

## PP-Module for MDM Agents

**This page is best viewed with JavaScript enabled!**



Version: 41.0

20182019-1104-2825

National Information Assurance Partnership

# Revision History

Version	Date	Comment
1.0	2013-10-21	Initial Release
1.1	2014-02-07	Typographical changes and clarifications to front-matter
2.0	2014-12-31	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	2016-11-21	Updates to align with Technical Decisions. Added requirements to support BYOD use case
4.0	<del>2018</del> 2019-12-03-2001	Convert to PP-Module.

## Contents

[1Introduction1.1Overview1.2Terms1.2.1Common Criteria Terms1.2.2Technical Terms1.3Compliant Targets of Evaluation1.3.1TOE Boundary1.4Use Cases2Conformance Claims3Security Problem Description3.1Threats3.2Assumptions3.3Organizational Security Policies4Security Objectives4.1Security Objectives for the TOE4.2Security Objectives for the Operational Environment4.3Security Objectives Rationale5Security Requirements5.1MDF PP Security Functional Requirements Direction 5.1.1Unmodified SFRs 5.1.2Modified SFRs 5.1.2.1Trusted Path/Channels \(FTP\)5.1.3Additional SFRs 5.1.3.1Cryptographic Support \(FCS\)5.1.3.2Trusted Path/Channels \(FTP\)5.2MDM PP Security Functional Requirements Direction 5.2.1UnmodifiedModified SFRs 5.2.2ModifiedAdditional SFRs 5.2.2.1Cryptographic Support \(FCS\)5.2.2.2Protection of the TSF \(FPT\)5.2.3Additional SFRs 5.3TOE Security Functional Requirements5.3.1Security Audit \(FAU\)5.3.2Identification and Authentication \(FIA\)5.3.3Security Management \(FMT\)6Consistency Rationale6.1Mobile Device Fundamentals Protection Profile6.1.1Consistency of TOE Type6.1.2Consistency of Security Problem Definition6.1.3Consistency of Objectives6.1.4Consistency of Requirements6.2Mobile Device Management Protection Profile6.2.1Consistency of TOE Type6.2.2Consistency of Security Problem Definition6.2.3Consistency of Objectives6.2.4Consistency of RequirementsAppendix A - Optional SFRsAppendix B - Selection-based SFRsAppendix C - Objective SFRsAppendix D - BibliographyExtended Component DefinitionsD.1Background and ScopeD.2Extended Component DefinitionsAppendix E - Use Case TemplatesAppendix F - BibliographyAppendix G - Acronyms](#)

# 1 Introduction

## 1.1 Overview

The scope of ~~this~~ the MDM Agent [PP-Module](#) is to describe the security functionality of a Mobile Device Management (MDM) Agent in terms of [\[CC\]](#) and to define functional and assurance requirements for such products This [PP-Module](#) is intended for use with the following ~~Base-PPs~~[PPs](#):

- Mobile Device Management (MDM) Protection Profile, Version 4.0
- Mobile Device ~~Fundamentals~~ [Fundamentals](#) (MDF) Protection Profile, Version 3.1

These ~~Base-PPs~~[PPs](#) are valid because a [MDM](#) Agent is either a 3rd party application manufactured by the [MDM](#) Server vendor or is a native application deployed on a mobile device.

## 1.2 Terms

The following sections list Common Criteria and technology terms used in this document.

### 1.2.1 Common Criteria Terms

Base Protection Profile (Base-PP)	Protection Profile used to build a PP-Configuration.
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.
Protection	An implementation-independent set of security requirements for a category of

Profile (PP)	products.		
Protection Profile	Protection Profile composed of Base Protection Profiles and Protection ProfileA		
Configuration (PP-Configuration)	comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.		
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles.		
Security Assurance Requirement (SAR)	A requirement for how the <a href="#">TOE</a> 's proper implementation of the <a href="#">SFRs</a> is verified by an evaluator.	Security Functional Requirement (SFR)	A requirement for security enforcement by the <a href="#">TOE</a> .
Security Target (ST)	A set of implementation-dependent security requirements for a specific product		
Target of Evaluation (TOE)	The security functionality of 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 <a href="#">TOE</a> satisfies the <a href="#">SFRs</a> in an <a href="#">ST</a> .		

## 1.2.2 Technical Terms

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 Application Store (MAS)	Mobile Application Store		
Mobile Device Management (MDM)	Mobile Device Management		
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 <a href="#">MDM</a> 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. This [PP-Module](#) specifically addresses the [MDM](#) Agent. A compliant MDM Agent 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, from which it receives policies to enforce on the mobile device. 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 [PP-Module](#) 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 [PP-Module](#).

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. This [PP-Module](#) builds on either the Mobile Device Fundamentals [PP](#) v3.1 MDF PP or the Mobile Device

Management Server MDM PP-v4.0. A TOE that claims conformance to this PP-Module must also claim conformance to one of those PPs as its Base-PP. A compliant TOE is obligated to implement the functionality required in the Base-PP along with the additional functionality defined in this PP-Module in order to mitigate the threats that are defined by this PP-Module.

This PP-Module shall build on Mobile Device Fundamentals the MDF PP if the TOE is a native part of a mobile operating system. The TOE for this PP-Module combined with the MDF PP is the mobile device itself plus the MDM Agent. 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 PP-Module 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 PP-Module.

This PP-Module shall build on the MDM Server PP if 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 distributed TOE for this PP-Module 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.

### 1.3.1 TOE Boundary

Figure 1 shows a high-level example of the PP-Module TOE boundary and its operational environment. As stated above, the MDM Agent 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 Agent 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 Use Cases

This PP-Module 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 Security Requirements of this Protection Profile along with the selections in the Use Case 2 template defined in Section G.2 Appendix E - Use Case Templates 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 Security Requirements](#) of this Protection Profile along with the selections in the Use Case 3 template defined in [Section G.3 Appendix E - Use Case Templates](#) 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 Security Requirements](#) of this [PP](#) are sufficient for the secure implementation of this BYOD use case.

## 2 Conformance Claims

### Conformance Statement

To be conformant to this [PP-Module](#), an [ST](#) must demonstrate Exact Conformance, as defined by the [CC](#) inherits exact conformance as required from the specified [Base-PP](#) and as defined in the [CC](#) and [CEM](#) addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017). Exact Conformance is described in [CC](#) and [CEM](#) addenda for Exact Conformance. An [ST](#) that conforms to this [PP-Module](#) must also demonstrate Exact Conformance to the [Base-PP](#) and also make any necessary inclusions, modifications, or exclusions as mandated by

The following [PPs](#) and [PP-Modules](#) are allowed to be specified in a [PP-Configuration](#) that includes both with this [PP-Module](#) and the [Base-PP](#).

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 [PP-Module](#).

- -Module for VPN Client, Version 2.1

### CC Conformance Claims

This [PP-Module](#) is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Revision Release 5 [\[CC\]](#).

### PP Package Claims

This [PP-Module](#) does not claim conformance to any Protection Profile.

### Package Claims

This [PP-Module](#) does not claim conformance to any package.  
is TLS Package Version 1.1 Conformant.

## 3 Security Problem Description

### 3.1 Threats

The following threats are specific to [MDM](#) Agents, and represents an addition to those identified in the [Base-PPs](#).

#### 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 the enterprise would detect compromise.

## 3.2 Assumptions

These assumptions are made on the ~~operational environment~~ Operational Environment in order to be able to ensure that the security functionality specified in the PP-Module can be provided by the TOE. If the TOE is placed in an ~~operational environment~~ Operational Environment that does not meet these assumptions, the TOE may no longer be able to provide all of its security functionality.

### 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 ~~MDFP~~ MDF PP 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

Addressed by: [FAU\\_ALT\\_EXT.2](#), [FAU\\_GEN.1\(2\)](#), [FAU\\_SEL.1\(2\)](#)

#### 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.

Addressed by: [FAU\\_STG\\_EXT.3](#) (optional objective), [FIA\\_ENR\\_EXT.2](#), [FMT\\_POL\\_EXT.2](#), [FMT\\_SMF\\_EXT.34](#), [FMT\\_UNR\\_EXT.1](#)

#### O.DATA\_PROTECTION\_TRANSIT

Data exchanged between the [MDM](#) Server and the [MDM](#) Agent must be protected from being monitored, accessed, or altered.

Addressed by: ~~FCS\_CKM\_EXT.4 (from MDM/MDF Base-PP), FCS\_CKM.1 (from MDM/MDF Base-PP), FCS\_CKM.2 (from MDM Base-PP), FCS\_CKM.2(1) (from MDF Base-PP), FCS\_COP.1(\*) (from MDM/MDF Base-PP), FCS\_DTLSS\_EXT.1 (from TLS Package), FCS\_DTLSC\_EXT.1 (from TLS Package), FCS\_HTTPS\_EXT.1 (from MDM/MDF Base), FCS\_RBG\_EXT.1 (from MDM/MDF Base), FCS\_TLSC\_EXT.1 (from TLS Package), FCS\_TLSC\_EXT.2 (from TLS Package), FCS\_TLSS\_EXT.1 (from TLS Package), FCS\_TLSS\_EXT.2 (from TLS Package), FIA\_X509\_EXT.1(\*) (from MDM/MDF Base), FIA\_X509\_EXT.2 (from MDM/MDF Base), FIA\_X509\_EXT.3 (from MDM/MDF Base), FIA\_X509\_EXT.4 (from MDM Base), FPT\_ITT.1 (refined from MDM Base-PP), FPT\_NET\_EXT.1 (optional objective), FTP\_ITC\_EXT.1 (refined from MDF-2) (if MDF is Base-PP), FTP\_TRP.1(\*2) (from MDM if MDF is Base-PP), TOE-SFR for MDF~~

#### O.STORAGE

To address the issue of loss of confidentiality of user data in the event of loss of a ~~Mobile Device~~ mobile device (T.PHYSICAL), conformant [TOEs](#) will use platform provide key storage. The [TOE](#) is expected to protect its persistent secrets and private keys.



## 4.2 Security Objectives for the Operational Environment

~~This module does not define any assumptions~~ The Operational Environment of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality (which is defined by the security objectives for the TOE). The security objectives for the Operational Environment consist of a set of statements describing the goals that the Operational Environment should achieve. This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means. The assumptions identified in Section 3 are incorporated as security objectives for the 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.

## 4.3 Security Objectives Rationale

This section describes how the assumptions, threats, and organization security policies map to the security objectives.

Threat, Assumption, or OSP	Security Objectives	Rationale
T.MALICIOUS_APPS	O.DATA_PROTECTION_TRANSIT,	The threat T.MALICIOUS_APPS is countered by O.DATA_PROTECTION_TRANSIT as this provides the capability to protect app loading/updates against malicious insertion from the network.
	O.APPLY_POLICY	The threat T.MALICIOUS_APPS is countered by O.APPLY_POLICY as this provides policy preventing loading of unapproved apps into the <a href="#">TOE</a> .
T.BACKUP	O.DATA_PROTECTION_TRANSIT,	The threat T.BACKUP is countered by O.DATA_PROTECTION_TRANSIT as this provides the capability to communicate using one (or more) standard protocols as a means to maintain the confidentiality of data that are transmitted between the Agent and other entities.
	O.APPLY_POLICY	The threat T.BACKUP is countered by O.APPLY_POLICY as this provides policy to enforce that backups be stored <del>only</del> only in secure, protected locations.
T.NETWORK_ATTACK	O.DATA_PROTECTION_TRANSIT,	The threat T.NETWORK_ATTACK is countered by O.DATA_PROTECTION_TRANSIT as this provides the capability to communicate using one (or more) standard protocols as a means to maintain the confidentiality of data that are transmitted between the Agent and other entities.
	O.APPLY_POLICY,	The threat T.NETWORK_ATTACK is countered by O.APPLY_POLICY as this provides a secure configuration of the Agent to protect data that it processes.
	OE.IT_ENTERPRISE	The threat T.NETWORK_ATTACK is countered by OE.IT_ENTERPRISE by reducing the network exposure of the mobile device.
		The threat T.NETWORK_EAVESDROP is countered by O.DATA_PROTECTION_TRANSIT as this provides the capability to communicate using one (or more) standard protocols as a means to maintain the confidentiality of data that are transmitted between the Agent and other entities.
	O.DATA_PROTECTION_TRANSIT,	

T.NETWORK_EAVESDROP	O.APPLY_POLICY, OE.IT_ENTERPRISE	<p>The threat T.NETWORK_EAVESDROP is countered by O.APPLY_POLICY as this provides a secure configuration of the Agent to protect data that it processes.</p> <p>The threat T.NETWORK_EAVESDROP is countered by OE.IT_ENTERPRISE by reducing the network exposure of the mobile device.</p> <p>The threat T.PHYSICAL_ACCESS is countered by O.ACCOUNTABILITY as this provides the capability to log attempts by unauthorized personnel to access data, and to log any access to the data or the device, as well as changes to the device during the time when it is not under the control of an authorized user.</p>
T.PHYSICAL_ACCESS	O.ACCOUNTABILITY, O.APPLY_POLICY, O.STORAGE	<p>The threat T.PHYSICAL_ACCESS is countered by O.APPLY_POLICY as this provides a secure configuration of the Agent to protect data that it processes.</p> <p>The threat T.PHYSICAL_ACCESS is countered by O.STORAGE as this provides the capability to encrypt all user and enterprise data and authentication keys to ensure the confidentiality of data that it stores.</p>
A.CONNECTIVITY	OE.WIRELESS_NETWORK	<p>The <del>operational environment</del> Operational Environment objective OE.WIRELESS_NETWORK is realized through A.CONNECTIVITY.</p>
A.MOBILE_DEVICE_PLATFORM	OE.MOBILE_DEVICE_PLATFORM	<p>The <del>operational environment</del> Operational Environment objective OE.MOBILE_DEVICE_PLATFORM is realized through A.MOBILE_DEVICE_PLATFORM.</p>
A.PROPER_ADMIN	OE.DATA_PROPER_ADMIN	<p>The <del>operational environment</del> Operational Environment objective OE.DATA_PROPER_ADMIN is realized through A.PROPER_ADMIN.</p>
A.PROPER_USER	OE.DATA_PROPER_USER	<p>The <del>operational environment</del> Operational Environment objective OE.DATA_PROPER_USER is realized through A.PROPER_USER.</p>
P.ACCOUNTABILITY	O.ACCOUNTABILITY	<p>O.ACCOUNTABILITY provides logging of personnel actions in order to provide accountability of all personnel actions within the <a href="#">TOE</a>.</p>
P.ADMIN	O.APPLY_POLICY	<p>The <a href="#">TOE</a> adheres to the Enterprise security policy through the application of O.APPLY_POLICY.</p>
P.DEVICE_ENROLL	O.APPLY_POLICY	<p>The <a href="#">TOE</a> enrolls mobile devices for specific users with policy through the application of O.APPLY_POLICY.</p>
P.NOTIFY	O.APPLY_POLICY	<p>The <a href="#">TOE</a> provides the capability for the administrator to apply remediation actions via the <a href="#">MDM</a> system through policy, which is applied through O.APPLY_POLICY.</p>

## 5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the TOE. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [\[CC\]](#). The following notations are used:

- **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 an "EXT" label after the SFR name

### 5.1 MDF PP Security Functional Requirements Direction



In a PP-Configuration the that includes Mobile Device Fundamentals-MDF PP, the TOE is expected to rely on some of the security functions implemented by the Mobile Device as a whole and evaluated against the Base-MDF PP. The following sections describe any modifications that the ST author must make to the SFRs defined in the Base-MDF PP in addition to what is mandated by section 5.43.

## 5.1.1

Unmodified

### Modified SFRs

The SFRs listed in this section are defined in the PP and are relevant to the secure operation of the TOE. When testing the TOE, it is necessary to ensure that these SFRs are tested specifically in conjunction with the Mobile Device Management Agents portion of the TOE. The ST author may complete all selections and assignments in these SFRs without any additional restrictions.

- FAU\_GEN.1
- FAU\_SAR.1
- FAU\_SEL.1
- FAU\_STG.1
- FAU\_STG.4
- FCS\_CKM.1
- FCS\_CKM.2(1)
- FCS\_CKM.2(2)
- FCS\_CKM\_EXT.1
- FCS\_CKM\_EXT.2
- FCS\_CKM\_EXT.3
- FCS\_CKM\_EXT.4
- FCS\_CKM\_EXT.5
- FCS\_CKM\_EXT.6
- FCS\_CKM\_EXT.7
- FCS\_COP.1(1)
- FCS\_COP.1(2)
- FCS\_COP.1(3)
- FCS\_COP.1(4)
- FCS\_COP.1(5)
- FCS\_HTTPS\_EXT.1
- FCS\_IV\_EXT.1
- FCS\_RBG\_EXT.1
- FCS\_RBG\_EXT.2
- FCS\_RBG\_EXT.3
- FCS\_SRV\_EXT.1
- FCS\_SRV\_EXT.2
- FCS\_STG\_EXT.1
- FCS\_STG\_EXT.2
- FCS\_STG\_EXT.3
- FDP\_ACF\_EXT.1
- FDP\_ACF\_EXT.2
- FDP\_ACF\_EXT.3
- FDP\_BCK\_EXT.1
- FDP\_PBA\_EXT.1
- FDP\_DAR
- FDP\_DAR\_EXT.1
- FDP\_DAR\_EXT.2
- FDP\_IFC\_EXT.1
- FDP\_STG\_EXT.1
- FDP\_UPC\_EXT.1
- FIA\_AFL\_EXT.1
- FIA\_BMG\_EXT.1
- FIA\_BMG\_EXT.2
- FIA\_BMG\_EXT.3
- FIA\_BMG\_EXT.4
- FIA\_BMG\_EXT.5
- FIA\_BMG\_EXT.6
- FIA\_PMG\_EXT.1
- FIA\_TRT\_EXT.1
- FIA\_UAU.5
- FIA\_UAU.6
- FIA\_UAU.7
- FIA\_UAU\_EXT.1
- FIA\_UAU\_EXT.2

- FIA\_UAU\_EXT.4
- FIA\_X509\_EXT.1
- FIA\_X509\_EXT.2
- FIA\_X509\_EXT.3
- FIA\_X509\_EXT.4
- FIA\_X509\_EXT.5
- FMT\_MOF\_EXT.1
- FMT\_SMF\_EXT.1
- FMT\_SMF\_EXT.2
- FMT\_SMF\_EXT.3
- FPT\_AEX\_EXT.1
- FPT\_AEX\_EXT.2
- FPT\_AEX\_EXT.3
- FPT\_AEX\_EXT.4
- FPT\_AEX\_EXT.5
- FPT\_AEX\_EXT.6
- FPT\_AEX\_EXT.7
- FPT\_BBD\_EXT.1
- FPT\_BLT\_EXT.1
- FPT\_JTA\_EXT.1
- FPT\_KST\_EXT.1
- FPT\_KST\_EXT.2
- FPT\_KST\_EXT.3
- FPT\_NOT\_EXT.1
- FPT\_NOT\_EXT.2
- FPT\_STM.1
- FPT\_TST\_EXT.1
- FPT\_TST\_EXT.2(1)
- FPT\_TST\_EXT.2(2)
- FPT\_TST\_EXT.3
- FPT\_TUD\_EXT.1
- FPT\_TUD\_EXT.2
- FPT\_TUD\_EXT.3
- FPT\_TUD\_EXT.4
- FPT\_TUD\_EXT.5
- FTA\_SSL\_EXT.1
- FTA\_TAB.1

## 5.1.2 Modified SFRs

The SFRs listed in this section are defined in the Mobile Device Fundamentals Protection Profile and relevant to the secure operation of the TOE. This PP-Module does not modify any SFRs defined by the MDF PP.

## 5.1.2 Additional SFRs

This section defines additional SFRs that must be added to the TOE boundary in order to implement the functionality in any PP-Configuration where the MDF PP is claimed as the Base-PP.

### 5.1.2.1 Cryptographic Support (FCS)

#### FCS\_STG\_EXT.4 Cryptographic Key Storage

##### 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.

### 5.1.2.1-2 Trusted Path/Channels (FTP)

#### FTP\_ITC\_EXT.1(2) Trusted Channel Communication

##### FTP\_ITC\_EXT.1.1(2)

**Refinement:** The TSF shall use [selection:

- *mutually authenticated TLS client as defined in the Package for Transport Layer Security*
- *mutually authenticated DTLS client as defined in the Package for Transport Layer Security*
- *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: The intent of this requirement is to protect the communications channel between [MDM](#) Server and Agent, post enrollment. [FTP\\_TRP.1\(2\)](#) is to protect the communications channel between [MDM](#) Server and Agent during enrollment.

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 requirement is

~~refined~~

iterated from the

~~base~~

MDF PP

; the

to indicate the protocols that the MDM Agent can use for a trusted channel. The mobile device is required to perform the mandated cryptographic protocols as in the

~~base~~

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 [MDM](#) Agent and the [MDM](#) Server. Only TLS, DTLS, or HTTPS are acceptable for this trusted channel.

Since this requirement is only for the case when the [PP-Module](#) builds on MDF PP and in this case it is expected that the [MDM](#) Agent will be a native part of the mobile operating system, it is expected that the [MDM](#) Agent will utilize the mobile device's implementation of the selected protocols. HTTPS (FCS\_HTTPS\_EXT.1) and TLS (FCS\_TLSC\_EXT.1) are already mandatory for a MDF ST. If "TLS" or "DTLS" is selected the following selections from the TLS Functional Package

~~shall~~

must be made:

- FCS\_TLS\_EXT.1:
  - either TLS

~~must be selected~~

- - or DTLS is selected depending on the selection made in [FTP\\_ITC\\_EXT.1.1](#)
  - client must be selected
- FCS\_TLSC\_EXT.1.1:

~~TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA cannot be selected~~

- - The cipher suites selected must correspond with the algorithms and hash functions allowed in [FCS\\_COP.1](#) from the MDF PP.
  - mutual authentication must be selected

~~If DTLS is selected, then the appropriate SFRs from Appendix B in MDF shall be 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\(2\)](#)

**Refinement:** 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 MDFPP.~~

#### [FTP\\_ITC\\_EXT.1.3\(2\)](#)

**Refinement:** 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~~

iterated from the MDF PP; it is expected that

Mobile Device

the 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.

## 5.1.3 Additional SFRs

This section defines additional SFRs that must be added to the TOE boundary in order to implement the functionality in any PP-Configuration where the Mobile Device Fundamentals Protection Profile is claimed as the Base PP.

### 5.1.3.1 Cryptographic Support (FCS)

#### FCS\_STG\_EXT.4 Cryptographic Key Storage

##### 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.

### 5.1.3.2 Trusted Path

#### FTP\_TRP.1(2) Trusted Path (for Enrollment)

##### FTP\_TRP.1.1(2)

**Refinement:** The MDM Agent shall ~~selection: invoke platform-provided functionality, implement functionality~~ to TSF shall use ~~selection:~~

- TLS client as defined in the Package for Transport Layer Security
- HTTPS

] to provide a trusted communication path between itself and another trusted IT product that is logically distinct from other communication paths and provides assured identification of its endpoints and protection of the communicated data from disclosure and detection of modification of the communicated data from ~~modification, disclosure~~.

##### FTP\_TRP.1.2(2)

**Refinement:** The TSF shall ~~selection: invoke platform-provided functionality, implement functionality~~ to permit MD users to initiate communication via the trusted path.

##### FTP\_TRP.1.3(2)

**Refinement:** The TSF shall ~~selection: invoke platform-provided functionality, implement functionality~~ to require the use of the trusted path for ~~all MD user actions~~.

Application Note: This requirement ensures that authorized MD users initiate all communication with the TOE via a trusted path, and that all communications with the TOE by MD users is performed over this path. The purpose of this connection is for enrollment by the MD user.

The ST author chooses the mechanism or mechanisms supported by the TOE. The data passed in this trusted communication channel are encrypted as defined by the protocol chosen in the first selection. The ST author chooses the mechanism or mechanisms supported by the TOE.

If "TLS" is selected the TLS Functional Package must be included in the ST, with the following selections selected.

Since this requirement is only for the case when the PP-Module builds on MDF PP and in this case it is expected that the MDM Agent will be a native part of the mobile operating system, it is expected that the MDM Agent will utilize the mobile device's implementation of the selected protocols. HTTPS (FCS\_HTTPS\_EXT.1) and TLS (FCS\_TLSC\_EXT.1) are already mandatory for a MDF ST. If "TLS" or "DTLS" is selected the following selections from the TLS Functional Package must be made:

- FCS\_TLS\_EXT.1:
  - TLS must be selected
  - client must be selected
- FCS\_TLSC\_EXT.1.1:
  - TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA cannot be selected The cipher suites selected must correspond with the algorithms and hash functions allowed in FCS\_COP.1 from the MDF PP.

## 5.2 MDM PP Security Functional Requirements Direction

In a PP-Configuration that includes Mobile Device Management MDM PP, the TOE is expected to rely on some of the security functions implemented by the MDM Server as a whole and evaluated against the Base-MDM PP. The following sections describe any modifications that the ST author must make to the SFRs defined in the Base-MDM PP in addition to what is mandated by section 5.4.3.

### 5.2.1

Unmodified

## Modified SFRs

The SFRs listed in this section are defined in the PP and are relevant to the secure operation of the TOE. When testing the TOE, it is necessary to ensure that these SFRs are tested specifically in conjunction with the Mobile Device Management Agents portion of the TOE. The ST author may complete all selections and assignments in these SFRs without any additional restrictions.

- FAU\_ALT\_EXT.1
- FAU\_CRP\_EXT.1
- FAU\_GEN.1(1)
- FAU\_GEN.1(2)
- FAU\_NET\_EXT.1
- FAU\_SAR.1
- FAU\_SEL.1
- FAU\_STG\_EXT.1
- FAU\_STG\_EXT.2
- FCO\_CPC\_EXT.1
- FCS\_CKM.1
- FCS\_CKM.2
- FCS\_CKM\_EXT.4
- FCS\_COP.1(1)
- FCS\_COP.1(2)
- FCS\_COP.1(3)
- FCS\_COP.1(4)
- FCS\_HTTPS\_EXT.1
- FCS\_IV\_EXT.1
- FCS\_RBG\_EXT.1
- FCS\_STG\_EXT.2
- FIA\_ENR\_EXT.1
- FIA\_UAU.1
- FIA\_UAU\_EXT.4(1)
- FIA\_UAU\_EXT.4(2)
- FIA\_X509\_EXT.1(1)
- FIA\_X509\_EXT.1(2)
- FIA\_X509\_EXT.2
- FIA\_X509\_EXT.3
- FIA\_X509\_EXT.4
- FIA\_X509\_EXT.5
- FMT\_MOF.1(1)
- FMT\_MOF.1(2)
- FMT\_MOF.1(3)
- FMT\_POL\_EXT.1
- FMT\_SAE\_EXT.1
- FMT\_SMF.1(1)
- FMT\_SMF.1(2)
- FMT\_SMF.1(3)
- FMT\_SMR.1(1)
- FMT\_SMR.1(2)
- FPT\_API\_EXT.1
- FPT\_LIB\_EXT.1
- FPT\_ITT.1(1)
- FPT\_ITT.1(2)
- FPT\_TST\_EXT.1
- FPT\_TUD\_EXT.1
- FTA\_TAB.1
- FTP\_ITC\_EXT.1
- FTP\_ITC.1(1)
- FTP\_ITC.1(2)
- FTP\_TRP.1(1)
- FTP\_TRP.1(2)
- FTP\_TRP.1(3)

### 5.2.2 Modified SFRs

The SFRs listed in this section are defined in the Mobile Device Management Protection Profile and relevant to the secure operation of the TOE. This PP-Module does not modify any SFRs defined by the MDM PP.

### 5.2.2 Additional SFRs

This section defines additional SFRs that must be added to the TOE boundary in order to implement the functionality in any

PP-Configuration where the MDM PP is claimed as the Base-PP.

### 5.2.2.1 Cryptographic Support (FCS)

#### FCS\_STG\_EXT.1(2) Cryptographic Key Storage

##### [FCS\\_STG\\_EXT.1.1\(2\)](#)

**Refinement:** 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.

## 5.

### 2.2.2 Protection of the TSF (FPT)

#### FPT\_ITT.1 Internal TOE TSF Data Transfer

##### [FPT\\_ITT.1.1](#)

The TSF shall *[selection: invoke platform-provided functionality, implement functionality]* to protect all data from [disclosure and modification] through use of *[selection: TLS, HTTPS, DTLS]* when it is transferred between separate parts of the TOE.

Note: The intent of this requirement is to protect the communications channel between MDM Server and Agent, post enrollment. [FTP\\_TRP.1\(2\)](#) from the base PP is to protect the communications channel between MDM Server and Agent during enrollment.

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 requirement is refined from the base PP. Since this requirement is only for the case when the [PP-Module](#) builds on MDM PP and in this case it is expected that the MDM Agent will be a third party application provided by the MDM Server, it is acceptable for the MDM Agent to utilize the protocol implementations from the mobile device. If that is the case then "invoke platform-provided functionality" shall be selected. If the MDM agent implements the protocol itself, then "implement functionality" shall be selected.

If "HTTPS" is selected the appropriate selection based SFRs from Appendix B of MDM PP shall be included in the ST, if not already present.

If "TLS" or "DTLS" is selected the TLS Functional Package must be included in the [ST](#), with the following selections made:

- [FCS\\_TLS\\_EXT.1](#):
  - either TLS or DTLS is selected depending on the selection made in [FPT\\_ITT.1.1](#)
  - either client or server is selected as appropriate
- [FCS\\_TLSC\\_EXT.1.1](#) or [FCS\\_TLSS\\_EXT.1.1](#) (as appropriate):
  - [TLS\\_RSA\\_WITH\\_AES\\_128\\_CBC\\_SHA](#) cannot be selected
  - mutual authentication must be selected

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

5.2.

## 3

Additional SFRs This module does not define any additional SFRs for any PP-Configuration where the Mobile Device Management Protection Profile is claimed as the Base-PP.

## 5.3 TOE Security Functional Requirements

The following section describes the SFRs that must be satisfied by any TOE that claims conformance to this PP-Module. These SFRs must be claimed regardless of which PP-Configuration is used to define the TOE

### 5.3.1 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(2) of the [Base-PP](#) 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~~ must be sent when the trusted channel is available.

This requirement is to ensure that the [MDM](#) Agent ~~shall~~ must 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.

#### [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~~ must be queued. When the trusted channel becomes available, the queued alerts ~~shall~~ must be sent.

### FAU\_GEN.1(2) Audit Data Generation

#### [FAU\\_GEN.1.1\(2\)](#)

**Refinement:** The [MDM](#) Agent shall [selection: invoke platform-provided functionality, implement functionality] to generate an [MDM](#) Agent audit record of the following auditable events:

##### ~~startup~~

- a. ~~Startup~~ and shutdown of the [MDM](#) Agent
- ~~Change in MDM policy~~
  - a. ;
  - b. All auditable events for [not specified] level of audit; and
  - c. [[MDM policy updated](#), any modification commanded by the [MDM](#) Server]

##### ~~Specifically~~

- a. , ~~specifically~~ defined auditable events listed in [Table 1](#)
- a. , and [selection: [assignment: other events], no 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 [Auditable Events](#) table in [FAU\\_GEN.1.1\(2\)](#); they are not limited to the list presented.

##### ~~The change of the~~

[MDM](#) policy update must minimally indicate that ~~the an update to policy~~ ~~changed~~ occurred. The event record need not contain the differences between the prior policy and the new policy; optionally, the specific change(s) to policy that were included in that update may be detailed. All updates to policy should trigger this alert. Modifications commanded by the [MDM](#) Server are those commands listed in [FMT\\_SMF.1.1](#).

The selection for the [FMT\\_UNR\\_EXT.1](#) auditable event in [Table 1 the Auditable Events table](#) corresponds to the selection in [FMT\\_UNR\\_EXT.1](#). If "apply remediation actions" is selected in [FMT\\_UNR\\_EXT.1](#), then the [ST](#) author selects "attempt to unenroll" in [FAU\\_GEN.1.1\(2\) Table 1 Auditable Events table](#) for [FMT\\_UNR\\_EXT.1](#); otherwise, "none" is selected.

### Table 1 Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_ALT_EXT.2	Success/failure of sending 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/	None.	
FCS_STG_EXT.1(2)	Failure to establish a TLS session.	Reason for failure.
FCS_TLSC_EXT.1	Failure to verify presented identifier.	Presented identifier and reference identifier.
	Establishment/termination of a TLS session.	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.4	Outcome (Success/failure) of function.	No additional information.
FMT_UNR_EXT.1.1	[selection: Attempt to unenroll, none]	No additional information.
FTP_ITC_EXT.1(2)	Initiation and termination of trusted channel.	Trusted channel protocol. Non-TOE endpoint of connection.

#### 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

- a. Date and time of the event
- a. , type of event
- a. , subject identity
- a. , (if relevant) the outcome (success or failure) of the event
- a. , and additional information in Table 1; and
- b. For each audit event type, based on the auditable event definitions of the functional components included in the PP-Module/ST, [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 must 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.

### FAU\_SEL.1(2) Security Audit Event Selection

#### FAU\_SEL.1.1(2)

**Refinement:** The TSE shall [selection: invoke platform-provided functionality, implement functionality] 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]
- a. , failure of auditable security events
- a. , [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" "no other attributes". This selection may be configured by the MDM Server.

## 5.3.2 Identification and Authentication (FIA)

### FIA\_ENR\_EXT.2 Agent 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 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~~).

### 5.3.3 Security Management (FMT)

#### FMT\_POL\_EXT.2 Agent 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 certificate that has been authorized for policy updates by the [MDM](#) Server.

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\(2\)](#) of the [Base-PP](#)). 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\(3\)](#).

##### [FMT\\_POL\\_EXT.2.2](#)

The [MDM](#) Agent shall not install policies if the policy-signing certificate is deemed invalid.

#### FMT\_SMF\_EXT.

~~3~~

### 4 Specification of Management Functions

#### [FMT\\_SMF\\_EXT.](#)

~~3~~

##### [4.1](#)

The [MDM](#) Agent shall be capable of interacting with the platform to perform the following functions:

- Import the certificates to be used for authentication of [MDM](#) Agent communications;
- [selection: administrator-provided management functions in [MDF\\_PP](#), administrator-provided device management functions in [MDM\\_PP](#)]
- [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 mobile device with the configuration policies sent from the [MDM](#) Server to the Agent. The [ST](#) author selects the ~~base~~ [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~~

5 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~~ 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~~

must not claim any functionality not provided by the supported

~~Mobile Device~~

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~~

mobile device [ST](#).

#### [FMT\\_SMF\\_EXT.](#)

~~3~~

4.2

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  
4.1).

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  
4.1) 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 MDM Agent does not support unenrollment prevention, remediation actions should be applied upon unenrollment (per FMT\_UNR\_EXT.1).

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.

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-MDF PP 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

6 Consistency Rationale

6.1 Mobile Device Fundamentals Protection Profile

6.1.1 Consistency of TOE Type

When this PP-Module is used to extend the MDF PP, the TOE type for the overall TOE is still a mobile device. The TOE boundary is simply extended to include the MDM Agent application that runs on the mobile device.

6.1.2 Consistency of Security Problem Definition

The threats defined by this PP-Module (see section 3.1) supplement those defined in the MDF PP as follows:

PP-Module Threat	Consistency Rationale
T.BACKUP	This threat protects user data from unauthorized logical access. An attacker would attempt to exploit this threat by first exploiting the T.PHYSICAL, T.FLAWAPP, or T.PERSISTENT threats defined in the Base-PP against the mobile device as a whole, and then using the device itself as an attack vector against any backup data stored on the TOE.

6.1.3 Consistency of Objectives

The objectives for the TOEs are consistent with the MDF PP based on the following rationale:

PP-Module	Threat	TOE Objective	Consistency Rationale
O.ACCOUNTABILITY			The <a href="#">Base-PP</a> provides an objective, O.INTEGRITY, that ensures that the integrity of the mobile device is maintained. This objective assists in the implementation of O.INTEGRITY by providing records of administrative activity, which would include actions that could cause the integrity of the mobile device to be lost.
O.APPLY_POLICY			This objective supports the implementation of the O.CONFIG objective defined in the <a href="#">Base-PP</a> by specifying an additional method by which the TSF may be configured.
O.DATA_PROTECTION_TRANSIT			This objective extends the <a href="#">Base-PP</a> 's O.COMMS objective by ensuring that the communications related to <a href="#">MDM</a> Agent functionality are secured in the same manner as other sensitive data transmitted to/from the mobile device.
O.STORAGE			This objective extends the <a href="#">Base-PP</a> 's O.STORAGE objective by ensuring that the mobile device's data-at-rest protection mechanisms can also be used to secure the <a href="#">MDM</a> Agent and related data.

The objectives for the TOE's ~~operational environment~~ Operational Environment are consistent with the MDF PP based on the following rationale:

PP-Module	Threat	Operational Environment Objective	Consistency Rationale
OE.DATA_PROPER_ADMIN			This objective extends the <a href="#">Base-PP</a> 's OE.CONFIG objective by expecting that TOE administrators act appropriately when installing or configuring the <a href="#">MDM</a> Agent.
OE.DATA_PROPER_USER			This objective extends the <a href="#">Base-PP</a> 's OE.NOTIFY and OE.PRECAUTION objectives by setting reasonable expectations for user security behavior.
OE.IT_ENTERPRISE			This objective helps mitigate the T.EAVESDROP and T.NETWORK threats defined by the <a href="#">Base-PP</a> by reducing the network exposure of the mobile device. This does not conflict with the <a href="#">Base-PP</a> because the <a href="#">Base-PP</a> does not set specific expectations for the level of security that the enterprise provides, but all use cases from the <a href="#">Base-PP</a> set expectations that the mobile device is used for some enterprise purposes so it is reasonable to expect the enterprise have security controls in place to protect these functions.
OE.MOBILE_DEVICE_PLATFORM			This objective is suitable because the <a href="#">MDM</a> Agent can reasonably expect the device it has been deployed on to be secure.
OE.WIRELESS_NETWORK			This objective is suitable because while the <a href="#">Base-PP</a> does not associate any availability metrics with wireless communications, the mobile device will always provide the ability to access a wireless network.

#### 6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the MDF PP that are needed to support MDM Agents functionality. This is considered to be consistent because the functionality provided by the MDF is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the MDF PP as well as new SFRs that are used entirely to provide functionality for MDM Agents. The rationale for why this does not conflict with the claims defined by the MDF PP are as follows: ~~FTP\_ITC\_EXT.1 does not define any mandatory requirements.~~

PP-Module Requirement	Consistency Rationale
	<b>Modified SFRs</b>
	This PP-Module does not modify any requirements when the MDF PP is the base.
	<b>Additional SFRs</b>
FCS_STG_EXT.4	This SFR requires the <a href="#">MDM</a> Agent to use functionality defined by the <a href="#">Base-PP</a> in FCS_CKM_EXT.1.
FTP_ITC_EXT.1(2)	The <a href="#">Base-PP</a> defines FTP_ITC_EXT.1 to define the secure protocols used for trusted channel communications. This <a href="#">PP-Module</a> iterates the SFR to specify a subset of these protocols that may be used for <a href="#">MDM</a> Agent communications in particular.
FTP_TRP.1(2)	This SFR uses the trusted channel protocols defined by the <a href="#">Base-PP</a> in FTP_ITC_EXT.1 to facilitate a trusted path that the <a href="#">MDM</a> Agent can use to enroll the mobile device it runs on into management. Even though the <a href="#">Base-PP</a> does not define FTP_TRP.1, the requirement was given an iteration label for consistency with the <a href="#">MDM</a> Server requirement of the same name.
	<b>Mandatory SFRs</b>
FAU_ALT_EXT.2	This SFR requires the <a href="#">MDM</a> Agent to use a trusted channel defined by FTP_ITC_EXT.1 in the <a href="#">Base-PP</a> to transmit data about its own behavior to the Operational Environment.
	defines a second iteration to use the same audit mechanism to generate audit records for the <a href="#">MDM</a> Agent's

FAU_GEN.1(2)	The <a href="#">Base-PP</a> defines FAU_GEN.1; this <a href="#">PP-Module</a>	behavior. It may alternatively allow the TSF to generate its own audit trail, which does not impede the MDF from enforcing its own security functionality.
FAU_SEL.1(2)	The <a href="#">Base-PP</a> defines FAU_SEL.1; this <a href="#">PP-Module</a> defines a second iteration to use the same audit mechanism to select the auditable events to be generated by the <a href="#">MDM</a> Agent. Note that the <a href="#">Base-PP</a> does not mandate this requirement so it is possible that only the <a href="#">MDM</a> Agent portion of the TOE may implement it. In this case, the SFR provides a selection for the <a href="#">MDM</a> Agent to implement its own mechanism to perform this function rather than a platform-provided one.	
FIA_ENR_EXT.2	This SFR requires the <a href="#">MDM</a> Agent to record data that it receives from the Operational Environment. It does not need to use any functionality defined in the <a href="#">Base-PP</a> to do this, and doing this does not prevent the enforcement of any security requirements from the <a href="#">Base-PP</a> .	
FMT_POL_EXT.2	This SFR requires the <a href="#">MDM</a> Agent to use a digital signature algorithm to validate data that it receives from the Operational Environment. To do this, the <a href="#">MDM</a> Agent will use the functionality defined by the <a href="#">Base-PP</a> in FCS_COP.1(3).	
FMT_SMF_EXT.4	This SFR defines the ability of the <a href="#">MDM</a> Agent to interact with the mobile device to execute the management functions defined by FMT_MOF_EXT.1 in the <a href="#">Base-PP</a> . The <a href="#">Base-PP</a> specifically indicates in FMT_MOF_EXT.1.2 that some management functions may be performed via MDM.	
FMT_UNR_EXT.1	This SFR defines the functions performed by the <a href="#">MDM</a> Agent when unenrolled from an <a href="#">MDM</a> . The <a href="#">Base-PP</a> defines unenrollment actions in FMT_SMF_EXT.2, and goes on to note that these actions may be performed "perhaps via an <a href="#">MDM</a> agent," so this is expected behavior.	

#### Optional SFRs

This PP-Module does not define any optional requirements

#### Selection-based SFRs

This PP-Module does not define any selection-based requirements

#### Objective SFRs

FAU_STG_EXT.3	This SFR defines the ability of the <a href="#">MDM</a> Agent to store generated audit data in the audit storage provided by the mobile device. The <a href="#">Base-PP</a> defines the capability for audit storage in FAU_STG.1.
FPT_NET_EXT.1	This SFR defines the ability of the <a href="#">MDM</a> Agent to maintain information about its last successful connection with the environmental <a href="#">MDM</a> Server (i.e., the last successful invocation of the trusted channel for that interface, as defined in FTP_ITC_EXT.1 of the <a href="#">Base-PP</a> ). It does not need to use any functionality defined in the <a href="#">Base-PP</a> to do this, and doing this does not prevent the enforcement of any security requirements from the <a href="#">Base-PP</a> .

## 6.2 Mobile Device Management Protection Profile

### 6.2.1 Consistency of TOE Type

When this [PP-Module](#) is used to extend the [MDM](#) PP, the TOE type for the overall TOE is still mobile device management. The TOE boundary is simply extended to include the [MDM](#) Agent(s) that reside on individual mobile devices and support the management functionality that the [MDM](#) Server component implements.

### 6.2.2 Consistency of Security Problem Definition

The threats defined by this PP-Module (see section 3.1) supplement those defined in the MDM PP as follows:

PP-Module Threat	Consistency Rationale
T.BACKUP	This threat protects user data from unauthorized logical access. If the backup data is stored outside the MDM or the mobile device that it protects, then there is no conflict with the MDM PP since it is a different security boundary. If the backup data is stored either on the MDM or on the protected device, an attacker would attempt to exploit this threat by first exploiting any of the threats that the MDM PP defines (T.MALICIOUS_APPS, T.NETWORK_ATTACK, T.NETWORK_EAVESDROP, T.PHYSICAL_ACCESS) depending on where and how



the backup data is stored, and then use successful exploitation of one of these threats to attempt to access the backup data itself.

### 6.2.3 Consistency of Objectives

The objectives for the TOEs are consistent with the MDM PP based on the following rationale:

PP-Module	Threat	TOE Objective	Consistency Rationale
O.ACCOUNTABILITY			The MDM PP contains this same objective with the same purpose.
O.APPLY_POLICY			The MDM PP contains this same objective with the same purpose.
O.DATA_PROTECTION_TRANSIT			The MDM PP contains this same objective with the same purpose.
O.STORAGE			This objective requires the MDM Agent to use platform key storage to protect secret and private key data. The MDM PP defines a requirement for key storage (FCS_STG_EXT.1) that allows the MDM Agent to satisfy this objective.

The objectives for the TOE's ~~operational environment~~ Operational Environment are consistent with the MDM PP based on the following rationale:

PP-Module	Threat	Operational Environment Objective	Consistency Rationale
OE.DATA_PROPER_ADMIN			The MDM PP contains this same objective with the same purpose.
OE.DATA_PROPER_USER			The MDM PP contains this same objective with the same purpose.
OE.IT_ENTERPRISE			The MDM PP contains this same objective with the same purpose.
OE.MOBILE_DEVICE_PLATFORM			The MDM PP contains this same objective with the same purpose.
OE.WIRELESS_NETWORK			The MDM PP contains this same objective with the same purpose.

### 6.2.4 Consistency of Requirements

This PP-Module identifies several SFRs from the MDM PP that are needed to support MDM Agents functionality. This is considered to be consistent because the functionality provided by the MDM is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the MDM PP as well as new SFRs that are used entirely to provide functionality for MDM Agents. The rationale for why this does not conflict with the claims defined by the MDM PP are as follows: ~~This PP-Module does not define any mandatory requirements.~~

PP-Module Requirement	Consistency Rationale
	<b>Modified SFRs</b>
	This PP-Module does not modify any requirements when the MDM PP is the base.
	<b>Additional SFRs</b>
FCS_STG_EXT.1	<del>FPT_ITT.1</del>
	<b>Additional SFRs</b>
	<del>This PP-Module does not add any requirements when the MDM PP is the base.</del>
	<b>Mandatory SFRs</b>
(2)	The <a href="#">Base-PP</a> requires the TOE to define a method of key storage. This <a href="#">PP-Module</a> iterates it to specify the use of platform key storage for <a href="#">MDM</a> Agents.
	<b>Mandatory SFRs</b>
FAU_ALT_EXT.2	This SFR provides the alerts that are received by the <a href="#">MDM</a> Server as per FAU_ALT_EXT.1 in the <a href="#">Base-PP</a> .
FAU_GEN.1(2)	This SFR requires the MDM Agent to generate audit records of its behavior. The mechanism by which it does this is not relevant to the MDM Server portion of the TOE as they reside on different platforms.
FAU_SEL.1(2)	The <a href="#">Base-PP</a> defines FAU_SEL.1 as an optional SFR to limit the audit events that are generated by the TSF. This <a href="#">PP-Module</a> adds another iteration that requires the <a href="#">MDM</a> Agent to include this capability by default.
FIA_ENR_EXT.2	This SFR provides information during agent enrollment that is required by the <a href="#">MDM</a> Server to meet the FIA_ENR_EXT.1 requirement defined by the <a href="#">Base-PP</a> .
FMT_POL_EXT.2	The <a href="#">Base-PP</a> defines an SFR (FMT_POL_EXT.1) that requires the <a href="#">MDM</a> Server to provide digitally signed policies and policy updates to the <a href="#">MDM</a> Agent. FMT_POL_EXT.2 completes this transaction by requiring the <a href="#">MDM</a> Agent to accept only signed policies and policy updates.
FMT_SMF_EXT.4	This SFR requires the <a href="#">MDM</a> Agent to interact with the underlying mobile device platform to enforce management functions that are configured by the <a href="#">MDM</a> Server (FMT_SMF.1(1) in the <a href="#">Base-PP</a> ).
FMT_UNR_EXT.1	This SFR requires the TSF to define its behavior upon unenrollment from management. Unenrollment from management is a management function that is specified in the <a href="#">Base-PP</a> .
	<b>Optional SFRs</b>
	This PP-Module does not define any optional requirements

## Selection-based SFRs

This PP-Module does not define any selection-based requirements

## Objective SFRs

FAU\_STG\_EXT.3 This SFR defines the ability of the MDM Agent to store generated audit data in the audit storage provided by the mobile device. This does not impact the Base-PP since it resides on a different platform from the MDM Agent.

FPT\_NET\_EXT.1

# Appendix A - Optional SFRs

As indicated in the introduction to this PP-Module, the baseline requirements (those that must be performed by the TOE or its underlying platform) are contained in the body of this PP-Module. Additionally, there are three other types of requirements specified in Appendices A, B, and C. 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 PP-Module. The second type (in Appendix B) are requirements based on selections in the body of the PP-Module: if certain selections are made, then additional requirements in that appendix will need to be included. The third type (in Appendix C) are components that are not required in order to conform to this PP-Module, but will be included in the baseline requirements in future versions of this PP-Module, so addition by TOE 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/or Appendix C but are not listed (e.g., FMT type requirements) are also included in the ST. This module

This SFR defines the ability of the MDM Agent to maintain information about its last successful connection with the environmental MDM Server (i.e., the last successful invocation of the trusted channel for that interface, as defined in FPT\_ITT.1(2) of the Base-PP). It does not otherwise impact the Base-PP since it describes behavior that occurs local to the MDM Agent during a period where it is not interacting with the MDM Server.

# Appendix A - Optional SFRs

This PP-Module does not define any optional SFRs.

# Appendix B - Selection-based SFRs

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

~~This module~~ This PP-Module does not define any selection-based SFRs.

# Appendix C - Objective SFRs

This section is reserved for requirements that are not currently prescribed by this PP-Module but are expected to be included in future versions of the PP-Module. Vendors planning on having evaluations performed against future products are encouraged to plan for these objective requirements to be met.

## FAU\_STG\_EXT.3 Security Audit Event Storage

### FAU\_STG\_EXT.3.1

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

Application Note: FAU\_STG\_EXT.3 shall ~~should~~ only be included in the ST for MDM Agent platforms (i.e., mobile devices) that conform to Mobile Device Fundamentals Protection Profile MDF PP version 3 or later.

## 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 (the first selection of function 56 in FMT\_SMF.1.1(1) function 56a within the MDM PP). If the first selection of FMT\_SMF.1.1(1) function 56a-56 is included in the ST, then FPT\_NET\_EXT.1.1 shall ~~must~~ 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 the second selection of function 56 must occur. For example if the Agent has not synced with the server in the allowed amount of time that the Agent shall must wipe the device without requiring a command from the Server

# Appendix D - Extended Component Definitions

This appendix contains the definitions for the extended requirements that are used in the PP-Module including those used in Appendices A through C.

## D.1 Background and Scope

This Appendix provides a definition for all of the extended components introduced in this PP-Module. These components are identified in the following table:

Functional Class	Functional Components
Cryptographic Support (FCS)	FCS_STG_EXT Trusted Channel
Security Audit (FAU)	FAU_ALT_EXT MDM Alerts
Identification and Authentication (FIA)	FIA_ENR_EXT Enrollment
	FMT_POL_EXT Trusted Policy Update
Security Management (FMT)	FMT_SMF_EXT Specification of Management Functions (Agent)
	FMT_UNR_EXT Unenrollment
Security Audit (FAU)	FAU_STG_EXT Protected Audit Event Storage
Protection of the TSF (FPT)	FPT_NET_EXT Network Reachability

## D.2 Extended Component Definitions

### FCS\_STG\_EXT Trusted Channel

This family is defined in both the MDF and the MDM **Base-PPs**. This **PP-Module** augments the extended family by adding one additional component, FCS\_STG\_EXT.4. This new component and its impact on the extended family's component leveling are shown below; reference the MDF or MDM PP for all other definitions for this family.

#### Component Leveling

FCS\_STG\_EXT.4, Cryptographic Key Storage, requires the TSF to define a specific location for its key storage.

#### Management: FCS\_STG\_EXT.4

There are no management functions foreseen.

#### Audit: FCS\_STG\_EXT.4

There are no auditable events foreseen.

### FCS\_STG\_EXT.4 Cryptographic Key Storage

Hierarchical to: No other components.

Dependencies to: FCS\_CKM.1 Cryptographic Key Generation

#### FCS\_STG\_EXT.4.1

The **MDM** Agent shall use the platform provided key storage for all persistent secret and private keys.

#### Component Leveling

FCS\_STG\_EXT.1(2), Cryptographic Key Storage,

### Management: FCS\_STG\_EXT.1(2)

There are no management functions foreseen.

### Audit: FCS\_STG\_EXT.1(2)

There are no audit events foreseen.

## FCS\_STG\_EXT.1(2) Cryptographic Key Storage

Hierarchical to: No other components.

Dependencies to: No dependencies.

### FCS\_STG\_EXT.1.1(2)

**Refinement:** The MDM Agent shall use the *platform-provided key storage*] for all persistent secret and private keys.

## FAU\_ALT\_EXT MDM Alerts

This family is defined in the [MDM Base-PP](#). This [PP-Module](#) augments the extended family by adding one additional component, FAU\_ALT\_EXT.2. This new component and its impact on the extended family's component leveling are shown below; reference the [MDM](#) PP for all other definitions for this family.

## Component Leveling

FAU\_ALT\_EXT.2, Agent Alerts, requires the TSF to define when and how an [MDM](#) Agent generates alerts and transmits them to an [MDM](#) Server based on its activity.

### Management: FAU\_ALT\_EXT.2

The following actions could be considered for the management functions in FMT:

- Ability to configure the specific events that result in generation of alerts.

### Audit: FAU\_ALT\_EXT.2

The following actions should be auditable if FAU\_GEN Security audit data generation is included in the PP/ST:

- Minimal: Success/failure of sending alert.

## FAU\_ALT\_EXT.2 Agent Alerts

Hierarchical to: No other components.

Dependencies to: FAU\_ALT\_EXT.1 Server Alerts

[FPT\_ITT.1(2) Basic Internal TSF Data Transfer Protection; or

FTP\_ITC.1 Inter-TSF Trusted Channel]

### 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*

].

## FAU\_ALT\_EXT.2.2

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

## FIA\_ENR\_EXT Enrollment

This family is defined in the [MDM Base-PP](#). This [PP-Module](#) augments the extended family by adding one additional component, FIA\_ENR\_EXT.2. This new component and its impact on the extended family's component leveling are shown below; reference the [MDM](#) PP for all other definitions for this family.

### Component Leveling

FIA\_ENR\_EXT.2, Agent Enrollment of Mobile Device into Management, requires the TSF to record specific information about the [MDM](#) Server (i.e. the entity that is enrolling it) during the enrollment process.

### Management: FIA\_ENR\_EXT.2

There are no management functions foreseen.

### Audit: FIA\_ENR\_EXT.2

The following actions should be auditable if FAU\_GEN Security audit data generation is included in the PP/ST:

- Minimal: Completion of enrollment process.

## FIA\_ENR\_EXT.2 Agent Enrollment of Mobile Device into Management

Hierarchical to: No other components.

Dependencies to: FIA\_ENR\_EXT.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.

## FMT\_POL\_EXT Trusted Policy Update

This family is defined in the [MDM Base-PP](#). This [PP-Module](#) augments the extended family by adding one additional component, FMT\_POL\_EXT.2. This new component and its impact on the extended family's component leveling are shown below; reference the [MDM](#) PP for all other definitions for this family.

### Component Leveling

FMT\_POL\_EXT.2, Agent Trusted Policy Update, requires the TSF to verify the validity of the source of a policy before applying it.

### Management: FMT\_POL\_EXT.2

There are no management functions foreseen.

### Audit: FMT\_POL\_EXT.2

The following actions should be auditable if FAU\_GEN Security audit data generation is included in the PP/ST:

- Minimal: Failure to validate policy.

## FMT\_POL\_EXT.2 Agent Trusted Policy Update

Hierarchical to: No other components.

Dependencies to: FCS\_COP.1 Cryptographic Operation

FMT\_POL\_EXT.1 Trusted Policy Update

### FMT\_POL\_EXT.2.1

The [MDM](#) Agent shall only accept policies and policy updates that are digitally signed by a certificate that has been

authorized for policy updates by the [MDM](#) Server.

## FMT\_POL\_EXT.2.2

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

## FMT\_SMF\_EXT Specification of Management Functions (Agent)

This family is defined in the MDF [Base-PP](#). This [PP-Module](#) augments the extended family by adding one additional component, FMT\_SMF\_EXT.4. This new component and its impact on the extended family's component leveling are shown below; reference the MDF PP for all other definitions for this family.

### Component Leveling

FMT\_SMF\_EXT.4, Specification of Management Functions, requires the TSF to support the execution of certain management functions that require interfacing with other TOE components.

### Management: FMT\_SMF\_EXT.4

The following actions could be considered for the management functions in FMT:

- Execution of management functions.
- Configuration of management functions behavior.

### Audit: FMT\_SMF\_EXT.4

The following actions should be auditable if FAU\_GEN Security audit data generation is included in the PP/ST:

- Minimal: Successful and failed execution of management functions.

## FMT\_SMF\_EXT.4 Specification of Management Functions

Hierarchical to: No other components.

Dependencies to: FCS\_CKM.1 Cryptographic Key Generation

### FMT\_SMF\_EXT.4.1

The [MDM](#) Agent shall be capable of interacting with the platform to perform the following functions:

- Import the certificates to be used for authentication of [MDM](#) Agent communications,
- **[selection:** *administrator-provided management functions in MDF [PP](#), administrator-provided device management functions in [MDM PP](#)*
- **[selection:** *[assignment: additional functions], no additional functions*].

### FMT\_SMF\_EXT.4.2

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*].

## FMT\_UNR\_EXT Unenrollment

### Family Behavior

Components in this family define requirements for TSF behavior when a user attempts to unenroll the TOE from mobile device management.

FMT\_UNR\_EXT FMT\_UNR\_EXT.1

### Component Leveling

FMT\_UNR\_EXT.1, User Unenrollment Prevention, requires the TSF either to prevent unenrollment entirely or to take some corrective action in the event that an unenrollment is initiated.

### Management: FMT\_UNR\_EXT.1



There are no management functions foreseen.

### **Audit: FMT\_UNR\_EXT.1**

The following actions should be auditable if FAU\_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unenrollment from [MDM](#).

### **FMT\_UNR\_EXT.1 User Unenrollment Prevention**

Hierarchical to: No other components.

Dependencies to: [FIA\_ENR\_EXT.1 Enrollment of Mobile Device into Management; or

FMT\_MOF\_EXT.1 Management of Functions Behavior]

#### **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*].

### **FAU\_STG\_EXT Protected Audit Event Storage**

This family is defined in the [MDM Base-PP](#). This [PP-Module](#) augments the extended family by adding one additional component, FAU\_STG\_EXT.3. This new component and its impact on the extended family's component leveling are shown below; reference the [MDM](#) PP for all other definitions for this family.

#### **Component Leveling**

FAU\_STG\_EXT.3, Security Audit Event Storage, requires the TSF to identify a location for audit record storage and the events that are stored at this location.

#### **Management: FAU\_STG\_EXT.3**

There are no management functions foreseen.

#### **Audit: FAU\_STG\_EXT.3**

There are no auditable events foreseen.

### **FAU\_STG\_EXT.3 Security Audit Event Storage**

Hierarchical to: No other components.

Dependencies to: FAU\_GEN.1 Audit Data Generation

#### **FAU\_STG\_EXT.3.1**

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

### **FPT\_NET\_EXT Network Reachability**

#### **Family Behavior**

Components in this family define requirements for tracking the availability of network components.

FPT\_NET\_EXT FPT\_NET\_EXT.1

#### **Component Leveling**

FPT\_NET\_EXT.1, Network Reachability, requires the TSF to keep track of failed attempts to communicate with a remote entity.

#### **Management: FPT\_NET\_EXT.1**

The following actions could be considered for the management functions in FMT:

- Configuration of unreachable threshold.

## Audit: FPT\_NET\_EXT.1

The following actions should be auditable if FAU\_GEN Security audit data generation is included in the PP/ST:

- Minimal: Reaching/exceeding unreachability threshold.

## FPT\_NET\_EXT.1 Network Reachability

Hierarchical to: No other components.

Dependencies to: FPT\_STM.1 Reliable Time Stamps

### 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.

# Appendix E - Use Case Templates

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 [SEFs](#) 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.

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

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

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

Requirement	Action
FAU_ALT_EXT.2.1 Function c	Include in <a href="#">ST</a> .
FMT_UNR_EXT.1.1	Select "prevent the unenrollment from occurring".

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

Requirement	Action
FMT_UNR_ENT.1.1	Select "apply remediation actions"

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

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

# Appendix F - Bibliography

Identifier	Title
	Common Criteria for Information Technology Security Evaluation -
[CC]	• <a href="#">Part 1: Introduction and General Model</a> , CCMB-2017-04-001, Version 3.1, Revision 5, April 2017.
	• <a href="#">Part 2: Security Functional Components</a> , CCMB-2017-04-002, Version 3.1, Revision 5, April 2017.
	• <a href="#">Part 3: Security Assurance Components</a> , CCMB-2017-04-003, Version 3.1, Revision 5, April 2017.

# Appendix

E

## G - Acronyms

Acronym	Meaning
ADB	Android Debug Bridge
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
BYOD	Bring Your Own Device
COPE	Corporately Owned, Personally Enabled
DN	Distinguished Name
DTLS	Datagram Transport Layer Security
GPOS	General Purpose Operating System
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
IPSec	Internet Protocol Security
MAS	Mobile Application Store
MD	Mobile Device
MDF	Mobile Device Fundamentals
MDM	Mobile Device Management
OS	Operating System
PP	Protection Profile
RBG	Random Bit Generation
SD	Supporting Document
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Summary Functionality
TSS	TOE Security Specification
VPN	Virtual Private Network
WiFi	Wireless Fidelity