration allows the user to unenroll, the evaluator shall configure the Agent to allow user unenrollment, attempt to unenroll, and verify the attempt succeeds.

5. Security Assurance Requirements

It is important to note that a TOE that is evaluated against this EP is inherently evaluated against the MDF PP or the MDM PP as well. Those PPs include a number of Assurance Activities associated with both Security Functional Requirements (SFRs) and SARs. Additionally, this EP includes a number of SFR-based Assurance Activities that similarly refine the SARs identified in the base PPs. The assurance activities associated with SARs that are prescribed by the MDF PP or MDM PP are performed against the entire TOE.

A. RATIONALE

In this EP, the focus in the initial sections of the document is to use a narrative presentation in an attempt to increase the overall comprehensibility of the threats addressed by MDM Agents; the methods used to mitigate those threats; and the extent of the mitigation achieved by compliant TOEs. This presentation style does not readily lend itself to a formalized evaluation activity, so this section contains the tabular artefacts that can be used for the assurance activities associated with this document.

A.1. Security Problem Definition

A.1.1. Assumptions

The specific conditions listed below are assumed to exist in the TOE's Operational Environment. These include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: TOE Assumptions

Assumption Name	Assumption Definition
A.CONNECTIVITY	The TOE relies on network connectivity to carry out its management activities. The TOE will robustly handle instances when connectivity is unavailable or unreliable.
A.MOBILE_DEVICE_PLATFORM	The MDM Agent relies upon Mobile platform and hardware evaluated against the MDFPP and assured to provide policy enforcement as well as cryptographic services and data protection. The Mobile platform provides trusted updates and software integrity verification of the MDM Agent.
A.PROPER_ADMIN	One or more competent, trusted personnel who are not careless, willfully negligent, or hostile, are assigned and authorized as the TOE Administrators, and do so using and abiding by guidance documentation.
A.PROPER_USER	Mobile device users are not willfully negligent or hostile, and use the device within compliance of a reasonable Enterprise security policy.

A.1.2. Threats

The threats to the mobile device listed below are addressed by Mobile Device Management systems.

Table 2: Threats

Threat	Description of Threat
T.MALICIOUS_APPS	An administrator of the MDM or mobile device user may inadvertently import malicious code, or an attacker may insert malicious code into the TOE or OE, resulting in the compromise of TOE or TOE data.
T.NETWORK_ATTACK	An attacker may masquerade as MDM Server and attempt to compromise the integrity of the mobile device by sending malicious management commands.
T.NETWORK_EAVESDROP	Unauthorized entities may intercept communications between the MDM and mobile devices to monitor, gain access to, disclose, or alter remote management commands. Unauthorized entities may intercept unprotected wireless communications between the mobile device and the Enterprise to monitor, gain access to, disclose, or alter TOE data.
T.PHYSICAL_ACCESS	The mobile device may be lost or stolen, and an unauthorized individual may attempt to access OE data.

A.1.3. 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 OSPs must be enforced by the TOE or its operational environment.

Table 3: Organizational Security Policies

Policy Name	Policy Definition
P.ADMIN	The configuration of the mobile device security functions must adhere to the Enterprise security policy.
P.DEVICE_ENROLL	A mobile device must be enrolled for a specific user by the administrator of the MDM prior to being used in the Enterprise network by the user.
P.NOTIFY	The mobile user must immediately notify the administrator if a mobile device is lost or stolen so that the administrator may apply remediation actions via the MDM system.
P.ACCOUNTABILITY	Personnel operating the TOE shall be accountable for their actions within the TOE.

A.2. Security Objectives

A.2.1. Security Objectives For the TOE

The following table identifies security objectives for the Mobile Device Management system.

Table 4: Security Objectives for the TOE

Objective	Objective Description
O.APPLY_POLICY	The TOE must facilitate configuration and enforcement of enterprise security policies on mobile devices via interaction with the mobile OS and the MDM Server. This will include the initial enrollment of the device into management, through its lifecycle including policy updates and through its possible unenrollment from management services.
O.ACCOUNTABILITY	The TOE must provide logging facilities which record management actions undertaken by its administrators
O.DATA_PROTECTION_TRANSIT	Data exchanged between the MDM Server and the MDM Agent must be protected from being monitored, accessed and altered.

A.2.2. Security Objectives for the Operational Environment

The following table contains objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

Objective	Objective Description
OE.IT_ENTERPRISE	The Enterprise IT infrastructure provides security for a network that is available to the TOE and mobile devices that prevents unauthorized access.
OE.MOBILE_DEVICE_PLATFORM	The MDM Agent relies upon the trustworthy Mobile platform and hardware to provide policy enforcement as well as

	cryptographic services and data protection. The Mobile platform provides trusted updates and software integrity verification of the MDM Agent.
OE.PROPER_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
OE.PROPER_USER	Users of the mobile device are trained to securely use the mobile device and apply all guidance in a trusted manner.
OE.WIRELESS_NETWORK	A wireless network will be available to the mobile devices.

A.3. Correspondence

A.3.1. Security Problem Definition Correspondence

The following table serves to map the threats and assumptions defined in this EP to the security objectives also defined or identified in this EP.

Table 6: Security Problem Definition Correspondence

Threat or Assumption	Security Objective
A.CONNECTIVITY	OE.WIRELESS_NETWORK
A.MOBILE_DEVICE_PLATFORM	OE.MOBILE_DEVICE_PLATFORM
A.PROPER_ADMIN	OE.PROPER_ADMIN,
A.PROPER_USER	OE.PROPER_USER
T.MALICIOUS_APPS	O.APPLY_POLICY
T.NETWORK_ATTACK	O.DATA_PROTECTION_TRANSIT
T.NETWORK_EAVESDROP	O.DATA_PROTECTION_TRANSIT
T.PHYSICAL_ACCESS	O.APPLY_POLICY
P.ADMIN	OE.PROPER_ADMIN
P.DEVICE_ENROLL	OE.IT_ENTERPRISE
P.NOTIFY	OE.PROPER_USER
P.ACCOUNTABILITY	O.ACCOUNTABILITY

A.3.2. Security Objective Correspondence

The correspondence between the Security Functional Requirements (SFRs) and the Security Objectives identified or defined in the PP is provided in Section 3.1

B. OPTIONAL REQUIREMENTS

As indicated in the introduction to this EP, the baseline requirements (those that must be performed by the TOE or its underlying platform) are contained in the body of this EP. Additionally, there are three other types of requirements specified in Appendices B, C, and D.

The first type (in this Appendix) are requirements that can be included in the ST, but do not have to be in order for a TOE to claim conformance to this EP. The second type (in Appendix C) are requirements based on selections in the body of the EP: if certain selections are made, then additional requirements in that appendix will need to be included. The third type (in Appendix D) are components that are not required in order to conform to this EP, but will be included in the baseline requirements in future versions of this EP, so adoption by MDM Agents is encouraged. Note that the ST author is responsible for ensuring that requirements that may be associated with those in Appendix B, Appendix C, and/or Appendix D but are not listed (e.g., FMT-type requirements) are also included in the ST.

At this time the no optional requirements identified are those that may be performed by the MDM Agent or its underlying platform.

C. Selection-Based Requirements

As indicated in the introduction to this EP, the baseline requirements (those that must be performed by the TOE or its underlying platform) are contained in the body of this EP. There are additional requirements based on selections in the body of the PP: if certain selections are made, then additional requirements below will need to be included.

At this time the no selection-based requirements have been identified.

D. Objective Requirements

As indicated in the introduction to this EP, the baseline requirements (those that must be performed by the TOE or its underlying platform) are contained in the body of this EP. There are additional requirements that specify security functionality that is desirable and these requirements are contained in this Appendix. It is expected that these requirements will transition from objective requirements to baseline requirements in future versions of this EP.

At any time these may be included in the ST such that the TOE is still conformant to this EP.

This Appendix is divided into two subsections: objective requirements that may be performed by the TSF and objective requirements that may be performed by the MDM Agent or its underlying platform.

D.1. Objective TOE Security Functional Requirements

D.1.1. Security Audit (FAU)

D.1.1.1 Audit Data Generation

FAU_GEN.1.1(2) Refinement: The **MDM Agent** shall be able to generate an **MDM Agent** audit record of the following auditable events:

- **Start-up and Shutdown of the audit functions;**
- **Change in MDM policy; and**
- **Any modification commanded by the MDM Server,**
- **Specifically defined auditable events listed in Table 7**
- **[assignment: *other events*].**

Application Note:

This requirement is added to the ST if the MDM Agent has the functionality to generate audit records. This requirement outlines the information to be included in the MDM Agent's audit records. The ST author can include other auditable events directly in the table in FAU_GEN.1.1; they are not limited to the list presented.

The change of the MDM policy must minimally indicate that the policy changed. The event record need not contain the differences between the prior policy and the new policy. Modifications commanded by the MDM Server are those commands listed in FMT_SMF.1.1.

Assurance Activity:

TSS

The evaluator shall check the TSS and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field.

TEST

The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed and administrative actions. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.

Table 7: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_ALT_EXT.2	Type of alert.	No additional information.
FAU_GEN.1	None.	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	No additional information.
FAU_STG_EXT.1	None.	
FCS_STG_EXT.4.1/ FCS_STG_EXT.1(1)	None.	
FCS_TLSC_EXT.1	Failure to establish a TLS session. Failure to verify presented identifier. Establishment/termination of a TLS session.	Reason for failure. Presented identifier and reference identifier. Non-TOE endpoint of connection.
FIA_ENR_EXT.2	Enrollment in management.	Reference identifier of MDM Server.
FMT_POL_EXT.2	Failure of policy validation.	Reason for failure of validation.
FMT_SMF_EXT.3	Success or failure of function.	No additional information.
FMT_UNR_EXT.1.1	Attempt to unenroll.	No additional information.
FTP_ITC_EXT.1 / FPT_ITT_EXT.1	Initiation and termination of trusted channel.	Trusted channel protocol. Non-TOE endpoint of connection.

D.1.1.2 Security Audit Event Selection

FAU_SEL.1.1(2) The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a. **event type;**
b. **success of auditable security events;**
c. **failure of auditable security events; and**
d. **[assignment: other attributes].**

Application Note:

The intent of this requirement is to identify all criteria that can be selected to trigger an audit event. For the ST author, the assignment is used to list any additional criteria or "none". This selection may be configured by the MDM Server.

Assurance Activity:

GUIDANCE

The evaluator shall review the administrative guidance to ensure that the guidance itemizes all event types, as well as describes all attributes that are to be selectable in accordance with the requirement, to include those attributes listed in the assignment. The administrative guidance shall also contain instructions on how to set the pre-selection as well as explain the syntax (if present) for multi-value pre-

selection. The administrative guidance shall also identify those audit records that are always recorded, regardless of the selection criteria currently being enforced.

TEST

Test 1: For each attribute listed in the requirement, the evaluator shall devise a test to show that selecting the attribute causes only audit events with that attribute (or those that are always recorded, as identified in the administrative guidance) to be recorded.

Test 2 [conditional]: If the TSF supports specification of more complex audit pre-selection criteria (e.g., multiple attributes, logical expressions using attributes) then the evaluator shall devise tests showing that this capability is correctly implemented. The evaluator shall also, in the test plan, provide a short narrative justifying the set of tests as representative and sufficient to exercise the capability.

D.1.1.3 Security Audit Event Storage

FAU_STG_EXT.1.1 The MDM Agent shall store MDM audit records in the platform-provided audit storage.

Assurance Activity:

TSS

The evaluator will verify that the TSS description of the audit records indicates how the records are stored. The evaluator shall verify that the Agent calls a platform-provided API to store audit records.

D.1.2. Security Management (FMT)

D.1.2.1 Trusted Policy Update

FMT_POL_EXT.2.1 The MDM Agent shall only accept policies and policy updates digitally signed by the Enterprise.

Application Note:

The intent of this requirement is to cryptographically tie the policies to the enterprise that mandated the policy, not to protect the policies in transit (as they are already protected by FPT_ITT.1). This is especially critical for users who connect to multiple enterprises.

Policies must be digitally signed by the enterprise using the algorithms in FCS_COP.1(3).

Assurance Activity:

TSS

The evaluator also ensures that the TSS (or the operational guidance) describes how the candidate policies are obtained by the MDM Agent; the processing associated with verifying the digital signature of the policy updates; and the actions that take place for successful (signature was verified) and unsuccessful (signature could not be verified) cases. The software components that are performing the processing must also be identified in the TSS and verified by the evaluators.

TEST

The evaluator shall perform a policy update from an available configuration interface (such as through a test MDM Server). The evaluator shall verify the update is signed and is provided to the MDM Agent. The evaluator shall verify the MDM Agent accepts the digitally signed policy.

The evaluator shall perform a policy update from an available configuration interface (such as through a test MDM Server). The evaluator shall provide an unsigned and an incorrectly signed policy to the MDM Agent. The evaluator shall verify the MDM Agent does not accept the digitally signed policy.

FMT_POL_EXT.2.2 The MDM Agent shall not install policies if the policy signing certificate is deemed invalid.

Assurance Activity:

The assurance activity for this requirement is performed in conjunction with the assurance activity for FIA_X509_EXT.1 and FIA_X509_EXT.2.

D.2. Objective TOE or Platform Security Functional Requirements

D.2.1. Security Audit (FAU)

D.2.1.1 Audit Data Generation

FAU_GEN.1.2(2) Refinement: The [selection: TSF, TOE platform] shall record within each **MDM Agent** audit record at least the following information:

- **date and time of the event,**
- **type of event,**
- **subject identity,**
- **(if relevant) the outcome (success or failure) of the event,**
- **additional information in Table 7**
- **[assignment: *other audit relevant information*].**

Application Note:

All audits must contain at least the information mentioned in FAU_GEN.1.2(2), but may contain more information which can be assigned. The ST author shall identify in the TSS which information of the audit record that is performed by the MDM Agent and that which is performed by the MDM Agent's platform.

Assurance Activity:

TSS

The evaluator shall check the TSS and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field.

TEST

When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.

E. Entropy Documentation and Assessment

This appendix describes the required supplementary information for each entropy source used by the TOE.

The documentation of the entropy source(s) should be detailed enough that, after reading, the evaluator will thoroughly understand the entropy source and why it can be relied upon to provide sufficient entropy. This documentation should include multiple detailed sections: design description, entropy justification, operating conditions, and health testing. This documentation is not required to be part of the TSS.

E.1. Design Description

Documentation shall include the design of each entropy source as a whole, including the interaction of all entropy source components. Any information that can be shared regarding the design should also be included for any third-party entropy sources that are included in the product.

The documentation will describe the operation of the entropy source to include, how entropy is produced, and how unprocessed (raw) data can be obtained from within the entropy source for testing purposes. The documentation should walk through the entropy source design indicating where the entropy comes from, where the entropy output is passed next, any post-processing of the raw outputs (hash, XOR, etc.), if/where it is stored, and finally, how it is output from the entropy source. Any conditions placed on the process (e.g., blocking) should also be described in the entropy source design. Diagrams and examples are encouraged.

This design must also include a description of the content of the security boundary of the entropy source and a description of how the security boundary ensures that an adversary outside the boundary cannot affect the entropy rate.

If implemented, the design description shall include a description of how third-party applications can add entropy to the RBG. A description of any RBG state saving between power-off and power-on shall be included.

E.2. Entropy Justification

There should be a technical argument for where the unpredictability in the source comes from and why there is confidence in the entropy source delivering sufficient entropy for the uses made of the RBG output (by this particular TOE). This argument will include a description of the expected min-entropy rate (i.e. the minimum entropy (in bits) per bit or byte of source data) and explain that sufficient entropy is going into the TOE randomizer seeding process. This discussion will be part of a justification for why the entropy source can be relied upon to produce bits with entropy.

The amount of information necessary to justify the expected min-entropy rate depends on the type of entropy source included in the product.

For developer provided entropy sources, in order to justify the min-entropy rate, it is expected that a large number of raw source bits will be collected, statistical tests will be performed, and the min-entropy rate determined from the statistical tests. While no particular statistical tests are required at this time, it is expected that some testing is necessary in order to determine the amount of min-entropy in each output.

For third party provided entropy sources, in which the TOE vendor has limited access to the design and raw entropy data of the source, the documentation will indicate an estimate of the amount of min-entropy obtained from this third-party source. It is acceptable for the vendor to “assume” an amount of min-entropy, however, this assumption must be clearly stated in the documentation provided. In particular, the min-entropy estimate must be specified and the assumption included in the ST.

Regardless of type of entropy source, the justification will also include how the DRBG is initialized with the entropy stated in the ST, for example by verifying that the min-entropy rate is multiplied by the amount of source data used to seed the DRBG or that the rate of entropy expected based on the amount of source data is explicitly stated and compared to the statistical rate. If the amount of source data used to seed the DRBG is not clear or the calculated rate is not explicitly related to the seed, the documentation will not be considered complete.

The entropy justification shall not include any data added from any third-party application or from any state saving between restarts.

E.3. Operating Conditions

The entropy rate may be affected by conditions outside the control of the entropy source itself. For example, voltage, frequency, temperature, and elapsed time after power-on are just a few of the factors that may affect the operation of the entropy source. As such, documentation will also include the range of operating conditions under which the entropy source is expected to generate random data. Similarly, documentation shall describe the conditions under which the entropy source is no longer guaranteed to provide sufficient entropy. Methods used to detect failure or degradation of the source shall be included.

E.4. Health Testing

More specifically, all entropy source health tests and their rationale will be documented. This will include a description of the health tests, the rate and conditions under which each health test is performed (e.g., at startup, continuously, or on-demand), the expected results for each health test, TOE behavior upon entropy source failure, and rationale indicating why each test is believed to be appropriate for detecting one or more failures in the entropy source.

F. Glossary

F.1. Technical Definitions

Mobile Device User (User)	This is the person who uses and is held responsible for the mobile device's physical control and operation.
Administrator	The Administrator is responsible for management activities, including setting the policy that is applied by the enterprise on the Mobile Device. This administrator is the Mobile Device Management (MDM) Administrator, acting through an MDM Agent.
Operating System (OS)	Software which runs at the highest privilege level and can directly control hardware resources. Modern mobile devices typically have at least two primary operating systems: one which runs on the cellular baseband processor and one which runs on the application processor. The platform of the application processor handles most user interaction and provides the execution environment for apps. The platform of the cellular baseband processor handles communications with the cellular network and may control other peripherals. The term OS, without context, may be assumed to refer to the platform of the application processor.
Unenrolled state	The state in which a Mobile Device is not managed by an MDM system.
Enrolled state	The state in which a Mobile Device is managed by a policy from an MDM system.

F.2. Common Criteria Definitions

Assurance	Grounds for confidence that a TOE meets the SFRs [CC1].
CC	Common Criteria
CM	Configuration Management
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
Security Target (ST)	Implementation-dependent statement of security needs for a specific identified TOE.
Target of Evaluation (TOE)	Set of software, firmware and hardware under evaluation, possibly accompanied by guidance.
TOE Security Functionality (TSF)	Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.
TOE Summary Specification (TSS)	Documentation which provides evaluators with a description of the implementation of SFRs in the TOE.

G. MANAGEMENT FUNCTIONS

For the reader's convenience this Appendix reproduces the Management Function table from FMT_SMF_EXT.1 in the MDF PP

Management Function **Status Markers:** M – Mandatory O – Optional/Objective	**FMT_SMF_EXT.1**	**FMT_MOF_EXT.1.1**	**Administrator**	**FMT_MOF_EXT.1.2**
1. configure password policy: a. minimum password length b. minimum password complexity c. maximum password lifetime	M	-	M	M
2. configure session locking policy: a. screen-lock enabled/disabled b. screen lock timeout c. number of authentication failures	M	-	M	M
3. enable/disable the VPN protection: a. across device [selection: *b. on a per-app basis* *c. no other method*]	M	O	O	O
4. enable/disable [assignment: *list of radios*]	M	O	O	O
5. enable/disable [assignment: *list of audio or visual collection devices*]: a. across device [selection: *b. on a per-app basis* *c. no other method*]	M	-	M	M
6. specify wireless networks (SSIDs) to which the TSF may connect	M	-	M	O
7. configure security policy for each wireless network: a. [selection: *specify the CA(s) from which the TSF will accept WLAN authentication server certificate(s), specify the FQDN(s) of acceptable WLAN authentication server certificate(s)*] b. security type c. authentication protocol d. client credentials to be used for authentication	M	-	M	O
8. transition to the locked state	M	-	M	-
9. TSF wipe of protected data	M	-	M	-
10. configure application installation policy by [selection: *a. restricting the sources of applications,* *b. specifying a set of allowed applications based on [assignment: application characteristics] (an application whitelist),* c. *denying installation of applications*]	M	-	M	M
11. import keys/secrets into the secure key storage	M	O	O	-

12. destroy imported keys/secrets and [selection: *no other keys/secrets, [assignment: list of other categories of keys/secrets]*] in the secure key storage	M	O	O	-
13. import X.509v3 certificates into the Trust Anchor Database	M	-	M	O
14. remove imported X.509v3 certificates and [selection: *no other X.509v3 certificates, [assignment: list of other categories of X.509v3 certificates]*] in the Trust Anchor Database	M	O	O	-
15. enroll the TOE in management	M	M	O	-
16. remove applications	M	-	M	O
17. update system software	M	-	M	O
18. install applications	M	-	M	O
19. remove Enterprise applications	M	-	M	-
20. configure the Bluetooth trusted channel: a. disable/enable the Discoverable mode (for BR/EDR) b. change the Bluetooth device name [selection: *c. allow/disallow additional wireless technologies to be used with Bluetooth,* *d. disable/enable Advertising (for LE),* *e. disable/enable the Connectable mode* *f. disable/enable the Bluetooth services and/or profiles available on the device,* *g. specify minimum level of security for each pairing ,* *h. configure allowable methods of Out of Band pairing* i. *no other Bluetooth configuration*]	M	O	O	O
21. enable/disable display notification in the locked state of: [selection: *a. email notifications,* *b. calendar appointments,* *c. contact associated with phone call notification,* *d. text message notification,* *e. other application-based notifications,* f. *all notifications*]	M	O	O	O
22. enable/disable all data signaling over [assignment: *list of externally accessible hardware ports*]	O	O	O	O
23. enable/disable [assignment: *list of protocols where the device acts as a server*]	O	O	O	O
24. enable/disable developer modes	O	O	O	O
25. enable data-at rest protection	O	O	O	O
26. enable removable media's data-at-rest protection	O	O	O	O
27. enable/disable bypass of local user authentication	O	O	O	O
28. wipe Enterprise data	O	O	O	-
29. approve [selection: *import, removal*] by applications of X.509v3 certificates in the Trust Anchor Database	O	O	O	O
30. configure whether to establish a trusted channel or disallow establishment if the TSF cannot establish a connection to determine the validity of a certificate	O	O	O	O

31. enable/disable the cellular protocols used to connect to cellular network base stations	O	O	O	O
32. read audit logs kept by the TSF	O	O	O	-
33. configure [selection: *certificate, public-key*] used to validate digital signature on applications	O	O	O	O
34. approve exceptions for shared use of keys/secrets by multiple applications	O	O	O	O
35. approve exceptions for destruction of keys/secrets by applications that did not import the key/secret	O	O	O	O
36. configure the unlock banner	O	-	O	O
37. configure the auditable items	O	-	O	O
38. retrieve TSF-software integrity verification values	O	O	O	O
39. enable/disable [selection: a. *USB mass storage mode,* b. *USB data transfer without user authentication,* c. *USB data transfer without authentication of the connecting system*]	O	O	O	O
40. enable/disable backup to [selection: *locally connected system, remote system*]	O	O	O	O
41. enable/disable [selection: a. *Hotspot functionality authenticated by [selection: pre-shared key, passcode, no authentication],* b. *USB tethering authenticated by [selection: pre-shared key, passcode, no authentication]*]	O	O	O	O
42. approve exceptions for sharing data between [selection: *application processes, groups of application processes*]	O	O	O	O
43. place applications into application process groups based on [assignment: *application characteristics*]	O	O	O	O
44. enable/disable location services: a. across device [selection: *b. on a per-app basis* c. *no other method*]	M	O	O	O
45. [assignment: *list of other management functions to be provided by the TSF*]	O	O	O	O

Table 8: Management Functions