Supporting Document
Mandatory Technical Document

PP-Module for MDM Agents
Version: 1.0
2019-04-25
National Information Assurance Partnership

Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

SDs may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the SD. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the CCRA.

Technical Editor:
National Information Assurance Partnership (NIAP)

Document 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	2019-03-01	Convert to PP-Module.

General Purpose:
The purpose of this SD is to define evaluation methods for the functional behavior of MDM Agents products.

Acknowledgments:
This SD was developed with support from NIAP MDM Agents Technical Community members, with representatives from industry, government agencies, Common Criteria Test Laboratories, and members of academia.

Table of Contents

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the PP-Module for MDM Agents is to describe the security functionality of MDM Agents products in terms of [CC] and to define functional and assurance requirements for them. The PP-Module is intended for use with the following Base-PPs:

- Protection Profile for Mobile Device Fundamentals, Version 3.1
- Protection Profile for Mobile Device Management, Version 4.0

This SD is mandatory for evaluations of TOEs that claim conformance to a PP-Configuration that includes the PP-Module for :

- MDM Agents, Version 1.0

As such it defines Evaluation Activities for the functionality described in the PP-Module as well as any impacts to the Evaluation Activities to the Base-PP(s) it modifies.

Although Evaluation Activities are defined mainly for the evaluators to follow, in general they also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in Evaluation Activities may in some cases clarify the meaning of Security Functional Requirements (SFR), and may identify particular requirements for the content of Security Targets (ST) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy analysis or cryptographic key management architecture).

1.2 Structure of the Document

Evaluation Activities can be defined for both SFRs and Security Assurance Requirements (SAR), which are themselves defined in separate sections of the SD.

If any Evaluation Activity cannot be successfully completed in an evaluation, then the overall verdict for the evaluation is a 'fail'. In rare cases there may be acceptable reasons why an Evaluation Activity may be modified or deemed not applicable for a particular TOE, but this must be approved by the Certification Body for the evaluation.

In general, if all Evaluation Activities (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a ‘pass’. To reach a ‘fail’ verdict when the Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

Similarly, at the more granular level of assurance components, if the Evaluation Activities for an assurance component and all of its related SFR Evaluation Activities are successfully completed in an evaluation then it would be expected that the verdict for the assurance component is a ‘pass’. To reach a ‘fail’ verdict for the assurance component when these Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

1.3 Terms

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

1.3.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes
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.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Extended Package (EP)	A deprecated document form for collecting SFRs that implement a particular protocol, technology, or functionality. See Functional Packages.
Functional Package (FP)	A document that collects SFRs for a particular protocol, technology, or functionality.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A 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 to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.

1.3.2 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 MDM system.
User	See Mobile Device User.

2 Evaluation Activities for SFRs

The EAs presented in this section capture the actions the evaluator performs to address technology specific aspects covering specific SARs (e.g. ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, and ATE_IND.1) – this is in addition to the CEM workunits that are performed in Section 3 Evaluation Activities for SARs.

Regarding design descriptions (designated by the subsections labeled TSS, as well as any required supplementary material that may be treated as proprietary), the evaluator must ensure there is specific information that satisfies the EA. For findings regarding the TSS section, the evaluator's verdicts will be associated with the CEM workunit ASE_TSS.1-1. Evaluator verdicts associated with the supplementary evidence will also be associated with ASE_TSS.1-1, since the requirement to provide such evidence is specified in ASE in the PP.

For ensuring the guidance documentation provides sufficient information for the administrators/users as it pertains to SFRs, the evaluator's verdicts will be associated with CEM workunits ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Finally, the subsection labeled Tests is where the authors have determined that testing of the product in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer's tests are executing both in the manner declared by the developer and as mandated by the EA. The CEM workunits that are associated with the EAs specified in this section are: ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

2.1 Protection Profile for Mobile Device Fundamentals

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the MDF PP.

2.1.1 Modified SFRs

The PP-Module does not modify any requirements when the MDF PP is the base.

2.1.2 Additional SFRs

This family is defined in both the MDF and the MDM s. This 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. This SFR requires the Agent to use functionality defined by the in FCS_CKM_EXT.1. requires the TSF to

define a specific location for its key storage. There are no management functions foreseen. There are no auditable events foreseen. FCS_CKM.1 Cryptographic Key Generation The Agent shall use the platform provided key storage for all persistent secret and private keys. This requirement ensures that persistent secrets (credentials, secret keys) and private keys are stored securely when not in use by the mobile platform. The evaluator will verify that the lists each persistent secret (credential, secret key) and private key needed to meet the requirements in the . For each of these items, the evaluator will confirm that the lists for what purpose it is used, and, for each platform listed as supported in the , how it is stored. The evaluator shall verify that the Agent calls a platform-provided API to store persistent secrets and private keys. The defines FTP_ITC_EXT.1 to define the secure protocols used for trusted channel communications. This iterates the SFR to specify a subset of these protocols that may be used for Agent communications in particular. Refinement: The TSF shall use 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. The intent of this requirement is to protect the communications channel between Server and Agent, post enrollment. is to protect the communications channel between 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 Agent and sent from the Agent to the Server, when commanded, or at configurable intervals, is properly protected. This trusted channel also protects any commands and policies sent by the Server to the Agent. Either the Agent or the Server is able to initiate the connection. This requirement is iterated from the MDF 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 for communication channels mandated in the MDF . The author must select one of TLS, DTLS, or HTTPS in order to establish and maintain a trusted channel between the Agent and the Server. Only TLS, DTLS, or HTTPS are acceptable for this trusted channel. Since this requirement is only for the case when the builds on MDF PP and in this case it is expected that the Agent will be a native part of the mobile operating system, it is expected that the 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: either TLS or DTLS is selected depending on the selection made in FTP_ITC_EXT.1.1 client must be selected FCS_TLSC_EXT.1.1: 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 Protocol, RBG, Certificate validation, algorithm, and similar services may be met with platform provided services. Refinement: The shall permit the TSF and the Server and MAS Server no other IT entities to initiate communication via the trusted channel. For all other use cases, the mobile device initiates the communication; however, for Agents, the Server may also initiate communication. Refinement: The TSF shall initiate communication via the trusted channel for all communication between the MDM Agent and the MDM Server and all communication between the MAS Server and the MDM Agent no other communication This element is iterated from the MDF ; it is expected that 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. The evaluator shall examine the to determine that the methods of Agent-Server communication are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the in support of remote administration are consistent with those specified in the requirement, and are included in the requirements in the . The evaluator shall confirm that the operational guidance contains instructions for configuring the communication channel between the MDM Agent and the MDM Server and conditionally, the MAS Server for each supported method. For each supported identifier type (excluding DNs), the evaluator shall repeat the following tests: The evaluators shall ensure that communications using each specified (in the operational guidance) Agent-Server communication method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful. The evaluator shall ensure, for each method of Agent-Server communication, the channel data is not sent in plaintext. The evaluator shall ensure, for each communication channel with the MDM Server, that a protocol analyzer identifies the traffic as the protocol under testing. Further evaluation activities are associated with the specific protocols. This SFR uses the trusted channel protocols defined by the in FTP_ITC_EXT.1 to facilitate a trusted path that the Agent can use to enroll the mobile device it runs on into management. Even though the does not define FTP_TRP.1, the requirement was given an iteration label for consistency with the Server requirement of the same name. Refinement: The TSF shall use 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]. Refinement: The TSF shall permit MD users to initiate communication via the trusted path. Refinement: The TSF shall require the use of the trusted path for [[all MD user actions]]. This requirement ensures that authorized MD users initiate all communication with the via a trusted path, and that all communications with the by MD users is performed over this path. The purpose of this connection is for enrollment by the MD user. The author chooses the mechanism or mechanisms supported by the . The data passed in this trusted communication channel are encrypted as defined by the protocol selected. Since this requirement is only for the case when the builds on MDF PP and in this case it is expected that the Agent will be a native part of the mobile operating system, it is expected that the 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: The cipher suites selected must correspond with the algorithms and hash functions allowed in FCS_COP.1 from the MDF PP. The evaluator shall examine the to determine that the methods of remote enrollment are indicated, along with how those communications are protected. The evaluator shall

also confirm that all protocols listed in the in support of enrollment are consistent with those specified in the requirement, and are included in the requirements in the . The evaluator shall confirm that the operational guidance contains instructions for establishing the enrollment sessions for each supported method. For each Agent/platform listed as supported in the : The evaluators shall ensure that communications using each specified (in the operational guidance) enrollment method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful. For each method of enrollment supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish enrollment sessions without invoking the trusted path. The evaluator shall ensure, for each method enrollment, the channel data is not sent in plaintext. Further evaluation activities are associated with the specific protocols.

2.2 Protection Profile for Mobile Device Management

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the MDM PP.

2.2.1 Modified SFRs

The PP-Module does not modify any requirements when the MDM PP is the base.

2.2.2 Additional SFRs

The requires the TOE to define a method of key storage. This iterates it to specify the use of platform key storage for Agents. Refinement: The MDM Agent shall use the [platform-provided key storage] for all persistent secret and private keys. This requirement ensures that persistent secrets (credentials, secret keys) and private keys are stored securely when not in use by the mobile platform. The evaluator will verify that the lists each persistent secret (credential, secret key) and private key needed to meet the requirements in the . For each of these items, the evaluator will confirm that the lists for what purpose it is used, and, for each platform listed as supported in the , how it is stored. The evaluator shall verify that the Agent calls a platform-provided API to store persistent secrets and private keys.

2.3 TOE SFR Evaluation Activities

This family is defined in the . This 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 PP for all other definitions for this family. requires the TSF to define when and how an Agent generates alerts and transmits them to an Server based on its activity. The following actions could be considered for the management functions in FMT: Ability to configure the specific events that result in generation of alerts. 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.1 Server Alerts [FPT_ITT.1(2) Basic Internal TSF Data Transfer Protection; or FTP_ITC.1 Inter-TSF Trusted Channel] The Agent shall provide an alert via the trusted channel to the Server in the event of any of the following audit events: successful application of policies to a mobile device, receiving generating periodic reachability events, change in enrollment state failure to install an application from the MAS Server failure to update an application from the MAS Server other events no other events . The trusted channel is defined in FPT_ITT.1(2) of the if Agent extends Server and FTP_ITC_EXT.1 if Agent extends MDF . “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 must be sent when the trusted channel is available. This requirement is to ensure that the Agent must notify the 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 Agent responds to Server polls to determine device network reachability, or the Agent can be configured to regularly notify the Server that it is reachable. The author must select “receiving” in the first case and “generating” in the second. The corresponding requirement for the Server is FAU_NET_EXT.1 in the . The author must either assign further events or select the “no other events” option. Note that alerts may take time to reach the Server, or not arrive, due to poor connectivity. The MDM Agent shall queue alerts if the trusted channel is not available. If the trusted channel is not available, alerts must be queued. When the trusted channel becomes available, the queued alerts must be sent. The evaluator shall examine the and verify that it describes how the alerts are implemented. The evaluator shall examine the and verify that it describes how the candidate policy updates are obtained and the actions that take place for successful (policy update installed) and unsuccessful (policy update not installed) cases. The software components that are performing the processing must also be identified in the and verified by the evaluator. The evaluator also ensures that the describes how reachability events are implemented, and if configurable are selected in FMT_SMF_EXT.4.2. The evaluator verifies that this description clearly indicates who (Agent or Server) initiates reachability events. The evaluator shall ensure that the describes under what circumstances, if any, the alert may not be generated (e.g., the device is powered off or disconnected from the trusted channel), how alerts are queued, and the maximum amount of storage for queued messages. The evaluator shall perform a policy update from the test environment server. The evaluator shall verify the Agent accepts the update, makes the configured changes, and reports the success of the policy update back to the Server. The evaluator shall perform each of the actions listed in FAU_ALT_EXT.2.1 and verify that the alert does in fact reach the Server. The evaluator shall configure the Agent to perform a network reachability test, both with and without such connectivity and ensure that results reflect each. The evaluator shall remove network connectivity from the MDM Agent and generate an alert/event as defined in FAU_ALT_EXT.2.1. The evaluator shall restore network connectivity to the MDM Agent and verify that the alert generated while the was disconnected is sent by the MDM Agent

upon re-establishment of the connectivity. Refinement: The Agent shall invoke platform-provided functionality implement functionality to generate an Agent audit record of the following auditable events: Startup and shutdown of the Agent; All auditable events for [not specified] level of audit; and [policy updated, any modification commanded by the Server, specifically defined auditable events listed in , and other events no other events]. This requirement outlines the information to be included in the Agent's audit records. The 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. policy update must minimally indicate that an update to policy 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 Server are those commands listed in FMT_SMF.1.1. The selection for the FMT_UNR_EXT.1 auditable event in 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 author selects "attempt to unenroll" in FAU_GEN.1.1(2) Auditable Events table for FMT_UNR_EXT.1; otherwise, "none" is selected. 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/ FCS_STG_EXT.1(2) None. FCS_TLSC_EXT.1 Failure to establish a TLS session.Reason for failure. 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 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 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. Refinement: The TSF TOE platform shall record within each Agent audit record at least the following information: Date and time of the event, type of event, subject identity, (if relevant) the outcome (success or failure) of the event, and additional information in ; and For each audit event type, based on the auditable event definitions of the functional components included in the PP-Module/ST, other audit relevant information. 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 author must identify in the which information of the audit record that is performed by the Agent and that which is performed by the Agent's platform. The evaluator shall check the and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. If "invoke platform-provided functionality" is selected, the evaluator shall examine the to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the Agent; nonetheless, that mechanism will be identified in the as part of this evaluation activity). The evaluator shall use the to perform the auditable events defined in the Auditable Events table in FAU_GEN.1.1(2) and observe that accurate audit records are generated with contents and formatting consistent with those described in the . Note that this testing can be accomplished in conjunction with the testing of the security mechanisms directly. Refinement: The shall 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: [event type] [success of auditable security events, failure of auditable security events, other attributes]. The intent of this requirement is to identify all criteria that can be selected to trigger an audit event. For the author, the assignment is used to list any additional criteria or "no other attributes". This selection may be configured by the MDM Server. If "invoke platform-provided functionality" is selected, the evaluator shall examine the of the to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Agent; nonetheless, that mechanism will be identified in the as part of this evaluation activity). The evaluator shall examine the operational guidance to determine that it contains instructions on how to define the set of auditable events as well as explains the syntax for multi-value selection (if applicable). The evaluator shall also verify that the operational guidance shall identify those audit records that are always recorded, regardless of the selection criteria currently being enforced. For each attribute listed in the requirement, the evaluator shall devise a test to show that selecting the attribute causes only audit events with that attribute (or those that are always recorded, as identified in the administrative guidance) to be recorded. [conditional]: If the TSF supports specification of more complex audit pre-selection criteria (e.g., multiple attributes, logical expressions using attributes) then the evaluator shall devise tests showing that this capability is correctly implemented. The evaluator shall also, in the test plan, provide a short narrative justifying the set of tests as representative and sufficient to exercise the capability.

FAU_ALT_EXT.2 Agent Alerts

FAU_ALT_EXT.2
TSS
The evaluator shall examine the and verify that it describes how the alerts are implemented.

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

The evaluator also ensures that the describes how reachability events are implemented, and if configurable are selected in FMT_SMF_EXT.4.2. The evaluator verifies that this description clearly indicates who (Agent or Server) initiates reachability events.

The evaluator shall ensure that the describes under what circumstances, if any, the alert may not be

generated (e.g., the device is powered off or disconnected from the trusted channel), how alerts are queued, and the maximum amount of storage for queued messages.

Tests

- **Test 1:** The evaluator shall perform a policy update from the test environment server. The evaluator shall verify the Agent accepts the update, makes the configured changes, and reports the success of the policy update back to the Server.
- **Test 2:** The evaluator shall perform each of the actions listed in FAU_ALT_EXT.2.1 and verify that the alert does in fact reach the Server.
- **Test 3:** The evaluator shall configure the Agent to perform a network reachability test, both with and without such connectivity and ensure that results reflect each.
- **Test 4:** The evaluator shall remove network connectivity from the MDM Agent and generate an alert/event as defined in FAU_ALT_EXT.2.1. The evaluator shall restore network connectivity to the MDM Agent and verify that the alert generated while the was disconnected is sent by the MDM Agent upon re-establishment of the connectivity.

FAU_GEN.1/AUDITGEN Audit Data Generation

FAU_GEN.1/AUDITGEN
TSS
The evaluator shall check the and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field.

If "invoke platform-provided functionality" is selected, the evaluator shall examine the to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the Agent; nonetheless, that mechanism will be identified in the as part of this evaluation activity).

Tests
The evaluator shall use the to perform the auditable events defined in the Auditable Events table in FAU_GEN.1.1(2) and observe that accurate audit records are generated with contents and formatting consistent with those described in the . Note that this testing can be accomplished in conjunction with the testing of the security mechanisms directly.

FAU_SEL.1/EVENTSEL Security Audit Event Selection

FAU_SEL.1/EVENTSEL
TSS
If "invoke platform-provided functionality" is selected, the evaluator shall examine the of the to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Agent; nonetheless, that mechanism will be identified in the as part of this evaluation activity).

Guidance
The evaluator shall examine the operational guidance to determine that it contains instructions on how to define the set of auditable events as well as explains the syntax for multi-value selection (if applicable). The evaluator shall also verify that the operational guidance shall identify those audit records that are always recorded, regardless of the selection criteria currently being enforced.

Tests

- **Test 1:** For each attribute listed in the requirement, the evaluator shall devise a test to show that selecting the attribute causes only audit events with that attribute (or those that are always recorded, as identified in the administrative guidance) to be recorded.
- **Test 2:** [conditional]: If the TSF supports specification of more complex audit pre-selection criteria (e.g., multiple attributes, logical expressions using attributes) then the evaluator shall devise tests showing that this capability is correctly implemented. The evaluator shall also, in the test plan, provide a short narrative justifying the set of tests as representative and sufficient to exercise the capability.

This family is defined in the . This 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 PP for all other definitions for this family. requires the TSF to record specific information about the Server (i.e. the entity that is enrolling it) during the enrollment process. There are no management functions foreseen. 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.1 Enrollment of Mobile Device into Management The Agent shall record the reference identifier of the Server during the enrollment process. The reference identifier of the Server may be the Distinguished Name, Domain Name, and/or the IP address of the Server. This requirement allows the specification of the information to be to be used to establish a network connection and the reference identifier for authenticating the trusted channel between the Server and Agent. The evaluator shall examine the to verify that it describes which types of reference identifiers are acceptable and how the identifier is specified (e.g. preconfigured in the Agent, by the user, by the server, in a policy). The evaluator shall examine the operational guidance to verify that it describes how to

configure reference identifier of the Server’s certificate and, if different than the reference identifier, the Domain Name or IP address (for connectivity) of the Server. The evaluator shall follow the operational guidance to establish the reference identifier of the server on the Agent and in conjunction with other evaluation activities verify that the Agent can connect to the Server and validate the Server’s certificate.

FIA_ENR_EXT.2 Agent Enrollment of Mobile Device into Management

FIA_ENR_EXT.2
TSS
The evaluator shall examine the to verify that it describes which types of reference identifiers are acceptable and how the identifier is specified (e.g. preconfigured in the Agent, by the user, by the server, in a policy).

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

Tests
The evaluator shall follow the operational guidance to establish the reference identifier of the server on the Agent and in conjunction with other evaluation activities verify that the Agent can connect to the Server and validate the Server’s certificate.

This family is defined in the . This 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 PP for all other definitions for this family. requires the TSF to verify the validity of the source of a policy before applying it. There are no management functions foreseen. The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST: Minimal: Failure to validate policy. FCS_COP.1 Cryptographic Operation FMT_POL_EXT.1 Trusted Policy Update The Agent shall only accept policies and policy updates that are digitally signed by a certificate that has been authorized for policy updates by the Server. 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). 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). The MDM Agent shall not install policies if the policy-signing certificate is deemed invalid. The evaluator ensures that the describes how the candidate policies are obtained by the Agent, the processing associated with verifying the digital signature of the policy updates, and the actions that take place for successful (signature was verified) and unsuccessful (signature could not be verified) cases. The software components that are performing the processing must also be identified in the and verified by the evaluators. This evaluation activity is performed in conjunction with the evaluation activity for FIA_X509_EXT.1 and FIA_X509_EXT.2 as defined in the s. The evaluator shall perform a policy update from an available configuration interface (such as through a test Server). The evaluator shall verify the update is signed and is provided to the Agent. The evaluator shall verify the Agent accepts the digitally signed policy. The evaluator shall perform a policy update from an available configuration interface (such as through a test Server). The evaluator shall provide an unsigned and an incorrectly signed policy to the Agent. The evaluator shall verify the Agent does not accept the digitally signed policy. This family is defined in the MDF . This 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. requires the TSF to support the execution of certain management functions that require interfacing with other TOE components. The following actions could be considered for the management functions in FMT: Execution of management functions. Configuration of management functions behavior. 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. FCS_CKM.1 Cryptographic Key Generation The Agent shall be capable of interacting with the platform to perform the following functions: Import the certificates to be used for authentication of Agent communications, administrator-provided management functions in MDF administrator-provided device management functions in additional functions no additional functions . This requirement captures all the configuration functionality in the Agent to configure the underlying mobile device with the configuration policies sent from the Server to the Agent. The author selects the (MDF or) as the source of the management functions. The administrator-provided management functions in MDF are specified in Column 4 of Table 5 in MDF and in FPT_TUD_EXT.1 (for version queries). The administrator-provided device management functions in are specified in FMT_SMF.1.1(1); the functions in the selection of FMT_SMF.1.1(1) in the are required to correspond to the functions available on the platforms supported by the Agent. The author can add more commands and configuration policies by completing the assignment statement; the mobile device must support these additional commands or configuration policies. The agent must configure the platform based on the commands and configuration policies received from the Server. The author must not claim any functionality not provided by the supported mobile device(s). All selections and assignments performed by the author in this requirement should match the selections and assignments of the validated mobile device . The Agent shall be capable of performing the following functions: Enroll in management Configure whether users can unenroll from management configure periodicity of reachability events other management functions no other functions . This requirement captures all of the configuration in the Agent for configuration of itself. If the 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.4.1). If the Agent is an application developed separately from the mobile device, the Agent performs the function “enroll the mobile device in management” (per FMT_SMF_EXT.4.1) by registering itself to the mobile device as a device administrator. The Agent itself is enrolled in management by configuring the Server to which the Agent answers. If the 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. This assurance activity may be performed in conjunction with other assurance activities in the . The evaluator shall verify that the any assigned functions are described in the and that these functions are documented as supported by the platform. The evaluator shall examine the to verify that any differences between management functions and policies for each supported mobile device are listed. The evaluator shall verify that the describes the methods in which the MDM Agent can be enrolled. The description shall make clear if the MDM Agent supports multiple interfaces for enrollment and configuration (for example, both remote configuration and local configuration). The evaluator shall verify the AGD guidance includes detailed instructions for configuring each function in this requirement. If the Agent is a component of the system (i.e. Server is the), the evaluator shall verify, by consulting documentation for the claimed mobile device platforms, that the configurable functions listed for this Agent are supported by the platforms. If the Agent supports multiple interfaces for configuration (for example, both remote configuration and local configuration), the AGD guidance makes clear whether some functions are restricted to certain interfaces. In conjunction with the evaluation activities in the , the evaluator shall attempt to configure each administrator-provided management function and shall verify that the mobile device executes the commands and enforces the policies. The evaluator shall configure the MDM Agent authentication certificate in accordance with the configuration guidance. The evaluator shall verify that the MDM Agent uses this certificate in performing the tests for FPT_ITT.1(2) (from the MDM PP). In conjunction with other evaluation activities, the evaluator shall attempt to enroll the MDM Agent in management with each interface identified in the , and verify that the MDM Agent can manage the device and communicate with the MDM Server. [conditional] In conjunction with the evaluation activity for FAU_ALT_EXT.2.1, the evaluator shall configure the periodicity for reachability events for several configured time periods and shall verify that the MDM Server receives alerts on that schedule. [conditional] The evaluator shall design and perform tests to demonstrate that the assigned function may be configured and that the intended behavior of the function is enacted by the mobile device. Components in this family define requirements for TSF behavior when a user attempts to unenroll the TOE from mobile device management. requires the TSF either to prevent unenrollment entirely or to take some corrective action in the event that an unenrollment is initiated. There are no management functions foreseen. The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST: Minimal: Unenrollment from . [FIA_ENR_EXT.1 Enrollment of Mobile Device into Management; or FMT_MOF_EXT.1 Management of Functions Behavior] The Agent shall provide a mechanism to enforce the following behavior upon an attempt to unenroll the mobile device from management: prevent the unenrollment from occurring apply remediation actions . 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 Server. For those configurations where unenrollment is allowed, for example a BYOD usage, the MDF PP describes remediation actions performed upon unenrollment, such as wiping enterprise data, in FMT_SMF_EXT.2.1; however, the Agent is limited to those actions supported by the mobile device on which the Agent is operating. The evaluator shall ensure that the describes the mechanism used to prevent users from unenrolling or the remediation actions applied when unenrolled. The evaluator shall ensure that the administrative guidance instructs administrators in configuring the unenrollment prevention in each available configuration interface. If any configuration allows users to unenroll, the guidance also describes the actions that unenroll the Agent. If ‘prevent the unenrollment from occurring’ is selected: The evaluator shall configure the Agent according to the administrative guidance for each available configuration interface, shall attempt to unenroll the device, and shall verify that the attempt fails. If ‘apply remediation actions’ is selected: If any configuration allows the user to unenroll, the evaluator shall configure the Agent to allow user unenrollment, attempt to unenroll, and verify that the remediation actions are applied.

FMT_POL_EXT.2 Agent Trusted Policy Update

FMT_POL_EXT.2
TSS
The evaluator ensures that the describes how the candidate policies are obtained by the Agent, the processing associated with verifying the digital signature of the policy updates, and the actions that take place for successful (signature was verified) and unsuccessful (signature could not be verified) cases. The software components that are performing the processing must also be identified in the and verified by the evaluators.

Tests
This evaluation activity is performed in conjunction with the evaluation activity for FIA_X509_EXT.1 and FIA_X509_EXT.2 as defined in the s.

- **Test 1:** The evaluator shall perform a policy update from an available configuration interface (such as through a test Server). The evaluator shall verify the update is signed and is provided to the Agent. The evaluator shall verify the Agent accepts the digitally signed policy.
- **Test 2:** The evaluator shall perform a policy update from an available configuration interface (such as through a test Server). The evaluator shall provide an unsigned and an incorrectly signed policy to the Agent. The evaluator shall verify the Agent does not accept the digitally signed policy.

FMT_SMF_EXT.4 Specification of Management Functions

FMT_SMF_EXT.4
This assurance activity may be performed in conjunction with other assurance activities in the .

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

The evaluator shall verify that the describes the methods in which the MDM Agent can be enrolled.

The description shall make clear if the MDM Agent supports multiple interfaces for enrollment and configuration (for example, both remote configuration and local configuration).

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

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

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

Tests

- **Test 1:** In conjunction with the evaluation activities in the , the evaluator shall attempt to configure each administrator-provided management function and shall verify that the mobile device executes the commands and enforces the policies.
- **Test 2:** The evaluator shall configure the MDM Agent authentication certificate in accordance with the configuration guidance. The evaluator shall verify that the MDM Agent uses this certificate in performing the tests for FPT_ITT.1(2) (from the MDM PP).
- **Test 3:** In conjunction with other evaluation activities, the evaluator shall attempt to enroll the MDM Agent in management with each interface identified in the , and verify that the MDM Agent can manage the device and communicate with the MDM Server.
- **Test 4:** [conditional] In conjunction with the evaluation activity for FAU_ALT_EXT.2.1, the evaluator shall configure the periodicity for reachability events for several configured time periods and shall verify that the MDM Server receives alerts on that schedule.
- **Test 5:** [conditional] The evaluator shall design and perform tests to demonstrate that the assigned function may be configured and that the intended behavior of the function is enacted by the mobile device.

FMT_UNR_EXT.1 User Unenrollment Prevention

FMT_UNR_EXT.1
TSS
The evaluator shall ensure that the describes the mechanism used to prevent users from unenrolling or the remediation actions applied when unenrolled.

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

Tests

- **Test 1:** If ‘prevent the unenrollment from occurring’ is selected: The evaluator shall configure the Agent according to the administrative guidance for each available configuration interface, shall attempt to unenroll the device, and shall verify that the attempt fails.
- **Test 2:** If ‘apply remediation actions’ is selected: If any configuration allows the user to unenroll, the evaluator shall configure the Agent to allow user unenrollment, attempt to unenroll, and verify that the remediation actions are applied.

2.4 Evaluation Activities for Optional SFRs

The PP-Module does not define any optional requirements.

2.5 Evaluation Activities for Selection-Based SFRs

The PP-Module does not define any selection-based requirements.

2.6 Evaluation Activities for Objective SFRs

This family is defined in the . This 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 PP for all other definitions for this family. requires the TSF to identify a location for audit record storage and the events that are stored at this location. There are no management functions foreseen. There are no auditable events foreseen. FAU_GEN.1 Audit Data Generation The MDM Agent shall store MDM audit records in the platform-provided audit storage. FAU_STG_EXT.3 should only be included in the for MDM Agent platforms (i.e., mobile devices) that conform to MDF PP version 3 or later. The evaluator shall verify that the description of the audit records indicates how the records are stored. The evaluator shall verify that the Agent calls a platform-provided API to store audit records.

FAU_STG_EXT.3 Security Audit Event Storage

FAU_STG_EXT.3
TSS
The evaluator shall verify that the description of the audit records indicates how the records are stored. The evaluator shall verify that the Agent calls a platform-provided API to store audit records.

Components in this family define requirements for tracking the availability of network components. requires the TSF to keep track of failed attempts to communicate with a remote entity. The following actions could be considered for the management functions in FMT: Configuration of unreachability threshold. 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_STM.1 Reliable Time Stamps The TSF shall detect when a configurable positive integer of missed reachability events occur time limit is exceeded related to the last successful connection with the server has been reached. 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) within the MDM PP). If the first selection of FMT_SMF.1.1(1) function 56 is included in the , then FPT_NET_EXT.1.1 must be included in the . If the Agent has been out of connectivity with the server for too long than the remediation actions specified in 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 must wipe the device without requiring a command from the Server. The evaluator shall verify that the contains a description of how the Agent determines how long it has been since the last successful connection with the Server (i.e., total number of missed reachability events or time). If total number of missed reachability events is selected, the evaluator shall verify that the contains a description of how often the reachability events are sent. The evaluator shall verify that the AGD guidance instructs the administrator, if needed, how to configure the to detect when the time since last successful connection with the server has been reached. The evaluator shall configure the Server configuration policy of the Agent per FMT_SMF.1.1(1) function 56 within the Mobile Device Managment PP. The device shall be placed in airplane mode to prevent connectivity with the Server. The evaluator shall verify that after the configured time, the remediation actions selected in function 56 occur.

FPT_NET_EXT.1 Network Reachability

FPT_NET_EXT.1
TSS
The evaluator shall verify that the contains a description of how the Agent determines how long it has been since the last successful connection with the Server (i.e., total number of missed reachability events or time). If total number of missed reachability events is selected, the evaluator shall verify that the contains a description of how often the reachability events are sent.

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

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

3 Evaluation Activities for SARs

The PP-Module does not define any SARs beyond those defined within the base-PP to which it must claim conformance. It is important to note that a TOE that is evaluated against the PP-Module is inherently evaluated against the Base-PP as well. The Base-PP includes a number of Evaluation Activities associated with both SFRs and SARs. Additionally, the PP-Module includes a number of SFR-based Evaluation Activities that similarly refine the SARs of the Base-PPs. The evaluation laboratory will evaluate the TOE against the chosen Base-PP and supplement that evaluation with the necessary SFRs that are taken from the PP-Module.

4 Required Supplementary Information

This Supporting Document has no required supplementary information beyond the ST, operational guidance,

and testing.

Appendix A - References

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