Extended Package for Mobile Device Management Agents

Version: 3.0

2016-11-21

National Information Assurance Partnership

Revision History

Version	Date	Comment
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.
3.0	21 November 2016	Updates to align with Technical Decisions. Added requirements to support BYOD use case.

Table of Contents

1 Introduction

1.1 Overview

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.

1.2 Terms

The following sections provide both Common Criteria and technology terms used in this PP.

1.2.1 Common Criteria Terms

Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Extended Package (EP)	An implementation-independent set of security requirements for a specific subset of products described by a PP.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Security Assurance Requirement (SAR)	A requirement for how the TOE's proper implementation of the SFRs is verified by an evaluator.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.

1.2.2 Technology Terms

Term	**Meaning**
Administrator	The person who is responsible for management activities, including setting the policy that is applied by the enterprise on the mobile device.

Enrolled State	The state in which a mobile device is managed by a policy from an MDM.
Mobile Device User	The person who uses and is held responsible for a mobile device.
Operating System	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
Unenrolled State	The state in which a mobile device is not managed by an MDM system.
User	See Mobile Device User.

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.

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

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

1.3.1 TOE Boundary

Figure 1 shows a high-level example of the TOE boundary and its operational environment. As stated above, note that the TOE resides on the MDM Agent and may either be provided as part of the mobile device itself (shown in red) or distributed as a third-party application from the developer of the MDM Server software (shown in blue).

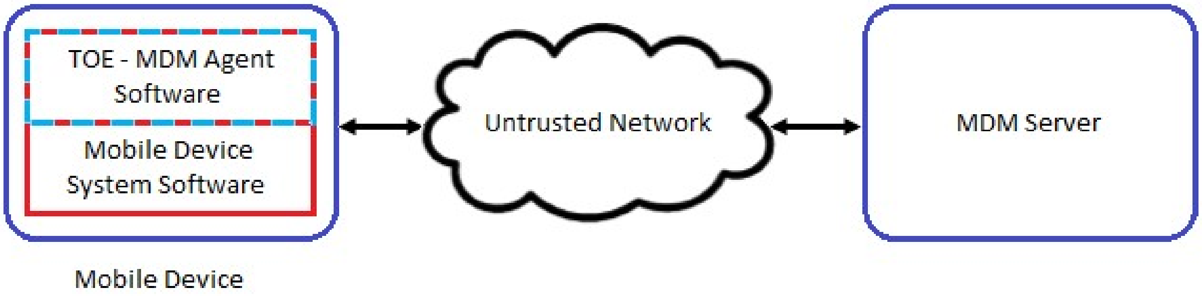

Figure 1. MDM System Operating Environment

The MDM Agent must closely interact with or be part of the mobile device's platform in order to establish policies and to perform queries about device status. The mobile device, in turn, has its own security requirements specified in the MDF PP. The mobile device must be evaluated against the MDF PP, either concurrently with the MDM Agent or prior to the evaluation of the MDM Agent. This is true regardless of whether the MDM Agent is a native part of the mobile device OS or a third-party application.

1.4 How to Use This Extended Package

This EP can extend the Mobile Device Fundamentals PP v3.x or the Mobile Device Management Server PP v3.x:

Extends Mobile Device

The TOE is a native part of a mobile operating system. The TOE for this EP combined with the MDF PP is the mobile device itself plus the MDM Agent.

Extends MDM Server

The TOE is a third-party application that is provided with an MDM Server and installed on a mobile device by the user after acquiring the mobile device. The TOE for this EP combined with the MDM Server PP is the entire MDM environment, which includes both the MDM Server and the MDM Agent. Even though the mobile device itself is not part of the TOE, it is expected to be evaluated against the MDF PP so that its baseline security capabilities can be assumed to be present.

1.5 Use Cases

This EP defines 4 use cases:

[USE CASE 1] Enterprise-owned device for general-purpose enterprise use

An Enterprise-owned device for general-purpose business use is commonly called Corporately Owned, Personally Enabled (COPE). This use case entails a significant degree of Enterprise control over configuration and software inventory. Enterprise administrators use an MDM product to establish policies on the mobile devices prior to user issuance. Users may use Internet connectivity to browse the web or access corporate mail or run Enterprise applications, but this connectivity may be under significant control of the Enterprise. The user may also be expected to store data and use applications for personal, non-enterprise use. The

Enterprise administrator uses the MDM product to deploy security policies and query mobile device status. The MDM may issue commands for remediation actions.

[USE CASE 2] Enterprise-owned device for specialized, high-security use

An Enterprise-owned device with intentionally limited network connectivity, tightly controlled configuration, and limited software inventory is appropriate for specialized, high-security use cases. As in the previous use case, the MDM product is used to establish such policies on mobile devices prior to issuance to users. The device may not be permitted connectivity to any external peripherals. It may only be able to communicate via its Wi-Fi or cellular radios with the Enterprise-run network, which may not even permit connectivity to the Internet. Use of the device may require compliance with usage policies that are more restrictive than those in any general-purpose use case, yet may mitigate risks to highly sensitive information. Based upon the operation environment and the acceptable risk level of the enterprise, those security functional requirements outlined in Section 5 of this Protection Profile along with the selections in the Use Case 2 template defined in Section G.2 are sufficient for the high-security use case.

[USE CASE 3] Personally owned device for personal and enterprise use

A personally owned device, which is used, for both personal activities and enterprise data is commonly called Bring Your Own Device (BYOD). The device may be provisioned for access to enterprise resources after significant personal usage has occurred. Unlike in the enterprise-owned cases, the enterprise is limited in what security policies it can enforce because the user purchased the device primarily for personal use and is unlikely to accept policies that limit the functionality of the device.

However, because the Enterprise allows the user full (or nearly full) access to the Enterprise network, the Enterprise will require certain security policies, for example a password or screen lock policy, and health reporting, such as the integrity of the mobile device system software, before allowing access. The administrator of the MDM can establish remediation actions, such as wipe of the Enterprise data, for non-compliant devices. These controls could potentially be enforced by a separation mechanism built-in to the device itself to distinguish between enterprise and personal activities, or by a third-party application that provides access to enterprise resources and leverages security capabilities provided by the mobile device. Based upon the operational environment and the acceptable risk level of the enterprise, those security functional requirements outlined in Section 5 of this Protection Profile along with the selections in the Use Case 3 template defined in Section G.3 are sufficient for the secure implementation of this BYOD use case.

[USE CASE 4] Personally owned device for personal and limited enterprise use

A personally owned device may also be given access to limited enterprise services such as enterprise email. Because the user does not have full access to the enterprise or enterprise data, the enterprise may not need to enforce any security policies on the device. However, the enterprise may want secure email and web browsing with assurance that the services being provided to those clients by the Mobile Device are not compromised. Based upon the operational environment and the acceptable risk level of the enterprise, those security functional requirements outlined in Section 5 of this PP are sufficient for the secure implementation of this BYOD use case.

2 Conformance Claims

Conformance Statement

To be conformant to this EP, an ST must demonstrate Exact Conformance, a subset of Strict Conformance as defined in [CC] Part 1 (ASE_CCL). The ST must include all components in this PP that are:

- Unconditional (which are always required)
- Selection-based (which are required when certain selections are chosen in the unconditional requirements)

It may also include components that are:

- Optional
- Objective

Unconditional requirements are found in the main body of the document (Section 5), while appendices contain the selection-based, optional, and objective requirements. The ST may iterate any of these components but it must not introduce any additional component (e.g., from CC Part 2 or 3) that is not defined in this EP.

CC Conformance Claims

This EP is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Revision 4 [CC].

PP Claims

This EP does not claim conformance to any Protection Profile. Note that this EP extends the MDF PP or the MDM PP, which means that it relies on the MDF PP or MDM PP to provide some set of 'base' functionality which is then expanded upon by this EP. This, however, does not imply that the EP is conformant to the MDF PP or the MDM PP.

Package Claims

This EP does not claim conformance to any packages.

3 Security Problem Description

3.1 Threats

T.MALICIOUS_APPS

Malicious or flawed application threats exist because apps loaded onto a mobile device may include malicious or exploitable code. An administrator of the MDM or mobile device user may inadvertently import malicious code, or an attacker may insert malicious code into the TOE, resulting in the compromise of TOE or TOE data.

T.BACKUP

An attacker may try to target backups of data or credentials and exfiltrate data. Since the backup is stored on either a personal computer or end user's backup repository, it's not likely enterprise would detect compromise.

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 user data. Although these attacks are primarily directed against the mobile device platform, the MDM Agent configures features, which address this threat.

3.2 Assumptions

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.

3.3 Organizational Security Policies

P.ACCOUNTABILITY

Personnel operating the TOE shall be accountable for their actions within the TOE.

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.

4 Security Objectives

4.1 Security Objectives for the TOE

O.ACCOUNTABILITY

The TOE must provide logging facilities, which record management actions undertaken by its administrators.

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 entire lifecycle, including policy updates and its possible unenrollment from management services.

O.DATA_PROTECTION_TRANSIT

Data exchanged between the MDM Server and the MDM Agent must be protected from being monitored, accessed, or altered.

4.2 Security Objectives for the Operational Environment

OE.DATA_PROPER_ADMIN

TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

OE.DATA_PROPER_USER

Users of the mobile device are trained to securely use the mobile device and apply all guidance in a trusted manner.

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.WIRELESS_NETWORK

A wireless network will be available to the mobile devices.

5 Security 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.

5.1 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:

- **Refinement** operation (denoted by **bold text**) is used to add details to a requirement, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text):* is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*) is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: are identified with a number inside parentheses (e.g. “(1)”).
- **Extended SFRs**: are identified by having a label “EXT” after the SFR name.

5.2 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.

5.3 MDF PP Security Functional Requirements Direction

If this EP is extending the MDF PP, the MDM 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(1), FCS_CKM_EXT.4, FCS_COP.1(*), FCS_RBG_EXT.1, FCS_TLSC_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3, FPT_TST_EXT.1, FCS_DTLS_EXT.1, and FCS_HTTPS_EXT.1.

5.3.1 Cryptographic Support (FCS)

FCS_STG_EXT.4 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 use the platform provided key storage for all persistent secret and private keys.

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.

5.3.2 Trusted Path/Channels (FTP)

FTP_ITC_EXT.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 [*selection: TLS, DTLS, HTTPS*] 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 all communication between the MDM Agent and the MDM Server and [*selection: all communication between the MAS Server and the MDM Agent, no other communication*].

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 each supported identifier type (excluding DNs), the evaluator shall repeat the following tests:

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.

5.4 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 include 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, 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.

5.4.1 Cryptographic Support (FCS)

FCS_STG_EXT.4 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 use the platform provided key storage for all persistent secret and private keys.

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.

FCS_TLSC_EXT.1 TLS Client Protocol

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

5.4.2 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.

5.5 TOE Security Functional Requirements

5.5.1 Security Audit (FAU)

FAU_ALT_EXT.2 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 audit events:

- successful application of policies to a mobile device,
- [*selection: receiving, generating*] periodic reachability events,

[*selection:*

- *change in enrollment state,*
- *failure to install an application from the MAS Server,*
- *failure to update an application from the MAS Server,*
- *[assignment: other events], no other events*]

Application Note: *The trusted channel is defined in FPT_ITT.1 if Agent extends MDM Server and FTP_ITC_EXT.1 if Agent extends MDF PP. "Alert" in this requirement could be as simple as an audit record or a notification. If any prior alerts exist in the queue, per FAU_ALT_EXT.2.2, those alerts shall be sent when the trusted channel is available.*

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.

Application Note: *If the trusted channel is not available, alerts shall be queued. When the trusted channel becomes available, the queued alerts shall be sent.*

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 as defined 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 upon re-establishment of the connectivity.

FAU_GEN.1(2) Audit Data Generation

Note that the following requirement is not listed alongside its corresponding FAU_GEN.1.2(2). This is because the generation of audit data is always the responsibility of the TSF (i.e. auditable events will occur based on TOE behavior) but the recording of the audit data will be either within the TOE boundary or by the underlying mobile device platform. For this reason, FAU_GEN.1.2(2) is defined in section 5.6.1 below. The ST author will always include both FAU_GEN.1.1(2) and FAU_GEN.1.2(2) regardless; the only difference is whether FAU_GEN.1.2(2) is performed by the TOE or if the TSF relies on the underlying platform.

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

- **startup and shutdown of the MDM Agent,**
- **change in MDM policy,**
- **any modification commanded by the MDM Server,**
- **specifically defined auditable events listed in Table 1,**
- **[*assignment: other* events]**

Application Note: *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 use the TOE to perform the auditable events defined in Table 1 and observe that accurate audit records are generated with contents and formatting consistent with those described in the TSS. Note that this testing can be accomplished in conjunction with the testing of the security mechanisms directly.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_ALT_EXT.2	Type of alert.	No additional information.
FAU_GEN.1	None	N/A

FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	No additional information.
FCS_STG_EXT.4/ FCS_STG_EXT.1(1)	None	N/A
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	Attempt to unenroll.	No additional information.
FTP_ITC_EXT.1/ FTP_ITT_EXT.1	Initiation and termination of trusted channel.	Trusted channel protocol. Non-TOE endpoint of connection.

Table 1 - Auditable Events

FAU_SEL.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:

- **event type;**
- **success of auditable security events;**
- **failure of auditable security events; and**
- **[*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 examine the operational guidance to determine that it contains instructions on how to define the set of auditable events as well as explains the syntax for multi-value selection (if applicable). The evaluator shall also verify that the operational guidance shall 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.

5.5.2 Identification and Authentication (FIA)

FIA_ENR_EXT.2 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.

5.5.3 Security Management (FMT)

FMT_POL_EXT.2 Trusted Policy Update

FMT_POL_EXT.2.1 The MDM Agent shall only accept policies and policy updates that are 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 as defined in the base PPs.

FMT_SMF_EXT.3 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:*

- *administrator-provided management functions in MDF PP,*
- *administrator-provided device management functions in MDM PP*]
- Import the certificates to be used for authentication of MDM Agent communications
- [*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 4 in MDF PP 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; the Mobile Device must support these additional commands or configuration policies.

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:

- Enroll in management,
- Configure whether users can unenroll from management,
- [*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, if assigned.

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.

FMT_UNR_EXT.1 User Unenrollment Prevention

FMT_UNR_EXT.1.1 The MDM Agent shall provide a mechanism to enforce the following behavior upon an attempt to unenroll the mobile device from management: [*selection: prevent the unenrollment from occurring, apply remediation actions*].

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, for example a BYOD usage, the MDFPP describes remediation actions performed upon unenrollment, such as wiping enterprise data, 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 from unenrolling or the remediation actions applied when unenrolled.

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

If 'prevent the unenrollment from occurring' is selected:

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.

If 'apply remediation actions' is selected:

Test 2: If any configuration allows the user to unenroll, the evaluator shall configure the Agent to allow user unenrollment, attempt to unenroll, and verify that the remediation actions are applied.

5.6 TOE or Platform Security Functional Requirements

5.6.1 Security Audit (FAU)

FAU_GEN.1(2) Audit Data Generation

FAU_GEN.1.2(2) 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 1,**
- **[*assignment: other relevant audit 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.

5.7 TOE 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 SFRs and Security Assurance Requirements (SARs). Additionally, this EP includes a number of SFR-based Assurance Activities that simply 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. Optional Requirements

As indicated in Section 2, the baseline requirements (those that must be performed by the TOE) are contained in the body of this PP. Additionally, there are three other types of requirements specified in Appendix A, Appendix B, and Appendix C.

The first type (in this Appendix) are requirements that can be included in the ST, but are not required in order for a TOE to claim conformance to this PP. The second type (in Appendix B) are requirements based on selections in the body of the EP: if certain selections are made, then additional requirements in that appendix must be included. The third type (in Appendix C) 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 vendors is encouraged. Note that the ST author is responsible for ensuring that requirements that may be associated with those in Appendix A, Appendix B, and Appendix C but are not listed (e.g., FMT-type requirements) are also included in the ST.

At this time no optional requirements are identified.

B. 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 the EP. There are additional requirements based on selections in the body of the EP: if certain selections are made, then additional requirements below will need to be included.

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

C. 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.

C.1 Objective TOE Security Functional Requirements

C.1.1 Security Audit (FAU)

FAU_STG_EXT.1 Security Audit Event Storage

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

Application Note: *FAU_STG_EXT.1 shall only be included in the ST for MDM Agent platforms (i.e., mobile devices) that conform to Mobile Device Fundamentals Protection Profile version 3.*

Assurance Activity

TSS

The evaluator shall 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.

C.1.2 Protection of the TSF (FPT)

FPT_NET_EXT.1 Network Reachability

FPT_NET_EXT.1.1 The TSF shall detect when a configurable [*selection: positive integer of missed reachability events occur, time limit is exceeded*] related to the last successful connection with the server has been reached.

Application Note: *This requirement is to enable the Agent to determine if it has been out of connectivity with the Server for too long. The configuration of the number of allowed missed reachability events or time limit since last successful connection with the server is handled in Server configuration policy of the Agent (FMT_SMF.1.1(1) function 56a). If FMT_SMF.1.1(1) function 56a is included in the ST, then FPT_NET_EXT.1.1 shall be included in the MDM Server ST.*

If the Agent has been out of connectivity with the server for too long than the remediation actions specified in function 56b shall occur. For example if the Agent has not synced with the server in the allowed amount of time that the Agent shall wipe the device without requiring a command from the Server.

Assurance Activity

TSS

The evaluator shall verify that the TSS contains a description of how the Agent determines how long it has been since the last successful connection with the Server (i.e., total number of missed reachability events or time). If total number of missed reachability events is selected, the evaluator shall verify that the TSS contains a description of how often the reachability events are sent.

Guidance

The evaluator shall verify that the AGD guidance instructs the administrator, if needed, how to configure the TOE to detect when the time since last successful connection with the server has been reached.

Test

Test 1: The evaluator shall configure the Server configuration policy of the Agent per FMT_SMF.1.1(1) function 56. The device shall be placed in airplane mode to prevent connectivity with the Server. The evaluator shall verify that after the configured time, the remediation actions selected in function 56 occur.

D. Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy source(s) beyond the requirements outlined in the ‘Entropy Documentation and Assessment’ sections of the MDF and MDM PPs. As with other base PP requirements, the only additional requirement is that the entropy documentation also applies to the specific MDM Agent capabilities of the TOE in addition to the functionality required by the base PP.

E. Use Case Template

The following use case templates list those selections, assignments, and objective requirements that best support the use cases identified by this Protection Profile. Note that the templates assume that all SFRs listed in Section 5 are included in the ST, not just those listed in the templates. These templates and deviations from the template should be identified in the Security Target to assist customers with making risk-based purchasing decisions. Products that do not meet these templates are not precluded from use in the scenarios identified by this Protection Profile.

Where selections for a particular requirement are not identified in a use case template, all available selections are equally applicable to the use case.

E.1 [Use Case 1] Enterprise-owned device for general-purpose enterprise use

E.2 [Use Case 2] Enterprise-owned device for specialized, high-security use

Requirement	**Action**
FAU_ALT_EXT.2.1 Function c	Include in ST.
FMT_UNR_EXT.1.1	Select “prevent the unenrollment from occurring”.

E.3 [Use Case 3] Personally owned device for personal and enterprise use

Requirement	**Action**
FMT_UNR_ENT.1.1	Select “apply remediation actions”

E.4 [Use Case 4] Personally owned device for personal and limited enterprise use

At this time no requirements are recommended for this use case.

F. References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012 • Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012 • Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 Revision 4, September 2012
[MDF PP]	Protection Profile for Mobile Device Fundamentals, Version 3.0, June 2016
[MDM PP]	Protection Profile for Mobile Device Management, Version 3.0, November 2016

F. Acronyms

All relevant acronyms for this EP are defined in the MDF PP and/or MDM PP.