

UNCLASSIFIED



**DoD ANNEX
FOR
EXTENDED PACKAGE FOR MOBILE DEVICE
MANAGEMENT AGENTS V3.0**

Version 1, Release 2

10 October 2018

Developed by DISA for the DoD

UNCLASSIFIED

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

REVISION HISTORY

Version	Date	Description
V1R2	10 October 2018	<ul style="list-style-type: none">- Removed FMT_SMF_EXT.3.2 from Table 3-1.- Updated FAU_ALT_EXT.2.1 in Table 3-1 to clarify intent.- Updated FMT_SMF_EXT.3.1 in Table 3-1 to clarify intent.- Updated text in paragraph 4.1 to clarify intent.
V1R1	12 January 2017	Initial Release
V1R0.3	12 December 2016	Draft based on Final EP for MDM Agents v3.0
V1R0.2	07 September 2016	Internal DISA draft based on Draft 2 of the EP for MDM Agents v3.0
V1R0.1	04 August 2016	Internal DISA draft based on Draft 1 of the EP for MDM Agents v3.0

TABLE OF CONTENTS

	Page
1. INTRODUCTION.....	1
1.1 Background	1
1.2 Scope	1
1.3 Relationship to Security Technical Implementation Guides (STIGs).....	1
1.4 Document Revisions	2
2. CONVENTIONS.....	3
3. DOD-MANDATED SECURITY TARGET CONTENT	4
3.1 DoD-Mandated Assignments and Selections	4
3.2 DoD-Mandated Optional, Selection-Based, and Objective Functions.....	4
4. OTHER DOD MANDATES	5
4.1 Federal Information Processing Standard (FIPS) 140-2	5
4.2 DoD-Mandated Configuration	5

LIST OF TABLES

	Page
Table 3-1: EP SFR Selections.....	4
Table 4-1: Configuration Values	5

1. INTRODUCTION

1.1 Background

This Annex to the Extended Package (EP) for Mobile Device Management Agents (Version 3.0, dated 21 November 2016) delineates EP content that must be included in the Security Target (ST) for the Target of Evaluation (TOE) to be fully compliant with DoD cybersecurity policies pertaining to information systems. This content includes DoD-mandated EP selections, assignments, and security functional requirements (SFRs) listed as optional or objective in the EP but mandated in DoD.

Deficiencies of the TOE with respect to the DoD Annex will be reported, as appropriate, under the Risk Management Framework for DoD Information Technology (DoD Instruction 8510.01). DoD may determine that a TOE that does not conform to this Annex may pose an unacceptable risk to DoD. Accordingly, any vendor seeking authorization for use of its product within DoD should include the additional EP specificity described in this Annex in its ST.

The EP for MDM Agents, in conjunction with this Annex, addresses the DoD-required cybersecurity controls in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. Taken together, they supersede the DoD Mobile Device Management Security Requirements Guide.

1.2 Scope

The additional information in this document is applicable to all DoD-administered systems and all systems connected to DoD networks.

The MDM Agents EP extends either the MDM Protection Profile (PP) or the Mobile Device Fundamentals (MDF) PP, depending on whether the MDM agent is deployed as a third-party app by the MDM vendor or included as a component of the mobile device operating system, respectively.

1.3 Relationship to Security Technical Implementation Guides (STIGs)

A successful Common Criteria evaluation certifies the capabilities of the TOE but does not assure its subsequent secure operation. To address security concerns with the ongoing operation of the TOE in the field, a product-specific STIG is prepared in conjunction with the Common Criteria evaluation. The STIG lists the configuration requirements for DoD implementations of the TOE and is published in Extensible Configuration Checklist Description Format (XCCDF) to facilitate automation where feasible.

This Annex contains the required DoD configuration of features implementing the security management (FMT) class of SFRs listed in the EP. For each applicable FMT SFR, the STIG will discuss the vulnerability associated with non-compliance configuration and provide step-by-step, product-specific procedures for checking for compliant configurations and fixing non-compliant configurations.

In most cases, the ST will not cover all security-relevant configurable parameters available in the TOE. However, the STIG will include these whenever they impact the security posture of DoD information systems and networks. Accordingly, the DoD Annex only addresses a subset of the controls expected to be included in a STIG.

If the EP extends the MDM PP, the requirements in this Annex will be included in the MDM STIG. If the EP extends the MDF PP, the requirements in this Annex will be included in the mobile device STIG.

1.4 Document Revisions

Comments or proposed revisions to this document should be sent via email to:
disa.stig_spt@mail.mil.

2. CONVENTIONS

The following conventions are used to describe DoD-mandated ST content:

- If an EP SFR is not listed, there is no DoD-mandated selection or assignment for that SFR.
- For SFRs included in this annex:
 - Underlined text indicates a required selection. The presence of the selection indicates this is a DoD-mandated selection.
 - If a selection is not listed, then its inclusion or exclusion does not impact DoD compliance.
 - **Bold** text indicates additional text provided as a refinement to add details to the requirement.
 - *Italicized* text indicates a required assignment.
 - ~~Strikethrough and underlined~~ text indicates that the ST author must exclude the selection.

The Annex provides the minimum text necessary to disambiguate selections and assignments. Readers will need to view both the MDM Agents EP and the DoD Annex simultaneously to place the Annex information in context.

3. DOD-MANDATED SECURITY TARGET CONTENT

3.1 DoD-Mandated Assignments and Selections

DoD mandates the following EP selections and assignments for SFRs in Section 4 of the EP:

Table 3-1: EP SFR Selections

SFR	Selections, Assignments, and Application Notes
FAU_ALT_EXT.2.1	<ul style="list-style-type: none"> - <u>change in enrollment status</u> - <u>failure to install an application from the MDM</u> (see Application note) - <u>failure to update an application from the MDM</u> (see Application note) <p>Application note: Selection is only required if the MDM supports MAS functions.</p>
FMT_SMF_EXT.3.1	<p>One of the following selections is required:</p> <ul style="list-style-type: none"> - <u>administrator-provided management functions in MDF PP</u> - <u>administrator-provided device management functions in MDM PP</u> <p>Additional functions:</p> <ul style="list-style-type: none"> - <i>read audit logs of the MD</i>

3.2 DoD-Mandated Optional, Selection-Based, and Objective Functions

At this time no optional, selection-based, or objective requirements are identified.

4. OTHER DOD MANDATES

4.1 Federal Information Processing Standard (FIPS) 140-2

Cryptographic modules supporting any SFR in the Cryptographic Support (FCS) class must be FIPS 140-2 validated. Information concerning FIPS 140-2 validation should be included in the ST. Failure to obtain validation to include applications could preclude use of the TOE within DoD.

4.2 DoD-Mandated Configuration

Table 4.1 below lists configuration values for product features implementing the EP Specification of Management Functions (FMT_SMF). The ST is not expected to include this configuration information, but it will be included in the product-specific STIG associated with the evaluated IT product.

Table 4-1: Configuration Values

SFR	DoD Selections and Values
FMT_SMF_EXT.3.1	<p><i>Enable read audit logs of the MD</i> (if function is not automatically implemented during MDM Agent install/device enrollment)</p> <p><i>Enable transfer MD audit records to the MDM server or third-party audit management server</i> (if function is not automatically implemented during MDM Agent install/device enrollment)</p>