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

**Version 1, Release 1**

**12 January 2017**

**Developed by DISA for the DoD**

## 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 |
|---|---|---|
| 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**

# LIST OF TABLES

**Page**

# 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 and assignments and EP 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.

In addition to interacting with the MDM server, the MDM agent may also set up connections with a separate Mobile Application Store (MAS) application server to download and install enterprise-hosted applications if a MAS server is included with the MDM system. If the MDM server includes organic MAS features, the MDM Agent to MDM server connection will be used to implement MAS services.

## 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 | - change in enrollment status<br>- failure to install an application from the MAS server or MDM (see Application note)<br>- failure to update an application from the MAS server or MDM (see Application note)<br>Application note: Selection is only required if the MDM supports MAS functions or the MDM platform includes a separate MAS Server. |
| FMT_SMF_EXT.3.1 | One of the following selections is required:<br>- administrator-provided management functions in MDF PP<br>- administrator-provided device management functions in MDM PP<br><br>Additional functions:<br>- *read audit logs of the MD*<br>- *configure the transfer of MD audit records (read by the MDM Agent via FMT_SMF.1.1(1) #19) to the MDM server or third-party audit management server* |
| FMT_SMF_EXT.3.2 | Other management functions:<br>- *configure wipe of Enterprise apps and data upon agent unenrollment from management (if MDM Agent cannot disable user's capability to unenroll agent from management)*<br>*-configure the generation of required MDM Agent audit record (FAU_GEN.1.1(2))*<br>- *configure the transfer of MDM Agent audit records (generated by FAU_GEN.1.1(2)) to the MDM server or third-party audit management server*<br>- *configure the transfer of MDM agent alerts (generated by FAU_ALT_EXT.2.1) to the MDM server or third-party audit management server* |

## 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. While information concerning FIPS 140-2 validation should not be included in the ST, failure to obtain validation 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 | ***Enable*** <u>administrator-provided management functions in MDF PP</u> or <u>administrator-provided device management functions in MDM PP</u> (if function is not automatically implemented during MDM Agent install/device enrollment)<br>***Enable*** *read audit logs of the MD* (if function is not automatically implemented during MDM Agent install/device enrollment)<br>***Enable*** *transfer MD audit records to the MDM server or third-party audit management server* (if function is not automatically implemented during MDM Agent install/device enrollment) |
| FMT_SMF_EXT.3.2 | ***Disable*** a mobile device users' capability to unenroll the agent from management (if function supported by the MD and is not automatically implemented during MDM Agent install/device enrollment)<br>OR<br>***Enable*** *wipe of Enterprise apps and data upon agent unenrollment from management* (if function is not automatically implemented during MDM Agent install/device enrollment and MDM Agent cannot disable user's capability to unenroll agent from management)<br>***Configure*** <u>periodicity of reachability events</u> = six hours or less<br>***Enable*** *MDM Agent Alerts* for all required audit events (FAU_ALT_EXT.2.1) (if function is not automatically implemented during MDM Agent install/device enrollment)<br>***Enable*** *MDM Agent audit record generation* for all required auditable events (FAU_GEN.1.1(2)) (if function is not automatically implemented during MDM Agent install/device enrollment) |

| SFR | DoD Selections and Values |
|---|---|
|  | ***Configure*** criteria to trigger audit event from selectable attributes (FAU_SEL.1.1(2)) (if function is not automatically implemented during MDM Agent install/device enrollment)<br>***Enable*** *transfer of MDM Agent audit records to the MDM server or third-party audit management server* (if function is not automatically implemented during MDM Agent install/device enrollment) |